"Responsabilidad con pensamiento positivo"

UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA: INGENIERÍA EN SISTEMAS

TEMA: Metodología para la selección de proveedores de seguridad perimetral

AUTOR: Jorge Fernando Armas Quiles

TUTOR: Msc. Juan Carlos Moreno

Quito - Ecuador
2014

"Responsabilidad con pensamiento positivo"

AUTORÍA

Yo, Jorge Fernando Armas Quiles, en calidad de estudiante de la Carrera de Ingeniería en Sistemas, declaro bajo juramento que el Trabajo de Titulación aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Jorge Fernando Armas Quiles

CC: 1712246758

Quito, 31 de Enero del 2014

DEDICATORIA

Dedico este trabajo de investigación a mi amada esposa Nancy Fabiola Chicaiza Acosta quien ha sido mi fuente de inspiración y permanente lucha, a mi hija Jhoselin Estefanía y a mi hijo Isaac Fernando, quienes me brindaron todo su apoyo, cariño y comprensión para que continúe mis estudios universitarios y para la elaboración de este proyecto de titulación.

Sin vuestro apoyo no habría sido posible conseguir esta anhelada meta en mi vida profesional y por ello os dedico este trabajo de Titulación.

Jorge Fernando Armas Quiles

"Responsabilidad con pensamiento positivo"

AGRADECIMIENTO

Agradezco a Dios por todas las bendiciones recibidas y por haberme permitido cumplir esta meta tan anhelada.

A mi padre Jorge Armas, por haberme apoyado en mis estudios universitarios y el esfuerzo dedicado para que nunca me falte nada.

A mi madre Magaly Quiles, por haberme brindado todo su cariño y comprensión a lo largo de mi formación estudiantil.

A mi esposa e hijos, por el sacrificio realizado a lo largo de este período de aprendizaje y en el cual estuvieron siempre brindándome todo su aliento para que no desmaye en este duro objetivo.

A la Universidad Israel, por haberme permitido culminar mis estudios de tercer nivel y actualizar mis conocimientos, por haberme permitido ser parte de este gran grupo humano.

Jorge Fernando Armas Quiles

RESUMEN

El presente proyecto de titulación busca apoyar a los gerentes de sistemas de las pymes, en lo que, a seleccionar el mejor proveedor de seguridad perimetral se refiere, a través de la aplicación de la metodología propuesta, la cual está basada en la norma ISO 9001.

Para garantizar productos de calidad y servicios acordes con las distintas exigencias del cliente, es necesario optimizar los procesos internos, y contar con proveedores confiables que permitan un buen desempeño del proceso en general.

De acuerdo a la norma ISO 9001, las organizaciones deben evaluar y seleccionar los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de las organizaciones, debiendo establecerse los criterios para la selección, la evaluación y la reevaluación manteniendo siempre los registros de los resultados de las diferentes evaluaciones realizadas.

Este documento pretende ser una guía sencilla y metodológica en el difícil proceso de seleccionar un proveedor de seguridad perimetral específicamente, y busca fortalecer la relación entre cliente y proveedor, al mismo tiempo que se reconoce su independencia tal como lo hace la norma ISO 9001 tomada tomo referencia para este texto.

Se busca además dotar a la organización de una herramienta metodológica multicriterio para la toma de decisiones, utilizando la valoración de los distintos criterios definidos para la selección del proveedor, considerando información importante del proveedor para el buen desempeño de su labor y el mejoramiento mutuo.

Se incluye en este documento los pasos que se deben considerar para definir los criterios a utilizar en la selección de proveedores, su ponderación, y algunas definiciones relacionadas con seguridad perimetral, al igual que las funcionalidades que se debe considerar contenga la solución. También se incluye definiciones de la norma ISO 9001 tomada como referencia para la realización de la metodología propuesta. Complementariamente, y con la finalidad de brindar un mayor apoyo, se incluye un esquema de red clásico y a la vez robusto; así como, un esquema de red basado en el uso de equipos de alta disponibilidad. Se muestra también un esquema de las zonas que se deben considerar proteger con la seguridad perimetral y el flujo de transmisión de datos que se debe considerar en el esquema de red.

ABSTRACT

This project seeks to support titling system managers of pymes, as to select the best provider of perimeter security is concerned, through the application of the proposed methodology, which is based on ISO 9001 .

To ensure quality products and services according to different customer requirements , it is necessary to optimize internal processes , and have reliable suppliers that allow good performance of the overall process .

According to ISO 9001 , organizations should evaluate and select suppliers based on their ability to supply product in accordance with the requirements of organizations must establish the criteria for selection , evaluation and re-evaluation while maintaining records the results of the different evaluations .

This document is intended as a simple and methodological guide in the difficult process of selecting a vendor Edge specifically security, and seeks to strengthen the relationship between customer and supplier , while independence is recognized as does ISO 9001 taken tome reference to this text .

It also seeks to provide the organization of a methodological tool for multi-criteria decision making , using the valuation of the various defined criteria for supplier selection , supplier information considered important for the proper performance of its work and mutual improvement.

Included in this document the steps to be considered to define the criteria used in the selection of suppliers, their weighting , and some definitions related to perimeter security, as well as the features to consider containing the solution. Definitions of ISO 9001 reference standard for the performance of the proposed methodology is also included. And a network scheme based on the use of equipment high availability ; Additionally, and in order to provide greater support, a classic scheme yet robust network is included . It also shows a schematic of the zones to be considered protected by the security perimeter and the flow of data that must be considered in the network schedule

Contenido

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INFORME FINAL DE RESULTADOS DEL TRABAJO DE TITULACIÓN

1 Datos generales.

Carrera	INGENIERÍA EN SISTEMAS INFORMÁTICOS
Autor/a del TT:	Jorge Fernando Armas Quiles
Tema del TT:	Metodología para la selección de proveedores de Seguridad Perimetral
Articulación con la Línea de Investigación Institucional:	Producción y Sociedad
Sublínea de Investigación Institucional:	Metodologías para la Optimización de la Productividad y Estructuras Financieras
Fecha de Presentación:	31-ENERO-2014

2 Introducción.

Debido a la gran oferta de software de seguridad perimetral y empresas que ofertan este tipo de productos, se hace necesario establecer una metodología que permita a los gerentes de sistemas de las pymes, tener una guía que apoye su toma de decisiones. Este documento pretende apoyar a las empresas en desarrollo que por lo general tienen un reducido presupuesto y cuentan con el mínimo personal de apoyo.

Los gerentes de sistemas de pymes que están implementando plataformas web, requieren de una guía que les permita decidir el proveedor de software de seguridad perimetral más apropiado para su organización. Es necesario considerar que el recurso más valioso para las organizaciones hoy en día es la información, siendo necesario invertir en seguridad, con la única finalidad de salvaguardar los datos.

El 90 % de las pymes están implementando software desarrollado en plataformas web, con la finalidad, de ser más competitivos en sus distintos giros de negocio. Esta necesidad muchas veces obliga al gerente de sistemas, implementar un software de seguridad perimetral, sin embargo, la gran oferta de proveedores de este producto en el mercado, hace difícil esta selección, más aún cuando la mayor parte de gerentes de sistemas no cuentan con un asistente que sea experto en infraestructura de redes.

La presente metodología pretende establecer los pasos necesarios que se deben seguir para facilitar la selección del proveedor de seguridad perimetral apropiado, considerando para ello, el tamaño de la empresa y su capacidad de inversión.

La selección de proveedores de seguridad perimetral es en general un problema multicriterio, el cual incluye necesariamente, factores cuantitativos y cualitativos que deben ser evaluados al momento de iniciar este tipo de procesos. Para seleccionar al mejor ofertante del mercado, es necesario, hacer una compensación entre los factores tangibles e intangibles, y entre los que puede generarse conflicto.

No es fácil tomar la decisión sobre cuál es el mejor proveedor de seguridad perimetral y por ello se han desarrollado métodos que apoyan el inicio, ejecución y finalización de este proceso, por lo que, la metodología propuesta es específica para este tipo de necesidades que se presentan tarde o temprano en las pymes y más aún cuando la organización tiene la necesidad de un sistema web.

2.1 Problema de Investigación

Uno de los principales problemas que afecta a las pymes del país, cuando implementan sistemas web con acceso externo, es la protección de la información. Muchas empresas desconocen que al abrir los puertos de red se corre el grave peligro de que la información este vulnerable y expuesta al ataque externo.

La mayor parte de empresas que han sufrido fraudes, buscan proteger su principal activo que es la información y para ello es necesario una herramienta de seguridad perimetral que les permita alcanzar ese objetivo al menor precio posible, sin considerar que también es un gran riesgo contratar con empresas que no tienen la capacidad de brindar un nivel de soporte adecuado a las necesidades de la organización, volviendo de la solución el peor de los problemas.

El principal inconveniente es entonces el poder aplicar una metodología que permita seleccionar el proveedor adecuado de seguridad perimetral, tomando en consideración que más que un proveedor se necesita un socio estratégico, que a más de proporcionar la herramienta adecuada de control, brinde altos niveles de servicio de satisfacción y calidad. Es importante establecer los criterios necesarios que se deben considerar en este proceso de selección, que lo único que busca es establecer los pasos necesarios, que ante la ausencia de una metodología de selección de proveedores de seguridad perimetral resultará muy útil para los gerentes de sistemas.

2.2 Objetivos

2.2.1 Objetivo General

- Establecer una metodología que facilite el proceso de selección de un proveedor de seguridad perimetral mediante el uso de criterios específicos que apoyen la toma de decisiones del gerente de sistemas.

2.2.2 Objetivos Específicos

- Estudiar la situación actual de la empresa para conocer su realidad.
- Establecer los criterios que se deben considerar para la selección del proveedor de seguridad perimetral.
- Realizar recomendaciones a la infraestructura actual.
- Apoyar la gestión de selección de herramientas de seguridad perimetral.
- Proteger la información de ataques externos.
- Establecer otras zonas de protección de la información.
- Definir si la solución perimetral debe incluir o no hardware.

2.3 Idea a defender

Elaborar una metodología específica para calificar los criterios establecidos para la selección de proveedores de seguridad perimetral y el software ofertado, siendo necesario, para cumplir con los objetivos planteados, realizar el levantamiento del modelo actual de la empresa ya que esto permitirá tener mayor claridad sobre el problema al cual se enfrenta; y, por ende identificar las necesidades de seguridad de la empresa de una manera más clara.

3 Presentación y descripción del producto.

La presente metodología pretende ser un apoyo para los gerentes del área de sistemas, que necesitan implementar una herramienta de seguridad perimetral en su empresa.

Se analizan varios aspectos que se deben tomar en cuenta para seleccionar un proveedor de seguridad perimetral desde que se establecen las bases del concurso hasta que se decide el proveedor ganador.

De manera resumida se estudiará a lo largo del desarrollo de este proyecto establecer qué es una metodología, que es seguridad perimetral, para qué sirve y cómo se debe implementar un software de seguridad perimetral.

Para la elaboración de este documento se toma como referencia la norma ISO 9001 y lo que se pretende es establecer una metodología sencilla en el proceso de selección de proveedores de seguridad perimetral en las pymes.

4 Fundamentación Teórica y metodológica del producto.

4.1 Análisis del proceso

Para comenzar el análisis de la seguridad informática se ha de definir o estudiar el objeto primordial que se busca proteger, y ese objeto es la información. La información es el conjunto de datos que aportan un conocimiento sobre un determinado tema y que constituye el activo más valioso y vulnerable de la empresa.

La información es algo con mucho valor dentro de la sociedad actual, y así se reflejó en la conferencia de la Quinta Generación celebrada en 1981 en Japón, donde el director del proyecto japonés Toru Moto-Oka decía: (Gonzalez, 2006)

"La riqueza de las naciones que durante sus fases agrícolas e industrial dependió de la tierra, del trabajo y del capital, de los recursos naturales y de la acumulación monetaria, en el futuro se basará en la información, en el conocimiento y en la inteligencia". (Gonzalez, 2006)

No es nuevo que siempre la información ha sido muy importante, pero actualmente toma una dimensión especial, básicamente por la existencia de la informática y las telecomunicaciones, mediante las cuales una determinada información puede llegar a todo el mundo en unos segundos.

De esta forma y situados en este contexto, podemos encontrarnos con situaciones algo peligrosas; tan solo con pensar en la cantidad de información recogida en ficheros informáticos sobre las personas, que aisladamente pueden revelar poco de la persona, pero que en conjunto pueden darnos una visión bastante exacta de esa persona; o la cantidad de información tan valiosa que hay en ficheros del gobierno, militares, o empresariales, que pueden sumir en el caos a un país entero si esa información cae en manos de personas que sepan utilizarla en contra de ese país o empresa; estamos hablando, por ejemplo, de datos obtenidos por servicios de inteligencia, secretos empresariales sobre nuevos productos, o la interceptación de comunicaciones entre órganos gubernamentales, militares o empresariales. De hecho, todas las agencias de seguridad de los EEUU, evalúan los efectos de "ciberguerra", y las medidas a tomar, tanto de protección como de contraataque. Como se puede deducir, la cantidad y la "sensibilidad" de la información que hay en los sistemas

informáticos o telemáticos, hacen imprescindible que se tomen las medidas de seguridad oportunas, tanto físicas como lógicas, para evitar los problemas antes mencionados.

4.2 La Seguridad

Cuando de seguridad se trata, lo primero que imaginamos es la protección ante incendios, inundaciones y robos. Sin embargo, la seguridad no es solo eso, sino que se compone también de una parte lógica, la cual intenta salvaguardar la confidencialidad y la autenticidad de los ficheros y datos que se almacenan en un sistema informático o en un red.

Para llevar a feliz término esta tarea se ha de tomar conciencia de la importancia de la seguridad, especialmente por parte de los directivos de la empresa. Como se suele decir, "una cadena es tan fuerte como eslabón más débil", es decir, los sistemas de seguridad, físicos y lógicos, pueden ser de última generación y a un nivel máximo, pero todo esto no sirve de nada si algún empleado es descuidado y no elimina los documentos confidenciales, o no guarda convenientemente su clave de acceso al sistema, o un tercero logra engañarle y obtiene la información que necesita para acceder al sistema sin estar autorizado. Todos estos aspectos son eslabones débiles que hay que reforzar, o nuestra cadena será tan débil como ellos.

Ningún sistema de seguridad, por bueno se sea, es fiable al cien por ciento, siendo esta la regla básica para conseguir un mejor nivel de seguridad; nunca se ha estar conforme con el nivel de seguridad que se tiene, porque cada día aparecen nuevos métodos de vulneración de los sistemas de seguridad antiguos, y se debe mover con el pasar del tiempo, y estar informados de cualquier cambio en ese sentido, pues, por ejemplo, la seguridad lógica podría quedar desfasada, y por ello inseguros, en muy poco tiempo, debido al continuo cambio de la informática. Además se debe considerar que en determinadas páginas web, listas de distribución, y grupos de noticias se divulgan todos los agujeros que se conocen de los sistemas de seguridad, ello quiere decir que si no se toman las medidas oportunas para remediar ese fallo, cualquier persona podría fácilmente vulnerar un sistema informático, ya que el fallo se divulga "a bombo y platillo", sobre todo entre la comunidad hacker.

La seguridad informática se encarga de la protección de:

- Las personas.
- Los datos y la información de los sistemas informáticos y sistemas de almacenamiento.
- Las comunicaciones.

Para establecer un buen sistema de seguridad, lo primero que hay que hacer es una evaluación de riesgos, para ello hemos de seguir los siguientes pasos:

1. **Detección de fallos.** Consiste en localizar los agujeros que tenga el sistema de seguridad. Es preferible que dicha detección la haga un tercero imparcial y experto (auditores informáticos).

2. **Análisis.** Se trata de medir las posibles pérdidas y la probabilidad de que se produzcan.

3. **Solución.** Establecer las medidas necesarias para reducir o eliminar las probabilidades de que ocurra, intentar reducir los efectos de una hipotética infiltración, o aceptar el riesgo si los daños o las probabilidades de que se produjeran fueran pequeños.

Lógicamente, cualquier sistema de seguridad requiere una inversión más o menos cuantiosa, dependiendo fundamentalmente de la clase de fallo que se detecte, y la mayor o menor facilidad para convencer a los directivos de hacer la inversión depende de las pérdidas que se puedan producir y las probabilidades de que esta se produzcan.

Las posibles amenazas son:

- Acceso directo a los equipos y a las instalaciones, donde el intruso puede apoderarse de la información que desea.

- Ataque remoto. Es aquel en el que el atacante inicialmente no tiene el control de la máquina a la que quiere asaltar (la máquina remota) y se puede acceder a través de algún protocolo de internet o de alguna otra red, corriendo peligro la información contenida en la red.

- Provocación de caídas de equipos, cortes en el suministro de energía, ruptura de las comunicaciones, etc.

El típico objetivo para un pirata son las redes pequeñas y privadas, ya que carecen de firewalls (por sus costos), y utilizan medidas de seguridad inferiores, además de otras razones:

- Sus propietarios son nuevos en internet y no conocen todo lo que deberían sobre seguridad.

- El administrador del sistema tiene más experiencia con LAN que con TCP/IP, y eso hace que los piratas se aprovechen de los fallos intrínsecos de dicho protocolo.

- Tanto el equipo como el hardware son antiguos y todos sus agujeros los conoce la comunidad de internet.

4.3 Seguridad Perimetral

La seguridad perimetral se define como la correcta implementación de los equipos de seguridad que controlan y protegen todo el tráfico de entrada y salida entre todos los puntos de conexión o el perímetro de la red a través de una correcta definición de las políticas de seguridad y una buena configuración de los dispositivos de protección. La solución de Seguridad Perimetral protege a las redes de las amenazas tales como Hackers, ataques de Negación de Servicio (Denied of Service -DoS), Malware, Spam, contenido malicioso en correos y Páginas Web en diferentes medios y puntos de conexión o perímetro de la red organizacional.

A continuación el cuadrante mágico de Gartner donde se puede apreciar las distintas soluciones de seguridad perimetral y su posición dentro del mismo.

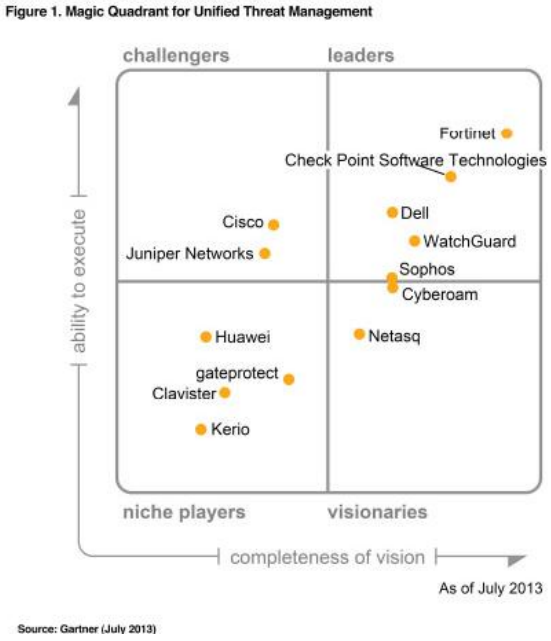

Figura 1. Cuadrante mágico de Gartner para herramientas de gestión de amenazas unificada.

En el informe Cuadrante Mágico sobre herramientas de Gestión de Amenazas Unificada (UTM), los analistas de Gartner han analizado la importancia de desplegar firewalls UTM en empresas de hasta 1.000 empleados, generando unos ingresos de hasta 1.000 millones de dólares. Asimismo, hacen foco en la importancia de capacidades como la incorporación de soporte Wireless LAN seguro y gestión basada en buscadores, no solo en las grandes empresas sino también en el mercado de las pymes.

Según los autores, el mercado de firewalls UTM se valoraba aproximadamente en 1.280 millones de dólares en 2011 y se espera que aumente con un índice de crecimiento anual del 15% hasta 2017.

Asimismo, este análisis de Gartner define a los líderes del mercado UTM como *" fabricantes en la vanguardia de fabricación y distribución de productos UTM que responden a las necesidades de las empresas de mediano tamaño. Los requisitos necesarios para posicionarse como líderes incluyen un amplio rango de modelos que cubran las necesidades de las medianas empresas, que soporten múltiples capacidades, así como capacidades de gestión e informes diseñados para facilidad de uso. Los fabricantes en este cuadrante lideran el mercado en cuanto a oferta de nuevas capacidades de seguridad, y permitiendo a los clientes desplegarlos a un precio reducido, sin afectar la experiencia del usuario final y sin incrementar la carga de los empleados. Estos fabricantes además poseen un impecable historial en la detección de vulnerabilidades en sus productos de seguridad. Entre las características comunes se incluyen fiabilidad, rendimiento consistente, y ser un producto fácil de gestionar y administrar".*

Bajo este criterio, ha reconocido como Líderes a Fortinet, SonicWALL, Check Point Software Technologies, WachtGuard y Sophos; en el área de Challengers ha situado a Cisco y Juniper Networks; en el cuadrante de Jugadores de Nicho ha identificado a Netgear, Trustwave, gateProtect, Clavister y Kerlo Technologies; en el espacio de Visionarios ha ubicado a Netasq y Cybercam.

4.4 Ventajas principales de La Seguridad Perimetral

Las innovaciones en seguridad perimetral han dado a las opciones de seguridad un nuevo significado. Una vez elegida la plataforma para seguridad perimetral se debe contemplar la existencia de un Security Gateway (appliance, software o appliance virtual), el mismo que debe estar en capacidad de añadir cualquier combinación de las aplicaciones que tiene a su disposición, de modo que cuando una compañía esté enfrentando nuevos retos, ésta tenga la libertad de adaptar su seguridad perimetral a voluntad.

El esquema de funcionamiento de la Seguridad Perimetral debe incluir mínimo 4 módulos funcionales, cada uno con distintas alternativas y funcionalidades de acuerdo a las necesidades del cliente:

- **Essentials.** Ofrece funciones básicas de seguridad para ayudar a proteger una red empresarial.
- **Network Security.** Debe incluir características totalmente integradas como un firewall configurado combinado con un sistema de Protección contra Intrusos (IPS), Denegación de Servicio (DoS), muchas herramientas de direccionamiento de tráfico y NAT.

- **Mail Security.** Se requiere para asegurar que el abuso al que el correo electrónico es sometido, tal como spam, virus y temas de privacidad, no afecte sus tareas de negocio diarias. El objetivo de esta aplicación, es garantizar que los mensajes válidos sean entregados apropiadamente y los empleados pueden encontrar lo que requieren sin ser expuestos a contenido peligrosos.
- **Web Security.** Protege a los empleados de una empresa de amenazas y les permite aplicar condiciones de cómo y dónde pueden utilizar su tiempo en línea. Los programas espía (spyware) y virus deben ser detenidos antes de que puedan entrar a la red y ocasionar daños. Todo debe ser registrado y organizado en reportes detallados los cuales muestren que tan efectiva es la política de seguridad implementada, de modo que se puedan realizar ajustes.

4.5 Essential.

Essential Firewall generalmente ofrece funciones de seguridad básicas para ayudar a proteger una red corporativa, por lo general protege un ilimitado número de direcciones IP y proporciona indefinidamente las siguientes características

- **Networking:** Router de Internet Router, Bridging, servidor DNS & proxy, DynDNS, servidor DHCP & relay, soporte NTP, automatic QoS automatic
- **Seguridad de Red:** Firewall con Stateful Packet Inspection Firewall & Network Address translation (DNAT/SNAT/Masquerading)
- **Acceso Remoto:** soporte de PPTP y L2TP sobre IPSec (incluyendo soporte de iPhone)
- **Registros / Informes:** Es necesario disponer de consultas y reportes en tiempo real para hardware, uso de la red y seguridad de la red, así como, reportes ejecutivos diarios.
- **Administración:** GUI basada en web, asistente de instalación, respaldo y restauración de configuración, notificaciones administrativas, soporte SNMP, administración centralizada mediante la seguridad perimetral Command Center

4.6 Network Security

El módulo de seguridad de red Security Gateway permite controlar y proteger a la red corporativa de ataques de hackers, intrusos y controlar el acceso desde el Internet. Dentro de sus funciones principales se destacan las siguientes:

- **Firewall:** Un buen firewall puede detener eventos costosos que pueden llevar a una pérdida o robo de información, infección a estaciones de trabajo así como otros incidentes que pueden minar la productividad. Apropiadamente configurado, un firewall puede mantener protegido mucho de la operación de su empresa.

El Firewall incluye una combinación de múltiples herramientas y características para controlar el flujo de información que circula desde el Internet a la red LAN y viceversa, entre las más importantes se menciona las siguientes:

- ✓ Stateful Packet Filter.
- ✓ Filtrado profundo de paquetes a nivel de aplicación.
- ✓ Administración flexible de reglas.

- **IPS / IDS:** Al analizar el tráfico de la red aprobado, el sistema de prevención de intrusos puede separar el tráfico peligroso y mantener su red a salvo de agresiones externas.
- **Control de DoS:** Las conexiones de Internet son fácilmente localizadas y utilizadas maliciosamente incluso por los malwares más simples. La prevención mediante la denegación de servicio mantiene sus recursos a salvo y sin daños durante estos ataques.
- **Control de Ancho de Banda:** El ancho de banda de Internet a menudo limita que tan rápido puede funcionar una red. Las empresas que aprovechan al máximo su ancho de banda disponible mantienen alta la productividad de sus empleados sin necesidad de que ellos experimenten demoras excesivas mientras trabajan.
- **Autenticación de Directorio:** La autenticación de directorio se enlaza con bases de datos externas y hace uso de sus usuarios y grupos en la configuración de seguridad. Una manera fácil de hacer que sus usuarios conecten sus VPN's con su misma clave de acceso.
- **Portal de Usuario:** Se requiere un portal de trabajo donde los empleados pueden trabajar con sus mensajes de email y tecnologías de acceso remoto previamente configuradas sin la necesidad de la ayuda de un Administrador.

4.7 Mail Security

Permite el control del tráfico de correo electrónico desde y hacia la red corporativa, asegurando que spam, virus no se conviertan en una amenaza para los usuarios. Dentro de sus características personales están:

- **Anti Spam:** Los correos no deseados o spam acarrean riesgos y roban valioso tiempo a sus empleados. Al utilizar el filtrado de correo, todo el correo electrónico no deseado es detenido antes que estos sean entregados y copen espacio en los buzones de correo.

- **Escaneo Antivirus:** Desvía contenido malicioso o dañino a la entrada de la red usando un doble motor antivirus que funcionan en paralelo. Esto permite que el contenido sea escaneado y bloqueado antes que éste tenga oportunidad de entrar a la red.
- **Encriptación de Correo:** Los correos electrónicos están lejos de ser privados. Cualquiera ubicado entre el remitente y el destinatario puede interceptar, leer e incluso copiar o alterar su contenido. Lo ideal es empaquetar sus mensajes de forma segura y cerrarlos con un sello de seguridad.
- **Portal de Usuario:** Su objetivo es permitir que los empleados puedan trabajar con sus mensajes de email y tecnologías de acceso remoto previamente configuradas sin la necesidad de la ayuda de un Administrador.

4.8 Web Security

Hace posible el permitir a sus colaboradores el tener acceso al Internet, sin que esto signifique pérdida de tiempo o recursos para la empresa. Adicionalmente la protección contra malware protege a su red de ataques externos desde sitios infectados. Sus características principales son:

- **Filtrado URL:** La navegación casual desperdicia tiempo y en algunas ocasiones puede ofrecer contenido, videos o imágenes indeseadas o inapropiadas. Con el filtrado de contenido se puede especificar a qué sitios web pueden tener acceso sus empleados.
- **Protección contra Spyware:** Los programas espía aún representan uno de los problemas más grandes para los administradores de red. La protección contra spyware puede mantener a salvo de infecciones a los usuarios a la vez que impide que información confidencial sea silenciosamente transmitida.
- **Escaneo Antivirus:** Desvía contenido malicioso o dañino a la entrada de la red. Esto permite que el contenido sea escaneado y bloqueado antes que éste tenga oportunidad de entrar a la red.
- **Escaneo HTTPS:** Una sesión de navegación segura protege los datos y la privacidad del usuario, pero amenaza la seguridad de la compañía a medida que sitios y archivos pueden traer contenido malicioso. El Filtrado HTTPS elimina este punto débil de la red y hace que el tráfico sea completamente transparente.
- **Filtrado IM / P2P:** La mensajería instantánea es a menudo utilizada para fines no laborales; las redes de compartición de archivos toman ancho de banda valioso reduciendo la velocidad de la red. Al usar el Filtrado IM/P2P ahorra dinero al restringir el acceso a este tipo de programas.

- **Reportes de Usuarios:** Es crítico el tener la retroalimentación de que tan efectivo es un dispositivo de seguridad ya que puede ahorrarle miles de dólares al proveer la información que requiere para hacer ajustes a la configuración, mediante reportes claros, detallados y de consulta.

4.9 Selección de proveedores y principales modelos.

La selección de proveedores puede verse como un toma de decisión multicriterio, en la cual se necesitan herramientas que aporten una mejor comprensión de los factores que influyen en la decisión, así como de las preferencias existentes.

La evaluación de desempeño del proveedor debe ser un proceso flexible, que permita evaluar las diferentes características de calidad y oportunidad de un producto o servicio prestado y la gestión de un proveedor. La empresa debe hacer seguimiento y acompañamiento a los planes de mejora que se generen de las evaluaciones hechas al proveedor y llevar control sobre toda la información generada por estos procesos, para decidir acerca de futuras negociaciones con los proveedores y la certificación.

El desarrollo de un programa de certificación de proveedores presume que la organización fije determinadas reglas de operación con el proveedor, de modo que se pueda definir un programa de trabajo para facilitar los intercambios, establecer políticas adecuadas de formas y plazos de pago, tiempos de entrega y especificaciones técnicas de calidad.

El proceso de selección de proveedores es un problema típico multicriterio que involucra factores tanto cualitativos como cuantitativos. Para abordarlo algunos autores han asumido gran variedad de técnicas, desde la programación lineal de múltiples objetivos hasta métodos probabilísticos. Al fundamentarse en datos puramente matemáticos, estas técnicas presentan desventajas notorias cuando son requeridas para considerar factores cualitativos, que son muy importantes en la selección de proveedores, en especial cuando se necesita desarrollar estrategias de dirección y gestión de la cadena de abastecimiento.

4.10 Metodología para la selección de proveedores.

El proceso de selección diseñado permitirá a las empresas disponer de una herramienta que correlaciona todos los factores críticos del proceso de compras, basándose en el análisis de las características propias de cada proveedor y que son consideradas relevantes para la empresa.

Debe entenderse según el espíritu de la norma al proceso de selección de proveedores, a la etapa previa al inicio del proceso de compra, mediante la cual se logra la validación o aprobación de algunos proveedores, que tienen las competencias para satisfacer las necesidades de la empresa.

4.11 Proceso de selección de proveedores de seguridad perimetral.

Vamos a considerar cuatros pasos fundamentales en la selección del proveedor de seguridad perimetral.

Figura 2. Pasos fundamentales en el proceso de selección de proveedores de seguridad perimetral.

- Lo primero que se debe considerar para el desarrollo del proceso de selección de proveedores propuesto es evaluar las necesidades de la compañía y establecer claramente los criterios para la toma de decisiones. Para ello es necesario realizar un estudio de la situación actual. Después se crea una lista con los criterios de selección que se tienen en cuenta para evaluar a los proveedores, el grupo de variables definidas responde a todas las necesidades y preocupaciones que la compañía ha experimentado en su actividad de compras. El primer grupo de criterios que se definan en el proceso corresponderán al conjunto de características internas que deben satisfacer los proveedores para entablar una relación de cooperación con la empresa. El segundo grupo de criterios considera las características propias del producto ofertado.

Establecidos claramente los dos grupos de criterios se requiere de un equipo multidisciplinario de decisión para analizar y decidir las características relevantes de cada proveedor. Todos los criterios se evalúan en base a la información proporcionada por los proveedores al momento de presentar su oferta para satisfacer la necesidad de seguridad perimetral.

Las empresas para las cuales va dirigido este estudio tienen en una gran mayoría un direccionamiento IP plano y no tienen implementado VLAN's o subredes en sus distintas instalaciones. Algunas disponen de un DMZ para sus servidores públicos y sus equipos de servicios privados son parte de su red local.

El acceso al servicio de internet es en algunos casos centralizado cuando se tiene más de una sucursal y pocas tienen dos proveedores de canal de datos, la mayor parte tienen un solo canal de datos y no se preocupan de la alta disponibilidad.

A continuación un esquema de red corporativo clásico y bastante robusto, sin embargo de lo cual, sufre de muchos ataques externos.

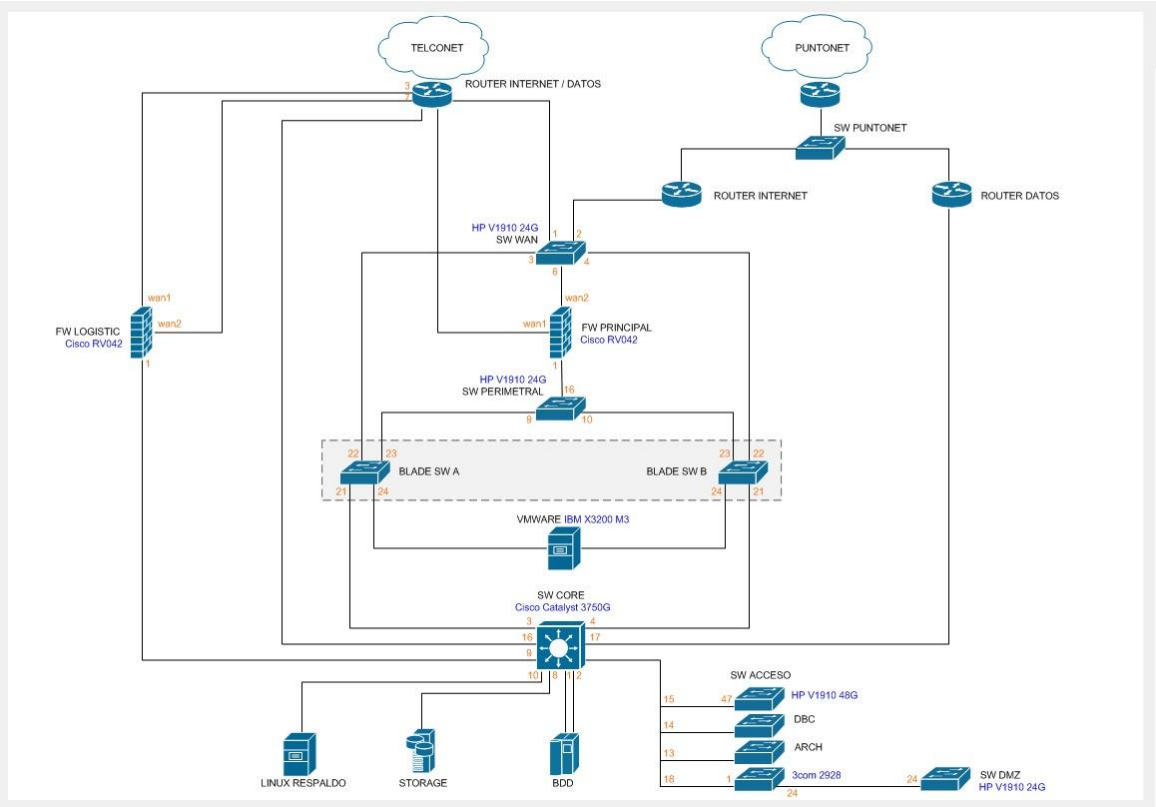

Figura 3. Esquema de red corporativo.

- El segundo paso a considerar es contactar los proveedores necesarios con la finalidad de que envíen una carta de presentación de sus servicios y junto con ella una oferta. Una carta de presentación se puede revisar en el Anexo C de este documento. Esta carta es importante, ya que habla de la seriedad de la empresa y su interés por participar en el concurso.

Una vez recibidas todas las ofertas se debe hacer una evaluación técnica y comercial de cada una de ellas, utilizando para ello una valoración de cada uno de los criterios definidos para la evaluación. Esta valoración permitirá seleccionar el proveedor adecuado y su ponderación dependerá mucho de la cantidad de personas o profesionales que estén al frente del proceso de contratación.

Para poder conocer cuáles son los proveedores que se encuentran mejor posicionados y así satisfacer los requisitos solicitados por la empresa tales como características del producto, el plazo y el precio, se debe realizar el proceso de evaluación de proveedores, considerando aquellos cuyo software de seguridad perimetral tenga de preferencia un posicionamiento en el cuadrante mágico de Gartner, esto garantizará que el producto ofrecido sea realmente una herramienta probada, robusta; y, por consiguiente nos enfocaremos en los beneficios y servicios ofertados por el proveedor y no en la herramienta.

A continuación un gráfico donde se puede apreciar los diferentes procesos que debe contemplar una evaluación de proveedores.

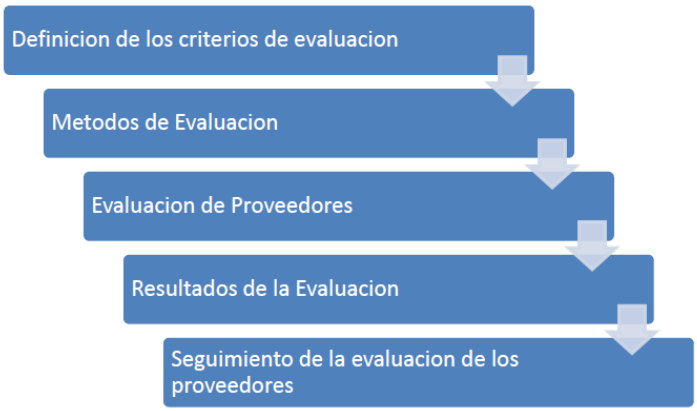

Figura 4. Proceso de selección de proveedores de seguridad perimetral.

4.12 Criterios de evaluación.

Es conocido que la decisión final para seleccionar un proveedor es muy compleja y es por ello que se vuelve necesario establecer los criterios de evaluación apropiados. El análisis de estos criterios ha sido discernido por muchos autores desde 1960.

La mayor parte de autores que analizan este tema mencionan los 23 criterios del estudio de Dickson, como los más importantes. Siendo los criterios más significativos de acuerdo a lo revisado: la calidad del producto, el cumplimiento de los tiempos y la garantía ofrecida por el proveedor.

Considerando la opinión de varios autores, amerita indicar 12 criterios que se considerarán en este proyecto. La importancia de uno u otro criterio dependerá de la necesidad de cada proceso de selección, pues ninguno es igual por mucho que se parezca.

A continuación un cuadro que considera los criterios sugeridos por Dickson y los criterios recomendados en este proyecto de titulación.

Estudio de Dickson	Estudio recomendado
1. Calidad del producto. 2. Entrega oportuna. 3. Rendimiento de la solución. 4. Garantía ofertada. 5. Capacidad de producción. 6. Precio de la solución. 7. Capacidad técnica del proveedor. 8. Situación financiera del proveedor. 9. Cumplimiento de procesos. 10. Sistema de comunicación. 11. Reputación del proveedor y posicionamiento. 12. Deseo de negociación. 13. Administración y organización. 14. Control de funcionamiento. 15. Servido de reparación. 16. Actitud de servicio. 17. Calidad de la impresión. 18. Habilidad de embalaje. 19. Relaciones laborales. 20. Ubicación geográfica. 21. Cantidad de negocios anteriores. 22. Formación de los empleados. 23. Acuerdos mutuos.	1. Calidad del producto. 2. Precio de la solución. 3. Cumplimiento de los plazos de entrega. 4. Servicio ofertado - Cotización. 5. Situación financiera del proveedor. 6. Tiempos cortos de entrega de la solución. 7. Habilidad técnica del proveedor. 8. Flexibilidad de la solución. 9. Desarrollo de la solución. 10. Actitud de gestión. 11. Ubicación geográfica.

Tabla 1. Criterios de evaluación

A continuación se describe cada uno de los criterios de selección que se han definido en la presente metodología, los cuales representan las características internas exigidas a los proveedores para entablar una relación de cooperación con la empresa. Es necesario indicar que dependiendo de la empresa se puede incluir o descartar otros criterios mencionados en el documento.

Sistema de gestión de calidad. El proveedor deberá demostrar su habilidad para establecer, documentar e implementar un sistema de gestión de calidad efectivo para lo cual se tomará como referencia la norma ISO 9001.

Capacidad administrativa. Se busca que los proveedores cuenten con madurez administrativa. Se busca que los proveedores cuenten con madurez administrativa que les permita entablar una relación de cooperación basada en el mantenimiento de niveles óptimos de calidad, costos y servicios.

Desempeño comercial. La organización requiere un proveedor que sea rentable para la compañía, en términos de descuentos y plazos de pago. Esta flexibilidad propia de cada proveedor demuestra su estabilidad comercial y brinda un respaldo de confianza en términos económicos.

Estabilidad financiera. Se debe requerir que los proveedores tengan una posición financiera estable y sólida, lo cual es un buen indicador en el momento de hacer negociaciones a largo plazo; también ayuda para que los estándares de desempeño puedan ser mantenidos y que los productos continúen disponibles.

Tratamiento de quejas y reclamaciones. El proveedor debe desarrollar estrategias efectivas para resolver quejas e inquietudes, investigar sus causas y, por ende, mejorar el servicio prestado a la empresa de manera continua.

Posicionamiento geográfico, centros de distribución y soporte técnico. La organización debe contar con proveedores eficientes, indiferentemente de su procedencia, teniendo en cuenta que el posicionamiento geográfico puede influir en los tiempos de entrega, costo en fletes-seguros y documentación legal.

Investigación y desarrollo. Se busca seleccionar proveedores que se encuentren fuertemente relacionados con la investigación y el desarrollo de sus productos.

Capacidad instalada de producción. El estudio de la capacidad es fundamental para la gestión empresarial en cuanto permite analizar el grado de uso de cada uno de los recursos en la organización y así tener oportunidad de optimizarlos.

El cumplimiento de las especificaciones y la correcta planificación de implementación del software de seguridad perimetral, es uno de los factores más importantes para la evaluación de los mismos.

Es importante medir el nivel de servicio considerando para ello factores como la rapidez, eficacia y flexibilidad en los distintos entregables del proyecto ya que ello afecta directamente al nivel de satisfacción de los clientes, influyendo en la evaluación de un proveedor de seguridad perimetral. Hay que considerar además que el precio no necesariamente es un factor gravitante cuando se pone en riesgo la calidad de un producto.

Otros factores importantes que se deben tener presentes en la selección de un proveedor, son la capacidad financiera y tecnológica del proveedor de seguridad perimetral, la facilidad de comunicación y cooperación, la flexibilidad y rapidez para adaptarse a las demandas y requerimientos de la empresa.

Los criterios descritos en este documento se evalúan en una escala de 1 a 5, donde el 5 es el máximo valor posible y 1 el menor valor posible, como ejemplo se presenta la siguiente descripción general:

Puntaje Obtenido	Descripción de cada criterio
5 Puntos	Aprobación **Plena** del Criterio según descripción
4 Puntos	Aprobación **Simple** del Criterio según descripción
3 Puntos	**Indecisión o Indiferencia** del Criterio según descripción
2 Puntos	Desaprobación **Simple** del Criterio según descripción
1 Punto	Desaprobación **Plena** del Criterio según descripción

Tabla 2.Ejemplo de ponderación

4.12.1 Evaluación de proveedores de seguridad perimetral.

La evaluación resulta de la información proporcionada por el proveedor, pudiendo definirse a más de los criterios varios subcriterios, logrando que la evaluación sea más detallada. Los criterios, su definición y la escala de puntaje, para el caso de proveedores de seguridad perimetral son los siguientes:

Criterio	Descripción Genérica Criterio	Puntaje	Recomendación
1.Cotización	Se refiere a la respuesta eficiente (Tiempo de atención en días hábiles) por parte del proveedor ante cualquier inquietud, cotización y/o solicitud realizada por la Organización, con respecto al producto que se quiera adquirir.	Menor a 1 día - 5 Puntos Entre 1 y 2 días - 4 Puntos Entre 3 y 5 días -3 Puntos Entre 5 y 10 días -2 Puntos Mayor de 10 días - 1 Puntos	• Aceptación inmediata de su interés en cotizar e indicar fecha en que enviará cotización (1 día) • Cumplir con fecha comprometida para cotizar • Utilizar formatos que se enviar para cotizar • Entregar Asesoría al comprador sobre la definición del producto por entregar.
2. Calidad	Este criterio está definido por el desempeño real de los mismos y su competencia para cumplir con los requisitos descritos en las especificaciones de la compra, incluyendo el tiempo efectivo de garantía de la adquisición realizada.	Satisface Totalmente la calidad - 5 Puntos Satisface Medianamente la calidad - 4 Puntos Satisface Regularmente la calidad -3 Puntos Presenta Baja calidad - 2 Puntos No Satisface la calidad - 1 Puntos	• Corregir cualquier observación en documento técnicos o planos entendiendo que son parte de su oferta. • Entrega final de protocolos, planos e instrucciones sin observaciones o correcciones pendiente en las fechas acordadas o establecidas. • Entregar una atención post venta
3.Plazo de Entrega	Este criterio se refiere al periodo de tiempo entre la notificación al proveedor de la aceptación de oferta o medio para la confirmación de la compra y la llegada del producto, insumo, material a las instalaciones de la empresa.	Entre 0 y 2 días - 5 Puntos Entre 3 y 4 días - 4 Puntos Entre 5 y 6 días - 3 Puntos Entre 7 y 8 días - 3 Puntos Sobre 9 días -1 Puntos	• Entregar aceptación de la PO al recibirla y aceptar en forma total o con observaciones de inmediato. • Cumplir con fechas de inspecciones en Fábrica acordadas o establecidas en la PO. • Cumplir con fechas de entrega de Producto acordadas o establecidas en la PO.
4.Cumplimiento de plazos de entrega	Este criterio indica el nivel de cumplimiento de los plazos y acuerdos establecidos en la oferta y/o cotización.	Satisface Totalmente los plazos y acuerdos - 5 Puntos Satisface Medianamente los plazos y acuerdos - 4 Puntos Satisface Regularmente los plazos y acuerdos - 3 Puntos Baja Desempeño en los plazos y acuerdos - 2 Puntos No Satisface los plazos y acuerdos - 1 Puntos	• Entregar información Técnica, protocolos y Planos en forma oportuna y en formatos solicitados e indicados en PO • Respetar las normas de seguridad de ABB cuando tenga que visitar faenas.
5.Precio	Este criterio se refiere al valor en pesos del producto adquirido.	Bajo el promedio (Descuento sobre un 5%) - 5 Puntos Bajo el promedio (hasta un 5% Descuento) - 4 Puntos Precios iguales al mercado - 3 Puntos Precios sobre el promedio (hasta un 5% más) - 2 Puntos Precios sobre el promedio (sobre un 5% más) - 1 Puntos	• Respetar el precio entregado en su oferta y comprometido al aceptar la PO, sin exigir modificaciones al tener que corregir o mejorar el producto para cumplir con lo especificado

Tabla 3. Subcriterios de evaluación ponderados

Para una apropiada gestión de compras es muy importante establecer el proceso de evaluación de proveedores, el cual debería tener en consideración al menos los siguientes aspectos:

- Experiencia del proveedor.
- Buen desempeño en relación a la competencia.
- Requisitos de calidad del producto ofertado, precio, fecha de entrega y tiempos de respuesta a los problemas que se pudiesen presentar.
- Evaluación financiera que garantice la viabilidad del proveedor.
- Respuesta del proveedor a consultas y solicitudes de ofertas.
- Cumplimiento de los requisitos legales.

Los criterios y sus subcriterios asociados tendrán asignado un peso relativo para la obtención de la calificación final, dada la agrupación de productos y servicios ofertados por el proveedor, según se indica a continuación:

Criterios	Ponderación Criterio	Descripción
Calidad del Servicio	**40%**	Trabajo o servicio realizado
		Cumplimiento normas de seguridad y prevención de riesgos
		Cumplimiento normativa ambiental
		Cumplimiento y Administración Sistema de Aseguramiento de Calidad
		Infraestructura, equipos, herramientas
		Calidad de materiales y suministros
		Iniciativa y cooperación
		Idoneidad del personal clave
Plazos	**40%**	Cumplimiento plazos
		Programación del trabajo
Aspectos Administrativos	**20%**	Cumplimiento leyes laborales y control administrativo
		Conducta interna del personal
TOTAL	**100%**	

Tabla 4.Criterios de evaluación ponderados

4.12.2 Escala de Calificación de Desempeño

La escala de calificación final del desempeño es única para todos los proveedores, siendo independiente si es de producto o servicio, y se realiza sobre la base de una escala continua de 0 a 100 %, obtenido de los puntajes ponderados (Ver Anexo B) de las evaluaciones

parciales del periodo evaluado. Puntaje Máximo de evaluación corresponde al 100%, quedando Clasificados como sigue:

Calificación de Desempeño (%)	Plan de Acción	Condición
Mayor o Igual a 70%	Se aconseja mantener como proveedor.	"CALIFICADO".
Mayor o Igual a 50% y Menor que 70%	Se aconseja condicionar su permanencia en el Registro de proveedores, a la espera de las mejoras en su desempeño en un periodo no mayor a 6 meses (Debe presentar plan de mejora)	"CALIFICADO CON RESERVA".
Menor que 50 %	Se aconseja que no sea Considerado como proveedor, ya que no cumple con los requerimientos establecidos por la empresa para el bien o servicio a solicitar; lo anterior no excluye la posibilidad de poder utilizar sus servicios posteriormente. (Debe presentar plan de mejora, para reevaluación).	"DESCALIFICADO".

Tabla 5.Cuadro de calificación

Los antecedentes de las selecciones, evaluaciones y reevaluaciones de los proveedores, deben ser analizados por el comité de evaluación de proveedores con una periodicidad anual.

- Los proveedores cuyo desempeño supere el 70%, serán notificados de su condición de "**CALIFICADO".**
- Los proveedores cuyo desempeño se encuentre entre el 50% y el 70%, deben ser notificados de su condición de "**CALIFICADO CON RESERVA**", y deberán presentar un plan de acción de mejora para enfrentar las debilidades detectadas, el cual deberá presentar dentro de un plazo prudencial, posteriores a la solicitud. El Plan se deberá desarrollar en los tres meses posteriores de su entrega, este proveedor puede seguir prestando servicio o productos y entrará al siguiente proceso de evaluación de proveedores.
- Los proveedores con un desempeño menor al 50%, serán notificados de su condición de "**DESCALIFICADO**" y no podrán continuar brindando servicios o productos, por el tiempo de suspensión o plazo de eliminación indicado por el comité de evaluación de proveedores de seguridad perimetral.

4.12.3 Periodicidad de la Calificación

La calificación de un proveedor será única y de carácter transversal para toda la empresa, reflejando el desempeño del proveedor en todas las Unidades de Negocio que haya prestado servicios o suministrado bienes en un período de tiempo, según se indica en el siguiente cuadro:

Tipo de Proveedor	Periodicidad de la Calificación
Servicios y Productos	**ANUALMENTE** se ejecutará el proceso que permitirá obtener la evaluación general del proveedor, que considerará todas las evaluaciones realizadas para un proveedor en cada uno de los contratos u órdenes de servicio, los documentos de compra, peticiones de oferta y documentos de recepción registrados durante el período. La evaluación es realizada según año vencido, y con inicio del proceso el Primer trimestre de cada año.

Tabla 6. Cuadro de servicios

4.12.4 Comunicación de la evaluación a los proveedores.

Los proveedores deberán contar con la información de sus procesos, las cuales serán informadas por la gerencia de sistemas y con el apoyo de la gerencia general:

4.12.5 Reevaluación de proveedores.

Consiste en el seguimiento posterior a la etapa de evaluación de proveedores, mejorando continuamente la prestación de los servicios de los proveedores, en este sentido, el sistema de Evaluación de Proveedores, estará abierto, para que el área usuaria pueda ingresar nuevas evaluaciones del proveedor Critico, como ellos convengan, a los servicios y/o productos que se repitan en el tiempo o tengan entregas parciales, permitiendo la mejora del desempeño del Proveedor.

4.13 ISO 9001

Entre los distintos requisitos que forman parte de la norma ISO 9001, se encuentra la relacionada con la evaluación de los proveedores ya que afecta a la calidad de la mayoría de la organizaciones, aunque no en igual grado de importancia. Estableciendo una cadena entre el proveedor y el cliente, ya que, no hay ninguna organización que no requiera de algún producto ajeno para prestar su servicio.

La norma ISO 9001 implica tener una evaluación/control en los siguientes términos:

- Determinación de los requisitos de los productos.
- Selección de los proveedores en función de la prestación de los productos con los estándares o características marcadas. De ahí que se establezcan procesos de “selección de proveedores” y de “evaluación de proveedores”.
- Aseguramiento por parte de la organización de que los productos comprados cumplen con los requisitos establecidos. Para ellos deben desarrollarse inspecciones o auditorías que muestren las evidencias del cumplimiento o no de los estándares marcados. Estas actividades deben de desarrollarse de forma continua. En primer lugar se debe partir de una evaluación inicial para establecer, de forma continua una re- evaluación.
- Esta evaluación y re-evaluación debe poseer unos criterios y parámetros que la organización considere como críticos.

Cualquier organización debe de aspirar a fortalecer las relaciones con los proveedores. Para ello pueden aplicarse las siguientes actividades:

- Generación de un contacto fluido entre el cliente y el proveedor para crear una relación de confianza mutua.

- Implicar al proveedor mediante la solicitud de aportaciones para la mejora continua.
- Creación de un sistema de medición que sirva para la comparación entre proveedores y que permita el seguimiento de cada uno de ellos de forma individual. La información obtenida se debe utilizar no sólo para seleccionar los proveedores, sino para ayudarles a mejorar.
- Cada proveedor debe de poseer objetivos. De esta forma, se puede estimar los "costes de la no calidad" derivados de los errores de cada proveedor.

De manera general, la evaluación de los proveedores es uno de los requisitos peor asimilados por las organizaciones que implementan la ISO 9001. Los principales problemas residen en que se dispone de un único proveedor de un tipo de producto e independientemente de los resultados de las evaluaciones, se debe seguir manteniéndolo.

En el resto de los casos, la norma obliga a que la organización evalúe y seleccione a los proveedores en función de su capacidad de suministrar productos de acuerdo a los requisitos de la organización.

4.14 Métodos para evaluación.

Existe una gran variedad de métodos para evaluar a los proveedores, en este proyecto se ven brevemente algunos de ellos.

4.14.1 Decision Matrix Method.

Este es un método para la selección concepto usando una matriz de puntuación llamado la Matriz de Pugh. Se lleva a cabo mediante el establecimiento de un equipo de evaluación, y la creación de una matriz de criterios de evaluación en comparación con realizaciones alternativas. Esta es la matriz de puntuación por lo general asociado con el método y el QFD es una forma de matriz de priorización. Por lo general, las opciones se obtuvo en relación con criterios utilizando un enfoque simbólico (un símbolo para mejor que, otro para el neutro, y otro para peor que la línea de base). Estos se convierten en puntuaciones y se combinan en la matriz para producir puntuaciones para cada opción.

- Eficaz para la comparación de los conceptos alternativos.
- Puntajes conceptos relativos el uno al otro.
- Método de evaluación iterativo.
- Más efectivo si cada miembro de un diseño tean realiza de forma independiente y los resultados se comparan.

Para definir los criterios de evaluación se recurre a dos técnicas:

Selección a través de expertos: Se consideran expertos a los directivos de la empresa ya que en base a su experiencia pueden decidir la mejor opción a implementar. En este tipo de procedimientos el número de expertos con los que cuente la organización, permitirá definir de manera más asertiva los criterios y las ponderaciones a aplicar a cada uno de los criterios.

Selección de los criterios de decisión: Son los expertos seleccionados en el paso anterior quienes después de algunas rondas de discusión y de aplicar algunas técnicas, decide los criterios de decisión. Así por ejemplo:

Criterio 1: Nivel de calidad de los productos suministrados.

Criterio 2: Tiempo de Entrega.

Criterio 3: Ubicación del Proveedor.

Criterio 4: Grado de adaptabilidad a los cambios sugeridos a la empresa.

Es importante construir una escala de valoración para la calificación de los proveedores en cada uno de los criterios definidos por el grupo de expertos seleccionado.

4.14.1.1 Ejemplo: A continuación un cuadro de resultados que puede ayudar a definir cuál es el mejor proveedor en base a los criterios definidos.

Características / EMPRESA	Emp01	Emp02	Emp03	Emp04	Emp05
Certificaciones y premios de la herramienta	5	5	5	5	5
Herramienta aparece en el cuadrante mágico de Gartner.	5	4	3	3	4
Contiene los módulos básicos	5	5	5	5	5
Tiene módulos adicionales.	5	4	1	1	2
Incluye appliance	5	5	5	4	3
Presenta Plan de Soporte	5	5	5	1	1
Propuesta incluye licenciamiento para alta disponibilidad.	5	5	3	3	3
Los servicios de instalación y configuración están incluidos en la propuesta.	5	5	1	5	5
Incluye capacitación	5	5	1	1	1
Precio de la herramienta y forma de pago	5	5	3	2	2

Tabla 7. Ejemplo de aplicación de criterios.

En el cuadro anterior se debe considerar que la puntuación más alta, es decir, "5" se asigna a la empresa que cumpla a satisfacción la característica y que tenga la mayor cantidad de beneficios respecto al resto de empresas participantes.
La calificación uno se asigna a aquellas empresas que no presentan nada en cuanto a la característica que se está evaluando.

4.14.2 Beneficios de la evaluación de proveedores.

A lo largo de todo el texto se ha insistido en la importancia del proceso de selección de proveedores de seguridad perimetral para la calidad global de la organización. Al respecto, resulta conveniente nombrar uno de los 8 principios que fundamentan el modelo ISO 9001:2008, específicamente aquel que alude a las *"relaciones mutuamente beneficiosas con el proveedor"*. Así, toda organización debería aspirar a un fortalecimiento de las relaciones con sus proveedores, de tal manera, que toda la cadena de suministro sea muy sólida.

En el marco de este principio se encuentran clasificadas las actividades destinadas para la evaluación de proveedores, cuyos beneficios en caso de que el proceso de selección sea llevado de una manera adecuada son los siguientes:

- Reducción de costos, mediante la optimización de procesos de control.
- Contar con una base de proveedores calificados para respaldar sólidamente las decisiones de compra o contratación.
- Evitar que proveedores no calificados participen en los diferentes concursos a fin de disminuir riesgos.
- Garantizar que los proveedores cuentan con los recursos necesarios para satisfacer las entregas de acuerdo a los requerimientos establecidos.
- Contar con herramientas de control de proveedores para calificarlos y medir su rendimiento.
- Garantizar la calidad en el servicio que brindan los proveedores.

4.15 Consideraciones que se deben tener en cuenta al implementar la seguridad perimetral.

A continuación se describen algunas consideraciones necesarias al momento de implementar la herramienta de seguridad perimetral.

4.15.1 Diseño de seguridad perimetral

Para asegurar el buen uso de los recursos informáticos de una organización y prevenir ataques hacia servicios publicados y accesos no autorizados es primordial la implementación de un sistema de seguridad perimetral.

Los beneficios alcanzados con una correcta implementación de seguridad perimetral son:

- **Perímetro confiable:** Delimitación de tráfico confiable de la red local y tráfico proveniente de Internet.
- **Protección de intrusiones:** Acceso autorizado a los recursos de la red y servicios publicados.
- **Niveles de acceso a información:** Permite establecer políticas de seguridad, definiendo los servicios y que clientes desde Internet pueden acceder a la información de la organización.
- **Optimización de acceso:** Se asigna los correspondientes permisos de acceso a servicios de Internet, optimizando el consumo de ancho de banda y evitando la saturación para el buen desempeño de los servicios publicados.
- **Alta disponibilidad:** Garantiza la continuidad operacional del sistema de seguridad perimetral.
- **Balanceo de carga:** Distribuir las peticiones realizadas hacia el servicio de Internet, proveniente de los usuarios de la red corporativa, entre dos proveedores de servicio diferentes

4.15.2 Requerimientos de diseño de Seguridad Perimetral.

Toda empresa requiere de un sistema de seguridad perimetral que garantice un control y filtrado de paquetes proveniente de la red local, canales de datos o Internet. El sistema de seguridad perimetral debe cubrir los siguientes requerimientos:

Requerimiento	Observaciones
Alta disponibilidad	Puesta en marcha de un sistema de seguridad perimetral en alta disponibilidad que garantice la continuidad operacional del servicio.
Creación de zonas dentro de DMZ.	Implementación de DMZ para un control exhaustivo de acceso a servicios desde las diferentes zonas, sean estas: servidores públicos, enlace de datos, red local y enlace de Internet.
Sistema de prevención y detección de intrusos.	Control de acceso hacia una red informática para proteger servicios publicados de manera privada o pública de ataques y abusos.
Filtrado de contenido Web.	Permitir bloquear el contenido no deseado de páginas Web, restringir el acceso a páginas de entretenimiento, compras, pornografía y páginas de chat, denegar y evitar los programas de descarga.
Bloqueo de puertos.	Establecer políticas de seguridad que restrinjan el acceso a puertos TCP y UDP desde la red local hacia las diferentes zonas.
Administración.	Administración por consola y vía Web del equipo de seguridad perimetral.

Tabla 8. Requerimientos del sistema de seguridad perimetral.

4.15.3 Esquema de Seguridad Perimetral.

Dentro del esquema de seguridad perimetral que se propone, se destaca la creación de 4 zonas para determinar los segmentos de red a ser configuradas. Estas son:

- **Zona Internet:** Se determina todos los elementos que no pertenecen a la red de la organización que se encuentran en Internet.
- **Zona Servidores:** Se determina los servidores públicos o semi-públicos. Se crean políticas de seguridad para acceso a DMZ de servidores.
- **Zona Datos:** Se determina todos los elementos que pertenecen a sucursales, puntos remotos o proveedores que se encuentran conectados a la empresa a través de un canal de Datos.
- **Zona Red Local:** Se determina todos los elementos que pertenecen a la red local de la empresa.

En el siguiente esquema se identifica las zonas a crear dentro del sistema de seguridad perimetral:

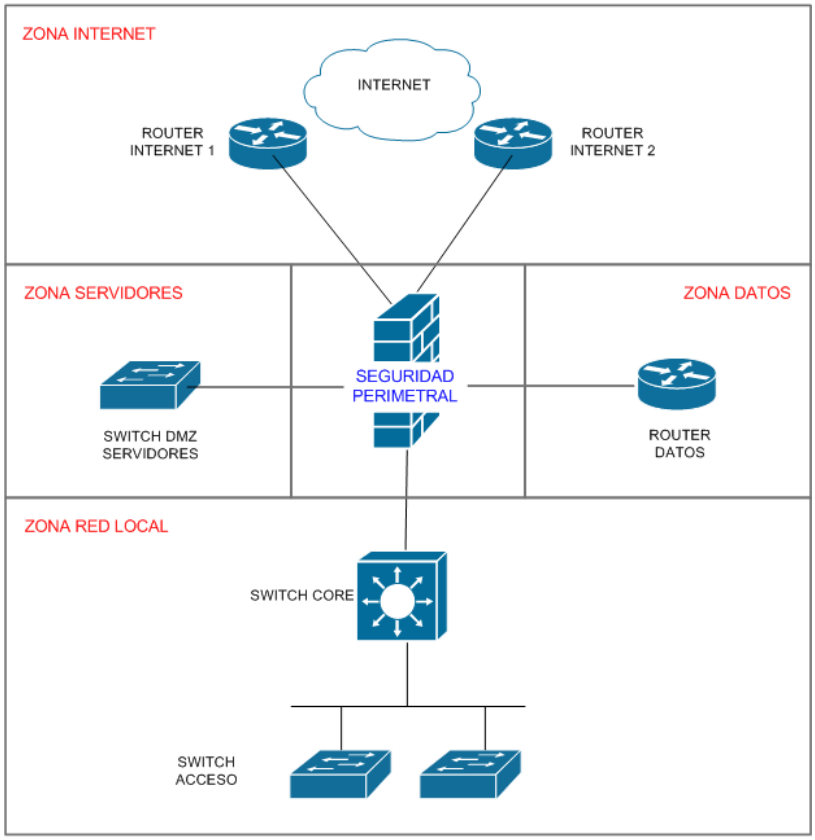

Figura 5. Identificación de zonas en sistema de Seguridad Perimetral.

4.15.4 Diseño de red corporativa y seguridad perimetral.

Se propone la implementación del siguiente diseño de red corporativa y seguridad perimetral, basado en equipos en alta disponibilidad:

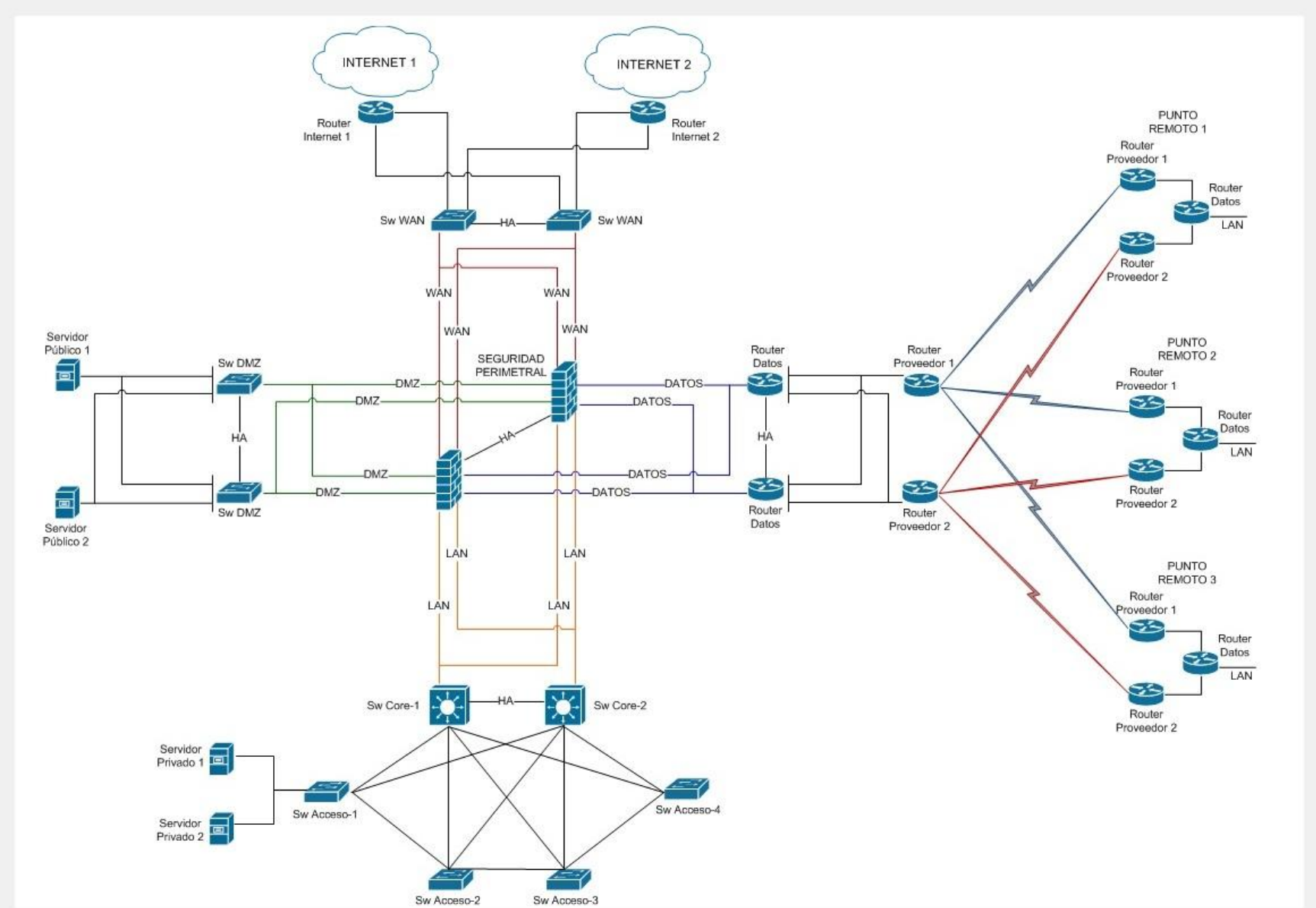

Figura 6. Diseño de red corporativa y seguridad perimetral.

4.15.5 Flujo de información con el diseño de networking.

El flujo de transmisión de datos a través del esquema de red corporativo se describe a continuación:

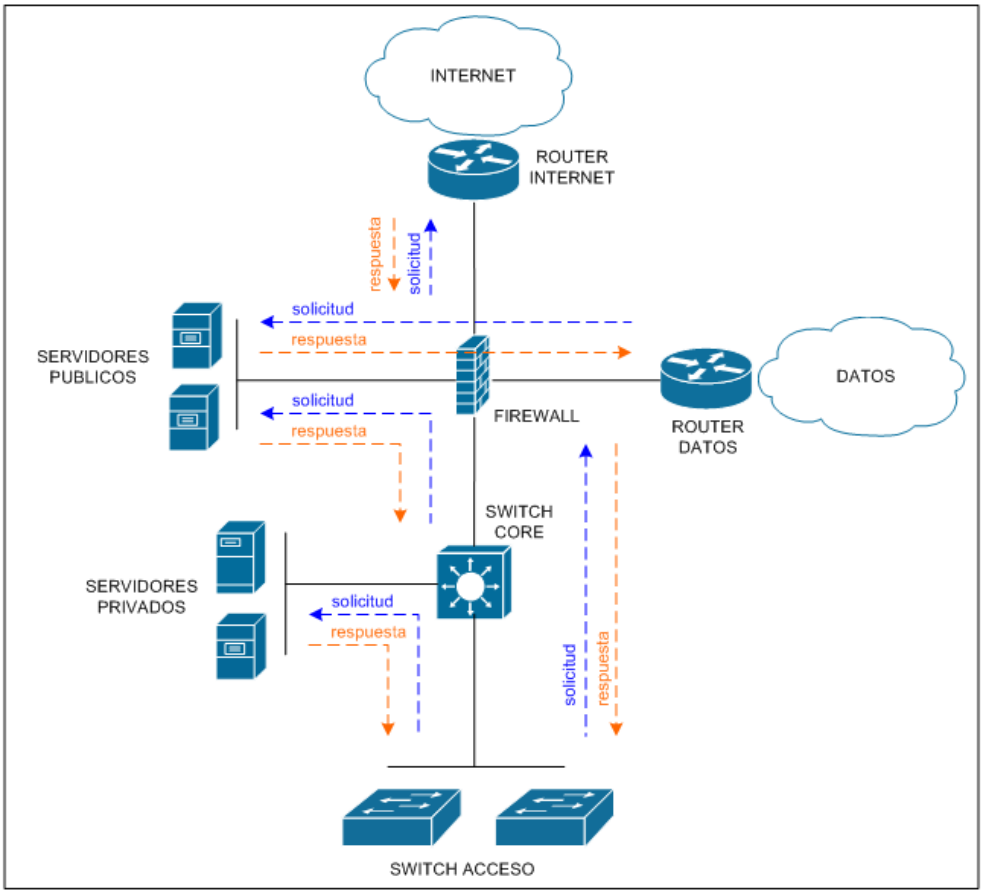

Figura 7. Flujo de información.

4.15.6 Beneficios con el diseño de networking y seguridad perimetral.

Con la implementación del diseño de Networking y Seguridad Perimetral en la empresa se tienen los siguientes beneficios:

- Filtrado de paquetes enviados desde puntos remotos, proveedores y red local a través del sistema de Seguridad Perimetral.
- Mejor nivel de seguridad con la implementación de políticas en el sistema de Seguridad Perimetral para mantener un control exhaustivo sobre las conexiones establecidas con los aplicativos.
- Conmutación automática del sistema de Seguridad Perimetral entre proveedores de canales de Datos como plan de contingencia para evitar indisponibilidad del servicio.

- Implementación de redes virtuales para la mejor administración de los recursos de la red corporativa. Se debe implementar control por listas de acceso como medida de seguridad y asignación de políticas para el uso de aplicativos.
- Conexión independiente de servidores en equipos de conectividad en redundancia, evitando, a través de la segmentación de la red corporativa, la saturación en el medio de transmisión por tormenta de broadcast o tráfico basura generado por virus o malware.
- Configuración en estaciones de trabajo y servidores privados como puerta de enlace, dependiente del segmento de red corporativa, al switch Core para el debido enrutamiento entre VLAN's y filtrado de paquetes mediante listas de acceso.

5 Conclusiones

- Conocer la situación actual de la empresa antes de iniciar cualquier actividad de implantación de soluciones perimetrales es primordial ya que permitirá poner en evidencia las debilidades y fortalezas del esquema de seguridad que tenga la empresa en ese momento, y a partir de entonces proceder a realizar las mejoras pertinentes. Es claro que no se pueden tomar acciones correctivas sobre lo desconocido.
- Una vez que se conoce la situación real de la empresa se debe tomar acciones correctivas sobre la infraestructura actual de la empresa en lo que a Networking se refiere. Debido a las características de alta disponibilidad que se busca en los sistemas informáticos a nivel de conectividad, se debe implementar un diseño redundante a nivel de esquema de red en las diferentes zonas de seguridad con equipos robustos de prestaciones acordes a las necesidades de la empresa.
- El estudio sirve para que los accionistas y el gerente de la empresa apoyen por completo el plan de adquisición de un sistema de seguridad perimetral, más aún cuando han comprendido los riesgos y lo importante de proteger la información. Normalmente este tipo de acciones permiten al jefe de sistemas, seleccionar el proveedor y la herramienta más apropiada para la organización.
- La protección de la información debe ser en adelante una prioridad en la empresa, y servirá para identificar las debilidades de protección, permitiendo definir políticas y procedimientos que acompañados del software de seguridad perimetral, minimizarán la fuga de información en la empresa.
- Se debe incorporar equipos de seguridad perimetral appliance con sistema operativo propietario fabricados exclusivamente para este fin. Estos equipos deberán cubrir las necesidades de alta disponibilidad, balanceo de carga entre proveedores de servicio de Internet, creación de zonas de seguridad, filtrado de paquetes mediante mecanismos automatizados y configuración de políticas de seguridad. En el mercado existen

equipamiento para seguridad informática fabricados por Checkpoint, Juniper, La Seguridad Perimetral o Fortinet que pueden cumplir esta función de firewall de manera cabal, mejorando los niveles actuales de seguridad.

- Establecer la infraestructura requerida para soportar el esquema de seguridad que se desea implementar es importante para no tener problemas al momento de implementar el software de seguridad perimetral. Es recomendable que la solución que se implemente incluya hardware propio para evitar fallas en el software.
- Seleccionar por lo menos 3 proveedores que cumplan con los requisitos solicitados en la oferta del concurso. Ser imparcial al momento de evaluar a todos los proveedores a fin de que la ponderación sea justa. Al final el que más puntos obtenga será el proveedor seleccionado. Es importante haber definido los criterios que se usarán para evaluar el proveedor adecuado considerando que el mismo más que un proveedor es un socio de negocios y como tal servirá de apoyo en las necesidades de la empresa a largo plazo.

6 Recomendaciones.

- Se debe establecer realizar un proceso de mejora continua de tal manera que estén siempre prevenidos a nuevas formas de ataque. En seguridad no es posible estancarse con una solución y olvidarse de fortalecerla.
- Para mantener un estricto control del tráfico proveniente de los puntos remotos, no se recomienda conectar los routers de proveedores a la red local, ya que esta vulnerabilidad puede comprometer de manera directa la información de la empresa. Por tal motivo, se recomienda conectar los equipos de proveedores en una zona de seguridad creada en el equipo de seguridad perimetral para proporcionar los debidos permisos de acceso a los recursos de la empresa.
- Es recomendable que la empresa que se contrate para proveer la seguridad perimetral tenga presencia en el territorio ecuatoriano, así como los certificados necesarios que garanticen ser partners de la herramienta que se implemente.
- Se recomienda la adquisición de equipos appliance de tal manera que permitan balancear la carga de ingreso a aplicativos principales del negocio de la empresa para garantizar su disponibilidad.
- Se recomienda que al momento de establecer un método para la evaluación de proveedores, este contemple que además de considerar los aspectos mencionados anteriormente, se definan determinados criterios que favorezcan una evaluación adecuada del desempeño de los proveedores. Algunos de estos criterios pueden ser entre otros: Analizar los plazos de entrega, Calidad del servicio que presta, Confiabilidad.

- Se recomienda integrar el sistema de evaluación de proveedores con el sistema de mejora continua de la empresa, en virtud de que la obtención y el tratamiento de información relativa a los proveedores es una parte muy importante para mejorar la performance general de una empresa.

Bibliografía

A. Toncovich, J. M.-J. (12 de Septiembre de 2007). *SELECCIÓN MULTICRITERIO DE UN SISTEMA ERP MEDIANTE.* Obtenido de http://www.cnc-logistica.org/congreso-cnc/documentos/80.pdf

A., C. E. (2005). *Metodología: Diseño y Desarrollo del proceso de investigación.* Mc Graw Hill Interamericana.

Gallego, L. V. (2011). *Revisión de los métodos, modelos y herramientas existentes para la selección de proveedores.* México: INSTITUTE OF TECHNOLOGY.

Gallego, L. V. (06 de 2011). *Universidad Carlos III de Madrid.* Obtenido de http://e-archivo.uc3m.es:8080/bitstream/handle/10016/12130/PFC_LauraVirsedaGallego_Resumen.pdf?sequence=1

Gonzalez, J. F. (08 de Octubre de 2006). *Seguridad Informática*. Obtenido de http://www.renacersantaclara.org/academico/mod/forum/discuss.php?d=156

Isotools. (09 de 12 de 2013). *Evaluación de proveedores según la ISO 9001.* Obtenido de http://www.isotools.org/2013/12/09/evaluacion-de-proveedores-segun-la-iso-9001/

López, P. A. (2010). *Seguridad informática.* Madrid: EDITEX.

Marañón, G. Á. (2009). *Como protegernos de los peligros de internet.* Madrid: Los libros de la Catarata.

ORTEGA, E. S. (2011). *SOLUCIONES PERIMETRALES_PLAN DE SEGURIDAD DE LA INFORMACIÓNSEGURIDAD PERIMETRAL CON FIREWALLS EN ZENTYAL.* Obtenido de http://es.scribd.com/doc/109622384/Zentyal-Todo

Osorio, J. C. (07 de 2011). *SELECCIÓN DE PROVEEDORES USANDO EL DESPLIEGUE DE LA FUNCIÓN DE CALIDAD DIFUSA.* Obtenido de http://revista.eia.edu.co/articulos15/art.%206%20(73-83).pdf

Peña, G. L. (2008). *Procedimientos y medidas de seguridad informática - Conceptos básicos de seguridad de redes.* Guatemala: GUIDO ECHEVERRIA.

Pereiro, J. (25 de 11 de 2005). *Gestión de las compras y la evaluación de proveedores en ISO 9001:2000.* Obtenido de http://www.portalcalidad.com/articulos/56-gestion_compras_y_evaluacion_proveedores_iso_9001:2000

Royer, J. -M. (2004). *Colección recursos informáticos.* Barcelona: ENI.

Sarache, W. A. (24 de 05 de 2004). *PROCEDIMIENTO PARA LA EVALUACIÓN DE PROVEEDORES MEDIANTE TÉCNICAS MULTICRITERIO.* Obtenido de http://blog.pucp.edu.pe/media/810/20080324-Seleccion_proveedores_multicriterio.pdf

ANEXO A

Anexo A. Escalas de calificación de cada criterio de proveedores de seguridad perimetral

Calidad del Servicio
Trabajo o servicio realizado

DESCRIPCIÓN	Puntaje
El trabajo cumple cabalmente con los niveles de calidad solicitados. En particular, para las obras, la calidad de las terminaciones y acabado, cumplen satisfactoriamente con lo solicitado. En el caso de consultorías, el informe final muestra ampliamente la calidad solicitada.	5 Puntos
El trabajo cumple razonablemente con los niveles de calidad solicitados. Puede haber falencias menores, de fácil corrección. En el caso de las obras, las terminaciones y acabados cumplen razonablemente los niveles de calidad solicitados. En caso de consultorías, el informe final cumple razonablemente el nivel de calidad solicitado.	4 Puntos
El trabajo cumple en los niveles mínimos de la calidad solicitada. El trabajo es suficiente. En el caso de las obras, sus terminaciones y acabados con suficientes, aunque se requiere algunas correcciones. En el caso de consultorías, el informe cumple con lo mínimo, pero es susceptible de ser mejorado.	3 Puntos
La calidad del trabajo es deficiente y no se logra cumplir con el mínimo solicitado. En el caso de obras, sus terminaciones y acabados son deficientes, así como en el caso del informe final de consultorías y es necesario intervenirlas para recuperarlas y hacer la Recepción, afectando plazos de entrega y Multas.	2 Puntos
Desaprobación **Plena** del Criterio o Servicios rechazados	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Cumplimiento normas de seguridad y prevención de riesgos

DESCRIPCIÓN	Puntaje
El proveedor cumple cabalmente las normas y reglamentos internos de seguridad durante la ejecución de los trabajos, como parte de su política interna. Demuestra, además, un constante interés en la capacitación de su personal en tal sentido. Cuenta con un programa propio de prevención de riesgos establecido y demostrable.	5 Puntos
El proveedor cumple con las normas y reglamento internos de seguridad y prevención de riesgos durante la ejecución de los trabajos o servicios prestados. Capacita a su personal, como está estipulado. Cuenta con un programa de prevención de riesgos establecido.	4 Puntos
El proveedor cumple con las normas y reglamentos de seguridad establecidos durante el desarrollo de su trabajo, como se estipula en el contrato. Capacita a su personal, cumpliendo básicamente con la normativa. Cuenta con un programa básico de prevención. Ocasionalmente se le debe llamar la atención en algún punto, que corrige rápidamente.	3 Puntos
El proveedor no cumple o cumple en forma irregular con las normas y reglamentos de seguridad y prevención de riesgos, durante el desarrollo de su servicio u obra. No demuestra interés en capacitar a su personal y no posee programa de prevención de riesgos.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Cumplimiento normativa ambiental

DESCRIPCIÓN	Puntaje
El proveedor cumple con todos los procedimientos y exigencias relativas a las normas ambientales internas de ABB y a la legislación vigente, en todas las etapas del trabajo o servicio realizado, especificado en el contrato u orden de Compra suscrita.	5 Puntos
El proveedor cumple regularmente con los procedimientos y exigencias relativas a las normas ambientales internas de ABB y a la legislación vigente, en todas las etapas del servicio realizado, especificado en el contrato u orden de Compra suscrita.	4 Puntos
El proveedor cumple de manera parcial con los procedimientos y exigencias relativas a las normas ambientales internas de ABB y a la legislación vigente, en todas las etapas del servicio realizado, pero requiere supervisión para ello. Corrige prácticas erróneas, cuando se le indican, especificado en el contrato u orden de Compra suscrita.	3 Puntos
El proveedor no cumple o cumple irregularmente con los procedimientos y exigencias relativas a las normas ambientales internas de ABB y a la legislación vigente, en las distintas etapas del servicio realizado. No logra corregir malas prácticas aunque se le indique, especificado en el contrato u orden de Compra suscrita.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Cumplimiento y Administración Sistema de Aseguramiento de Calidad

DESCRIPCIÓN	Puntaje
El proveedor cumple en forma cabal lo indicado en su Sistema de Aseguramiento de Calidad y en la administración y manejo de no conformidades.	5 Puntos
El proveedor cumple, en general, lo indicado en su Sistema de Aseguramiento de Calidad. Corrige y soluciona las no conformidades que se le presentan.	4 Puntos
El proveedor cumple con reparos lo indicado en su Sistema de Aseguramiento de Calidad. Corrige con dificultad las no conformidades que se le presentan.	3 Puntos
El proveedor no logra cumplir satisfactoriamente lo indicado en su Sistema de Aseguramiento de Calidad y presenta dificultades importantes o no logra dar solución a no conformidades.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Infraestructura, equipos, herramientas

DESCRIPCIÓN	Puntaje
La calidad de la infraestructura, equipos y herramientas es óptima. La mantención de éstas es óptima, presentando y ejecutando programas de mantención establecidos y demostrables.	5 Puntos
La calidad de la infraestructura, equipos y herramientas es buena. Puede haber equipos con fallas menores, que son reparadas oportunamente. La mantención de éstas es adecuada, presentando y ejecutando programas de mantención establecidos.	4 Puntos
La calidad de la infraestructura, equipos y herramientas es suficiente. La mantención de éstas es regular, presentando y ejecutando programas de mantención, aunque no siempre oportunos. Ocasionalmente pueden presentarse fallas de mediana importancia que son corregidas por evento, si riesgos para las personas o la operación.	3 Puntos
La calidad de la infraestructura, equipos y herramientas es deficiente. La mantención de éstas no es adecuada, pudiendo carecer el proveedor un programa de mantención establecido y demostrable. Puede presentarse fallas importantes afectando la operación.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Calidad de materiales y suministros

DESCRIPCIÓN	Puntaje
La calidad de los materiales y suministros aportados es óptima. Además, en el caso de las Obras, existe control total sobre la calidad de los bienes y su adquisición.	5 Puntos
La calidad de los materiales y suministros aportados es buena. Además, en el caso de las Obras, existe control parcial sobre la calidad de los bienes y su adquisición, lo que permite corregir fallas adicionales.	4 Puntos
La calidad de los materiales y suministros aportados es suficiente. Además, en el caso de las Obras, existe un control rudimentario sobre la calidad de los bienes y su adquisición, lo que usualmente permite corregir fallas.	3 Puntos
La calidad de los materiales y suministros aportados es mala. Es absolutamente necesario mejorar la calidad de todos los elementos.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Iniciativa y cooperación

DESCRIPCIÓN	Puntaje
El personal demuestra, sistemática y evidentemente, iniciativa y compromiso, durante la prestación del trabajo o desarrollo del servicio.	5 Puntos
El personal demuestra, usualmente, iniciativa y compromiso, durante la prestación del trabajo o desarrollo del servicio.	4 Puntos
El personal demuestra poca o regular iniciativa, aunque suficiente cooperación, durante la prestación del trabajo o desarrollo del servicio.	3 Puntos
El personal demuestra poca o ninguna iniciativa y poca cooperación, incluso cuando se le solicita, lo que desmejora la calidad del trabajo o el servicio.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Idoneidad del personal clave

DESCRIPCIÓN	Puntaje
El proveedor cuenta con personal altamente calificado, con experiencia e instrucción, tanto para las tareas que debe desarrollar como para contribuir de manera eficiente a la gestión técnico-administrativa del trabajo o servicio prestado	5 Puntos
El proveedor cuenta con personal calificado, con experiencia e instrucción para las tareas que debe desarrollar, que contribuye a la gestión técnico-administrativa del trabajo o servicio prestado.	4 Puntos
El proveedor cuenta con personal calificado, con experiencia e instrucción básica, aunque suficiente y que no contribuye significativamente a la gestión técnico-administrativa del trabajo o servicio prestado.	3 Puntos
El proveedor no cuenta con personal con la debida calificación para realizar las tareas necesarias tendientes a entregar un trabajo o servicio según los estándares requeridos.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Plazos

Cumplimiento plazos

DESCRIPCIÓN	Puntaje
El proveedor cumple permanentemente con los plazos en lo que respecta a la entrega del trabajo o servicio. Además, en todos los servicios que corresponde, el proveedor cumple siempre con los plazos en los aspectos administrativos del contrato y su personal.	5 Puntos
El proveedor cumple usualmente con los plazos en lo que respecta a la entrega del trabajo o servicio. Además, en todos los servicios que corresponde, el proveedor cumple usualmente con los plazos en los aspectos administrativos del contrato y su personal. Si hay retrasos, son menores y corrige espontáneamente.	4 Puntos

El proveedor cumple con los plazos en lo que respecta a la entrega del trabajo o servicio, aunque puede presentar ocasionalmente retrasos que logra compensar. Además, en todos los servicios que corresponde, aunque el proveedor cumple en general con los plazos en los aspectos administrativos del contrato y su personal, puede presentar retrasos que debe compensar. Se requiere control permanente y las mejoras son evidentemente posibles.	3 Puntos
El proveedor no cumple con los plazos o cumple en forma irregular en lo que respecta a la entrega del trabajo o servicio. Además, en todos los servicios que corresponde, el proveedor no cumple oportunamente con los plazos en los aspectos administrativos del contrato y su personal,. Se requiere control intenso y permanente por parte del administrador del contrato.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Programación del trabajo

DESCRIPCIÓN	Puntaje
El proveedor hace una programación formal de los trabajos o servicios realizados, siendo demostrable y logrando un uso eficiente y eficaz de los recursos, permitiendo una respuesta, a los clientes internos, dentro de los plazos establecidos.	5 Puntos
El proveedor hace una programación formal de los trabajos o servicios realizados, lo que permite un uso adecuado de los recursos, que, sin ser óptimo, entrega una respuesta dentro de los plazos establecidos.	4 Puntos
El proveedor hace una programación informal de los trabajos o servicios realizados, que no perjudica de manera importante la entrega del servicio, pero en la que son evidentes las posibilidades de mejora. Esta programación precaria, de todas maneras, permite una entrega dentro de plazos aceptables, aunque no siempre dentro de lo programado.	3 Puntos
0No existe programación de los trabajos o servicios realizados, o éstos se ejecutan sin utilizar programación, de manera improvisada, lo que no permite satisfacer los requerimientos internos. La falta de programación causa demoras que afectan la operación o la calidad del servicio.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Aspectos Administrativos
Cumplimiento laboral y administrativo

DESCRIPCIÓN	Puntaje
El proveedor cumple en forma estricta y oportuna con el orden administrativo, es riguroso en el cumplimiento de plazos y en la calidad en la presentación de la documentación.	5 Puntos
El proveedor cumple razonablemente con el orden administrativo, es preciso en el cumplimiento de plazos y calidad en la presentación de la documentación. Ocasionalmente puede haber fallas o atrasos menores que son corregidos espontáneamente.	4 Puntos
El proveedor cumple suficientemente con el orden administrativo, el cumplimiento de plazos y la calidad en la presentación de la documentación. Puede haber fallas o atrasos que son corregidos cuando se le indican.	3 Puntos
El proveedor no cumple con el orden administrativo, cumplimiento de plazos y calidad en la presentación de la documentación o cumple en forma irregular.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

Conducta interna

DESCRIPCIÓN	Puntaje
El proveedor muestra una conducta intachable, tanto en aspectos personales como laborales, dentro de las dependencias e instalaciones de ABB	5 Puntos
El proveedor muestra una conducta intachable, tanto en aspectos personales como laborales, dentro de las dependencias e instalaciones de ABB. Ocasionalmente puede cometer faltas menores, que no afectan la seguridad ni el desarrollo de los servicios y que corrige rápidamente.	4 Puntos
El proveedor muestra una conducta usualmente correcta, aunque algo irregular, en aspectos personales y laborales, dentro de las dependencias e instalaciones de ABB. Ocasionalmente se le ha debido indicar faltas menores, que no han afectado en forma importante la seguridad ni el desarrollo de los servicios y que logra corregir.	3 Puntos
El proveedor no muestra una conducta satisfactoria en aspectos personales y/o laborales, dentro de las dependencias e instalaciones de ABB o bien, su conducta es tan irregular que no permite confiar en su actuar.	2 Puntos
Desaprobación **Plena** del Criterio	1 Puntos

☐ Obras y Servicios ☐ Consultoría y otros servicios ☐ Consultoría y otros servicios en terreno

ANEXO B

ANEXO B. Ponderación de criterios del proceso

Evaluación y Reevaluación
Ponderación de proveedores de Bienes y Productos

Criterios	Ponderación
1. Atención oportuna (Cotización)	25%
2. Calidad.	25%
3. Plazo de Entrega	15%
4. Precios	15%
5. Seriedad	20%

Ponderación de proveedores de Servicios

Criterios	Ponderación Criterio	Descripción
Calidad del Servicio	**40%**	Trabajo o servicio realizado
		Cumplimiento normas de seguridad y prevención de riesgos
		Cumplimiento normativa ambiental
		Cumplimiento y Administración Sistema de Aseguramiento de Calidad
		Infraestructura, equipos, herramientas
		Calidad de materiales y suministros
		Iniciativa y cooperación
		Idoneidad del personal clave
Plazos	**40%**	Cumplimiento plazos
		Programación del trabajo
Aspectos Administrativos	**20%**	Cumplimiento leyes laborales y control administrativo
		Conducta interna del personal
TOTAL	**100%**	

ANEXO C

El cibercrimen, la principal amenaza para las grandes empresas españolas

Según un informe de EY, una de cada dos empresas tiene previsto aumentar su presupuesto de TI, en 2014 y el 16% del presupuesto de TI se destinará a innovación y protección frente a las tecnologías emergentes.

escrito por: Redacción Computing16 de enero 2014

Mientras las empresas informan de un aumento de las amenazas y vulnerabilidades tecnológicas derivadas del uso de los sistemas de información, una de cada dos planea incrementar su presupuesto de seguridad de la información para el próximo año. Esta es la principal conclusión de la decimosexta edición de la Encuesta Global de Seguridad de la Información de EY, titulada Under Cyber Attack.

A través de la opinión de cerca de 2.000 altos ejecutivos y responsables de TI de grandes compañías procedentes de 64 países, entre ellos, España, el informe analiza el grado de concienciación y la actitud de las empresas frente a amenazas informáticas. Los resultados del sondeo muestran cómo las empresas siguen invirtiendo de forma sustancial para protegerse de potenciales ataques informáticos y del llamado cibercrimen.

En España, el 44% de los directivos consultados asegura que los incidentes de seguridad dentro de su empresa han aumento un 5% durante la pasado año. Ante esta situación, muchas compañías se han dado cuenta del alcance y las consecuencias que supone para ellas sufrir un ataque sobre sus sistemas de información. Por ello, un 80% de las mismas cuenta con un alto directivo responsable de la seguridad informática: Chief Information Officer (CIO), un porcentaje que a nivel global alcanza el 70%.
Para **Manuel Giralt, Socio Director de Consultoría y de Seguridad de la Información de EY**, "el informe demuestra que las empresas se están moviendo en la dirección correcta, aunque todavía queda mucho por hacer. Por ejemplo, en la actualidad, un 30% de los directivos presenta al consejo de

administración cuestiones relacionadas con la seguridad de la información, lo que indica que estos asuntos comienzan a ser estratégicos para la alta dirección".

Hemos pasado de considerar si una compañía sufrirá un ataque a darlo por supuesto y empezar a evaluar cuándo se producirá. La cantidad de ataques y de intentos de violación de la seguridad que reciben las compañías han hecho replantearse su estrategia, lo que ha desembocado en mayor asignación de recursos, según se recoge en el informe de EY.
En este sentido, la mitad de los encuestados afirma que incrementará su presupuesto de TI en al menos un 5% durante el próximo año, a pesar de que la inmensa mayoría asegura que la dotación es insuficiente. De hecho, el 90% considera que un presupuesto en TI insuficiente es el principal obstáculo para seguir aportando valor a la compañía.

Además, a medida que las nuevas formas de comunicación se van consolidando, como es el caso de las redes sociales, las compañías deben ser conscientes de qué manera les puede afectar el uso de las mismas en la actividad de su empresa. Según los consultados, el 16% de los presupuestos de TI se destinará a tareas de innovación en materia de seguridad y para protegerse frente a las tecnologías emergentes.

Amenazas y vulnerabilidades

Para Francisco Javier Ferré, Socio Responsable de Consultoría TI y de Seguridad de la Información, "la sofisticación de las actuales amenazas, la adopción de nuevas tecnologías en el entorno empresarial y la globalización de las operaciones, exige a un gran número de empresas revisar su estrategia en la gestión y operación de la seguridad. Además, debe considerarse el apoyo de especialistas y sistemas automatizados que puedan ofrecer una respuesta global".

Según los propios directivos consultados, las principales vulnerabilidades que más riesgo generan en su empresa son las procedentes de las tecnologías móviles, seguida por el uso de las redes sociales y por las posibles acciones de empleados desinformados o descuidados en el uso de las tecnologías de la información.

Por último, el informe recoge cómo el spam, el malware y el phishing son amenazas que se han incrementado en los últimos doces meses y, en menor medida, el espionaje o los ataques internos realizados por empleados descontentos.

Por su parte, **Juan Luis Fernández, Socio de Consultoría de Riesgos Tecnológicos y Seguridad de la Información** para el sector financiero de EY, explica que "el área de seguridad de las compañías del sector financiero tiene también el reto de transformar su modelo operativo, tradicionalmente reactivo a incidentes de seguridad, a uno donde su funcionamiento sea clave para la gestión integral de la seguridad y el control del fraude, tanto de empleados como de clientes. Es ahora cuando toma sentido la seguridad end to end, en la que no sólo se verifica si los terminales o puntos de conexión son seguros, sino que incluso se comprueba si el modo de operación de los usuarios/clientes y su 'huella biométrica' asociada, se corresponde con los parámetros normales de operación".

http://www.computing.es/seguridad/tendencias/1071897002501/cibercrimen-principal-amenaza-grandes.1.html

ANEXO D.

Ejemplo sin metodología

PROCESO: LICITACIÓN PARA DESARROLLO A LA MEDIDA	SUBPROCESO: PRESENTACION Y APROBACION DEL PROYECTOS DE DESARROLLO

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO

OBJETIVO: Establecer los lineamientos de desarrollo requeridos por la empresa TRAMACOEXPRESS, a fin de automatizar los diferentes procesos operativos.

ALCANCE: Este proceso inicia con la elaboración de las bases de concurso y su divulgación a las empresas dedicadas al desarrollo de sistemas de información; y, finaliza con la firma y registro del acta de finalización del proyecto.

DOCUMENTOS DE REFERENCIA:

1. TRA-201107.001 Elaboración y divulgación de los resultados finales de la convocatoria.
2. TRA-201107.002 Diagramas de procesos de la empresa.

EMPRESAS PARTICIPANTES Y PRODUCTOS OFERTADOS:

EMPRESA	Carta de presentación	Personal certificado	Certificados	Incluye Appliance	Herramienta robusta	Satisface necesidad de la empresa	Incluye capacitación y soporte
Totaltek	X	X		X	X		
GMS	X	X	X	X	X	X	X
Adistec	X		X				X
InputOne	X				X		X
InforSecurity	X	X	X	X	X	X	X

En el cuadro anterior se observa que hay dos empresas que destacan sobre las demás, por lo que, se analizará algunos detalles de las propuestas para la toma de decisión final.

EMPRESAS PARTICIPANTES E INDICADORES DE EVALUACION

EMPRESA	Presenta metodología	Presenta documentación técnica	Presenta documentación de usuario	Presenta diseño de la solución	Temario de la capacitación	Cronograma macro de actividades	Soporte incluido
Totaltek	X	X		X		X	
GMS	X	X	X	X	X	X	X
Adistec		X	X	X	X	X	X
InputOne	X	X				X	X
InforSecurity	X	X	X	X	X	X	X

De acuerdo a los cuadros resumen anteriores y considerando el contenido de las propuestas recibidas, se puede observar que aún hay un empate técnico entre dos de las empresa ofertantes:

Costos por empresa:

EMPRESA	Incluye equipo de backup	Tiempo del Proyecto	Costo del Proyecto	Soporte técnico
GMS	X	2 semanas	60.000,00 USD	Por 3 años
InforSecurity	X	2 semanas	85.800,00 USD	Por 1 año

Conclusión:

En el análisis financiero se destaca la empresa GMS, por lo que, se recomienda contratar con GMS.

ANEXO E. Ejemplo aplicando la metodología propuesta.

PROCESO: LICITACIÓN PARA ADQUISICIÓN DE SEGURIDAD PERIMETRAL	SUBPROCESO: PRESENTACION Y APROBACION DEL PROYECTO DE SEGURIDAD PERIMETRAL

1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO

OBJETIVO: Evaluar los proveedores de seguridad perimetral.

ALCANCE: Evaluar los proveedores de acuerdo a los criterios establecidos en la metodología propuesta por el Sr. Jorge Armas.

DOCUMENTOS DE REFERENCIA:

3. TRA-201107.001 Elaboración y divulgación de los resultados finales de la convocatoria.
4. TRA-201107.002 Diagramas de procesos de la empresa.

EMPRESAS PARTICIPANTES Y PRODUCTOS OFERTADOS:

CRITERIOS DE EVALUACIÓN \ EMPRESA	TOTALTEK	GMS	ADISTEC	INPUTONE	INFOSECURITY
Calidad del producto	5	5	5	5	5
Precio de la solución	4	5	4	4	3
Cumplimiento de los plazos de entrega	4	4	4	4	4
Servicio ofertado - Cotización	5	5	5	5	5
Situación financiera del proveedor	5	5	5	5	5
Tiempos cortos de entrega de la solución	5	5	5	4	5
Habilidad técnica del proveedor	5	5	5	5	5
Flexibilidad de la solución.	5	5	5	5	5
Desarrollo de la solución	5	5	5	5	5
Actitud de Gestión	4	5	4	3	5
Ubicación geográfica	5	5	5	5	5

Total:	52	54	52	50	52

A continuación cuadro de subcriterios definidos para el proceso, el cual permite un análisis más detallado de los proveedores de seguridad perimetral.

SUBCRITERIOS DE EVALUACION

Criterios	TOTALTEK	GMS	ADISTEC	INPUTONE	INFOSECURITY
El proveedor presenta alguna metodología de trabajo	5	5	5	5	5
Se entrega material técnico junto a la propuesta	1	5	4	3	5
La empresa presenta certificados de calidad ISO	3	5	3	3	5
La solución incluye hardware	5	5	5	5	5
Se incluye soporte de la solución	5	5	5	5	5
Incluye certificados de proyectos ejecutados en otras empresas	4	5	4	2	5
Total:	23	30	26	23	30

De los resultados observados en los cuadros anteriores se puede observar que el proveedor que alcanza la puntuación más alta es GMS, por lo tanto, se puede tomar una decisión respecto al proveedor que debe ser contratado.