# MÉTODO DE ANÁLISIS Y SELECCIÓN DE SOLUCIONES TECNOLÓGICAS DE SEGURIDAD INFORMÁTICA PARA EL SECTOR EMPRESARIAL Y LAS ORGANIZACIONES

DAVID ENRIQUE ZORNOSA FAJARDO
Cód.:2112408

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2016

# MÉTODO DE ANÁLISIS Y SELECCIÓN DE SOLUCIONES TECNOLÓGICAS DE SEGURIDAD INFORMÁTICA PARA EL SECTOR EMPRESARIAL Y LAS ORGANIZACIONES

DAVID ENRIQUE ZORNOSA FAJARDO
Cód.:2112408

MONOGRAFÍA PARA OPTAR POR EL TITULO DE INGENIERO DE TELECOMUNICACIONES

Ing. GUSTAVO CHICA PEDRAZA
Docente Tutor

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C.
2016

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

Bogotá día, mes año

ÍNDICE DE CONTENIDO

**Contenido**

ÍNDICE DE IMAGÉNES

ÍNDICE DE TABLAS

# 1. RESUMÉN DEL PROYECTO

En el siguiente documento se realiza el análisis y selección de soluciones tecnológicas de seguridad informática para el sector empresarial y diferentes tipos de organizaciones. Por medio de la descripción técnica y económica de cada una de las alternativas propuestas, se realiza un estudio comparativo de componentes, servicios, funcionalidades, modos de operación y administración, impactos económicos y sociales.

El estudio está respaldado por una base teórica que describe las tecnologías y protocolos que utiliza cada solución propuesta, evidenciando como estos son aplicables a la necesidad de negocio particular de cada una de las empresas y de las personas en general. El modo de selección está sustentado en **el sistema de toma de decisiones multicriterio AHP** de ***Saaty***, que permite evaluar cualitativamente aspectos puntuales, ventajas y desventajas de cada solución frente a las distintas alternativas contempladas.

Lo anterior permite realizar un seguimiento riguroso al proceso de selección que brinda las herramientas suficientes para escoger de forma acertada la mejor solución tecnológica para cada tipo de empresa u organización, a través del establecimiento de nuevos esquemas de infraestructura tecnológica o a partir de la renovación de los mismos. Todo lo anterior con miras a facilitar la operación y administración de la infraestructura tecnológica, fomentar el teletrabajo y la implementación de personal satélite o de sucursales, gracias a los servicios y funcionalidades que ofrece cada solución propuesta.

**Palabras Clave:**

Optimización de infraestructuras tecnológicas, fomento al teletrabajo, análisis y selección de alternativas, escalabilidad de los sistemas, convergencia de tecnologías.

## 2. JUSTIFICACIÓN

Día a día las tecnologías de la información van adquiriendo mayor protagonismo y participación en la operación del sector empresarial y de las organizaciones. La mayoría de empresas han reemplazado sus antiguos sistemas contables y financieros, han cambiado la forma de comercializar sus productos y servicios, han implementado en su proceso productivo nuevas formas de realizar inventarios y han adquirido nuevas plataformas de comunicación.

Dicha evolución se ha presentado gracias a la aparición de nuevas tecnologías que permiten el manejo automatizado de la información, almacenable y manejada por robustos motores de bases de datos, accesible por la infraestructura de telecomunicaciones existente y propagable ó fácil de difundir gracias a Internet y a las redes privadas.

A partir de lo anterior, la motivación de realizar este estudio surge por la experiencia que se adquiere al trabajar en un proveedor de servicios tecnológicos. Evidenciando día a día, en los labores realizados como administrador de redes y seguridad, todo el proceso que realizan los proveedores de tecnología al vender servicios de almacenamiento de información (*storage*), administración de bases de datos (**Oracle, DB2, Informix, SQL**), de aplicaciones (correo, SAP, software a medida), de sistemas de colaboración (telefonía IP, mensajería instantánea, videollamadas), de *networking* (infraestructura de telecomunicaciones basadas en redes IP), de seguridad (administración de sistemas de control de acceso, firewall, IDS, IPS) entre otros, a clientes cuyo *core* de negocio no está relacionado en lo absoluto con la tecnología y que en ocasiones, quizás por inexperiencia o desconocimiento, se equivocan en la selección de soluciones tecnológicas .

Entonces, surge un cuestionamiento fundamental: ¿Cómo seleccionar de la mejor forma, soluciones de seguridad informática que ofrezcan las funcionalidades idóneas y tengan el costo adecuado de compra y operación para cada tipo de cliente, empresa u organización?

Es evidente que la selección equivocada de soluciones de seguridad informática, de sistemas de comunicaciones, de software y de hardware, limita la operación de las empresas, las induce a pérdidas de dinero y produce deficiencias en la producción o prestación del servicio con los cuales cada empresa comercia en el mercado. También se ha evidenciado que un mal análisis, acompañado de un diseño equivocado, puede provocar subutilización o explotación inadecuada de las tecnologías de la información, desgastando al máximo soluciones ideadas para ambientes pequeños (Pymes) o desperdiciando funcionalidades y servicios de soluciones ideadas para ambientes grandes (multinacionales y grandes compañías).

Por ende resulta necesario realizar un estudio que permita escoger la solución tecnológica más adecuada y que más se acomode al perfil de las empresas u organizaciones. Para ello se analiza la capacidad de adquisición de los productos/servicios por parte de las empresas, su facilidad de operación y administración de las soluciones, teniendo en cuenta si poseen personal capacitado que las administre, si realmente la solución escogida aporta y fomenta la optimización de procesos, si cumple con las necesidades planteadas y si preserva de la mejor manera uno de los activos más importantes de las compañías: la información.

Para ello, se proponen para el análisis cuatro soluciones tecnológicas, que ofrecen servicios de seguridad informática, acceso a distancia, administración de redes y administración de aplicaciones, para cualquier tipo de empresa u organización. Las soluciones propuestas para el análisis son: el **Identity Service Engine** de **Cisco**, el **Firewall PA50-50 de Palo Alto Networks**, el **Firewall Fortigate 90D series** y el **balanceador BIG-IP 2000/4000 series con el aplicativo WAF**. Las cuáles serán analizadas en términos de:

- Cómo promueven la convergencia de tecnologías al servicio de las compañías.
- Cómo estas soluciones fomentan el teletrabajo y facilitan la realización de actividades de forma remota, a partir de conexiones seguras.
- Cómo pueden proteger la infraestructura de telecomunicaciones y la información.

Finalmente, cabe resaltar la importancia de este estudio, puesto que el espectro de interesados y clientes potenciales es demasiado amplio: firmas de abogados, supermercados, universidades, fábricas, almacenes de cadena, clínicas, petroleras, gaseras, entidades públicas, bancos y demás, son grandes demandantes de los servicios anteriormente nombrados. Por ello, al analizar la viabilidad técnica, económica y operativa de cada solución, se adquiere un fundamento importante y contundente a la hora de ofrecer o adquirir alternativas y soluciones tecnológicas de seguridad informática.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL:

Realizar un análisis comparativo que caracterice cada una de las soluciones tecnológicas propuestas, con el fin de brindar herramientas que permitan seleccionar acertadamente una solución a la medida del cliente, empresa u organización que lo requiera.

## 3.2 OBJETIVOS ESPECÍFICOS:

- Caracterizar técnicamente cada una de las soluciones propuestas, exponiendo funcionalidades, servicios y operación de cada una de ellas.
- Realizar estudio comparativo referente al costo/beneficio entre las diferentes soluciones.
- Analizar el impacto que generan en la operación de las empresas, la aparición de nuevos protocolos y nuevas tecnologías de seguridad informática.
- Facilitar la selección de herramientas de autogestión de seguridad informática para Pymes.
- Describir como estas soluciones de seguridad fomentan el teletrabajo y facilita la creación de sucursales por medio de accesos remotos.
- Exponer como se logra la convergencia de tecnologías en una sola solución de seguridad informática.

# 4. ESTADO DEL ARTE

## 4.1 ACTUALIDAD DE LAS SOLUCIONES TECNOLÓGICAS

El espectro de soluciones tecnológicas enfocadas hacia la seguridad informática crece de forma exponencial con el transcurrir del tiempo. A diario salen al mercado dispositivos con innumerables características técnicas y funcionalidades que brindan un gran número de alternativas a las compañías que desean preservar de forma óptima su información e infraestructura tecnológica.

En los últimos años, fabricantes como **Cisco, PaloAlto Networks, Fortinet, F5, Juniper, Huawei, IBM, CheckPoint y Bluecoat** (Para aplicaciones Web), han liderado el mercado de soluciones tecnológicas y de seguridad informática, enmarcados en un contexto de competencia y rivalidad, donde cada uno de ellos busca ir más adelante que los demás. Esta "competencia" expande la franja de alternativas que poseen los clientes para seleccionar soluciones tecnológicas y de seguridad, según su necesidad.

Para este caso, las soluciones de estudio seleccionadas provienen de los fabricantes: **Cisco, PaltoAlto networks, Fortinet y F5**., las cuales son sometidas a un análisis profundo y comparativo de funcionalidades, de precios y costos de operación, de revisiones en la relación costo/beneficio de cada una de estas, donde se identifica cual es la más adecuada según la actividad de negocio y tamaño de la empresas.

Dicho análisis inicia con las preguntas: ¿Con que se cuenta? y ¿A dónde se quiere llegar?

La tradicional característica de los equipos de seguridad de permitir y/o denegar tráfico entrante o saliente, basados en listas de control de acceso o políticas de seguridad, donde se estipula un origen, un destino, un protocolo de red, un protocolo de transporte de datos delimitado en el número de puerto y si utiliza la encapsulación TCP o UDP, está siendo mejorada a través de nuevas formas de aplicar seguridad y preservar la estabilidad de la infraestructura de red y de la información.

Estas nuevas formas se dan gracias al desarrollo de técnicas emergentes que permiten realizar las mismas políticas de seguridad, basado en diferentes criterios que permiten ejercer un control dinámico e inteligente de los equipos de seguridad sobre el tráfico que viaja por la red. Estas nuevas formas de establecer políticas de seguridad ya no están orientadas hacia el número de puerto por donde se establecen las comunicaciones, sino por la aplicación que utiliza de forma dinámica estos puertos a nivel de transporte (basado en el modelo OSI).

Esta nueva tendencia de visibilidad y control de tráfico, permite identificar de forma dinámica los puertos que utilizan las aplicaciones en su proceso de comunicación entre dispositivos. Categorizando las aplicaciones según su funcionalidad como bases de datos, virtualización (Citrix), las aplicaciones basadas en Google (google mail, google calendar, google video), colaboración (correo y telefónica), etc. La ventaja que esta funcionalidad provee es por ejemplo: permitir el tráfico por un puerto "X" para una aplicación en específico y denegar el tráfico por el mismo puerto "X" para otra aplicación, esto permite no solapar el funcionamiento de las aplicaciones y evita la denegación de servicios involuntaria.

Otra funcionalidad en la que han avanzado estas nuevas opciones de seguridad es el perfilamiento de usuarios y la creación de políticas basadas en dicho perfilamiento. Tanto el ISE, como el Fortigate 90D y el PA50-50 permiten la creación de usuarios, la relación de los mismos con diferentes roles (administrador, solo lectura o auditor), la creación de grupos a partir de ubicación física, rol, tecnología de trabajo o cargo en las compañías, obviamente con diferentes alcances de configuración según la solución implementada.

El perfilamiento es por lejos la característica más fuerte de estos productos frente a las otras opciones tradicionales, ya que representa algo mucho más sofisticado que el común y tradicional control de acceso de usuarios y contraseñas. Esta nueva tendencia de perfilamiento incluye: revisión de certificados digitales, acceso vía VPN basado en el servicio SSL a equipos de forma remota, integración con equipos o servidores de autenticación que trabajen con **TACACS,RADIUS, LDAP o KERBEROS.**

Por otra parte una de las ventajas más importantes de estos equipos es la convergencia e integración de tecnologías. Tanto a nivel de acceso donde los generadores de tráfico pueden ser cualquier tipo de dispositivo que tenga acceso a internet o a la red corporativa, como a nivel de integración de distintos dispositivos de red que componen el Data Center o la red corporativa, donde se permite incluir al espectro de administración: equipos de monitoreo (gestores SNMP), controladoras inalámbricas (WLCs), Servidores AAA, Routers , Switches de acceso, Switches de Data Center, etc., en algunos casos de diferentes fabricantes y en otros limitados a un solo fabricante.

Las cuatro opciones contempladas apuntan a preservar la seguridad informática de forma diferente:

El Firewall PA50-50 apunta a la "virtualización" de firewalls en un solo chasis, creando instancias independientes llamados "*Virtual Systems*" que permiten separar el tráfico y las funcionalidades por cliente, por departamento ó por sede. Además provee herramientas anti-ataques como el *Threath Prevention*, herramienta incluida de monitoreo de tráfico, de amenazas, de uso de red por sesión, por tráfico ó por aplicación, posee caracterización de tráfico por aplicación que se actualizan automáticamente y de forma periódica, y permite la autenticación de VPN *client-to-site* a partir de autenticación personal o corporativa con el *HIP-Profile*.

La solución **Cisco (ISE)** apunta a generar sistemas completos de autenticación, asignación y administración de recursos de red como controladoras inalámbricos (WLC), equipos de red, y demás. Perfilamiento de usuarios y está especialmente enfocado en asignar permisos de ingreso, administración y uso, dependiendo, rol, ubicación. Nombre, etc.

Cisco también ha lanzado al mercado una nueva característica similar a la del firewall **Palo Alto PA50-50**, conocido como *Cisco FirePower*, el cual representa un competidor directo para este firewall. La desventaja de este dispositivo es que es un *appliance* que debe ser adquirido por separado y debe ser integrado con el equipo de seguridad de Cisco (ASA, *Adaptative Security appliance*) o debe ser puesto en marcha en modo autónomo e independiente.

El dispositivo **BIG-IP F5** por naturaleza es un balanceador de carga, por ende está diseñado para funcionar en entornos redundantes, donde se evita la saturación y caída de servidores. Tiene además una gran cantidad de funcionalidades y tiene una característica importante conocida como el WAF

(*Web Aplication Firewall*) que permite ejercer políticas de seguridad a los servicios web alojados en distintos servidores.

Finalmente el *Fortigate 90D Series,* al ser un firewall bastante robusto, aparte de las funcionalidades básicas basadas en políticas de seguridad, apunta a la protección de amenazas y ataques DoS( Deny of services), Control de aplicaciones, Filtrado Web por URL o certificado y establecimiento de VPNs *site-to-site* y *client-to-site*. Tiene una característica interesante y de vanguardia conocida como *Wan Optimization*, característica que será abordada en la caracterización técnica del equipo.

La base teórica que fundamenta esta investigación esta soportada sobre dos pilares fundamentales:

- La parte técnica conceptual: Comprende todos los términos y respectivos significados que deben ser considerados para entender el funcionamiento de un equipo de seguridad informática.

- La parte de toma de decisiones: Donde se describe en este caso, el modelo de toma de decisiones multicriterio. Seleccionado para evaluar todas las características de las soluciones propuestas y proporcionar un marco comparativo que vislumbre las ventajas y desventajas de cada una las opciones establecidas.

## 4.2 FUNDAMENTOS TÉCNICOS Y TERMINOLOGÍA

Todo el estudio se origina a partir de la necesidad de crear, diseñar, implementar o administrar sistemas informáticos y/ó de telecomunicaciones seguros, que garanticen dos tipos de requisitos: los fundamentales o primarios donde prima la preservación de la integridad, la confidencialidad y la disponibilidad de la información y de los dispositivos que la almacenan, y los secundarios que velan por asegurar la autenticidad, permitir la trazabilidad de datos o de sistemas (informática forense) y evitar el no repudio por parte de los atacantes.

La afirmación anterior resume de forma general el objetivo de la aplicación de la seguridad informática en el sector TIC y aplica tanto para el uso común de las personas, como para el uso industrial de las compañías o de las instituciones gubernamentales.

Esta definición es un punto de convergencia entre numerosos conceptos y definiciones de autores y fabricantes, por ejemplo María del pilar Alegro en su libro SEGURIDAD INFORMATICA se refiere a Seguridad Informática como : "El conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo" [1]

Bajo esta premisa y para abarcar la amplitud del término seguridad informática se debe involucrar todo lo relacionado con amenazas, ataques, riesgos, protecciones, clasificación de la información,

clasificación de los activos, seguridad física y la responsabilidad que tiene el factor humano en la preservación de los sistemas informáticos y de su información.

### 4.2.1 Activos. ¿Qué se debe proteger?

Según la metodología Magerit 3.0, existen dos tipos de activos esenciales: La información y los servicios. Estos activos esenciales representan en la mayoría de empresas un activo intangible, que de fallar puede generar un gran caos que altere la producción, la comercialización, el secreto industrial, la distribución y el buen nombre de las empresas.

La información de las empresas es diversa y clasificable según la importancia que esta tenga en el "qué hacer" de la compañía. Se puede almacenar desde la información menos relevante y accesible al público, hasta la información más sensible y clasificada como confidencial, donde se encuentran listados de proveedores, clientes y *partners*, nominas, productos, investigaciones y desarrollos, información sensible de clientes y secretos industriales que deben ser conservados en la base de datos de conocimientos de la empresa.

Los servicios pueden representar el conjunto de herramientas que utilizan las compañías en su labor diario o pueden ser el producto que la empresa le ofrece al mercado en sí. Los servicios respaldan la operación de las compañías y la indisponibilidad de estos puede generar pérdidas inmensurables a la compañía.

Los activos en forma concisa pueden plasmarse en la realidad en objetos físicos como un disco duro, una memoria USB, una granja de servidores, ó puede plasmarse en objetos intangibles como el "*goodwill*" de la compañía. Cada activo debe poseer un valor propio para la compañía (según esta metodología) que represente su importancia y determine el impacto que tiene la afectación o falla de este; finalmente el valor del activo se puede determinar en el costo que produce repararlo o sustituirlo. [2]

### 4.2.2 Amenazas informáticas. ¿De qué se deben proteger los activos?:

Según la metodología Magerit, una amenaza está definida como: "La causa potencial de un incidente que puede causar daños a un sistema de información o a una organización". Dado lo anterior, una amenaza puede estar representada en muchas formas. Puede estar ejemplificada en vulnerabilidades, ataques (acciones deliberadas) y errores humanos (no deliberados), que por ignorancia o desacato de las normas básicas de seguridad pueden generar problemas para los sistemas de información o para las organizaciones.

Las amenazas pueden ser físicas o lógicas. A nivel físico se debe ejercer control sobre los factores ambientales, la energía, los sistemas de vigilancia y los sistemas antirrobo. A nivel lógico se debe contemplar todo lo relacionado con software incorrecto, bacterias, gusanos, troyanos, *backdoors*,

bombas lógicas, etc. que puedan ocasionar consumo exagerado de recursos en los dispositivos, bugs y generar espacios vulnerables a recibir ataques.

En el ámbito de amenazas informáticas se destacan cuatro categorías fundamentales: [3]

4.2.2.1 ***Ataques:***

DoS (*Denial of service*). Los cuales pretenden inhabilitar algún recurso de la red que debe estar protegido, ya sea saturando un canal de datos, un servidor, un equipo de comunicaciones, etc; generando una gran cantidad de tráfico basura hacia estos dispositivos, logrando en algunos equipos el consumo excesivo de CPU y generando errores, congelamientos y reinicios en los sistemas.

4.2.2.2 ***Pirateo:***

Referente a "el acceso no autorizado de un tercero a todo o parte del sistema de información de la empresa. Los piratas que tiene obtienen acceso, incluso de nivel de usuario, pueden entonces modificar los datos, detener algunos servidores vitales e incluso destruir el conjunto de los datos."

4.2.2.3 ***Virus informáticos***:

Son conocidos en el mundo de la tecnología como el *malware* o software malicioso. Al igual que las amenazas, existen infinidades de tipos de virus informáticos presentes en internet, donde se encuentran los troyanos, los gusanos, los virus residentes, las bombas lógicas, los parásitos, los macros y los virus de arranque.

Los virus son caracterizados por tener una carga infecciosa (programa malicioso), un vector (medio por donde se trasporta el virus: unidades extraíbles, intranets, etc) y un huésped (que por lo general son los dispositivos y pueden ser infectados en su sistema operativo, en sus aplicaciones o en sus archivos.).

4.2.2.4 ***Intercepción de datos confidenciales***:

Cuando un tercero no autorizado, consigue tener acceso a los archivos o a la data importante de la compañía, sin necesidad de perpetrar los dispositivos puede generar daños importantes.

### 4.2.3 Modos de protección. ¿Cómo proteger los activos?

Cada vez que aparece una amenaza en consecuencia aparece una forma de mitigarla. Los grandes fabricantes están en constante investigación de todas las tácticas fraudulentas de afectar activos

TIC que aparecen a diario. Por ende basados en numerosas técnicas, opciones y dispositivos, buscan reducir al mínimo las posibilidades de ser atacados.

#### 4.2.3.1 ***Antivirus***:

Por definición son sistemas de detección de intrusos (IDS). Su labor principal radica en el trabajo de escanear y comparar, ya sea tráfico circulante por la red o archivos alojados en los dispositivos. Son instalados generalmente en computadores y servidores.

Están constituidos por cinco elementos básicos:

- Generador de eventos: Se refiere a los distintos canales de comunicación o a las unidades de almacenamiento donde pueden estar ubicadas las amenazas. Dichos generadores de eventos le envían los posibles avisos de amenaza al motor de análisis.

- Motor de análisis: Donde se analiza el patrón que entrega el generador de eventos y es comparado con la información residente en la base de datos de patrones y firmas. Para decidir si se efectúa o no alguna acción.

- Motor de consulta: Trabaja conjuntamente con la base de datos, es el que le suple de patrones y de firmas al motor de análisis para que puede realizar la comparación entre los patrones maliciosos confirmados que se alojan en la base de datos y los patrones provenientes del generador de eventos.

- Base de datos: Es el lugar donde se tiene registro confirmado de todos los patrones de software malicioso, firmas corruptas o contenido prohibido con el cual el motor de análisis realiza las comparaciones con los contenidos que envía el generador de eventos.

- Módulo de respuesta: Es el encargado de recibir la información del motor de análisis y a partir de allí generar un reporte de novedad de la amenaza detectada y aplicar la acción correspondiente que contrarreste el efecto del virus.

#### *4.2.3.2 Firewalls o Cortafuegos*:

"Un firewall es un dispositivo, o conjunto de ellos, que está configurado para impedir el acceso no autorizado a una determinada zona de red o dispositivo, pero que al mismo tiempo permite el paso a aquellas comunicaciones autorizadas". [4]

Basado en el concepto anterior, un Firewall de por si es uno de los elementos más importantes en una red de comunicaciones, el cual tiene una función principal: Permitir o denegar el tráfico a través de una red. Existen firewalls a nivel de software que son aplicaciones o programas instalables sobre computadores o servidores, y existen los

firewalls *Hardware+Software* que ya constituyen un equipo independiente con una funcionalidad especifica.

La aparición de los firewalls reforzó el concepto de organización de dispositivos dentro de una red, dando cabida al establecimiento de un "perímetro de seguridad" o repartición de dispositivos por zonas, los cuales blindan la infraestructura y la información, de tráfico o comportamientos indeseados.

Por ende se resaltan términos como *Back End* y *Front end* en una red y la comúnmente conocida DMZ (Zona Desmilitarizada). En el *Front End* reposan todos los dispositivos y/ó servidores con los que los clientes interactúan. Allí se requiere de un flujo de tráfico de alta velocidad con muy pocas limitaciones, ya que se debe procurar ofrecer una excelente experiencia al usuario y un óptimo rendimiento de las aplicaciones.

En el *Back End* se deben ubicar todos los equipos, dispositivos y servidores encargados del procesamiento de las solicitudes enviadas por el *Front End*. En esta zona se encuentran los equipos que deben ser protegidos con la mayor precaución posible, por ejemplo los servidores de bases de datos.

La DMZ o zona desmilitarizada, debe ser la zona donde se alojen los dispositivos y servidores que van a recibir todas las peticiones de comunicación percibidas desde internet o desde una red interna, en términos generales son la cara de la infraestructura frente a la red

Por otro lado el funcionamiento de los firewalls está fundamentando en la creación de políticas de acceso tanto "restrictivas donde se impide todo el tráfico salvo el autorizado expresamente en la configuración, como las permisivas que permiten el paso de toda comunicación salvo la expresamente prohibida." [4]

Dichas políticas de acceso son el término genérico de todas las configuraciones que se pueden realizar sobre un firewall. Las políticas de acceso comprenden desde la creación de reglas, hasta la configuración de NATs y el establecimiento de VPNs *Client-to-site* (Agente Remoto) o *Site-to-site.*

#### 4.2.3.3 ***Certificados digitales y entidades certificadoras:***

"Los certificados digitales son documentos en los que una autoridad de certificación, que es una empresa u organismo de confianza que se encarga de emitir y revocar los certificados digitales y certificados de firmas electrónicas, garantiza que una clave pública y un determinado sujeto están realmente asociados, evitando de esta forma posibles suplantaciones de identidad." [4]

Los certificados digitales a nivel mundial están basados en el estándar UIT-T X.509 y a nivel Colombia están referenciadas en la Ley 527 de 1999 y el decreto 1747 del 2000. La arquitectura general de un certificado digital consta de:

- Firma digital
- Huella digital
- Certificado digital
- Autoridad de Registro

Y está compuesto por: [4]

- Firma digital de la autoridad de certificación: Para comprobar que realmente la autoridad garantiza que la información contenida es cierta y la vinculación entre clave y sujeto es correcta.
- Nombre y dirección: Del solicitante del certificado digital
- Nombre y dirección: De la entidad certificadora.
- Clave pública: Del propietario del certificado
- Método de verificación: De la firma digital incluida en el certificado.
- Número de serie: Que identifica el certificado.
- Fecha de validez: Indicando fecha de emisión y expiración del certificado.

Los certificados digitales y específicamente la firma digital consisten en "Un valor numérico codificado que se adhiere a un mensaje de datos. Cuando una empresa o persona registra una firma digital, recibe una llave pública que se distribuye a los interesados por la red, y una llave privada que nadie debe conocer.

Cada firma digital de una misma persona que se estampa en varios documentos es diferente, ya que corresponde a ese único documento. El certificado de firma digital es un mensaje de datos firmado por la entidad certificadora, que identifica a quien lo expide y al firmante, e incluye la clave pública de este" [5]

En síntesis, las firmas digitales son una añadidura de un archivo que viaja por la red. A los archivos enviados (inicialmente desde el emisor) se les aplica una función de encriptado llamado HASH (MD5) que representa un resumen único de dicho archivo, a estos no se les puede aplicar ingeniería inversa para ser descifrados. Posterior a ello, tanto al resumen obtenido como al archivo se les aplica un cifrado con la **clave PRIVADA** del emisor, generando así un único elemento llamado firma digital.

Finalmente en Colombia cerca del año 2002, la Superintendencia de Industria y comercio aprobó a la entidad Cérticamara como la autoridad que provee de certificados digitales al público en general, promoviendo la verificación de autenticidad de las personas o las compañías en internet, evitando suplantaciones y fraudes.

#### 4.2.3.4 ***Criptografía***:

Este es un aparte muy importante en la intención de establecer comunicaciones seguras entre dispositivos. La criptografía permite codificar o transformar mensajes en formatos determinados para que no puedan ser entendidos por terceros, asegurando que en su trayecto por la red no pueda ser visible ni revisado en su contenido.

La encripción de mensajes permite utilizar canales en común para millones de comunicaciones independientes y privadas. Este uso compartido se logra asegurando que los mensajes solo puedan ser reconocidos por el emisor o por el receptor del mismo, ya que estos deben ser los únicos con la capacidad de descifrar los mensajes y validar su contenido.

Para ello, a lo largo de la historia se han desarrollado numerosos protocolos, algoritmos y técnicas de cifrado-encripción que permiten blindar los mensajes, de espionajes e intrusiones no autorizadas de terceros.

Dado lo anterior, el valor fundamental que se quiere preservar con la criptografía es la **Confidencialidad.** La criptografía se divide en dos tipos principales:

- **Asimétrico**: Diseñado para pequeños volúmenes de información pero que requieren un alto grado de seguridad. Siendo utilizado generalmente para encriptar las **huellas digitales** junto a los **hash de los mensajes de datos** generando las **firmas digitales**.

  Este sistema está basado en la criptografía de dos claves, donde existe una **clave pública** accesible para todo el mundo, y una **clave privada** exclusiva para el emisor o el receptor que desea descifrar el mensaje.

  Los protocolos o algoritmos más conocidos de esta categoría son: RSA, DSA, Diffie-Hellman.

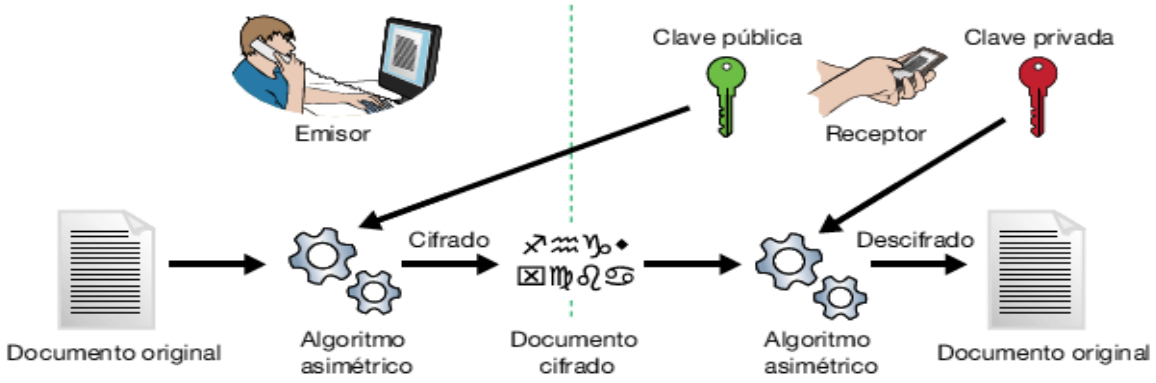


**Figura 1** Criptografía asimétrica. Extraída **[6]**

- **Simétrico:** Diseñado para grandes volúmenes de información con un nivel más bajo grado de seguridad. El encriptado simétrico es un sistema de una sola clave, donde el emisor y el receptor deben acordar con anterioridad dicho parámetro.

  Esta única clave será utilizada para cifrar y descifrar el mensaje de datos. Los protocolos más conocidos son: DES, 3DES, AES e IDEA.

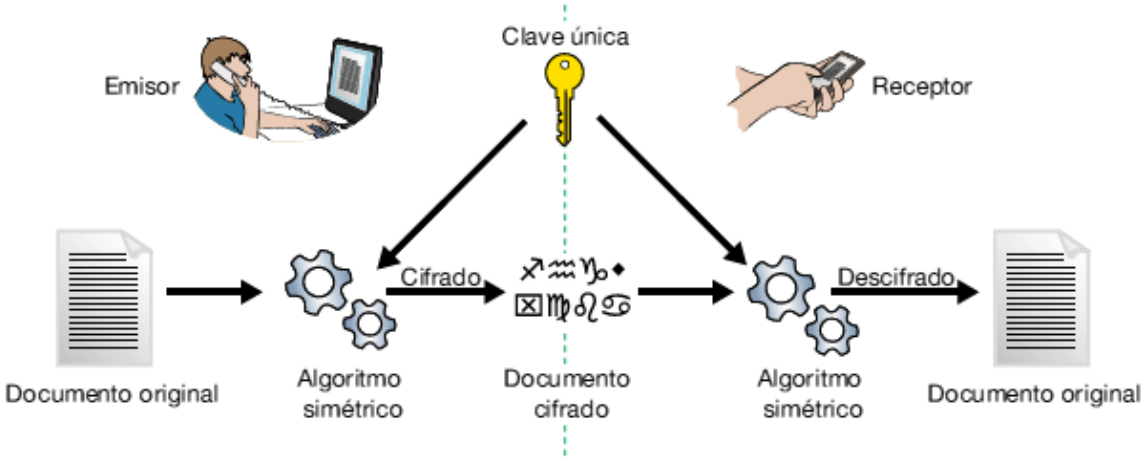


**Figura 2** Criptografía simétrica **[6]**

4.2.3.5 ***Protección a sistemas operativos:***

Según [6], la protección a los sistemas operativos debe abarcar desde el nivel físico (Hardware) hasta el nivel lógico. En cuanto hardware se deben proteger los equipos de accesos físicos no permitidos, ya sea con la dotación de tarjetas de identificación o sistemas de reconocimiento biométrico a los empleados, custodias de vigilancia, candados, jaulas y elementos de seguridad que no permitan que terceros no autorizados atenten contra la integridad de los dispositivos, ya sea por partes o en su totalidad.

A nivel lógico los sistemas operativos de los equipos, ya sea en computadores, servidores, equipos de comunicaciones, APs, entre otros, deben tener los siguientes parámetros de protección: [6]

- **Elevación de privilegios**:

  En esta etapa se debe definir los poderes y atributos que tienen los usuarios al trabajar en el sistema operativo de los dispositivos. Comúnmente en los sistemas operativos los usuarios privilegiados son conocidos como **ADMINISTRADORES** en Windows o usuarios **ROOT** en las distribuciones Linux.

  Esta clasificación establecerá los límites que tienen los usuarios en el sistema operativo, agregando o eliminando permisos de escritura, lectura y ejecución.

- **Actualizaciones y parches**:

  Es la forma en la que los proveedores de dispositivos y aplicaciones brindan soporte y garantizan el normal funcionamiento de sus productos. Las actualizaciones y los parches

son fragmentos de código fuente, scripts, *daemons* del sistema operativo diseñados para corregir errores, eliminar bugs, minimizar vulnerabilidades y mejorar el rendimiento del S.O de los equipos.

El no uso de actualizaciones o parches deja los equipos y las aplicaciones expuestas y vulnerables a errores de funcionamiento, reinicios o ataques. Dependiendo del tipo de producto, del fabricante y del tipo de contrato de compra, las actualizaciones o parches pueden ser provistas en un marco de garantía, en un marco de soporte o asesorías post-venta.

- **Monitoreo**:

El monitoreo es fundamental para revisar en tiempo real el funcionamiento de los dispositivos y permite evidenciar eventuales comportamientos anormales, ataques, usos excesivos de CPU o acontecimientos que alteran el normal funcionamiento del equipo.

Existen demasiadas herramientas y modalidades de monitorear los equipos y su funcionamiento, a nivel de infraestructura de data center las herramientas más utilizadas son los gestores SNMP que recopilan alertas, incidentes, sucesos y estadísticas de consumo; y los servidores SYSLOG que almacenan bitácoras minuto a minuto de los sucesos que ocurren durante el funcionamiento de los dispositivos.

#### 4.2.3.6 ***Protección de redes***:

El espectro de opciones para protección de redes es muy grande y crece exponencialmente con el tiempo. Existen numerosos mecanismos, prácticas y configuraciones disponibles para proteger dispositivos de red, servidores y elementos intermedios de accesos y/o conexiones no autorizadas. [7]

Los parámetros más comunes son:

- **VLANs**:

La primera medida de protección es segmentar las conexiones por medio de agrupamientos lógicos por medio de VLANs (LANs virtuales), separando dominios de *broadcast* y tránsito de tráfico gracias a la configuración de equipos de acceso como *Switches*, *Hubs*, o APs.

- **Conexiones cableadas**:

Esta medida está orientada hacia el control de las conexiones por medio de cables utp, fibras ópticas, cables seriales, entre otros. El objetivo es limitar el número de dispositivos que se pueden conectar a los equipos de acceso, ya sea configurando los equipos para que limiten las conexiones en sus puertos basados en número de dispositivos terminales

permitidos, listado de direcciones MAC aprobadas ó por configuración de servidores AAA externos que controlen y administren los accesos.

- **Conexiones inalámbricas:**

  Está relacionado con el acceso a las redes IP de forma inalámbrica, ya sea por conexiones WiFi, vía red telefonía celular ó vía radiocomunicaciones. Existen varias formas para controlar la forma y la cantidad de usuarios que pueden conectarse a la red vía inalámbrica.

  Las estrategias más comunes para asegurar las redes inalámbricas son: asociar contraseñas a los SSID propagados en la red, no hacer visible por los dispositivos finales los SSID que propagan los APs y encriptar las comunicaciones entre el dispositivo final y el AP, para que en caso de intercepciones la información no pueda ser extraída de los mensajes, etc.

  Para ello existen protocolos que soportan las conexiones seguras, que encriptan las comunicaciones entre los APs y los dispositivos finales, como por ejemplo WEP (Wireline Equivalent Privacy) WPA (WiFi Protected Access) y WPA2 (WiFi Protected Acces v2).

- **VPNs:**

  Las Virtual Private Networks ó Redes Virtuales Privadas son el mecanismo más utilizado para realizar conexiones de una red LAN con un host no residente a esa red LAN (físicamente) o con otra red LAN distantes, utilizando Internet como medio de transporte.

  Las VPNs permiten que los *hosts* remotos trabajen como si estuvieran conectados directamente en la red LAN, con el mismo direccionamiento de la red y los mismos accesos. Dada la condición de estar ubicados en otro lugar, las VPNS establecen túneles seguros entre la ubicación del *host* remoto y la ubicación de la red LAN por medio de Internet.

  Las VPNs añaden seguridad a estas conexiones, puesto que al crear un túnel se crea una especie de "canal dedicado" virtual entre las dos locaciones de interés. Dichos túneles encriptan todo el tráfico que circula a través de ellos, siendo las dos terminales VPN las únicas entidades que puedan descifrar el contenido y establecer comunicaciones de forma exitosa.

  Existe dos tipos de VPNs muy comunes : Las *Site-To-Site* donde se establecen túneles entre dos terminales VPN fijos, donde en su mayoría son *Routers, Firewalls* o servidores, donde se crea una única sesión entre los dos dispositivos.

  Y por otro lado existen las VPNs *Client-To-Site* referentes a la creación de túneles entre un terminal VPN fijo (*Router, Firewall* o servidor) y distintos clientes remotos (Celulares, Tablets, computadores portátiles) donde debe ser instalado un software cliente (Agente

VPN) que permita establecer túneles a través de Internet, creando una sesión por usuario conectado. [8]

- **NATs (Network Address Translation):**

  Es un mecanismo muy utilizado por los administradores de red para preservar en primer lugar el uso de direcciones IP públicas y en segundo lugar para brindar seguridad a las redes LAN frente a Internet o redes WAN.Los NATs permiten traducir direccionamiento de redes privadas a direccionamiento de redes públicas, donde dicha traducción puede ser uno a uno, muchos a uno, muchos a muchos.

  Los NATs pueden ser **estáticos** donde una dirección IP privada siempre va a ser reemplazada por una IP Pública previamente definida; pueden ser **dinámicos** donde un pool de direcciones IP privadas pueden ser traducidas en una o más direcciones IP públicas; o pueden ser de tipo **PAT** donde la traducción se realiza de forma **dinámica** a través de puertos de transporte de una o varias direcciones IP públicas.

  Los NATs dinámicos no permiten que las comunicaciones puedan ser iniciadas desde afuera hacia adentro, es decir, ningún host alojado en Internet o en la red WAN puede iniciar comunicación alguna con un host alojado en la red LAN, esto permite asegurar los equipos de la red LAN de conexiones no autorizadas.

- **Monitoreo:**

  A nivel de red, el monitoreo es algo fundamental para validar en tiempo real el funcionamiento de la red administrada. Esta tarea es vital y de gran utilidad, pues a partir de ella se pueden generar indicadores de rendimiento, visualizar amenazas, identificar funcionamientos anormales e identificar patrones de fallos, que le permiten a los administradores de red identificar con facilidad la causa raíz de los acontecimientos y tener control sobre las variables que afectan los sistemas.

  Las técnicas más comunes de monitoreo están relacionadas a la revisión de tráfico al más bajo nivel, es decir, revisar el tráfico desde los bits enviados, hasta las tramas, paquetes y segmentos. Existen herramientas muy utilizadas para dicha labor, como los aplicativos tipo *Sniffer* como Wireshark que permiten ver en tiempo real todo el tráfico que transita a traves de una tarjeta de red en un dispositivo terminal o una interfaz en un equipo de red.

  También es común la configuración de puertos espejo en dispositivos de comunicaciones que permiten replicar todo el tráfico de un puerto hacia a otro, para poder ser analizado. Por último los gestores SNMP son la herramienta más utilizada por los administradores, pues permiten centralizar en un solo aplicativo toda la recolección de eventos, incidentes, alarmas y novedades que tiene la red a diario.

- **Ingeniería Social**:

  A menudo este aspecto no está contemplado como debería, ya que no está directamente relacionado con la parte técnica de la infraestructura tecnológica. En muchos casos el ejercicio de la ingeniería social por parte de los atacantes, puede ser la principal causa de ataques, acciones maliciosas no deliberadas, indisponibilidades y afectaciones.

  Los catalogados "errores humanos" representan todas las acciones que realizan las personas en los dispositivos o en la infraestructura de TI en general, que produce consecuencias negativas en el funcionamiento y desempeño de los mismos, debido al mal uso, la utilización de malas prácticas y la omisión de protocolos de seguridad, ya sea por ignorancia o de forma deliberada con la intención de producir afectaciones.

  El error humano puede generar afectación a la infraestructura en dos niveles: en el mal desempeño de la infraestructura y los sistemas, y al nivel de los escapes de información confidencial y clasificada. En conclusión, un recurso humano no capacitado acerca de políticas de seguridad informática y confidencialidad de la información de la compañía, puede ser más peligroso que todo un grupo de atacantes informáticos trabajando al mismo tiempo, con la infraestructura TI de la compañía como objetivo.

### 4.2.4 Protocolos de seguridad y encripción:

El aspecto de seguridad en los dispositivos tecnológicos está soportado por un gran número de tecnologías, protocolos y algoritmos que son fundamentales en tareas de autenticación de usuarios, encripción de comunicaciones, verificación de autenticidad de emisores/receptores, registro de actividades, control de situaciones y cualquier tipo de monitoreo.

Están las tecnologías o protocolos de seguridad como TACACS (TACACS+), Radius (AAA), Kerberos, LDAP, IPsec, SSL/TLS y SSH implementados en dispositivos de red y servidores, y existen los algoritmos de cifrado y encripción como RSA, MD5, SHA-X, AES, DES, RC5, Diffie-Hellman e IDEA que soportan varias de las actividades que realizan dichos protocolos.

El cifrado (tal como fue tratado anteriormente) corresponde a la actividad realizada por un conjunto de algoritmos matemáticos de gran complejidad, que por medio de mecanismos de sustitución o rotación de caracteres, de operaciones lógicas, de alfabetos de encripción y de claves (pivote de encripción), logran transformar parcial o totalmente un mensaje de datos en un lenguaje alterno con una metodología definida. Evitando la revisión del contenido y significado de los mensajes, en caso de presentarse una eventual intercepción de un tercero no autorizado.

Basado en [9], se relacionan a continuación los algoritmos de cifrado más importantes :

#### 4.2.4.1 ***RSA:***

Este algoritmo de cifrado fue desarrollado en 1977 por Rivest, Shamir y Adleman (RSA) en MPT. RSA es un algoritmo de encripción asimétrico de llave pública y cuenta con un tamaño típico es de 1024 bits. Es utilizado para realizar firmas digitales y para cifrar mensajes de datos.

#### 4.2.4.2 ***MD5 (Message-Digest Algorithm 5):***

"Este algoritmo toma como entrada un mensaje de longitud indefinida y produce un "*fingerprint"* o "*message digest"* (es decir un resumen del mensaje inicial) de 128 bits. MD5 es un estándar de la IETF y esta descrito en el RFC 1321." [10]

MD5 es utilizado para obtener huellas de los mensajes de datos. Es decir, MD5 es un algoritmo que arroja una muestra de 128 de bits (hash) que identifica el mensaje de datos inicial. Esta acción promueve la verificación de la integridad de los archivos, puesto que si el emisor y el receptor generan la misma huella (hash con MD5) del mensaje de datos, significa que el archivo no fue modificado en el camino, si el mensaje es modificado en al menos un carácter, la huella (*hash)* va a cambiar.

MD5 es fundamental en los procesos de firmas digitales.

#### *4.2.4.3 SHA(Secure Hash Algorithm):*

"SHA es considerado el sucesor de MD5. La institución FIPS (Federal Information Processing Standard) especifica cuatro algoritmos SHA: SHA-1, SHA-256, SHA-384 y SHA-512. Los cuatro algoritmos son iterativos, no reversibles y pueden procesar mensajes de longitud máxima entre $2^{64} - 2^{128}$ bits, para producir huellas (hash) de 160 a 512 bits. Los cuatro algoritmos difieren del tamaño de mensaje inicial que a pueden procesar, y el tamaño de la huella (hash) que arrojan que para SHA-1 es 160 bits, SHA-256 es 256 bits, SHA-384 es 384 bits y SHA-512 es 512 bits.

El algoritmo SHA al producir huellas (hash o message disgests) más extensos que MD5, es considerado más seguro." [10] El algoritmo SHA al igual que MD5 , es un algoritmo para obtener *hash* o huellas digitales de algún mensaje de datos. Promueve la verificación de integridad de los mensajes y es fundamental en procesos de firmas digitales.

#### *4.2.4.4 AES (Advamced Encryption Standard):*

Es un algoritmo de cifrado simétrico creado aproximadamente en el año 1997, gracias a la realización de un concurso que hizo el NIST (*National Institute of Standards and Technology*) donde se buscaba un algoritmo que sucediera al ya existente 3DS y optimizara el uso de hardware y software donde este algoritmo fuera ejecutado.

El algoritmo AES maneja una longitud de bloque de 128 bits y trabaja con claves de 128, 192, y 256 bits. En contraparte con los algoritmos que lo precedian como el 3DES que manejaba bloques de longitud de 64 bits.

El algoritmo AES es ideal para encriptar grandes volúmenes de información, es decir para cifrar archivos de gran cantidad de bytes. Al ser un cifrador simétrico se utiliza una sola llave/clave para cifrar y descifrar los archivos, por ende el emisor cifra determinado archivo con una llave definida previamente, dando origen a un criptograma que es el que finalmente es enviado al receptor. A su vez, el receptor cuando recibe el criptograma debe ser capaz de descifrarlo utilizando el algoritmo AES con la llave/clave acordada con el emisor. [9]

#### *4.2.4.5 DES (Data Encryption Standard):*

"Es un algoritmo simétrico que codifica bloques de 64 bits con claves de 56 bits más 8 bits de paridad. Es de muy fácil implementación a nivel de *hardware* y *software* , pero posee un inconveniente importante: dispone de una clave de cifrado muy corta." [11]

Este algoritmo surgió en el año 1976 y fue considerado uno de los primeros estándares FIPS (*Federal Information Processing Standard/ Standard Federal de Procesamiento de la Información*). Al tener una clave bastante corta fue fácilmente corruptible y dado la inseguridad de cifrar objetos con este algoritmo se le dio pie al surgimiento de un algoritmo mejorado pero basado en la misma lógica: el algoritmo 3DES.

El algoritmo 3DES aumenta el tamaño de la clave proporcionando un poco más de seguridad, pero triplica y en ocasiones excede el procesamiento que conlleva ejecutar el algoritmo DES. Aún es ampliamente utilizado en el cifrado de transacciones electrónicas, pero día a día va perdiendo lugar con el algoritmo AES.

#### *4.2.4.6 RC5 (Rivest Cipher 5):*

"Fue diseñado y desarrollado por Ron Rivest para el RSA Data Security. A diferencia de muchos esquemas, RC5 es configurable o variable en todos sus aspectos, puede utilizar distintos tamaños de bloque ( 32, 64, ó 128 bits), permite tamaño variable de clave (entre 0 y 2040 bits) y numero de iteraciones entre 0 y 255. La combinación sugerida originalmente era bloques de 64 bits, claves de 128 bits y 12 vueltas. Es el algoritmo elegido por Netscape para su implementación de SSL" [11]

RC5 es otro algoritmo de cifrado simétrico y resalta sobre los demás, por la flexibilidad que le brinda a los usuarios de escoger las distintas características y determinar a conveniencia la robustez del algoritmo. El algoritmo como tal, es más simple que los otros y brinda un nivel más alto de seguridad. Dada su simplicidad el procesamiento es mucho menor en los

dispositivos donde se ejecuta este algoritmo, siendo idóneo para ser aplicado en dispositivos electrónicos que no cuentan con gran capacidad de memoria.

#### *4.2.4.7 Diffie-Hellman:*

Más que un algoritmo de encripción, puede ser tratado como un protocolo de seguridad. Este algoritmo difiere en los demás porque su proceso es bastante diferente. Está diseñado para establecer las claves de cifrado (simétricas) que utilizaran dos *hosts* en una conexión que no cuenta con seguridad y confidencialidad.

Por medio de operaciones en matemática modular, ambos *hosts* pueden definir una clave simétrica, en medio de un canal no seguro, basado en un envió constante de mensajes entre ellos con resultados de las operaciones modulares ejecutadas. Como producto ambos *host* habrán logrado establecer una clave sin haber tenido contacto previo y sin contar con un canal de comunicación seguro.

El algoritmo *Diffie-Hellman*, tiene una variable configurable que fija el tamaño de la clave que se va a negociar entre los dos *host*, esta variable es conocida como el *Diffie-Hellman group*, los valores más comunes son *DHgroup* 2 con 1024 bits, *DHgroup14*: 2048 bits.

Posee tres variaciones: *Fixed Diffie-Hellman (DH)* donde los parámetros son configurados y parte de esa configuración también afecta la clave pública presente en el certificado digital; *Ephemeral Diffie-Hellman (DHE)* donde los parámetros no son configurados y al contrario son generados dinámicamente promoviendo la autenticación en una sola vía, generalmente uno de los dos *hosts* envía los mensajes *Diffie-Hellman* firmados con su llave privada; y el *anonymus Diffie-Hellman (DHanon)* donde se hace el intercambio de mensajes, pero los parámetros no son autenticados, es decir la clave resultante puede ser víctima de un ataque *man-in-the-middle*. [12]

El algoritmo *Diffie-Hellman* es fundamental en el establecimiento y configuración de VPNs, es un parámetro esencial para lograr la conexión de dos equipos por medio de un túnel. También participa en el proceso que ejecuta el protocolo SSL.

#### *4.2.4.8 IDEA (International Data Encryption Algorithm):*

Es un cifrador de bloques simétrico surgido a inicios de la década del 90 y fue ideado como un complemento (y a futuro reemplazo) que mejoraría el funcionamiento del algoritmo DES en los equipos en los este era utilizado.

A comparación de DES, IDEA resulta ser un algoritmo mucho más robusto y confiable, pues tiene un tamaño de clave de 128 bits y realiza 8 iteraciones, manejando bloques con longitud de 64 bits. IDEA es aun utilizado en varias aplicaciones tecnológicas y es poco vulnerable a ataques externos, solo se han comprobado irregularidades con ataques a algoritmos con claves de 56 y 64 bits.

#### *4.2.4.9 Radius:*

*Remote Authentication Dia-In User Service*, es uno de los protocolos de autenticación más utilizados a nivel mundial y esta categorizado como un protocolo AAA, es decir, puede realizar tareas de **A**utenticación, de **A**utorización y de **A**ccounting o contabilización/tarificación.

*Radius* es un protocolo abierto que utiliza el puerto UDP 1812 y es utilizado en infinidad de ambientes. En cuanto a la autenticación, *Radius* puede ser la herramienta principal para controlar los accesos a distintos aplicativos, dispositivos, archivos, etc, basado en la revisión de nombres de usuario y contraseñas.

Dispositivos de comunicaciones como Routers, Switches, Servidores, Acces-Point, Firewalls, entre otros, son compatibles con la autenticación externa que provee un aplicativo *Radius* alojado en un servidor.

La Autorización es manejada en cuanto a la cesión de privilegios que *Radius* puede otorgarle a un usuario, ya sea por su rol, por su cargo, por su ubicación física, por su ubicación lógica, entre otras. Los privilegios se ven reflejados en la prohibición o permiso de acceso a herramientas y recursos ubicados en diferentes niveles.

Para el *Accounting* o tarificación *Radius* permite realizar seguimiento y control de las sesiones establecidas, evidenciado duración, tiempos de inicio y tiempos de finalizado de cada una de estas. En proveedores de servicio esta funcionalidad es esencial pues brinda los datos necesarios para cobrar por los servicios prestados, datos que indican duración de la sesión establecida y tipo de servicio utilizado durante la sesión.

Finalmente *Radius* está definido mediante los RFC 2865 y 2866, maneja un funcionamiento cliente/servidor y una de las herramientas libres más comunes en el mercado es el software *FreeRadius*.

#### *4.2.4.10Tacacs:*

*"Terminal Access Controller Access Control System*, es un protocolo AAA para control de acceso desarrollado inicialmente por Bolt, Beranek y Newman (BBN) para la red de defensa militar Estadounidense MILNET. *Tacacs* es similar en su funcionamiento a *Radius* y está definido en el RFC 1942, también fue trabajado y desarrollado por Cisco dando como fruto el protocolo TACACS+ que ofrece una amplia variedad de servicios y es compatible en su totalidad con versiones anteriores de TACACS.

Como *Radius*, TACACS+ es un tecnología cliente/servidor donde los clientes generalmente son NAS (Network Access Servers) y el servidor TACACS+ es un *appliance* instalado en un servidor con sistema operativo basado en UNIX o en una plataforma Windows. Este servicio utiliza el puerto TCP 49, y en versiones anteriores se utiliza además el puerto UDP 49." [13]

*Tacacs* al igual que *Radius* es un protocolo AAA, que tiene las mismas funcionalidades de Autenticación, **A**utorización y **A**ccounting, con una diferencia principal, mientras que en *Radius* las funciones de Autenticación y Autorización están ligadas y son dependientes una de la otra, en *Tacacs* la función de Autenticación puede ser ejecutada de forma independiente y aislada de la función de Autorización, esto permite adecuar la solución en una mayor cantidad de ambientes, donde la autorización dependa de otros factores no relacionados con la identidad del usuario .*Tacacs* soporta PAP, CHAP, SLIP, Appletalk, Kerberos, Telnet, SSH, L2TP y PPTP.

#### *4.2.4.11Diameter*

Es un protocolo AAA basado en *Radius*, utilizado principalmente en las redes de telefonía conmutada y en las redes de telefonía celular. Diseñado principalmente para ambientes con dispositivos móviles, *Diameter* es muy robusto en la parte de **A***ccouting* , dado el formato de su mensaje, *Diameter* permite agregar una mayor cantidad de datos de interés acerca de las sesiones establecidas y los tipos de servicio consumidos por los usuarios.

*Diameter* también maneja la tecnología Cliente/Servidor y al igual que TACACS, el cliente generalmente resulta ser un NAS. En la actualidad es el protocolo utilizado por los equipos de *core* de las redes móviles para llevar registro, control y administración de los servicios provistos por cliente, ciudad, país o región.

#### *4.2.4.12Kerberos*

Es un protocolo AAA desarrollado en el MIT, donde la función principal es Autenticar usuarios en redes de datos. *Kerberos* se apoya en algoritmos de cifrado simétrico como DES, para el intercambio de credenciales y claves entre dos *hosts*. Maneja también la tecnología Cliente/Servidor con la variación de que ambos deben autenticarse frente al otro, en los otros protocolos el único que se autentica es el cliente.

Maneja una estructura donde existe un servidor *kerberos*, un cliente que puede ser un NAS o un equipo de comunicaciones y un *Key Distribution Center* el cual es un tercer dispositivo encargado de administrar las peticiones y las sesiones producidas por los clientes, además de ejecutar la labor de autenticación. Este tercer dispositivo es vital en el proceso de autenticación y también es el lugar donde reside toda la información de usuarios y la relación de contraseñas.

#### *4.2.4.13LDAP (Lightweight Directory Access Protocol)*

Es el protocolo que soporta la operación de directorios activos a nivel de aplicación en los sistemas operativos. La operación de los directorios activos está relacionada con el control y manejo de usuarios al interior de un dominio, estableciendo políticas de autorización y acceso a diferentes tipos de recursos como archivos, aplicaciones, conexiones de red y a sistemas operativos en general.

Los directorios activos son una herramienta importante de seguridad que le permite a los administradores de la infraestructura tecnológica tener un control preciso de los recursos que administran y les permite también asignar atributos, roles y capacidades a los usuarios a partir de su cargo en la compañía, ubicación geográfica o actividad laboral.

LDAP surge como mejora y reemplazante del ya utilizado conjunto de protocolos X.500, dado que simplifica en grandes medidas los procesos, el transporte de información y añade novedades de configuración y flexibilidad en su uso.

#### *4.2.4.14PPTP (Point to Point Tunneling Protocol)*

Es uno de los primeros protocolos que permitieron el establecimiento de VPNs (Redes Virtuales Privadas) a lo largo de las redes de datos. Este protocolo se puede definir como una evolución del protocolo PPP (*Point To Point Protocol*) dado que permite enviar el tráfico producido por este protocolo a través de túneles seguros.

PPTP maneja una estructura cliente/servidor y utiliza un encapsulamiento genérico de enrutamiento (GRE) que permite ejercer un control más eficaz sobre los paquetes o tramas PPP que transitan por el túnel seguro.

PPTP actualmente está obsoleto ya que el mecanismo de conexiones seguras presenta numerosas vulnerabilidades que ya fueron explotadas por atacantes cibernéticos.

#### *4.2.4.15L2TP (Layer 2 Tunneling Protocol):*

Es considerado como un protocolo que evoluciona las funciones realizadas por el protocolo PPTP. Permite a los nodos tener acceso a redes LAN remotas a partir del establecimiento de VPNs a través de Internet.

L2TP mezcla las funcionalidades de PPTP y L2F (*Layer 2 Forwarding* de Cisco), y establece un sistema "dial-up" entre un cliente y un servidor conocidos como LAC (L2TP *Access Concentrator*) y LNS (L2TP *Network Server*) respectivamente, donde los distintos nodos se comunican con el LAC para establecer conexiones seguras con la red que representa el LNS.

L2TP encapsula tramas PPP en un túnel y permite el transporte de tráfico multiprotocolo entre dos *Peers* previamente conectados. También trabaja de forma complementaria con el protocolo IPSec.

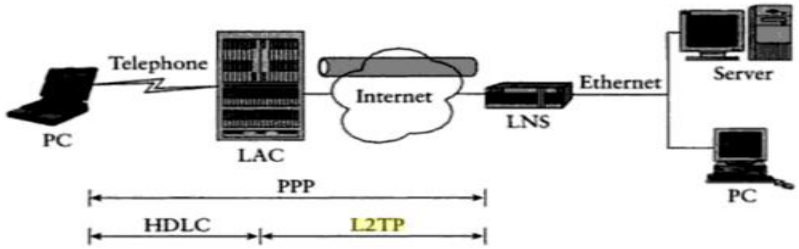


**Figura 3.** Esquema de negociación L2TP. **[14]**

### *4.2.4.16IPSec (Internet Protocol Security):*

Junto a L2TP son el conjunto de protocolos más utilizados para transportar información de forma segura y confidencial a través de Internet. IPSec es un protocolo categorizado "Capa 3" según el modelo OSI y presenta importantes funcionalidades en contraparte a L2TP (uso único) y PPTP.

IPSec permite establecer comunicación entre *hosts* validando la identidad de ambos y cifrando los paquetes, ya sea parcialmente la carga útil o en la totalidad del paquete, también comprueba estados y ciclos de vida de las comunicaciones.

En IPSec se manejan firmas digitales, certificados, cifrado de los mensajes, recolección de claves/llaves y configuración de parámetros para establecer VPNs multiprotocolo, es decir, el mismo túnel es funcional para cualquier tipo de tráfico a nivel de aplicación, a contraposición de SSL y TLS que al ser protocolos denominados de "Capa 4" deben variar su configuración a partir del servicio que estén encapsulando.

Este protocolo es implementable en el IOS de Cisco, en los sistemas operativos de Windows, en los sistemas operativos de servidores AIX y Z-Series de IBM, entre otros. [15]

### *4.2.4.17SSL/TLS (Secure Socket Layer / Transport Layer Security)*

SSL y su sucesor TLS, son protocolos de capa de transporte que brindan seguridad, autenticidad y confiabilidad en las comunicaciones realizadas a través de internet. Estos protocolos están basados en las funcionalidades X.509 (Arquitectura de Certificados digitales) y por ende en la estructura PKI (*Public Key Infrastructure*) .

SSL y TLS identifican a los nodos a partir de su firma digital, donde generalmente el único que se autentica es el que actúa como servidor en la comunicación, el ejemplo más preciso es el uso del protocolo **https,** donde los servidores que alojan las páginas de internet tienen configurado un certificado digital para cada una de ellas, validando la autenticidad de las mismas y evitando suplantaciones.

También tienen la capacidad de cifrar el tráfico, dada una negociación entre las dos partes comunicantes. Siempre utilizando cifrado simétrico o PKIs como las llaves producidas por el algoritmo *Diffie-Hellman*.

Tiene bastantes aplicaciones en la actualidad como el servicio https, ftps, smtps, sip, entre otros.

#### *4.2.4.18SSH (Secure Shell):*

Es un protocolo de capa de aplicación diseñado par a acceder a los dispositivos de forma remota, similar a la función que desarrolla el protocolo Telnet. SSH utiliza el puerto TCP/22 y cifra todo el tráfico entre nodos, identificándolos por medio de los certificados digitales de ambos, evitando las autenticaciones de tipo usuario y contraseña.

### 4.2.5 Estándares y recomendaciones de seguridad

#### *4.2.5.1 ISO /IEC 27002:*

Es un estándar de seguridad emitido por la ISO (*International Standard Organization*) en conjunto con la IEC ( *International Electrotechnical Commission*) en el año 2007, que resulta ser un instructivo de buenas prácticas y controles oportunos que deben ser aplicados en las compañías para preservar la seguridad informática.

Este estándar maneja temáticas relacionadas con:

- Políticas de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de Activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y del entorno.
- La gestión de comunicaciones y operaciones.
- Control de Acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes en la seguridad de la información
- Gestión de la continuidad del negocio.
- Cumplimiento
-

#### *4.2.5.2 Magerit:*

Es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que tiene como consigna "Establecer los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información. Garantizando que sus organizaciones siguen estos

principios ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.” [2]

Esta metodología se enfoca principalmente en la preservación de activos y la mitigación de riesgos y amenazas a los que se enfrentan. Para ello proponen una metodología orientada en los siguientes tópicos:

- Métodos de análisis de riesgos.
- Proceso de gestión de riesgos.
- Proyectos de análisis de riesgos.
- Planes de Seguridad.
- Desarrollo de sistemas de información.
- Consejos prácticos.

#### *4.2.5.3 X.805 de la UIT-T:*

Es una recomendación emitida por la UIT-T en el año 2003, perteneciente a la serie X (Redes de Datos y comunicación entre sistemas abiertos), donde se describe todo lo relacionado con la Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.

Como se encuentra definido en [16], la recomendación maneja los siguientes tópicos:

- Términos y definiciones.
- Arquitecturas de seguridad.
- Dimensiones de Seguridad, sobre control de acceso, autenticación, no repudio, confidencialidad, seguridad, integridad, disponibilidad y privacidad.
- Capas de seguridad (Infraestructura, servicios y aplicaciones).
- Planos de seguridad (En cuanto a gestión, control y usuarios).
- Amenazas contra la seguridad.
- Objetivos que se consiguen aplicando dimensiones de seguridad a las capas de seguridad.
-

#### *4.2.5.4 ITIL:*

Referente a la abreviación de *Information Technology Infrastructure Library*, es una recopilación de buenas prácticas y definición de un proceso que consta de cinco etapas para gestionar todos los servicios TIC en una compañía. Define el proceso de gestión de acuerdo a las siguientes etapas:

- Estrategia del Servicio
- Diseño del Servicio
- Transición del Servicio
- Operación del servicio

- Mejora del Servicio

#### *4.2.5.5 FIPS (Federal Information Processing Standard)*

Es toda la familia de estándares utilizados por el gobierno de E.U para estandarizar todos los procesos relacionados con el manejo de la seguridad de la información. Entre ellos se destacan algoritmos de cifrados, protocolos de seguridad, normativas y recomendaciones.

## 4.3 SISTEMAS DE TOMA DE DECISIONES

En el ámbito empresarial, la gran mayoría de compañías en la actualidad requieren la presencia de infraestructura TI que soporte y contribuya a la optimización de su operación diaria, sin importar el modelo de negocio, producto o servicio de comercialización. La infraestructura TI le permite a las compañías darle un manejo automatizado a la información, establecer estaciones de trabajo interconectadas por una misma red LAN, establecer estaciones de trabajo remotas a través de Internet o una red WAN y lo más importante permite poner la tecnología al servicio de las tareas que ejecutan los colaboradores a diario, mejorando resultados y optimizando procesos.

Para la instalación, operación y administración de la infraestructura TI, las compañías tienen una tarea importante en seleccionar la mejor alternativa que cumpla con todas las necesidades tecnológicas de su modelo de negocio. Existen numerosos parámetros que se deben tener en cuenta para seleccionar de forma correcta la tecnología, los dispositivos y los productos con los que se proveerá todo el andamiaje tecnológico que va a soportar la operación de las compañías

Los parámetros de selección surgen a partir de la revisión del modelo de negocio de la compañía, de un estudio acerca de la población de usuarios que va a consumir los servicios de la infraestructura, de la capacidad de despliegue de la tecnología en las instalaciones de la empresa y en exteriores, y el poder adquisitivo de la misma tanto para la compra de los dispositivos como para su administración y operación.

El sistema que se utilice para elegir o seleccionar las alternativas, debe estar fundamentando en una exhaustiva investigación y una amplia recolección de datos, fichas técnicas, cotizaciones, conceptos de asesoría y consultoría. Debe cumplir con el visto bueno, la aceptación y el concepto que emita el cliente en cuanto a sus intereses, y debe tener trazabilidad en el proceso de selección, es decir, definir las etapas y los criterios a los que se va a enfrentar cada alternativa para ser estudiada. [17]

Para motivos de este trabajo de investigación, se encontraron varios sistemas de toma de decisiones basados en modelos matemáticos, estadísticos y probabilísticos, donde resaltan modelos como: *Scoring*, Multicriterio (Proceso Analítico Jerárquico), Entropía, métodos de decisión bajo incertidumbre, entre otros, que utilizan bases matemáticas orientadas a la

solución de ecuaciones, series y sucesiones, análisis probabilístico y uso de matrices, para permitir tomar decisiones de forma correcta siguiendo un proceso trazable verificable.

Para este caso, se utilizará el modelo multicriterio referente al Proceso Analítico Jerárquico (AHP) de **Thomas L. Saaty** como modelo de toma de decisiones, pues permite evaluar de forma puntual aspectos relevantes y específicos de cada alternativa propuesta, valorando la importancia de forma dinámica e independiente para cada aspecto evaluado.

### 4.3.1 Modelo de toma de decisiones multicriterio: AHP. [18], [19]

Este modelo fue diseñado por Thomas L. **Saaty** a finales de los años setenta (70) y está orientado a la ejecución de un estudio completo de propósitos, criterios de selección y alternativas, organizadas en una estructura jerárquica que permite valorar la importancia de cada aspecto a evaluar según el papel que esta tenga en la consecución de los propósitos definidos.

Esta modelo es ampliamente utilizado a nivel mundial y es multidisciplinario, es decir, es adoptado por las cumbres ejecutivas de las compañías sin importar el modelo de negocio. Es utilizado por gerentes y administradores que apoyados en un modelo matemático pueden dar solución a procesos de selección de recursos, de tecnologías, de productos, de procesos, etc.

El modelo establece la jerarquización de los elementos de decisión en tres niveles fundamentales:

- **Nivel 1:** Donde se relacionan todas las metas y objetivos principales, por los que se está trabajando para su consecución.

- **Nivel 2:** Donde se relacionan todos los criterios que deben ser analizados para llegar a la realización del objetivo.

- **Nivel 3: Donde** se relacionan todas las alternativas que tiene cada criterio para ser tenido en cuenta, donde la persona que decide o "decisor" identificará la alternativa que más se acomode al criterio evaluado.

Con la definición jerárquica de los elementos a tener en cuenta para tomar una decisión, ***Saaty*** propone en su modelo una forma organizada y guiada por un lineamiento, donde es necesario cumplir con las siguientes tareas para poder tomar una decisión acertada:

***1)*** Definir el problema y determinar el tipo de conocimiento necesario para solucionarlo.

***2)*** Estructurar jerárquicamente todos los elementos de decisión. Ubicando en la parte superior de la pirámide los objetivos principales ó metas, seguido de los objetivos

secundarios definidos y los criterios de selección, finalizando en el último peldaño con las alternativas que otorgan solución a cada criterio establecido.

***3)*** Construir matrices de comparación. Matrices donde cada elemento de un nivel superior sea comparado con un elemento de un nivel inmediatamente inferior. Por ejemplo, se debe evaluar un objetivo principal a partir de los criterios de selección establecidos, o evaluar un criterio de selección a partir de las alternativas con las que se cuentan.

***4)*** Usar las prioridades obtenidas en las matrices de comparación para evaluar de forma total o promedio las prioridades de cada uno de los elementos. En esta etapa, la prioridad de los criterios se da a partir del peso obtenido del objetivo de donde se desprenden. Por tanto, la prioridad de las alternativas surgirá a partir del peso obtenido por el criterio del cual se desprenden.

Para realizar las comparaciones entre elementos, el modelo impone la siguiente escala de valoración numérica donde se indica la importancia de un elemento sobre otro. Esta medida es realizada en relación de proporción, es decir, se identifica cuantas veces es más importante un elemento frente al otro.

| Importancia | Definición | Explicación |
|---|---|---|
| **1** | Igual importancia | Dos actividades contribuyen de igual manera al mismo objetivo. |
| **3** | Importancia moderada | La experiencia y los juicios críticos, favorecen ligeramente un a elemento frente a otro. |
| **5** | Fuerte Importancia | La experiencia y el juicio crítico, favorecen fuertemente a un elemento frente a otro. |
| **7** | Muy fuerte ó importancia demostrada | La experiencia y el juicio crítico favorecen fuertemente a un elemento frente a otro y la dominancia de uno frente a otro está demostrada. |
| **9** | Extrema Importancia | Las evidencias favorecen un elemento sobre otro en el más alto nivel de afirmación. |
| **1.1 – 1.9** | Si ambos tienen ligeramente la misma importancia | Cuando la comparación entre elementos difiere mínimamente en los parámetros analizados. |

**Tabla 1. Escala de valoración. Modelo AHP.**

**Nota**: "Los valores 2, 4, 6 y 8 suelen utilizarse en situaciones intermedias, y las cifras decimales en estudios de gran precisión." [20]

A partir de la identificación de criterios, esta metodología busca categorizar cada uno de estos a partir de su importancia en la decisión de alternativas. Es decir, en el conjunto de criterios a tener en cuenta, a cada uno de ellos se les debe asignar un nivel de importancia frente a los demás, dicho nivel se asigna de forma numérica según la tabla anterior, y

permite identificar qué criterio o aspecto tiene mayor influencia en la decisión que se piensa tomar.

El mismo proceso debe ser realizado con los "subcriterios" o elementos a tener en cuenta en los criterios generales. A estos "subcriterios" también se les debe categorizar según su nivel de importancia, y a partir de allí se establece la cadena de "pesos" o grados de importancia que permite identificar el camino correcto para la toma de decisiones.

Basado en [21], a continuación se describen los procesos o etapas que deben ser ejecutados durante la aplicación del sistema de toma de decisiones multicriterio AHP:

### 4.3.2 Proceso de creación de matrices:

En primer lugar se debe crear un esquema jerárquico que distinga el objetivo principal, los criterios de selección y las alternativas presentes:

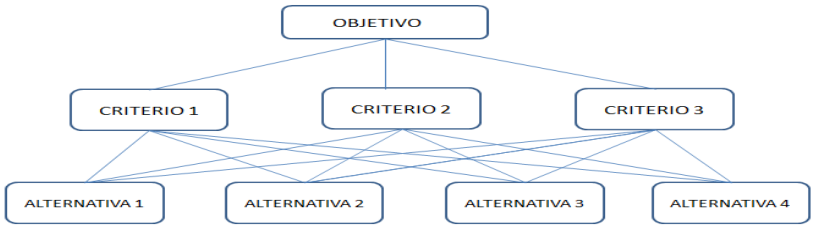


**Figura 4.** Esquema Jerárquico de modelo de toma de decisiones Multicriterio.

A partir de allí, se deben generar matrices a nivel de criterios, donde se relaciona todos los criterios propuestos y se obtiene la importancia o "peso" de cada uno de estos frente a los demás. A nivel de alternativas, se deben crear otras matrices donde se relacionan todas las alternativas propuestas en base a cada uno de los criterios de selección, identificando que alternativa tiene más importancia frente a las demás.

- ¿Qué Criterio tiene más importancia?: Basado en la escala de valoración de **Saaty,** se procede a calificar la importancia de un criterio con respecto a la importancia de otro:

| | CRITERIO 1 | CRITERIO 2 | CRITERIO 3 |
|---|---|---|---|
| CRITERIO 1 | 1 | 1/2 | 4 |
| CRITERIO 2 | 2 | 1 | 8 |
| CRITERIO 3 | 1/4 | 1/8 | 1 |

**Tabla 2.** Ejemplo de Matriz de comparación entre criterios.

Según este ejemplo de valoración inicial, de la matriz se interpreta que el criterio 2 es más importante que el criterio 1. También se identifica que el criterio 1 es más importante que el criterio 3, por ende el criterio 2 es mucho más importante que el criterio 3.

Luego de obtener las matrices de comprobación, se debe obtener el vector propio de cada criterio o "fila" y de esta forma identificar el "peso" o importancia que este tiene con respecto a los demás. Para ello es necesario tomar cada columna y normalizarla, tomando cada dato de la columna y dividiéndolo por la suma de todos los datos de la columna:

$$\text{Criterio 1: } 1 + 2 + \frac{1}{4} = 3{,}25$$

$$\text{Valores normalizados } \frac{1}{3{,}25} ; \frac{2}{3{,}25} ; \frac{1/4}{3{,}25} = 0{,}307; 0{,}61\ 0{,}086$$

$$\text{Criterio 2: } 1/2 + 1 + \frac{1}{8} = 1{,}62$$

$$\text{Valores normalizados: } \frac{1/2}{1{,}62} ; \frac{1}{1{,}62} ; \frac{1/8}{1{,}62} = 0{,}30 ;\ \ 0{,}61 ;\ \ 0{,}087$$

$$\text{Criterio 3: } 4 + 8 + 1 = 13$$

$$\text{Valores normalizados: } \frac{4}{13} ; \frac{8}{13} ; \frac{1}{13} = \ \ 0{,}30 ; 0{,}61 ; 0{,}087$$

Matriz normalizada:

| | CRITERIO 1 | CRITERIO 2 | CRITERIO 3 |
|---|---|---|---|
| CRITERIO 1 | 0,307 | 0,30 | 0,30 |
| CRITERIO 2 | 0,61 | 0,61 | 0,61 |
| CRITERIO 3 | 0,086 | 0,087 | 0,087 |

**Tabla 3.** Ejemplo de Matriz normalizada de comparación entre criterios.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de cada criterio, sumando todos los valores de cada fila y dividiéndolo por el número de datos presentes en cada fila:

$$\text{Criterio 1: } \frac{0{,}307+0{,}30+0{,}30}{3} = \ 0{,}30 \ = 30\ \%$$

$$\text{Criterio 2: } \frac{0{,}61+0{,}61+0610}{3} = \ 0{,}61 \ = 61\ \%$$

$$\text{Criterio 3: } \frac{0{,}86+0{,}87+0{,}87}{3} = \ 0{,}087 \ = 9\%$$

Para este ejemplo práctico, se puede concluir que el criterio más importante es el criterio 2 con un peso de 61%.

**NOTA:** La suma de los porcentajes de todos los criterios debe ser 100%, para ello es recomendable tomar más de tres cifras decimales en cada operación que se realice.

- ¿Qué alternativa tiene más importancia?: Se debe repetir el proceso anterior con la matriz de alternativas por cada criterio disponible (para este ejemplo es una matriz 4x4) donde se debe realizar el proceso de normalizar la matriz y hallar el vector propio de cada alternativa que permita obtener el "peso" o importancia de esta con respecto a cada criterio de decisión.

Por ejemplo al realizar el proceso anterior se obtuvo que la importancia de cada alternativa para cada uno de los criterios es:

Criterio 1: Alt1= $X_1\%$ ; Alt2 = $X_2\%$ ; Alt3= $X_3\%$ ; Alt4= $X_4\%$.

Criterio 2: Alt1= $X_5\%$ ; Alt2 = $X_6\%$ ; Alt3= $X_7\%$ ; Alt4= $X_8\%$.

Criterio 3: Alt1= $X_9\%$ ; Alt2 = $X_{10}\%$ ; Alt3= $X_{11}\%$ ; Alt4= $X_{12}\%$.

Luego de obtener los "pesos" de los criterios y de cada alternativa, se debe realizar la relación de importancias entre alternativas y criterios de decisión, para identificar cual alternativa cumple de forma más acertada con el objetivo general.

Para ello, se halla la importancia total de cada alternativa, a partir de la multiplicación de la importancia de la alternativa en cada criterio por el "peso" propio del criterio. Obteniendo como resultado la siguiente consideración:

Alternativa 1: $(X_1\% \,.\, 30\%) + (X_5\% \,.\, 61\%) + (X_9\% \,.\, 9\%) = 0{,}35 = 35\%$

Alternativa 2: $(X_2\% \,.\, 30\%) + (X_6\% \,.\, 61\%) + (X_{10}\% \,.\, 9\%) = 0{,}16 = 16\%$

Alternativa 3: $(X_3\% \,.\, 30\%) + (X_7\% \,.\, 61\%) + (X_{11}\% \,.\, 9\%) = 0{,}27 = 27\%$

Alternativa 4: $(X_4\% \,.\, 30\%) + (X_8\% \,.\, 61\%) + (X_{12}\% \,.\, 9\%) = 0{,}22 = 22\%$

Para este ejemplo práctico, se puede concluir que la alternativa 1 es la más **acertada** para cumplir el objetivo inicial propuesto

### 4.3.3 Consistencia de las matrices:

Este parámetro es muy importante en este proceso de selección de alternativas, pues permite

comprobar que las matrices y los datos que la componen, representan **correctamente** la información recopilada, es decir, se verifica que las matrices sean coherentes con la realidad y se descarta un análisis equivocado con datos incorrectos.

Este parámetro es conocido como **Ratio de Consistencia (CR) de matrices** y debe cumplir con las siguientes determinaciones:

| Tamaño Matriz | % máximo de CR |
|---|---|
| 3x3 | 5% |
| 4x4 | 9% |
| + 5x5 | 10% |

**Tabla 4**. Relación de equivalencias permitidas para Ratio de Consistencia (CR).

## 5. METODOLOGÍA

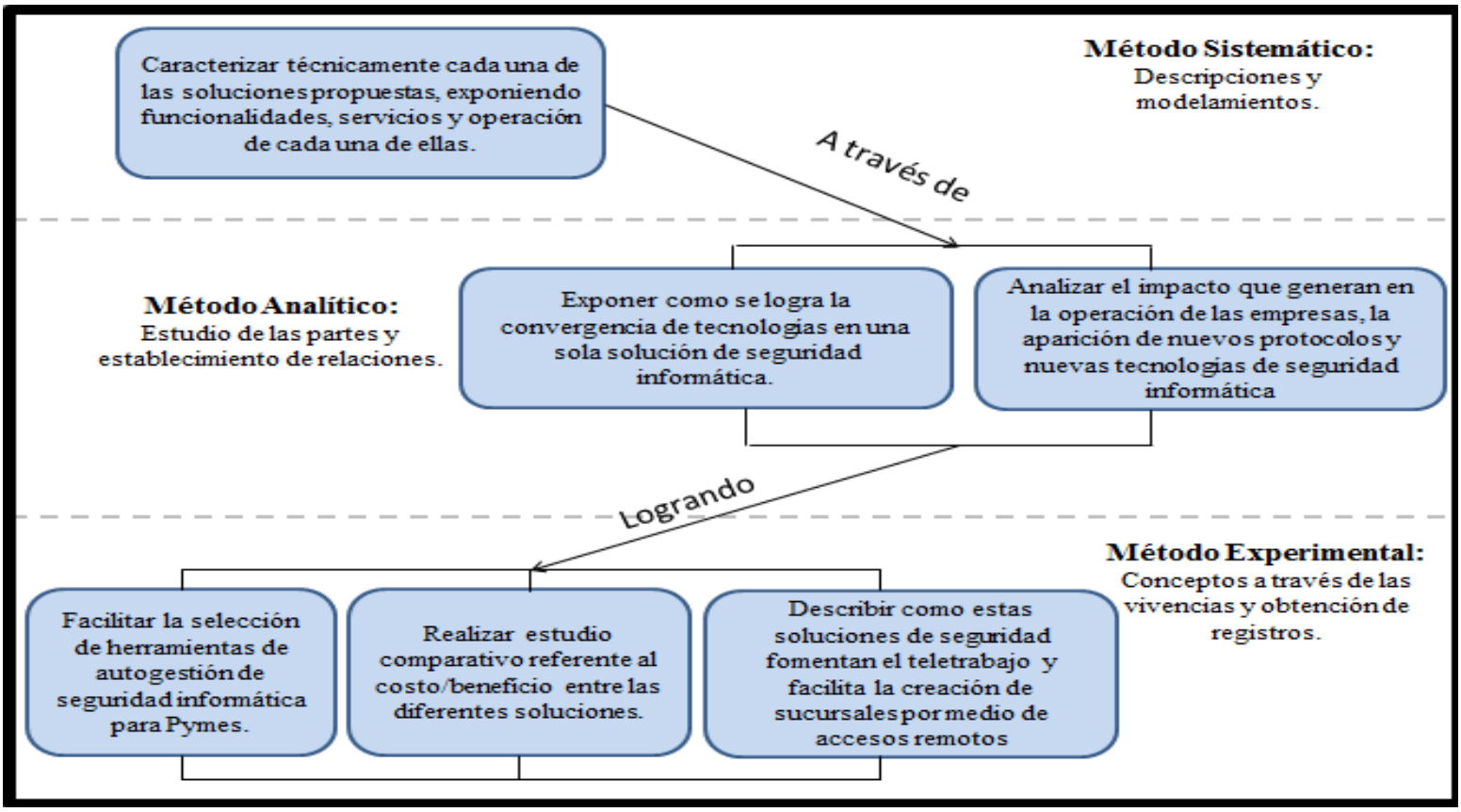


**Figura 5.** Metodología descrita en diagrama de bloques.

La metodología utilizada para cumplir con los objetivos de la investigación está basada en los conceptos analizados de [22] y [23]. Donde se basa el mecanismo de investigación en el método experimental, método sistemático y método analítico.

**En cuanto al método sistemático** que consiste en "realizar una descripción y modelamiento de los objetos a partir de sus componentes como su relación entre ellos", se pueden contemplar los objetivos: [22]

- Caracterizar técnicamente cada una de las soluciones propuestas, exponiendo funcionalidades, servicios y operación de cada una de ellas.

Donde se realiza un estudio a profundidad de cada alternativa propuesta, teniendo en cuenta su descripción general, su descripción física o de *Hardware*, sus funcionalidades (*software*), las características que lo diferencian de las otras alternativas y un precio económico estimado.

**En cuanto al método analítico** que consiste en estudiar las partes de un objeto de forma separada e independiente, evidenciando la relación que existe entre estas, y verificando que efectos tienen con respecto al entorno exterior, se pueden contemplar los objetivos:

- Exponer como se logra la convergencia de tecnologías en una sola solución de seguridad informática.

- Analizar el impacto que generan en la operación de las empresas, la aparición de nuevos protocolos y nuevas tecnologías de seguridad informática.

Donde se recopila toda la información técnica de las alternativas propuestas y se busca un camino común entre ellas. Un camino común que permita afirmar y consolidar a la tecnología y la seguridad informática como herramienta principal de desarrollo, progreso y crecimiento de las compañías, fomentando la expansión de mercados, la globalización la renovación del concepto laboral de las compañías , a través de la creación de puestos remotos de trabajo. [24]

**En cuanto al método experimental** se tiene la intención de dar respuesta a interrogantes a partir de la experiencia y los registros obtenidos a través de la interacción con las circunstancias o los objetos.

Este método persigue la respuesta a interrogantes a partir de la experiencia de las personas con las soluciones propuestas, donde las personas puedan dar a conocer su punto de vista y percepción frente a cada una de estas y relacionar de forma directa o indirecta los efectos que estas herramientas tienen en la operación de las compañías.

Por ende los siguientes objetivos pueden estar abarcados bajo esta premisa, pues a partir de los conceptos emitidos por los especialistas, se busca responder como este estudio permite vislumbrar respuestas de cómo afectan la implementación de estas soluciones a las personas.

- Facilitar la selección de herramientas de autogestión de seguridad informática para Pymes.
- Describir como estas soluciones de seguridad fomentan el teletrabajo y facilita la creación de sucursales por medio de accesos remotos.
- Realizar estudio comparativo referente al costo/beneficio entre las diferentes soluciones.

“Esta premisa experimental permite el esclarecimiento de determinadas relaciones o propiedades de los objetos, que permita verificar una hipótesis, una teoría o un modelo” [22]

# 6. SOLUCIÓN

La solución de esta investigación consiste en aplicar el sistema de toma de decisiones multicriterio AHP propuesta por ***Saaty*** , a partir de una preselección de cuatro propuestas de equipos de seguridad informática. Cada alternativa presenta funcionalidades diferentes, donde pueden ser implementadas de forma exclusiva o de forma complementaria.

Para ello se realizaron tres procesos de selección: el primero en cuanto al objetivo que se busca cumplir, que es establecer un modelo de análisis y selección que permite escoger la mejor herramienta de seguridad informática a nivel empresarial.

El segundo proceso se refiere a la preselección de alternativas, donde se caracterizan técnica y económicamente cada una de las propuestas. Y finalmente el tercer proceso de selección, referente al análisis de criterios de selección de cada una de las propuestas, donde se proponen tres criterios fundamentales que permiten valorar y comparar cada solución frente a las otras.

## 6.1 Selección de alternativas

### 6.1.1 IDENTITY SERVICE ENGINE – CISCO.

El **Cisco Identity Service Engine** es una plataforma de nueva generación de control de acceso y manejo de identidades, que le permite a las empresas reforzar su esquema de seguridad informática, mejorar la seguridad de la infraestructura TI y optimizar la operación de sus servicios. La arquitectura del ISE de Cisco, le permite a las empresas obtener información en tiempo real de las redes, de los usuarios que se conectan a través de ellas y de los dispositivos que las componen. [25]

Los administradores de esta herramienta, podrán utilizar información detallada referente a usuarios, dispositivos, perfilamiento, políticas de seguridad e integración con otras plataformas convergentes, para realizar seguimiento y verificación del buen funcionamiento de los sistemas. Dando pie al análisis y a la adopción de medidas proactivas de seguridad relacionando la identidad de los usuarios con los diferentes elementos de red: *Switches* de Acceso, enrutadores, controladoras Inalámbricas (WLCs), *Gateway*s VPN y *switches* de data center.

#### *6.1.1.2 Hardware:*

La serie ISE 3300 de **Cisco** , tiene tres modelos principales: **Cisco ISE 3315**, **Cisco ISE 3355** , **Cisco ISE 3395**.

A continuación se expone las características físicas de un *appliance* **Cisco ISE 3355**. Cabe resaltar que los otros dos modelos (3315 y 3395) son similares en dimensiones, condiciones

de operación y formas de instalación. Y se diferencian en cantidad de memoria RAM disponible, capacidad de almacenamiento en discos duros y disposición de tarjetas aceleradoras.

**Figura 6** Appliance ISE 3355 de **Cisco [26]**

El chasis del modelo **Cisco ISE 3355** está compuesto de:

- 1 Procesador Quad-Core Intel Xeon.
- 4 GB de memoria RAM.
- 2 Discos duros de 300 GB c/u.
- Cuatro interfaces LAN (10/100/1000) . Definidas en dos tarjetas de red (NIC) integradas y 2 tarjetas de red de 2 GB con la tecnología PCI-E.
- Bandeja de CD/DVD-ROM
- 4 Puertos USB
- 2 puertos GBE
- 1 Puerto Serial
- 2 Puertos VGA.
- Tarjeta aceleradora Cavium CN-1620-400-NHB-G.
- 6 unidades ventiladoras.
- Temperatura soportada de operación de 10 a 35 °C.
- 2 fuentes de alimentación eléctrica AC, basados en el sistema redundante y conmutación de fuente de energía automática. Cada fuente provee 675 Watts.

#### *6.1.1.3 El dispositivo permite:*

- Combinar la autenticación, la autorización, el *accounting, (AAA),* la postura de dispositivos (atributos y roles que lo identifican en la red) y el perfilamiento de usuarios en un solo *appliance.*

- Proveer accesos y permisos de administración de la herramienta a la medida, para usuarios administradores invitados.

- Reforzar el funcionamiento y el esquema de seguridad de los dispositivos finales, por medio de mediciones y valoraciones de la postura de los dispositivos que acceden a la red, incluyendo los ambientes 802.1X.

- Habilitar políticas consistentes en despliegues centralizados y distribuidos para permitir que los servicios sean aprovisionados inmediatamente cuando sean requeridos.

- Emplear capacidades avanzadas de reforzamiento de la seguridad, implementando *Security Group Access (SGA)* a través del uso de *Security Group Tags (SGTs)* y *Security Access Control Lists (SGACLs).* [27]

- Soportar la escalabilidad y crecimiento de múltiples escenarios de despliegue de la herramienta, desde las pequeñas oficinas hasta los entornos de grandes corporaciones. [25]

#### *6.1.1.4 Software (Funcionalidades):* [28]

- ***Refuerzo de políticas de seguridad:***

  Provee un modelo flexible y más robusto de configuración de reglas de acceso. La flexibilidad se ve demostrada en la habilidad de configurar políticas de acceso de forma granular, permitiendo tener numerosos parámetros de configuración como: identidad de usuarios finales y su respectivo dispositivo de acceso, validación de la postura de los dispositivos, uso de protocolos de autenticación, perfilamiento de identidades, entre otros.

  Además permite la integración de dispositivos y protocolos de seguridad externos para la configuración de políticas de autorización y autenticación (AAA) como : LDAP, *Radius*, Microsoft Active Directory, RSA OTP (One-time password) y autoridades certificadoras.

- ***Control de acceso:***

  Provee un amplio rango de opciones al momento de configurar políticas de acceso, donde se contemplan: ACLs descargables (Access Control Lists), asignaciones y *tags* de Vlan, re direccionamiento de URLs, *STGs* (Security Group Tags), entre otros, utilizando las más avanzadas capacidades de la tecnología ***TrustSec*** de **Cisco**.

- ***Control de acceso de alta seguridad sin requerir identificación y contraseñas:***

  Provee la capacidad de establecer modelos de control de acceso sin la requerir de forma explícita credenciales de acceso como nombre de usuario y contraseña. El control de acceso se realiza a partir de la autenticación de los usuarios en los aplicativos directamente, sin necesidad de implementar ninguna herramienta tipo 802.1x para la autenticación de sus usuarios a partir de puerto de conexión.

- ***Soporta el protocolo SXP (Source-Group Exchange Protocol)***

  El *feature* ***Cisco TrustSec*** permite la creación de redes seguras a partir del establecimiento de dominios. Cada dispositivo pertenece a un dominio y cada dominio tiene características y perfilamiento diferentes, donde se permiten o deniegan alcances y recursos, a partir de políticas de seguridad comunes.

  En el interior del dominio, cada dispositivo es autenticado por sus *peers* de red y la comunicación entre los dispositivos adentro del dominio, se asegura a partir de la encripción de tráfico, de la revisión de integridad de los mensajes (hash) y del monitoreo de la trayectoria de la información y sus mecanismos de protección.

  SXP permite la implementación de ***Cisco TrustSec*** a través de redes que no soportan el etiquetado de paquetes

- ***Manejo del ciclo de vida de los invitados:***

  Proporciona un manejo simplificado de la implementación y customización de las políticas de acceso a la red para invitados, permitiendo la configuración de acceso a la red a través de *Hotspots* (portales Cautivos), *sponsored networks* (permitidos por los administradores de red y con avisos publicitarios Ej: conexiones Wifi en Aeropuertos) y accesos" Autoservicio".

  Donde el administrador de red puede monitorear en tiempo real todo el tráfico y todas y cada una de las conexiones establecidas, evidenciando datos de interés como límites de tiempo por conexión, cuentas expiradas y vigentes, verificación de identidades vía SMS y demás controles de seguridad, que permiten hacer un rastreo exacto de todo el movimiento de los invitados a través de la red, tanto físico como lógico.

- ***Incorporación simplificada de dispositivos a las redes:***

  El personal encargado del despliegue de la solución está en capacidad de implementar y customizar herramientas de *self-assessment* o auto-servicio, donde los clientes pueden manejar de forma simplificada la incorporación y conexión de nuevos dispositivos a sus dominios de red.

  Se pueden crear ambientes con apariencia y diseño del cliente, donde se puede gestionar la autorización de ingreso de nuevos dispositivos a la red, que accedan por cable o por red inalámbrica. Esta funcionalidad permite auto gestionar muchos de los requerimientos que los clientes escalan a los proveedores en las mesas de ayuda.

- ***Protocolos AAA:***

  Soporta un gran número de protocolos AAA. Soporta Radius, EAP (Extensible Authentication Protocol, PEAP(Protected EAP), EAP FAST, EAP/TLS, EAP/TTLS, y demás.

- ***Administración de control de acceso a los dispositivos y auditoria:***

  Utiliza el protocolo TACACS+ para autenticar, autorizar y auditar usuarios que tratan de acceder a la red mediante dispositivos configurados bajo el protocolo TACACS+. Se puede auditar y configurar el nivel de acceso que tienen los usuarios en cuanto a niveles de ejecución en los IOS de los equipos, a formas de conexión, lugares de conexión y que acciones pueden o no ejecutar adentro del dispositivo.

- ***Manejo Interno de Certificados:***

  ISE ofrecer una consola para administrar los certificados digitales de los dispositivos finales. Tiene la capacidad de verificar el *status* de los certificados y su relación con los dispositivos en tiempo real a través de OCSP (Online Certificate Status Protocol), además provee revocaciones automáticas de certificados cuando se detecta que un dispositivo fue robado o violentado.

  Permite el aprovisionamiento de certificados digitales de forma simplificada para los dispositivos de los usuarios finales, evitando los complejos procedimientos que conllevan la generación de certificados digitales por autoridades certificadores.

- ***Perfilamiento de dispositivos:***

  Permite la creación de *templates* o plantillas predeterminadas para perfilar cualquier tipo de dispositivo, ya sea un teléfono IP, una impresora, una cámara IP, smartphones o tablets. Estos *templates* de perfilamiento permiten de forma automática detectar, clasificar y asociar políticas de acceso e identidad cuando los dispositivos se conectan a la red.

  La tecnología *ISE Sense* implementada en varios dispositivos *Catalyst tipo Switches* , permite recolectar rápidamente información de atributos e identidad de los dispositivos que acceden a la red. Luego, utilizando Radius organizan la información obtenida y se la envían al ISE, para que este realice la clasificación del dispositivo y aplique las políticas de acceso necesarias.

  Este feature del *ISE Sense* permite hacer procesos más eficientes de recolección de información de dispositivos finales, incrementando la escalabilidad, la capacidad de

despliegue y disminuyendo el tiempo de clasificación y reconocimiento de los dispositivos

- ***Manejo de Información de perfilamiento de dispositivos entre equipamiento Cisco y equipamiento multi-vendor:***

  Este *feature* permite "heredar" configuraciones e información de perfilamiento de dispositivos almacenado en equipamiento Cisco, a equipamiento de otros proveedores que tengan alcanzabilidad vía IP.

  Esto permite compartir la información entre dispositivos **Cisco** y dispositivos de otros fabricantes, donde el ISE recopila esta información la analiza y la redistribuye si es necesario.

  Esto permite tener actualizaciones automáticas, cuando se detectan nuevos dispositivos que intentan acceder a la red. Esto reduce el seguimiento que se debe realizar periódicamente a todos los nuevos dispositivos que intentan acceder a la red.

- ***Postura en los dispositivos finales:***

  Esta utilidad permite verificar la postura que tienen los dispositivos finales como PCs, computadores portátiles, Smartphones y tablets, con respecto a las políticas de seguridad de la compañía para dispositivos que intentan ingresar a la red.

  Provee la habilidad de crear políticas de seguridad que permiten verificar, controlar y configurar periódicamente las últimas actualizaciones y parches de los SO de los dispositivos, tener información actualizada de los aplicativos antivirus y antispyware, tener conocimiento de registros, administración de actualizaciones, encripción de discos, entre otros. [29]

- ***Soporte para integrar en un solo ambiente varios directorios activos:***

  Provee autenticación y autorización en dominios de directorio activo de Microsoft de tipo *multiforest.* Puede agrupar múltiples dominios desarticulados, en grupos lógicos para simplificar la configuración de directorios activos en topologías complejas, que habitan en entornos en constante cambio.

  Soporta *Microsoft active directory* 2003, 2008, 2008R2, 2012 y 2012R2.

- ***Servicio de protección para dispositivos finales:***

  Le permite a los administradores tomar acciones correctivas de forma inmediata, ubicando los dispositivos en cuarentena o apagándolos según el grado de compromiso y riesgo que tiene el dispositivo frente a la red. Este servicio reduce el riesgo y aumenta la seguridad en la red.

- ***Manejo y administración centralizada:***

  Le permite a los administradores realizar configuraciones de administración de perfiles, administración de posturas, de invitados, autenticación y autorización de servicios y recursos en una única consola WEB GUI.

- ***Monitoreo y troubleshooting:***

  Incluye en la consola WEB-GUI , una consola especializada en monitoreo, reportes y *troubleshooting* que le permite al personal de *help desk* y a los administradores identificar y resolver problemas e incidentes.

  El ISE ofrece reportes robustos en tiempo real de todos los servicios, del *logging* (acceso) de todas las actividades, de métricas de todos los usuarios y dispositivos que se conectan a la red.

- ***Opciones multiplataforma:***

  El ISE puede ser aprovisionado de forma física o a través de un *appliance* virtual. El virtual *appliance* puede ser provisto en plataformas VMware ESXi o KMV (Solución Linux: Kernel Based virtual Machine) a través de la creación de máquinas virtuales con el sistema operativo del ISE.

  De forma física, se adquiere el chasis del equipo y requiere ser instalado en un ambiente de data center, con medidas especiales de alimentación eléctrica y condiciones ambientales idóneas.

#### *6.1.1.5 Licenciamiento:*

Actualmente existen ocho (8) paquetes de licencias disponibles para la implementación de una nueva solución basada en el ISE de **CISCO**.

- Perpetuas: Hay disponibles 3 paquetes de licencias, el paquete **BASE,** el paquete de **ADMINISTRACIÓN DEL DISPOSITIVO** y el paquete **EXPRESS.**

- Opcionales: Hay disponibles 5 paquetes de licencias, el paquete **PLUS,** el paquete **APEX**, el paquete **MOBILITY ,** el paquete **MOBILITY UPGRADE** y el paquete de **EVALUATION.**

#### *6.1.1.6 Precio en el mercado*

La cotización varía si se desea adquirir el *appliance* (Hardware) ó adquirir el producto a través de una máquina virtual instalable en un servidor. Actualmente el producto más económico está U$16.000 (*appliance*), a lo cual se le debe adicionar el valor de las licencias que habilitan el uso de los diferentes *features,* que oscilan entre los U$5.000 y U$ 700.000. Los precios de las máquinas virtuales oscila entre los U$6.000 y los U$30.000.

### 6.1.2 FIREWALL PA-5000 Series (50-50) – PALOALTO NETWORKS.

"La serie PA-5000 es una serie de firewalls NG (Next-Generation) que previenen amenazas y permiten el transporte seguro de información y aplicaciones, a través de una configuración versátil de alto rendimiento. Donde resaltan los Gateways de Internet, la infraestructura de Data Center y los entornos de Service Provider.

Esta serie permite preservar la seguridad informática de las organizaciones mediante un avanzado control y visibilidad de las aplicaciones, de los usuarios y del contenido, transportados físicamente a través de un firewall con un *throughput* de hasta 20 Gbps.

Finalmente, cuenta con recursos de procesamient dedicados de forma independiente a procesos de *networking* ,seguridad, análisis de firmas y funciones de administración que garantizan un funcionamiento controlado y predictible." [30]

El firewall permite la creación de instancias virtuales, las cuales pueden ser utilizadas para crear "firewalls" independientes para clientes, sedes o ambientes productivos/contigencia de forma separada.Las instancias virtuales son llamadas *"Virtual Systems"* y cuentan con configuraciones independientes y aisladas, que cuentan con sus propias configuraciones de políticas de acceso, de listado de usuarios, de aplicaciones, de rutas y de conectividad.

Cada "*Virtual System"* aparte de tener todo un sistema de seguridad, detección y protección de intrusos de manera independiente, cuenta con su propia configuración de enrutamiento. El enrutamiento es manejado por instancias virtuales de *routers* llamados "*Virtual Routers*", en los cuales se puede configurar toda la parte de redes: rutas, *vlans* y protocolos de enrutamiento.

Finalmente, que la operación este basada en la virtualización de firewalls, permite que en un ambiente de Data Center o *Service Provider*, se pueda brindar servicios de *networking,*

seguridad , IDS, IPS, reportes, monitoreo y logging, a un rango de 10 a 225 clientes con un solo dispositivo (dependiendo la referencia del firewall) .

#### *6.1.2.1 Hardware*

La serie 5000 de Firewalls NG de Palo Alto, cuenta con tres modelos principales: PA **50-20 , PA50-50 , PA50-60**

**Figura 7.** Appliance firewall PaloAlto PA50-50 **[30]**

A continuación se exponen las características físicas de un *appliance* **Palo Alto PA50-50.** Cabe resaltar que los otros modelos (PA50-20 y PA50-60) son similares en dimensiones, condiciones de operación y formas de instalación. Se diferencian en el *Throughput* disponible, capacidad de número de sesiones (1´000.000 – 4´000.000 según modelo), cantidad de usuarios VPN, cantidad de "v*irtual Systems*" y "v*irtual Routers*", zonas de seguridad y cantidad de políticas de seguridad.

El chasis **Palo Alto PA 50-50** en cuanto a *performance* y capacidades, está definido de la siguiente forma:

- *Throughput* de 10 Gbps.
- *Threat prevention throughput* 5 Gbps.
- IPSec VPN throughput 4 Gbps.
- Nuevas sesiones por segundo: 120.000
- Número máximo de sesiones: 200.000
- Numero de *Virtual Systems* :25 a 125.

El chasis del modelo **Palo Alto PA 50-50** está compuesto de:

- 12 Interfaces 10/100/1000.
- 8 interfaces SFP.
- 10 Interfaces SFP+.
- 2 Interfaces 10/100/1000 para H.A (High Availability)
- 1 Interfaz de 10/100/1000 de administration.
- 1 Interfaz de consola RJ45.
- Ocupa 2 unidades estándar de Rack de 19´´ apróx.

- 2 fuentes de alimentación eléctrica AC, basados en sistema redundante con conmutación de fuente de energía automática. Cada fuente provee 450 Watts.
- Disco duro de estado sólido de 120 GB o 240 GB.
- Unidades ventiladoras.
-

***6.1.2.2 El dispositivo permite***

Los Firewall Palo Alto de la Serie 5000, especialmente en su referencia PA50-50, resultan ser una herramienta fundamental para suplir necesidades de seguridad de varios clientes, ambientes, sedes o dominios, de forma independiente y autónoma, utilizando únicamente un dispositivo de hardware.

Este Firewall, mezcla tareas de *Networking*, Seguridad, IDS, IPS, Syslogs y Reportes avanzados.

- **Networking:**

El firewall tiene la capacidad de realizar tareas de enrutamiento de paquetes a través de redes IPv4 e IPv6. Maneja el concepto de *"Virtual Routers"*, los cuales son configurados para actuar como puertas de enlace de las instancias virtuales de los clientes ("Virtual Systems" ) hacia redes externas como Internet y redes WAN (MPLS, Lan2Lan, Canales dedicados). Soporta protocolos de enrutamiento como OSPF, RIP, BGP, EIGRP, RIPng, EIGRPv6 y OSPFv3.

- **Seguridad:**

Manejan un sistema bastante completo y granular de configuración de políticas de seguridad, ya sea para creación de reglas o políticas, configuración de NATs o aplicación de políticas de encripción y decripcion, basados en numerosos parámetros de configuración como zonas de origen/destino, ID de usuarios, aplicaciones, puertos, permisos programados en el tiempo y *features* de protección como el *threat prevention* y los *vulnerabilty profiles.*

- **IDS e IPS:**

El firewall cuenta con una amplia base de datos de firmas de amenazas, virus, malwares y patrones de ataques, los cuales bajo una configuración determinada, son la materia prima para realizar labores de detección de intrusos (IDS) revisando todo el tráfico y generando alarmas o eventos de alerta cuando el tráfico coincide con alguna firma de software malicioso.

En cuanto a tareas de IPS, el firewall tiene *features* especializados como el ***Threat Prevention*** que bajo la configuración dada por el administrador, puede tomar medidas de bloqueos, suspensión de servicios y recursos.

- **Monitoreo**:

  Cuenta con un módulo de monitoreo, que permite analizar de forma independiente el tráfico de cada *virtual system*, filtrando la información por origen/destino, puertos, aplicaciones, usuarios, direcciones NAT, etc. También permite monitorear tráfico de forma granular, donde se analizan sesión por sesión TCP, amenazas, vulnerabilidades, urls visitadas y alarmas.

- **Reportes:**

  La herramienta de reportes conocida como *Application Command Center* (ACC), permite obtener información detallada y estadísticas del tráfico de las aplicaciones, de las urls visitadas, de las amenazas identificadas, etc.

  Tiene la posibilidad de generar reportes automatizados donde se relacionan por aplicación los máximos generadores de tráfico, los máximos receptores de tráfico, los países con mayor número de solicitudes y tráfico, entre otros. También gestiona la creación de informes automáticos en formato PDF con envíos programados vía correo electrónico.

- **Syslogs:**

  Tiene la funcionalidad de almacenar y mostrar *Logs* de interés en cuanto a tráfico que transita por el dispositivo, amenazas detectadas, urls visitadas/permitidas/bloqueadas, alarmas y eventos.

***6.1.2.3 Software (funcionalidades):*** [31]**,** [30]**,** [32]

- **Firewall:**

  El Firewall permite la clasificación de tráfico en más de 2000 aplicaciones, identificadas por medio de APP-IDs. Por ejemplo: google-based (servicios google), ms-rdp ( Remote Desktop Microsoft) , informix ( Aplicativo IBM) ,entre otros.

  Permite la customización de las aplicaciones, añadiendo puertos o modificando *timeouts*. Permite la configuración de políticas de seguridad basado en usuarios, direcciones IP, aplicaciones, categorías de las aplicaciones, tecnologías, factor de riesgo o características importantes, con una configuración fija en el tiempo o programable según demanda.

  También facilita la adición de políticas de encripción o desencripción SSL a las políticas de seguridad ya configuradas, a través de las interfaces túnel VPN IPSec *Site-to-Site* o *Site-To-Client* con el agente Global Protect.

Además ejerce control de usuarios a partir de la integración con tecnologías como directorio activo, LDAP, Exchange (Microsoft) y *edirectory* para dispositivos terminales Citrix y Microsoft.

- **Threat Prevention / Prevención de amenazas:**

  Incluye tres modos fundamentales de prevención: En primer lugar tiene protección contra virus, basado en el estudio y revisión de tráfico, donde se analiza tráfico con contenido malicioso embebido en HTLM, Javascript, PDF, Spywares y gusanos.

  En segunda instancia tiene protección de *Drive-by downloads*, lo cual se refiere a proteger todo el perímetro de seguridad de aquellos virus alojados en páginas de internet, donde los usuarios con tan solo visitar estos sitios pueden ser víctimas de instalación no autorizada de malware.

  En tercer lugar tiene detección de *botnets*, referente a todos los ataques realizados por programación de robots. Que buscan generar indisponibilidad de servicio en portales o páginas de internet, servidores de aplicaciones o servidores de bases de datos.

- **Modern Malware Protection / Protección de Malware:**

  Posee análisis dinámico y detección de malware desconocido en información embebida en archivos tipo PDF, Java, Android APKs, Adobe Flash y todas las extensiones de archivos Microsoft Office y web.

  Maneja generación automatizada de firmas para malware detectado. Controla todas las apariciones de posibles infecciones de malware y le da un manejo especial a estas, sin afectar el normal funcionamiento de las redes productivas.

- **URL Filtering / Filtrado de URLs:**

  Permite la configuración de categorías, listas permitidas, listas prohibidas y paginas bloqueadas, basados en la customización de una base de datos de URLs. Permite establecer *safe search* o búsqueda segura a través de Google, Bing y Yahoo.

- **File And Data filtering / Filtrado de Archivos e Información.**

  Posee control bidireccional (trafico entrante/saliente) de transferencias de archivos no autorizados para más de 60 tipos de contenidos. Además controla de forma segura la transferencia de información sensible como números y claves de tarjetas de crédito, transacciones electrónicas, identificaciones, etc.

- **QoS / Calidad de Servicio:**

  Permite ajustar las políticas de seguridad basados en prioridad, necesidad de garantía y disponibilidad por aplicación, por usuario, por túnel VPN ó por interfaz. Este *feature* prioriza la transferencia de determinado servicio frente a otro a través de la red. Por

ejemplo, se puede priorizar un servicio sensible *delays* como **Citrix** , frente a otros servicios como la **navegación web** que son menos sensibles a dichos *delays.*

- **VPN Connectivity / Conectividad VPN:**

  Tiene dos *f*eatures principales: Uno para la configuración de VPNs *site-to-site* a través de la creación de túneles IPSec entre dos terminales VPN fijos (*Gateways*) , donde uno de ellos es el Firewall Palo Alto y el otro puede ser un firewall, un servidor, un terminador de VPN o un *router*.

  El segundo *feature* referente a la configuración de VPNs *client-to-site* a través de la creación de portales o *gateways* VPN (Firewall PaloAlto) y a la instalación de agentes **Global Protect** en los distintos dispositivos remotos, logrando conectividad por medio de túneles SSL o IPsec.

- **Mobile Security / Seguridad Móvil :**

  Monitorea y permite hacer reportes en tiempo real del estado de los dispositivos, como alertar cuando algún dispositivo fue violentado o "*rooteado*". Permite administrar las configuraciones internas de los dispositivos, parametrizar la seguridad de los mismos y detectar malware/software malicioso en dispositivos **Android**. A su vez, permite el despliegue de prevención de amenazas /*Threath Prevention* basado en aplicaciones, usuarios, contenidos, dispositivos y estados.

- **Networking:**

  Tiene la capacidad de manejar enrutamiento dinámico con los protocolos: BGP, OSPF y RIP. Maneja diferentes configuraciones de interfaces como: *tap mode*, *virtual wire*, interfaces capa 2 (*switchport*) e interfaces capa 3 (IP), configurables a través de *tags* de Vlan bajo el encapsulamiento 802.1Q.

  Permite la configuración de NATs , configuraciones de firewall como servidor DHCP, configuración de rutas y enrutamiento en IPv6 y manejo de envío de paquetes Multicast.

- **High Availability / Alta Disponibilidad:**

  Permite la configuración de alta disponibilidad entre dos *peers* (firewalls PaloAlto), en configuración activo/activo o activo/pasivo. Permite configurar las sesiones de sincronización entre dispositivos con monitoreo constante de fallas tanto en el enlace entre ambos (de forma general) como en la ruta o *path* por donde están conectados, es decir, es capaz de identificar donde hay una falla de conectividad en un equipo intermediario que permita la conexión de HA.

- **Management and Viability Tools / Herramientas de viabilidad y administración:**

  Tiene un manejo integrado entre la interfaz Web, el CLI (administración por consola) y administración centralizada con el *feature* **Panorama**. Maneja **Syslog** y es compatible con el protocolo SNMP en v2 y v3. Cuenta con el ACC (*Application Command Center*) que

permite recopilar de forma ordenada información y estadísticas de aplicaciones, urls, amenazas , usuarios e información de interés general.

Tiene la opción de configurar reportes automáticos y customizables en formato PDF. También permite la visualización y exportación de Logs de tráfico, de amenazas, de URLs y filtrado de archivos.

#### *6.1.2.4 Licenciamiento*

Para los *features* **Threat Prevention y URL filtering** se requiere subscripción o licenciamiento pago. Para el *feature* **Modern Malware Protection** se requiere la suscripción a la extensión **WildFire**. Para el *feature* **Mobile Security** se necesita la adquisición de licencias de **Global Protect Mobile Security Manager**.

La versión de software recomendada es la 7.2 que cuenta con el licenciamiento de **Panorama** y **Wildfire**. Y la versión 7.0 que no incluye licencias para **Panorama**.

#### *6.1.2.5 Precio en el mercado*

Este producto se adquiere únicamente en *appliance* y es uno de los más costosos en el mercado, teniendo un precio base que oscila entre U$ 71.000 a U$75.000, sin contemplar costos de licenciamiento de *features.*

### 6.1.3 BIG-IP 2000/4000 SERIES – F5 LAB.

El dispositivo **F5 BIG-IP de la serie 2000,** es por definición un balanceador de carga que opera basado en el análisis de tráfico a nivel de transporte (UDP, TCP) y a nivel de Aplicación, con todos los protocolos que existen referentes a servicios informáticos.

El objetivo principal del balanceador, es ser un intermediario entre los clientes ubicados en el entorno externo que demandan servicios constantemente y los dispositivos o redes ubicados en un entorno interno de Data Center que proveen de servicios a los clientes.

Este dispositivo permite balancear cargas entre los servidores de aplicación que brindan un mismo servicio, aprovechando al máximo las capacidades de los dispositivos y evitando saturaciones e indisponibilidades.

### *6.1.3.1 Hardware*

**Figura 8.** Appliance Big-IP 2000 series **[33]**

El balanceador **BIG-IP 2000 F5**. En cuanto a *performance* y capacidades:

- Procesamiento inteligente de trafico: Maneja 212.000 peticiones L7 por segundo; 75.000 conexiones L4 por segundo, 550.000 conexiones HTTP L4 por segundo; 5´000.000 de sesiones simultaneas L4 y tiene un *Throughput* de 5 Gbps L4/L7.
- En cuanto a conexiones SSL, tiene la capacidad de mantener 2000 TPS (Transacciones por segundo) con manejo de 2.000 Llaves. Cuenta con 4 Gbps de cifrado masivo.
- Arquitectura de software de 64-bits.
- Cuenta la capacidad de actualización bajo demanda y en "caliente".

El *appliance* del modelo **BIG-IP 2000 F5** está compuesto de:

- Procesador Intel Dual core.
- Memoria Ram de 8 GB
- Disco duro de 500 GB.
- 8 interfaces GbE RJ45
- 2 interfaces GbE Fibra óptica.
- 1 interfaz de administración 10/100/1000.
- 2 interfaces RJ45 de consola (1 para failover).
- 2 interfaces USB 2.0
- Alimentación eléctrica de 400 Watts con doble fuente de alimentación redundante.
- Consumo de 74 Watts aprox.
- Ocupa una unidad estándar de rack.
- Temperatura de operación de 0 a 40 °C.

### *6.1.3.2 El dispositivo permite:* [34]

- **Consolidar la infraestructura con hardware especializado:**

La Plataforma BIG-IP permite distribuir tareas a los diferentes equipos de forma equitativa según su especialidad. Al realizar un análisis de tráfico a nivel de transporte y aplicación, este dispositivo puede ser configurado para balancear carga de Servidores, de equipos de

Data Center, de servicios DNS, de **Web Application Firewall (WAF)**, de administración y control de acceso, de optimización de performance web y optimización de conectividad Wan.

- **Balancear servidores de aplicaciones:**

  La plataforma BIG-IP permite administrar las peticiones que se realizan desde ambientes externos a los servidores de aplicaciones. De esta forma se pueden distribuir tareas de resolución de peticiones y procesamiento de los servidores, reduciendo la carga y consumo de recursos a los que anteriormente estaba expuesto un solo servidor. Esta característica genera un uso de recursos más eficiente.

- **Asegurar las redes:**

  Permite realizar el despliegue de un sistema de protección basado en el análisis de tráfico de tipo capa 3 a capa 7, donde se revisa cuidadosamente todo el tráfico IP y sus respectivos encapsulamientos hasta llegar al tráfico de aplicaciones. Provee seguridad a nivel de políticas y de filtrado de paquetes a través de la funcionalidad **Web Application Firewall (WAF).**

- **Reducir costos de operación:**

  Permite ahorrar tiempo en configuraciones, actualizaciones y mantenimientos con una plataforma de administración sencilla, donde a través de una *Web GUI* se pueden configurar parámetros de actualizaciones en "caliente", soporte USB, administración de los recursos y monitoreo de *Front-End* . También tiene un consumo menor de energía y se acomoda a condiciones basicas de Data Center para su funcionamiento.

- **Maximiza los tiempos de actividad:**

  Permite asegurar que toda la infraestructura crítica sea compatible con tareas de mantenimiento y reemplazo de componentes en "caliente". Cuenta con instalación de fuentes de energía redundantes y soporte *multi-boot* a partir de varios medios.
  El *appliance* puede ser configurado en múltiples ambientes HA (alta disponibilidad), a partir de configuraciones de redundancia como Activo/Activo, Activo/Pasivo, o en clúster.

#### *6.1.3.3 Software (funcionalidades)*

"La funcionalidad de seguridad que ofrece el **F5 BIG-IP 2000**, es un servicio tipo *cloud* desplegado a través del BIG-IP *Application Security Manager* (ASM), el cual tiene como objetivo general brindar soporte especializado 24x7x365 para proteger las aplicaciones y la información, cumpliendo con los estándares mundiales de seguridad ." de [35]

A modo general, la configuración de esta herramienta permite combatir ataques informáticos como:

- Ataques DoS(Deny of service) y DDoS (Distribuited Deny of Service) a nivel de aplicación.

- Ataques fuerza bruta.

- Desbordamiento de buffers.

- Manipulación de Cookies.

- Ataques Zero-Day (exploits no reconocidos por los fabricantes).

- Fuga de información sensible.

- Ingeniería inversa.

A través de técnicas y *features* especializadas en el tratamiento de la información y del tráfico, a nivel de capa de aplicación, diferenciándose del modo de operación de un Firewall común que opera a nivel de capa de red y de transporte. Las utilidades que utiliza para combatir las anteriores amenazas son:

- Configuración de políticas de seguridad.

- Monitoreo proactivo de alertas.

- Protección de BOTS.

- Bloqueo de Geo localización.

- Reportes de cumplimiento de PCIs (*Payment Card Industry*)

Por otra parte, enfocando únicamente el aspecto de seguridad hacia las utilidades del **Web Application Firewall WAF** y a la prestación de servicios de seguridad bajo un solo *appliance*, el **f5 BIG-IP 2000**, maneja los siguientes aspectos:

- Firewall de RED.
- Administración de Trafico.
- Seguridad de Aplicaciones.
- Control de Acceso.
- Mitigación de ataques DDoS.
- Inspección SSL y de certificados.
- Seguridad DNS.

El manejo de estas utilidades es realizado a partir de dos instancias paralelas, basadas en la dirección en la que se dirige el tráfico.

En primer lugar, el **WAF** analiza todo el tráfico saliente, es decir, todo el tráfico producido por los usuarios alojados en la red perimetral, que realizan solicitudes a recursos externos

ubicados en Internet o en otras sedes a través de conectividad WAN. El análisis se concentra en la revisión de identidades de los usuarios, del control de acceso de los mismos a los recursos de red y a la administración del tráfico que producen.

En segundo lugar, el **WAF** analiza todo el tráfico entrante, es decir, todo el tráfico producido por dispositivos externos a la red perimetral, que responden a las solicitudes iniciales de los usuarios o que simplemente buscan iniciar comunicación. El análisis en este aspecto, se enfoca a nivel de aplicación en inspeccionar y verificar las negociaciones SSL y la comprobación de certificados, en proteger los dispositivos internos de ataques DoS, DDoS, *SQL Injections* o *Cookie poisoning.*

Esta utilidad se concentra en combatir ataques como SYNfloods, UDP Floods, ACK Floods (TCP), ICMP FLoods y Ping Floods, con técnicas como SynCheck, forwarding TCP estricto y visibilidad completa de tráfico proxy, todo esto a nivel de capa física, enlace de datos y red.

A nivel de capas superiores del modelo OSI, previene ataques de sesión de capa 4 a 6 mitigando ataques como DNS Floods, DNS Querys Floods y SSL Floods, con la aplicación de técnicas como DNS Express, Terminación SSL, Reglas y validación de renegociaciones SSL.

Previene ataques de denegación de servicio como los Slow Posts, los HashDos, los Get Floods y los Slowloris a través del reforzamiento de políticas de seguridad , de la configuración de proxy HTTP, de la revisión constante de patrones anormales y de la creación de reglas de seguridad.

#### *6.1.3.4 Licenciamiento*

Los equipos de este serie **F5 Big-IP 2000** cuentan con una licencia de uso básico. Todas las licencias que deban ser adquiridas por demanda, pueden ser buscadas a través de la página Web del fabricante, donde se puede encontrar la opción idónea de licenciamiento a partir del requerimiento de actualización, el modelo de los equipos, el *performance* requerido y el costo de adquisición disponible.

#### *6.1.3.5 Precio en el mercado*

Variable a partir de los *feautres* y modulos que se adquieran. Con una cotización base por *appliance* de U$28.000 y que oscila entre U$20.000 y U$ 120.000.

### 6.1.4 FORTIGATE 90D SERIES – FORTINET

"La serie Fortigate/FortiWifi 90 D de Fortinet, es un conjunto de dispositivos tipo Firewall diseñado para ser implementado en ambientes corporativos pequeños o medianos. Esta serie maneja el concepto de dispositivo todo en uno bajo la categorización de soluciones UTM (*Unified Threat Management*) donde proveen servicios propios de Firewall, Antivirus, Antispam, IPS, IDS, control de navegación segura e implementación de conexiones VPN.

Esta serie de Fortinet esta especialmente diseñada para ser el CPE de las organizaciones frente a los proveedores de conectividad Wan ó Internet. Estas soluciones ofrecen seguridad informática, conectividad y performance a la medida de los clientes con un bajo costo en el mercado." [36]

#### *6.1.4.1Hardware*


**Figura 9.** Appliance Fortinet 90D**: [37]**

A continuación se expone las características físicas de un *appliance* **Fortigate 90D.** Los otros modelos de la serie 90D son similares en dimensiones, condiciones de operación y formas de instalación, se diferencian a nivel de hardware en cantidad de puertos PoE, puertos de Switch e interfaces inalámbricas. En cuanto a *performance* se diferencian en el *Throughput* que manejan, la alimentación eléctrica que requieren y la disipación de calor que son capaces de realizar.

El firewall **Fortigate 90D,** no es un chasis, es un equipo que no tiene la posibilidad de instalar nuevos módulos o tarjetas. En cuanto a *performance* y capacidades cuenta con:

- Throughput (bytes) de 3,5 Gbps.
- Latencia de 4 µs.
- Throughput (paquetes) de 5,3 Mbps.
- Soporta 2´000.000 de sesiones establecidas en simultáneo.
- Soporta el inicio de 4.000 sesiones por segundo.
- Configuración de 5.000 políticas de seguridad.

- Throughput VPN (paquetes de 512 bytes) de 1 Gbps.
- Establece 200 túneles VPN *site-to-site*.
- Establece 1000 túneles VPN-SSL *client-to-site.*
- Throughput de VPN *client-to-site* de 35 Mbps.
- Maneja 10 Dominios virtuales.
- Maneja 100 FortiTokens.
- Alcance máximo de 200 clientes registrados
- Configuración HA : Activo/Activo , Activo/Pasivo, En clúster.

El *appliance* del modelo **Fortigate 90D** está compuesto de:

- 2 Interfaces Wan (GE RJ45).
- 14 Interfaces Switchport.
- 1 puerto USB.
- 1 Puerto de consola RJ45
- Almacenamiento interno de 32 GB.
- Requiere alimentación eléctrica de 100-240 V AC / 50-60 Hz.
- Soporta corriente máxima de 110 V /1.5 A; 220 V / 0.75 A.
- Consume de 18 a 22 Watts.
- Temperatura ambiente de operación tolerable de 0 a 40 °C.
- Procesador especial FortiASIC SOC2, que permite mejorar el rendimiento de los firewall, diseñado a medida para suplir las necesidades de procesamiento de los mismos.

#### *6.1.4.2 El dispositivo permite*

El firewall **Fortigate 90 D** es una de las mejores alternativas en cuanto a opciones funcionales y económicas se refiere. Puede ser utilizado como un dispositivo de escritorio y no requiere necesariamente de un entorno de Data Center para ofrecer un buen *performance.* Los modelos **Fortigate 90 D,** tienen funcionalidades PoE y son convergentes en ámbitos inalámbricos.

Tiene 4 *features* expansibles que lo caracterizan de otras alternativas en el mercado.

- **FortiAP:**

Es el mecanismo de integración del ámbito inalámbrico con el dispositivo **Fortigate**. Permite configurar ambientes seguros de control de acceso desde redes inalámbricas WLAN, manejando parámetros de rendimiento a través de una consola de controladora inalámbrica, que cuenta con módulos como **FortiManager**, **FortiAnalyzer** y un manejo centralizado de administración y reportes. [38]

**- FortiClient:**

Es el agente VPN que se instala en los dispositivos terminales para establecer túneles de comunicación segura a través de internet. Este *feature* permite la operación de Antivirus en tiempo real, el soporte de conexión de túneles VPN IPSec y SSL, siendo compatible con

múltiples plataformas desde *smartphones*, *tablets*, computadores portátiles hasta computadores de escritorio.

Cuenta con un motor automático de actualizaciones de los agentes y tiene un control avanzado sobre manejo de amenazas. [39]

**- FortiToken:**

Es un *feature* designado para administrar identidades de usuarios. El uso de **FortiToken** radica en un mecanismo de autenticación que tienen los usuarios para acceder a redes protegidas y dispositivos de seguridad. Los métodos de autenticación están basados en el concepto de las PKI (*Public Key Infrastructure*) y pueden ser utilizados a través de un aplicativo en un *smartphones,* de un dispositivo *Token* generador de códigos numéricos (como los del ámbito bancario) ó una PKI almacenada en un ejecutable de una memoria USB.

La solución de **FortiToken** debe ser complementada con otro *appliance* conocido como el ***User Identity Management FortiAuthenticato****r*. [40]

**- Forti Switch:**

Al igual que la solución **FortiToken**, este *feature* permite la integración entre equipos de alto rendimiento como la serie de *Switches* de Data Center y los Firewalls **Fortigate**. Permite que los Firewall tengan administración y total visibilidad de las conexiones, sesiones, cantidad de usuarios y dispositivos que acceden a la red a través de estos *Switches* de Data Center.

**FortiSwitch** permite mezclar dos mundos, el "mundo" de Data Center con equipamiento dedicado de gran ancho de banda donde se encuentran *throughputs* de 10 a 40 Gbps y el "mundo" de seguridad con *features* de control de acceso a los puertos basados en la tecnología 802.1X y en la administración y control centralizado desde los firewalls UTM. [41]

### *6.1.4.3 Software (funcionalidades)*

Una de las funcionalidades más innovadoras del firewall **Fortigate 90 D** es la posibilidad de poder ser administrado desde un *Smartphone* que opere bajo el sistema operativo IOS de Apple.

A través de la conexión del celular a l puerto usb del firewall y a través de la aplicación **iOS FortiExplorer App**, el administrador puede configurar parámetros de interés en cuanto al funcionamiento del firewall.

En cuanto a funcionalidades, **Fortigate 90D** maneja utilidades de un firewall común:

- Establecimiento de túneles VPN (SSL ó IPSec).
- Administración de Antivirus en los dispositivos pertenecientes a su dominio.

- Labores de IPS e IDS, con módulos especializados en la WEB Gui , que permiten monitorear todo el tráfico entrante y saliente, analizarlo y compararlo con numerosas firmas de Malware ya identificados, y a partir de allí emitir alarmas sobre ello o tomar medidas correctivas.
- Configuración de hasta 5000 políticas de seguridad.
- Existen *features* adicionales que permiten la administración de **FortiWan**, ideal para hacer balanceo de carga entre enlaces principales y redundantes.
- Compatible con **FortiMail** que permite añadir seguridad a todo el servicio de correo electrónico, evitando amenazas de inyecciones de código malicioso, intercepción de información e indisponibilidad del servicio.
- Compatible con **FortiWeb** que permite configurar un Firewall virtual basado en aplicaciones, donde la identidad de los usuarios se adquiere de forma inteligente a través de la solicitud de credenciales de distintos sitios Web o aplicaciones
- Compatible con **FortiDB**, con características de protección especiales para todos los servidores, aplicativos y discos de almacenamiento relacionados con bases de datos.
- Compatible con **FortiDDoS**, que se encarga de mitigar al máximo todos los ataques de denegación de servicio provenientes desde Internet.

#### *6.1.4.4 Licenciamiento:*

Maneja un licenciamiento simplificado, con un número ilimitado de usuarios para despliegue de diferentes *features.* Cada *feature* adicional tiene su propio licenciamiento y su precio está indicado en la página web del fabricante.

#### *6.1.4.5 Precio en el mercado*

El precio de adquisición de un Fortigate 90D o de los demás dispositivos de la serie 90D, oscila entre los U$750 y los U$9800, dependiendo de la cantidad de licencias y *features* que se pretendan obtener.

## 6.2 Selección de Criterios

En esta instancia se seleccionan los criterios generales que permiten juzgar cada alternativa y valorarla numéricamente, para obtener información suficiente que permita realizar un estudio comparativo que identifique cuál de las soluciones propuestas es más idónea para la necesidad de negocio presente.

El mecanismo de selección de los criterios se fundamenta en la revisión bibliográfica, la revisión técnica, las preguntas a expertos y a partir de la experiencia obtenida en el ámbito laboral, en el "quehacer" diario de las compañías *Service Provider*. De allí, se obtiene un gran conjunto de criterios que permiten calificar las alternativas, pero se identificaron tres factores en común que tienen en cuenta los clientes, los gerentes de proyecto y los

comerciales, a la hora de comprar/vender servicios de tecnología, ya sea en la modalidad de *Housing* (Infraestructura dedicada) *o Hosting* (Infraestructura compartida):

- Factor Económico.

- Factor Técnico.

- Factor Humano.

### 6.2.1 Factor Económico:

Este aspecto está directamente relacionado con la capacidad económica y el músculo financiero que tienen las compañías al momento de comprar, implementar, administrar y mantener en operación cualquiera de las soluciones propuestas.

#### *6.2.1.1 Capacidad Adquisitiva:*

Referente al presupuesto con el que cuenta la compañía para comprar o rentar servicios de alguna de las soluciones propuestas. Este parámetro responde a los cuestionamientos: ¿La empresa cuenta con el dinero suficiente para adquirir la solución?, ¿la empresa tiene la capacidad de contratar soporte directo con el fabricante?, ¿qué tipo de soporte puede contratar la empresa a partir de sus capacidades económicas?, ¿la empresa puede adquirir todas las licencias que necesita para sacar el mayor provecho a la solución?

#### *6.2.1.2 Capacidad de administración y Operación:*

Referente al presupuesto con el que cuentan las compañías para administrar, mantener en operación y actualizar cualquiera de las soluciones propuestas. Este parámetro responde a los cuestionamientos: ¿La empresa cuenta con personal capacitado que administre la solución? , ¿La solución resolverá de la mejor forma los requerimientos de los usuarios?, ¿La empresa cuenta con equipos especializados, mediante los cuales se administre la solución propuesta?

#### *6.2.1.3 Capacidad de Infraestructura:*

Referente al tipo de infraestructura que tienen las compañías para desplegar la solución contratada .Este parámetro responde a los cuestionamientos: ¿La empresa cuenta con espacios adecuados para el despliegue de la solución?, ¿qué capacidad económica tiene la empresa para adecuar espacios que permitan el correcto despliegue de la solución?, ¿la empresa cuenta con entornos de Data Center? ¿Qué clasificación tienen los espacios de Data Center de la empresa?¿Se puede adquirir configuraciones de HA (Alta disponibilidad)?

### 6.2.2 Factor Técnico:

Este aspecto está orientado hacia el correcto estudio de necesidades, rendimientos y recursos técnicos presentes en las compañías, para hacer una selección acertada y objetiva de alguna de las soluciones propuestas. La **Guía para compradores de Firewall** de **Palo Alto Networks** [42], sugiere que se evalúen los siguientes criterios, a la hora de seleccionar un dispositivo de seguridad:

#### *6.2.2.1 Visibilidad y control de aplicaciones:*

¿Cómo maneja la solución la clasificación de tráfico a partir de la identidad de las aplicaciones y no exclusivamente del puerto que utilicen? ¿Cómo la solución tiene en cuenta la identificación y control de las aplicaciones evasivas que utilizan SSL o SSH con tráfico encriptado?

#### *6.2.2.2 Prevención de amenazas:*

¿Cómo se garantiza la seguridad del dispositivo sin disminuir el rendimiento del mismo, en un entorno real caracterizado por amenazas que acceden a la red de forma comprimida por puertos alternativos? ¿Qué capacidad de verificación y que técnicas de prevención (IPS,IDS,Malware y Contenido) utiliza la solución ?

#### *6.2.2.3 Controles de seguridad para acceso a distancia:*

¿Cómo se garantiza que los accesos a distancia sean tratados con la misma política empleada para accesos internos?, ¿Qué grado de complejidad tiene la administración e instalación de herramientas que permitan el acceso a distancia? ¿La solución garantiza la seguridad de los accesos remotos a través de conexiones SSL VPN?

#### *6.2.2.4 Administración:*

¿Qué grado de complejidad tiene la administración del dispositivo? ¿Cuál es el grado de disponibilidad que tienen las herramientas de visualización que ofrece la solución? ¿Se pueden ejecutar tares de control de seguridad de aplicaciones, ejercer controles de Firewall y aplicar funciones preventivas desde un mismo editor? ¿Cómo se puede acceder a la administración de la solución: mediante navegador web o mediante CLI?

#### *6.2.2.5 Rendimiento:*

¿La solución rinde de forma óptima teniendo en cuenta el tamaño de la compañía?, ¿La solución es sobre utilizado o subutilizada? ¿Es estable la solución o presenta constantes eventos de indisponibilidad? ¿Se puede medir el rendimiento?

### 6.2.3 Factor Humano:

Referente al impacto que genera cada una de las soluciones en la calidad de vida de los usuarios, clientes, proveedores, empleados, etc., y como este impacto beneficia a la empresa que adquiere la solución.

#### *6.2.3.1 Optimización de tareas:*

Este aspecto verifica si la solución propuesta permite aumentar el rendimiento de las labores ejecutadas por el personal humano, verificando si las funcionalidades que ofrece la solución optimizan y permite obtener mejores resultados de las tareas realizadas.

#### *6.2.3.2 Desarrollo de habilidades:*

¿La implementación de alguna de las soluciones propuestas, impulsa el desarrollo de habilidades y adquisición de *skills* por parte de los empleados o los usuarios?

#### *6.2.3.3 Inclusión social:*

¿Cómo las soluciones propuestas, pueden mejorar la calidad de vida las personas, permitiendo la inclusión de personas discapacitadas a ambientes laborales, instalando estaciones remotas de trabajo?

#### *6.2.3.4 Generación de oportunidades:*

¿Cómo impulsa el crecimiento y a la expansión de mercados de las compañías, la adopción de alguna de las soluciones?, ¿Que nuevas oportunidades de negocio pueden surgir a partir de las funcionalidades de las soluciones propuestas?

## 7. RESULTADOS

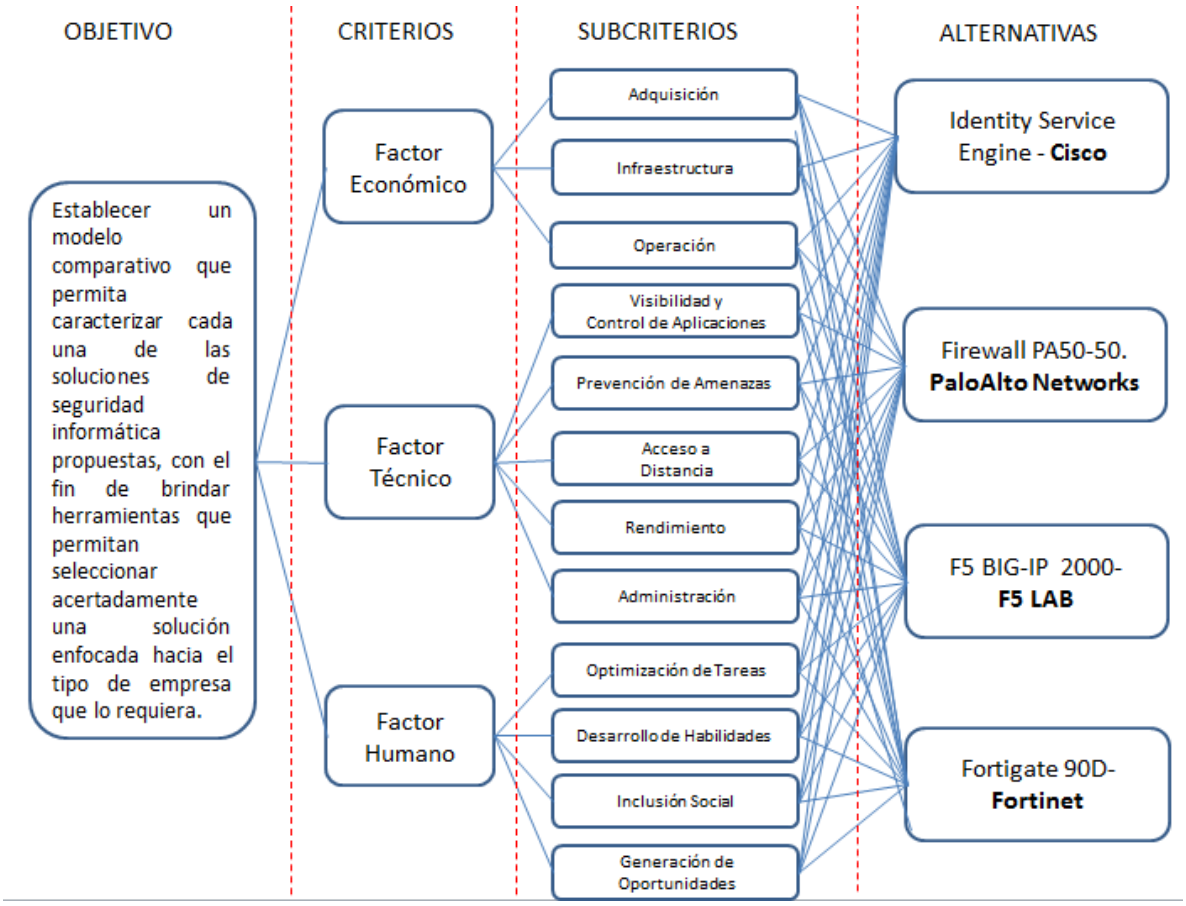


**Figura 10.** Esquema jerárquico del modelo de selección de herramientas de seguridad.

La formulación de matrices de comparación, fueron realizadas en tres niveles: en el nivel de **criterios**, donde especifica cuál de los tres factores es más importante a la hora de tomar la decisión. En el nivel de **subcriterios**, donde se especifica que tópico (subcriterio) tiene más importancia en el interior de cada uno de los criterios de selección. Y en el nivel de alternativas, donde se especifica que alternativa cumple de forma más adecuada con cada uno de los tópicos (subcriterios) analizados.

La evaluación de parámetros se realiza a partir de la escala de valores de **Saaty (Tabla 1)**:

**7.1 Evaluación de Criterios frente al Objetivo General:**

Esta etapa de valoración inicial tiene como objetivo identificar ¿Qué peso tiene cada criterio al momento de seleccionar una alternativa que cumpla con los objetivos propuestos?

Esta primera valoración se aplica a partir de la importancia del aspecto económico, técnico y humano que caracterizan a las compañías, las cuales establecen un camino de prioridades a la hora de adquirir una solución de seguridad informática.

***NOTA:*** Todas las valoraciones fueron realizadas a partir de un consenso general con integrantes del *pool* de *Networking* y Seguridad de una compañía proveedora de servicios de *Hosting* y *Housing.*

Todo el proceso matemático de obtención de matrices, matrices normalizadas, vectores propios y porcentajes de peso esta descrito en el marco teórico Pag:

Matriz de comparación entre **criterios:**

| | **Factor Económico** | **Factor Técnico** | **Factor Humano** |
|---|---|---|---|
| **Factor Económico** | 1 | 1/3 | 4 |
| **Factor Técnico** | 3 | 1 | 5 |
| **Factor Humano** | 1/4 | 1/5 | 1 |

**Tabla 5.** Matriz de comparación entre criterios

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **Factor Económico** | **Factor Técnico** | **Factor Humano** |
|---|---|---|---|
| **Factor Económico** | 0,235 | 0,217 | 0,400 |
| **Factor Técnico** | 0,706 | 0,652 | 0,500 |
| **Factor Humano** | 0,059 | 0,130 | 0,100 |

**Tabla 6.** Matriz normalizada de comparación entre criterios.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" de cada criterio:

**Factor Económico**: $0{,}284 = \mathbf{28}\ \%$

**Factor Técnico**: $= 0{,}619 = \mathbf{62}\ \%$

**Factor humano**: $= 0{,}096 = \mathbf{10}\ \%$

### 7.2 Evaluación de Subcriterios frente a Criterios.

Esta segunda etapa de valoración, tiene como objetivo desglosar en subcriterios o dependencias, cada uno de los criterios anteriormente seleccionados. Lo cual permite plantear y solucionar cuestionamientos cómo: ¿De qué depende la importancia de cada criterio? Y ¿Qué peso tiene cada una de esas dependencias a la hora de seleccionar una alternativa?

#### 7.2.1 Factor Económico

Esta valoración se aplica a partir de la importancia que tiene el poder adquisitivo, el poder de administración y la capacidad a nivel de infraestructura que tienen las compañías para desplegar cualquiera de las soluciones de seguridad informática propuesta.

Matriz de comparación entre **subcriterios / factor económico:**

| | **Adquisición** | **Infraestructura** | **Operación** |
|---|---|---|---|
| **Adquisición** | 1 | **3** | **5** |
| **Infraestructura** | **1/3** | **1** | **3** |
| **Operación** | **1/5** | **1/3** | **1** |

**Tabla 7**. Matriz de comparación de subcriterios/ factor económico.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **Adquisición** | **Infraestructura** | **Operación** |
|---|---|---|---|
| **Adquisición** | 0,652 | 0,692 | 0,555 |
| **Infraestructura** | 0,217 | 0,230 | 0,333 |
| **Operación** | 0,130 | 0,076 | 0,111 |

**Tabla 8**. Matriz normalizada de comparación de subcriterios/ factor económico.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de cada criterio:

**Adquisición**: 0,633 $= \mathbf{63}\%$

**Infraestructura**: 0,26 $= \mathbf{26}\ \%$

**Operación:** 0,105 $= \mathbf{11}\ \%$

### 7.2.2 Factor Técnico

Esta valoración se aplica a partir de la importancia que tiene la visibilidad y el control de aplicaciones, la prevención de amenazas, el grado de complejidad en la administración de las herramientas, los controles de seguridad para acceso a distancia y el rendimiento que ofrece cada una de las alternativas propuestas.

Matriz de comparación entre **subcriterios / factor técnico:**

| | **Visibilidad y Control** | **Prevención de Amenazas** | **Acceso a distancia** | **Rendimiento** | **Administración** |
|---|---|---|---|---|---|
| **Visibilidad y Control** | 1 | 1/3 | 3 | 1/4 | 4 |
| **Prevención de amenazas** | 3 | 1 | 4 | 1/4 | 6 |
| **Acceso a distancia** | 1/3 | 1/4 | 1 | 1/5 | 3 |
| **Rendimiento** | 4 | 3 | 5 | 1 | 7 |
| **Administración** | 1/4 | 1/6 | 1/3 | 1/7 | 1 |

**Tabla 9.** Matriz de comparación de subcriterios / factor técnico**.**

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **Visibilidad y Control** | **Prevención de Amenazas** | **Acceso a distancia** | **Rendimiento** | **Administración** |
|---|---|---|---|---|---|
| **Visibilidad y Control** | 0,117 | 0,070 | 0,225 | 0,136 | 0,190 |
| **Prevención de amenazas** | 0,350 | 0,211 | 0,300 | 0,136 | 0,286 |
| **Acceso a distancia** | 0,039 | 0,053 | 0,075 | 0,109 | 0,143 |
| **Rendimiento** | 0,466 | 0,632 | 0,375 | 0,543 | 0,333 |
| **Administración** | 0,029 | 0,035 | 0,025 | 0,078 | 0,048 |

**Tabla 10**. Matriz normalizada de comparación de subcriterios/ factor técnico.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de cada criterio:

Visibilidad y control: $= 0{,}15 = \mathbf{15}\%$

Prevención de amenazas: $= 0{,}254 = \mathbf{25}\%$

Acceso a distancia: $= 0{,}08 = \mathbf{8}\%$

Rendimiento: $= 0{,}47 = \mathbf{47}\%$

Administración: $= 0{,}05 = \mathbf{5}\%$

### 7.2.3 Factor Humano

Esta valoración se aplica a partir de la importancia que tiene la optimización de tareas, el desarrollo de habilidades, la inclusión social y la generación de oportunidades, en cuanto al impacto social y humanitario que genera la implementación y utilización de cada una de las soluciones propuestas.

Matriz de comparación entre **subcriterios / factor humano:**

| | **Optimización de tareas** | **Desarrollo de Habilidades** | **Inclusión social** | **Generación de Oportunidades** |
|---|---|---|---|---|
| **Optimización de tareas** | 1 | 2 | 4 | 5 |
| **Desarrollo de Habilidades** | 1/2 | 1 | 3 | 4 |
| **Inclusión social** | 1/4 | 1/3 | 1 | 2 |
| **Generación de Oportunidades** | 1/5 | 1/4 | 1/2 | 1 |

**Tabla 11.** Matriz de comparación de subcriterios / factor humano.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | Optimización de tareas | Desarrollo de Habilidades | Inclusión social | Generación de Oportunidades |
|---|---|---|---|---|
| **Optimización de tareas** | 0,513 | 0,558 | 0,471 | 0,417 |
| **Desarrollo de Habilidades** | 0,256 | 0,279 | 0,353 | 0,333 |
| **Inclusión social** | 0,128 | 0,093 | 0,118 | 0,167 |
| **Generación de Oportunidades** | 0,103 | 0,070 | 0,059 | 0,083 |

**Tabla 12**. Matriz normalizada de comparación de subcriterios/ factor humano.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de cada criterio:

Optimización de Tareas: $= 0{,}490 = \mathbf{49}\%$

Desarrollo de Habilidades: $= 0{,}31 = \mathbf{31}\%$

Inclusión social: $= 0{,}13 = \mathbf{13}\%$

Generación de oportunidades: $0{,}07 = \mathbf{7}\%$

### 7.3 Evaluación de Alternativas frente a Subcriterios.

La selección de las alternativas propuestas se lleva a cabo a partir de la experiencia laboral adquirida en la empresa *Service Provider*, ya que allí se manejan estas soluciones para brindar servicios de seguridad informática, control de acceso, administración de redes y de aplicaciones. Además, son las soluciones más utilizadas y que más se ofrecen a los clientes para cumplir con los requerimientos empresariales

En esta última etapa de valoración, se tiene como objetivo evidenciar que alternativa cumple de la forma más adecuada con cada uno de los subcriterios propuestos.

Esta valoración permitirá caracterizar la importancia de cada alternativa con respecto a aspectos puntuales, lo cual permite realizar un análisis granular de ventajas y desventajas de las mismas.

Estos son los últimos porcentajes de "pesos" que se obtienen para proceder con el cálculo de la "importancia" general que tiene cada una de las alternativas, en la búsqueda de cumplir con todos los objetivos propuestos.

### 7.3.1 Capacidad de adquisición

Matriz de comparación entre **Alternativas / capacidad de adquisición:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 1/3 | 1/6 | 1/8 |
| **PA50-50** | 3 | 1 | 1/5 | 1/7 |
| **BIG-IP 2000** | 6 | 5 | 1 | 1/5 |
| **Fortigate 90D** | 8 | 7 | 5 | 1 |

**Tabla 13.** Matriz de comparación alternativas/ capacidad de adquisición.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,056 | 0,025 | 0,026 | 0,085 |
| **PA50-50** | 0,167 | 0,075 | 0,031 | 0,097 |
| **BIG-IP 2000** | 0,333 | 0,375 | 0,157 | 0,136 |
| **Fortigate 90D** | 0,444 | 0,525 | 0,785 | 0,681 |

**Tabla 14**. Matriz normalizada de comparación alternativas/ capacidad de adquisición.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,05 = **5**%

Firewall PA50-50: = 0,09 = **9** %

BIG-IP 2000: = 0,25 = **25** %

Fortigate 90D: = 0,61 = **61**%

### 7.3.2 Capacidad de Infraestructura:

Matriz de comparación entre **Alternativas / capacidad de Infraestructura:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 5 | 2 | 1/4 |
| **PA50-50** | 1/5 | 1 | 1/2 | 1/6 |
| **BIG-IP 2000** | 1/2 | 2 | 1 | 1/3 |
| **Fortigate 90D** | 4 | 6 | 3 | 1 |

**Tabla 15**. Matriz de comparación de alternativas/ Capacidad de Infraestructura.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,175 | 0,357 | 0,308 | 0,143 |
| **PA50-50** | 0,035 | 0,071 | 0,077 | 0,095 |
| **BIG-IP 2000** | 0,088 | 0,143 | 0,154 | 0,190 |
| **Fortigate 90D** | 0,702 | 0,429 | 0,462 | 0,571 |

**Tabla 16**. Matriz normalizada de comparación de alternativas/ Capacidad de Infraestructura.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,25 = **25**%

Firewall PA50-50: = 0,07 = **7** %

BIG-IP 2000: = 0,14 = **14** %

Fortigate 90D: = 0,54 = **54**%

### 7.3.3 Capacidad de Operación:

Matriz de comparación entre **Alternativas / capacidad de operación:**

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 1 | ¼ | 2 | 1/8 |
| **PA50-50** | 4 | 1 | 5 | 1/4 |
| **BIG-IP 2000** | 1/2 | 1/5 | 1 | 1/9 |
| **Fortigate 90D** | 8 | 4 | 9 | 1 |

**Tabla 17**. Matriz de comparación de alternativas/ capacidad de operación.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 0,074 | 0,046 | 0,118 | 0,084 |
| **PA50-50** | 0,296 | 0,183 | 0,294 | 0,168 |
| **BIG-IP 2000** | 0,037 | 0,037 | 0,059 | 0,075 |
| **Fortigate 90D** | 0,593 | 0,734 | 0,529 | 0,673 |

**Tabla 18**. Matriz normalizada de comparación de alternativas/ capacidad de operación.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,08 = 8%

Firewall PA50-50: = 0,24 = **24** %

BIG-IP 2000: = 0,05 = **5** %

Fortigate 90D: = 0,63 = **63**%

### 7.3.4 Visibilidad y Control de aplicaciones:

Matriz de comparación entre **Alternativas / Visibilidad y Control de aplicaciones:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 1/3 | 4 | 8 |
| **PA50-50** | 3 | 1 | 5 | 9 |
| **BIG-IP 2000** | 1/4 | 1/5 | 1 | 3 |
| **Fortigate 90D** | 1/8 | 1/9 | 1/3 | 1 |

**Tabla 19**.Matriz de comparación de alternativas / Visibilidad y Control de aplicaciones.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,229 | 0,203 | 0,387 | 0,364 |
| **PA50-50** | 0,686 | 0,608 | 0,484 | 0,409 |
| **BIG-IP 2000** | 0,057 | 0,122 | 0,097 | 0,182 |
| **Fortigate 90D** | 0,029 | 0,068 | 0,032 | 0,045 |

**Tabla 20**. Matriz normalizada de comparación de alternativas / Visibilidad y control de aplicaciones.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,3 = **30**%

Firewall PA50-50: = 0,55 = **55** %

BIG-IP 2000: = 0,11 = **11** %

Fortigate 90D: = 0,04 = **4** %

### 7.3.5 Prevención de amenazas:

Matriz de comparación entre **Alternativas / Prevención de amenazas:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 1/4 | 4 | 6 |
| **PA50-50** | 4 | 1 | 5 | 7 |
| **BIG-IP 2000** | 1/4 | 1/5 | 1 | 5 |
| **Fortigate 90D** | 1/6 | 1/7 | 1/5 | 1 |

**Tabla 21.** Matriz de comparación de alternativas / Prevención de amenazas.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,185 | 0,157 | 0,392 | 0,316 |
| **PA50-50** | 0,738 | 0,628 | 0,490 | 0,368 |
| **BIG-IP 2000** | 0,046 | 0,126 | 0,098 | 0,263 |
| **Fortigate 90D** | 0,031 | 0,090 | 0,020 | 0,053 |

**Tabla 22**. Matriz normalizada de comparación de alternativas / Prevención de amenazas.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,26 = **26**%

Firewall PA50-50: = 0,56 = **56** %

BIG-IP 2000: = 0,13 = **13** %

Fortigate 90D: = 0,05 = **5** %

### 7.3.6 Acceso a distancia:

Matriz de comparación entre **Alternativas / Acceso a distancia:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 6 | 8 | 9 |
| **PA50-50** | 1/6 | 1 | 5 | 7 |
| **BIG-IP 2000** | 1/8 | 1/5 | 1 | 5 |
| **Fortigate 90D** | 1/9 | 1/7 | 1/5 | 1 |

**Tabla 23**. Matriz de comparación de alternativas/ Acceso a distancia.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,713 | 0,817 | 0,563 | 0,409 |
| **PA50-50** | 0,119 | 0,136 | 0,352 | 0,318 |
| **BIG-IP 2000** | 0,089 | 0,027 | 0,070 | 0,227 |
| **Fortigate 90D** | 0,079 | 0,019 | 0,014 | 0,045 |

**Tabla 24**. Matriz normalizada de comparación de alternativas / Acceso a distancia.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,63 = **63**%

Firewall PA50-50: = 0,23 = **23** %

BIG-IP 2000: = 0,1 = **10** %

Fortigate 90D: = 0,04 = **4** %

### 7.3.7 Rendimiento:

Matriz de comparación entre **Alternativas / Rendimiento:**

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 1 | 2 | 5 | 8 |
| **PA50-50** | 1/2 | 1 | 4 | 7 |
| **BIG-IP 2000** | 1/5 | ¼ | 1 | 5 |
| **Fortigate 90D** | 1/8 | 1/7 | 1/5 | 1 |

**Tabla 25**.Matriz de comparación de alternativas / Rendimiento.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 0,548 | 0,589 | 0,490 | 0,381 |
| **PA50-50** | 0,274 | 0,295 | 0,392 | 0,333 |
| **BIG-IP 2000** | 0,110 | 0,074 | 0,098 | 0,238 |
| **Fortigate 90D** | 0,068 | 0,042 | 0,020 | 0,048 |

**Tabla 26.** Matriz normalizada de comparación de alternativas / Rendimiento.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,5 = **50**%

Firewall PA50-50: = 0,32 = **32**%

BIG-IP 2000: = 0,13 = **13** %

Fortigate 90D: = 0,05 = **5** %

### 7.3.8 Facilidades de administración:

Matriz de comparación entre **Alternativas / Facilidades de Administración:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 1/4 | 1/2 | 1/3 |
| **PA50-50** | 4 | 1 | 5 | 3 |
| **BIG-IP 2000** | 2 | 1/5 | 1 | 1/3 |
| **Fortigate 90D** | 3 | 1/3 | 3 | 1 |

**Tabla 27**.Matriz de comparación de alternativas/ Facilidades de Administración.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,100 | 0,140 | 0,053 | 0,071 |
| **PA50-50** | 0,400 | 0,561 | 0,526 | 0,643 |
| **BIG-IP 2000** | 0,200 | 0,112 | 0,105 | 0,071 |
| **Fortigate 90D** | 0,300 | 0,187 | 0,316 | 0,214 |

**Tabla 28**.Matriz normalizada de comparación de alternativas/ Facilidades de Administración.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,09 = **9**%

Firewall PA50-50: = 0,53 = **53**%

BIG-IP 2000: = 0,12 = **12** %

Fortigate 90D: = 0,25 = 2**5** %

### 7.3.9 Optimización de tareas:

Matriz de comparación entre **Alternativas / Optimización de tareas:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 5 | 4 | 6 |
| **PA50-50** | 1/5 | 1 | 3 | 4 |
| **BIG-IP 2000** | 1/4 | 4 | 1 | 5 |
| **Fortigate 90D** | 1/6 | 1/4 | 1/5 | 1 |

**Tabla 29**.Matriz de comparación de alternativas / Optimización de tareas.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,619 | 0,488 | 0,488 | 0,375 |
| **PA50-50** | 0,124 | 0,098 | 0,366 | 0,250 |
| **BIG-IP 2000** | 0,155 | 0,390 | 0,122 | 0,313 |
| **Fortigate 90D** | 0,103 | 0,024 | 0,024 | 0,063 |

**Tabla 30**.Matriz normalizada de comparación de alternativas/ Optimización de tareas.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,49 = 4**9**%

Firewall PA50-50: = 0,21 = **21**%

BIG-IP 2000: = 0,24 = **24** %

Fortigate 90D: = 0,05 = **5** %

### 7.3.10 Desarrollo de Habilidades:

Matriz de comparación entre **Alternativas / Desarrollo de Habilidades:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 3 | 4 | 7 |
| **PA50-50** | 1/3 | 1 | 3 | 5 |
| **BIG-IP 2000** | 1/4 | 1/3 | 1 | 4 |
| **Fortigate 90D** | 1/7 | 1/5 | 1/4 | 1 |

**Tabla 31**. Matriz de comparación de alternativas / Desarrollo de habilidades.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,579 | 0,662 | 0,485 | 0,412 |
| **PA50-50** | 0,193 | 0,221 | 0,364 | 0,294 |
| **BIG-IP 2000** | 0,145 | 0,074 | 0,121 | 0,235 |
| **Fortigate 90D** | 0,083 | 0,044 | 0,030 | 0,059 |

**Tabla 32**. Matriz normalizada de comparación de alternativas / Desarrollo de habilidades.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,53 = **53**%

Firewall PA50-50: = 0,27 = **27**%

BIG-IP 2000: = 0,14 = **14** %

Fortigate 90D: = 0,06 = **6** %

### 7.3.11 Inclusión social:

Matriz de comparación entre **Alternativas / Inclusión social:**

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 1 | 3 | 8 | 5 |
| **PA50-50** | 1/3 | 1 | 7 | 4 |
| **BIG-IP 2000** | 1/8 | 1/7 | 1 | 1/5 |
| **Fortigate 90D** | 1/5 | 1/4 | 5 | 1 |

**Tabla 33**.Matriz de comparación de alternativas / Inclusión social.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | ISE | PA50-50 | BIG-IP 2000 | Fortigate 90D |
|---|---|---|---|---|
| **ISE** | 0,603 | 0,683 | 0,381 | 0,490 |
| **PA50-50** | 0,201 | 0,228 | 0,333 | 0,392 |
| **BIG-IP 2000** | 0,075 | 0,033 | 0,048 | 0,020 |
| **Fortigate 90D** | 0,121 | 0,057 | 0,238 | 0,098 |

**Tabla 34**.Matriz normalizada de comparación de alternativas / Inclusión social.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,54 = **54**%

Firewall PA50-50: = 0,29 = **29**%

BIG-IP 2000: = 0,04 = **4** %

Fortigate 90D: = 0,13 = **13** %

### 7.3.12 Generación de oportunidades:

Matriz de comparación entre **Alternativas / Generación de oportunidades:**

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 1 | 2 | 5 | 7 |
| **PA50-50** | 1/2 | 1 | 4 | 6 |
| **BIG-IP 2000** | 1/5 | 1/4 | 1 | 3 |
| **Fortigate 90D** | 1/7 | 1/6 | 1/3 | 1 |

**Tabla 35**.Matriz de comparación de alternativas / Generación de oportunidades.

Obtención de pesos: Matriz normalizada y vector propio de cada criterio de selección:

| | **ISE** | **PA50-50** | **BIG-IP 2000** | **Fortigate 90D** |
|---|---|---|---|---|
| **ISE** | 0,543 | 0,585 | 0,484 | 0,412 |
| **PA50-50** | 0,271 | 0,293 | 0,387 | 0,353 |
| **BIG-IP 2000** | 0,109 | 0,073 | 0,097 | 0,176 |
| **Fortigate 90D** | 0,078 | 0,049 | 0,032 | 0,059 |

**Tabla 36**.Matriz normalizada de alternativas / Generación de oportunidades.

Luego de obtener la matriz normalizada, se procede a obtener el "peso" (vector propio) de alternativa frente al criterio establecido:

Identity Service Engine= 0,51 = **51**%

Firewall PA50-50: = 0,33 = **33**%

BIG-IP 2000: = 0,11 = **11**%

Fortigate 90D: = 0,05 = **5** %

### 7.4 Obtención de peso general de cada alternativa propuesta

En esta etapa se realiza la sumatoria de los productos de todas los "pesos" contemplados, obteniendo el peso o la importancia general de cada solución propuesta respecto al cumplimiento de los objetivos trazados.

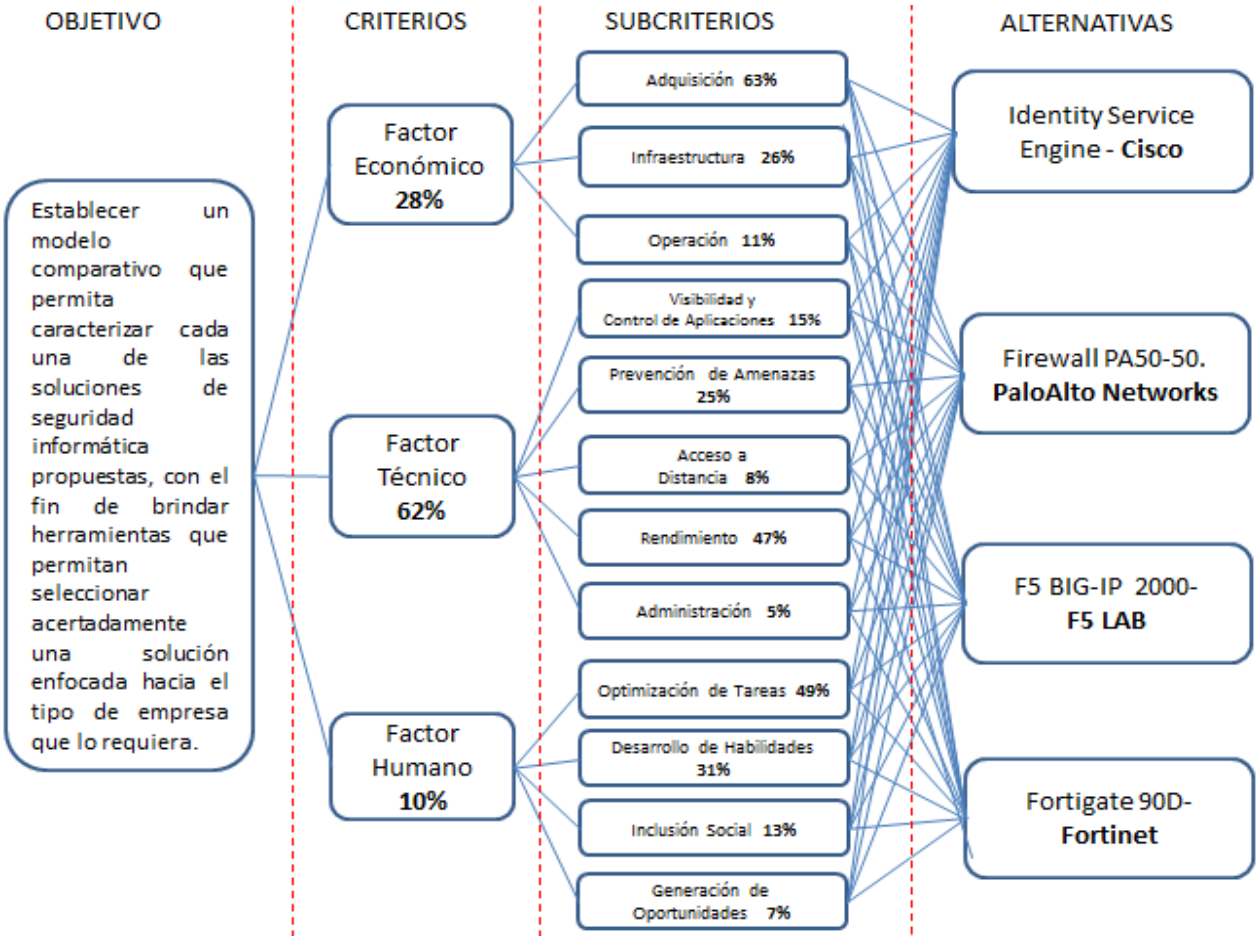


**Figura 11** Esquema jerárquico del modelo de selección de herramientas de seguridad con porcentajes de peso.

Este resultado permite concluir de manera general, cual es la alternativa más idónea y que más se acomoda a las condiciones económicas, técnicas y humanas de las compañías. El modelo es una propuesta que se compone de la formulación de criterios, subcriterios y alternativas, donde cada compañía o persona que desee tomar el modelo para realizar un proceso de selección objetivo de herramientas de seguridad, puede calificar cada uno de los parámetros a partir de su experiencia, convicción o recolección de información.

La siguiente tabla expone la relación existente entre las soluciones, los subcriterios y los criterios:

| SOLUCIONES | CRITERIOS | | | | | | | | | | | | Porcentaje de cada Solución |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Factor Economico | | | Factor Tecnico | | | | | Factor Humano | | | | |
| | 28% | | | 62% | | | | | 10% | | | | |
| | SUBCRITERIOS | | | | | | | | | | | | |
| | Adquisición | Infraestructura | Operación | Visibilidad | Prevención | Acceso a Distancia | Rendimiento | Administración | Optimización | Desarrollo de Hab. | inclusión | Generación Op. | Σ Total |
| | 63% | 26% | 11% | 15% | 25% | 8% | 47% | 5% | 49% | 31% | 13% | 7% | |
| Identity Service Engine | 0,05 | 0,25 | 0,08 | 0,30 | 0,26 | 0,63 | 0,50 | 0,09 | 0,49 | 0,53 | 0,54 | 0,51 | 0,32 |
| Firewall PA50-50 | 0,09 | 0,07 | 0,24 | 0,55 | 0,56 | 0,23 | 0,32 | 0,53 | 0,21 | 0,27 | 0,29 | 0,33 | 0,31 |
| BIG-IP 2000 | 0,25 | 0,14 | 0,05 | 0,11 | 0,13 | 0,10 | 0,13 | 0,12 | 0,24 | 0,14 | 0,04 | 0,11 | 0,16 |
| Fortigate 90 D | 0,61 | 0,54 | 0,63 | 0,04 | 0,05 | 0,04 | 0,05 | 0,25 | 0,05 | 0,06 | 0,13 | 0,05 | 0,21 |

**Tabla 37**. Matriz de comparación final de criterios/subcriterios/alternativas.

A continuación se exponen las operaciones realizadas para obtener el "peso" total de cada solución:

### *7.4.1 Identity Service Engine:*

$$28\% * (5\% * 63\% + 25\% * 26\% + 8\% * 11\%)$$

$$+$$

$$62\% \, (30\% * \ 15\% + 26\% * 25\% + 63\% * 8\% + 50\% * 47\% + 9\% * 5\%)$$

$$+$$

$$10\% \, (49\% * 49\% + 53\% * 31\% + 54\% * 13\% + 51\% * 7\%)$$

$$=$$

$$\textbf{Prioridad Total } \mathbf{0,32} \ = \mathbf{32}\%$$

Esta solución resulta ser la mejor de las cuatro alternativas propuestas, pues cumple de forma más acertada con los objetivos planteados y con los requerimientos generales de seguridad informática que tienen las empresas y las organizaciones.

Supera a las otras alternativas a nivel de funcionalidad, pues teniendo en cuenta los parámetros planteados de fomentar la convergencia de tecnologías, facilitar la autogestión de herramientas, fomentar el teletrabajo a partir de conexiones seguras y reforzar la seguridad de la información y de la infraestructura TI de las empresas y organizaciones, el ISE de Cisco cumple con las tareas de otros dispositivos como los ACS ( Access Control Server), IDS (Sistemas de detección de intrusos) y terminales de VPNs, además de ser compatibles con sistemas de directorio activo y servidores AAA, fusionando en una sola consola todas las labores de administración de dichos dispositivos.

A nivel de fomentar el teletrabajo y facilitar la autogestión de las herramientas, el ISE permite establecer conexiones remotas con altos niveles de seguridad, basando el control de acceso en múltiples variables y configuraciones, que sobrepasan los controles clásicos de usuarios y contraseñas, permitiendo organizar ambientes de trabajo para todo el personal de las empresas, donde tengan niveles de acceso basados en identidad de las personas, identidad de los dispositivos, identidad de los lugares de conexión y roles.

Finalmente, también es pertinente resaltar que el costo de adquisición de esta solución es mucho mayor que el de las otras alternativas propuestas, por ende requiere de un análisis profundo de costo/beneficio, con miras a no adquirir un producto costoso para subutilizarlo.

### *7.4.2 Firewall PA50-50:*

$$28\% * (9\% * 63\% + 7\% * 26\% + 24\% * 11\%)$$

$$+$$

$$62\% \ (55\% * \ 15\% + 56\% * 25\% + 23\% * 8\% + 32\% * 47\% + 53\% * 5\%)$$

$$+$$

$$10\% \ (21\% * 49\% + 27\% * 31\% + 29\% * 13\% + 33\% * 7\%)$$

$$=$$

$$\textbf{Prioridad Total } \mathbf{0,31 = 31}\%$$

Esta solución es la segunda mejor alternativa, debido a que tiene funcionalidades de Firewall para redes NGN.

Esta solución ataca un amplio espectro de amenazas informáticas y las mitiga o minimiza a partir de las funcionalidades que ofrece a través de su configuración. Maneja el control de acceso a partir de la creación de usuarios y grupos de usuarios a un nivel más limitado, pues entre sus funcionalidades no se contempla un análisis dedicado y granular como el que ofrecen otras soluciones especializadas en control de acceso como la solución ISE de Cisco.

Su frente de acción está directamente enfocado a la protección de redes corporativas y ambientes *service provider*. Es una solución bastante robusta y funcional para proteger la infraestructura a partir del análisis de tráfico basado en aplicaciones, diferenciándose de los firewalls tradicionales que analizan el tráfico a partir de la utilización de puertos.

Otro aspecto en el que supera a la solución Fortigate 90D, es la capacidad de virtualizar ambientes, generando instancias de firewalls independientes y autónomos, que promueven el uso compartido de la solución, lo cual puede ser un ahorro importante en infraestructura, debido a que un solo equipo puede suplir los requerimientos de numerosos clientes, sin la necesidad de tener un dispositivo dedicado para cada uno de ellos.

### *7.4.3 BIG-IP 2000 Series:*

$$28\% * (25\% * 63\% + 14\% * 26\% + 5\% * 11\%)$$

$$+$$

$$62\% \ (11\% * \ 15\% + 13\% * 25\% + 10\% * 8\% + 13\% * 47\% + 12\% * 5\%)$$

$$+$$

$$10\% \ (24\% * 49\% + 14\% * 31\% + 4\% * 13\% + 11\% * 7\%)$$

$$=$$

$$\textbf{Prioridad Total } \mathbf{0,16} = \ \mathbf{16}\%$$

Esta solución es la tercera mejor alternativa, debido a que su funcionalidad principal (con respecto a seguridad informática) es preservar la funcionalidad, la disponibilidad y la información de la infraestructura TI específicamente a nivel de las aplicaciones.

Maneja funcionalidades más rigurosas para brindar seguridad en las aplicaciones. Mientras que las alternativas de firewall analizan el tráfico a más bajo nivel (enlace de datos, red y transporte), el

BIG-IP 2000 series, analiza el tráfico que generan directamente las aplicaciones y brinda la seguridad necesaria a ese nivel.

Ataca directamente amenazas de tipo *cookie poisoning, sql injection* y *dns floods*, que buscan a partir de la modificación de los mensajes de datos de las aplicaciones, afectar su funcionamiento, su disponibilidad y degradar la experiencia del usuario.

A nivel económico, la adquisición y despliegue de esta solución es menos costosa que las anteriormente contempladas, pero debe ser profundamente analizada pues preserva principalmente solo un nivel de seguridad (el de las aplicaciones) y no tiene la misma robustez para preservar la información y la infraestructura en niveles más bajos (tráfico IP, de "capa 2" y de transporte), donde los firewalls y los sistemas de control de acceso son mucho más idóneos.

### *7.4.4 Fortigate 90D:*

$$28\% * (61\% * 63\% + 54\% * 26\% + 63\% * 11\%)$$

$$+$$

$$62\% \ (4\% * \ 15\% + 5\% * 25\% + 4\% * 8\% + 5\% * 47\% + 25\% * 5\%)$$

$$+$$

$$10\% \ (5\ \% * 49\% + 6\ \% * 31\% + 13\ \% * 13\% + 5\% * 7\%)$$

$$=$$

$$\textbf{Prioridad Total } \mathbf{0,21} = \mathbf{21}\%$$

Esta solución es la cuarta mejor alternativa, aunque a nivel económico sea la más fácil de adquirir y poner en operación, sus funcionalidades son limitadas en comparación a las otras alternativas propuestas.

Lo anterior no indica que la solución Fortigate 90D sea deficiente, al contrario es una de las mejores opciones de firewall que está diseñado e ideado para ambientes pequeños. Según la investigación realizada y las funcionalidades relacionadas en la descripción de la solución, este firewall cumple de forma acertada con los requerimientos de seguridad básicos de una red pequeña/mediana.

A su favor tiene que no requiere de las condiciones de Data Center que requieren las otras tres soluciones para su operación, sino que puede ser acomodado fácilmente en un ambiente de oficina. Aporta con la convergencia e integración de tecnologías, pues permite fusionar la administración de

las redes WLAN, de los sistemas de control de acceso y demás, a partir de una sola consola web, con soluciones del mismo fabricante.

Por último, aunque el dispositivo de por si posee limitaciones en sus funcionalidades en comparación con las otras alternativas propuestas, si es complementado con otras soluciones que provee el fabricante Fortinet como el FortiAP, FortiToken,FortiClient y Forti Switch, se puede llegar a obtener una solución robusta que ataque los frentes de conexiones remotas con alto nivel de seguridad, de preservación de la disponibilidad de la infraestructura de Data Center, y la gestión de control de acceso a partir de la identificación de usuarios y la utilización de Tokens.

# 8. CONCLUSIONES

1. En referencia al aspecto de convergencia tecnológica, se identifica que este es un objetivo común en todas las soluciones propuestas. Todas las soluciones ofrecen agrupar de forma funcional todos los dispositivos y la infraestructura tecnológica, para ponerla al servicio del negocio o proceso productivo de los clientes. También tienden a ofrecer cada día el aprovisionamiento de más y más servicios a través de una sola plataforma tecnológica, que incluye soluciones diversas de aplicaciones, de almacenamiento, de seguridad, de *networking*, etc.

   La convergencia tecnológica permite seguir la filosofía de la "Interoperabilidad de sistemas abiertos", donde se tiene como objetivo lograr una sinergia entre productos de diferentes fabricantes, en la cual se busca obtener el mejor rendimiento de cada uno de estos y potenciar las funcionalidades de las soluciones adquiridas, generando mejora continua y valor agregado en los clientes.

2. En cuanto al factor humano, es necesario cambiar la postura humano-máquina y cambiar a la perspectiva máquina-humano. Esto con el fin de disminuir la dependencia del hombre con los dispositivos e identificar como las nuevas tecnologías pueden aportar a mejorar la vida y el "qué hacer" diario de las personas.

   El factor humano debe ser la principal razón de la creación de nuevas tecnologías y gracias a esta premisa, se ha permitido darle acceso a la tecnología a un porcentaje mayor de la población, el cual orientándolo hacia el ambiente laboral, ha permitido cambiar el paradigma de las personas que tradicionalmente trabajan 5 días a la semana , 8 horas por día, inmersos en ambiente de oficina, que muchas veces no contribuye a la salud o al sano desarrollo de las relaciones familiares.

   Por ello la importancia del uso de estas herramientas se evidencia en la generación de puestos de empleo remotos, donde la gente pueda laborar desde su hogar, donde las personas en estado de discapacidad o mujeres embarazadas no tengan que desplazarse diariamente a un lugar para ser funcionales con la empresa donde trabajan. Finalmente, si se incluye más porcentaje de la población, se puede dar origen a más generación de empleo, al crecimiento de las empresas y al desarrollo de todo un país.

3. Por otro lado se afirmó que la relación costo/beneficio en la adquisición de herramientas de seguridad, es un tema de suma importancia. En el ámbito de la tecnología y con la reputación que tienen algunos fabricantes en el mercado, cada día puede tomar más fuerza la expresión "lo barato sale caro".

   Puesto que la relación costo/beneficio no puede ser limitada al precio de adquisición de los productos, sino que debe ser parte de un análisis completo de capacidades de dimensionamiento, de implementación, de uso y administración, en los que se debe

garantizar la infraestructura necesaria, el personal encargado adecuado y la proporcionalidad de rendimiento con la cantidad de usuarios a los que se van a ofrecer los servicios.

4. Es fundamental tener en cuenta más perspectivas de revisión o tener una visión más amplia del contexto actual de la necesidad tecnológica de las industrias colombianas, para elegir de forma idónea cualquiera de las alternativas propuestas. En la valoración de criterios se deben considerar la perspectiva del proveedor, del cliente, del administrador, de los usuarios, de los beneficiados y de los afectados para identificar que alternativa genera el mayor impacto positivo en ellos

5. En base a la experiencia laboral, se identifica que la solución más utilizada para administrar la seguridad informática y el *networking* de los clientes es el Firewall **PaloAlto PA50-50**, debido a que es la solución más integral. A nivel del cliente, es un elemento poli funcional, que permite administrar de forma óptima la seguridad informática de la infraestructura tecnológica y además sirve como enlace entre las redes internas LAN y las redes externas WAN o Internet. A nivel del proveedor, cuenta con la facilidad de crear instancias virtuales y prestar servicios de forma independiente y aislada a diferentes clientes, a través de un solo *appliance*, centralizando administración y operación, generando más ganancias y disminuyendo costos de adquisición y administración de equipos.

6. Es pertinente encontrar más parámetros de decisión que permitan eliminar el empate "técnico" que existe entre una solución y otra, facilitando la selección y estableciendo una prioridad marcada entre alternativas. Este estudio puede ser complementado con un análisis de sensibilidad a través de un software especializado como **Expert Choice** , que permite obtener de manera más exacta una valoración cualitativa entre las alternativas, validando la información obtenida a partir de los cálculos manuales.

7. Finalmente, la propuesta realizada a lo largo de este trabajo de investigación, cumple con un análisis profundo de criterios, características, opciones y alternativas que incluido en un marco metodológico de toma de decisiones multicriterio AHP**,** garantizan la selección objetiva de cualquier opción entre un conjunto de alternativas para el cumplimiento de un objetivo propuesto. Esta metodología es aplicable en todos los procesos de decisión presentes en la cotidianidad.

## 9. BIBLIOGRAFÍA


[1] M. d. P. Alegre, A. Garcia y C. Hurtado, Seguridad Informática, Madrid: Paraninfo SA, 2011.

[2] España, Dirección General de Modernizacion Administrativa. Gobierno de, «MAGERIT - versión 3.0.,» Madrid, 2012.

[3] J.-M. Royer, Seguridad en la informática de la empresa. Riesgos , amenazas, prevención y soluciones., Barcelona: Eni ediciones.

[4] P. A. Lopez, Seguridad Informática, Editex, 2010.

[5] El Tiempo, «Certificados Digitales Llegan a Colombia,» *El Tiempo,* 4 Febrero 2002.

[6] J. F. R. Buendia, Seguridad informática, McGraw Hill, 2013.

[7] D. O. G. ,. A. A. I. ,. S. R. E. CASTRO GIL Manuel Alonso, Procesos y herramientas para la seguridad de redes., Madrid: UNED, 2014.

[8] I. P. J. A. Jim Guichard, MPLS and VPN Architectures, Volume 2, Cisco Press, 2003.

[9] W. Stallings, Fundamentos de seguridad en redes: Aplicaciones y estándares., Madrid: Pearson Educación S.A, 2004.

[10] B. Furht, Encyclopedia of Multimedia, Boca raton, Florida: Springer, 2008.

[11] F. Maciá, F. Mora, J. Gil, V. Gilart, D. Marcos, J. Berná, J. Monllor, H. Ramos, A. Albaladejo y A. Hernandez, Administración de servicios de Internet: De la teoría a la práctica, Universidad de Alicante.

[12] R. Oppliger, SSL and TLS : Theory and Practice, Boston ; Londres: Artech House.

[13] T. King, Security + Training guide, Ed Tittel.

[14] R. Shea, L2TP Implementation and Operation, ADDISON-WESLEY , 2000.

[15] A. G. Blank, TCP / IP JumpStart: Internet Protocol Basics, John Wiley & Sons,, 2011.

[16] UIT, «Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo (Recomendación X.805),» 2003.

[17] G. Mitra, Mathematical Models for Decision Support, Springer Science & Business Media, 2012.

[18] T. L. Saaty y L. G. Vargas, Decision Making With The Analytic Network Process, Springer, 2006.

[19] C. Romero, Teoría de la decisión multicriterio: conceptos, técnicas y aplicaciones, Alianza Editorial, 1993.

[20] G. A. C. Pedraza, «Estudio y Análisis de la Viabilidad de la Implementación de Tecnologia PLT (Power Line Telecommunications) en Colombia, en el Ámbito de la Transmisión de Datos Sobre Redes de Baja Tensión,» Bogotá, 2012.

[21] Unniversitat Politecnica de Valencia- UPV, «AHP (Analytic Hierarchy Process),» www.youtube.com, [En línea]. Available: https://www.youtube.com/watch?v=SVivfG6Iaaw. [Último acceso: 14 Marzo 2016].

[22] «www.gestiopolis.com,» [En línea]. Available: http://www.gestiopolis.com/metodos-y-tecnicas-de-investigacion/. [Último acceso: 14 Marzo 2016].

[23] M. N. Namakforoosh, Metodología de la investigación, Limusa Noriega Editores, 2005.

[24] H. L. A. Baray, Introducción a la metodologia de la investigación, eumed.net, 2006.

[25] Cisco Systems, «Cisco Identity Services Engine User Guide,» 2015.

[26] Cisco Systems, «www.cisco.com,» [En línea]. Available: www.cisco.com. [Último acceso: 2 Marzo 2016].

[27] Cisco Systems., «SGT Exchange Protocol over TCP (SXP),» [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_config.html. [Último acceso: 5 Marzo 2016].

[28] Cisco Systems, «www.cisco.com,» 2015. [En línea]. Available: http://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html. [Último acceso: 3 Marzo 2016].

[29] Cisco systems., «Posture services on the Cisco ISE configuration guide,» [En línea]. Available: http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116143-config-cise-posture-00.html#anc5. [Último acceso: 4 Marzo 2016].

[30] PaloAlto Networks, «www.paloaltonetworks.com,» [En línea]. Available: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-5000-series. [Último acceso: 3 Marzo 2016].

[31] PaloAlto Networks, «PAN-OS Adminsitrator´s Guide Version 7.0,» Santa Clara, California., 2016.

[32] PaloAlto Networks, «www.paloaltonetworks.com,» [En línea]. Available: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/product-summary-specsheet. [Último acceso: 2 Marzo 2016].

[33] F5 Networks Inc., «www.f5.com,» [En línea]. Available: https://f5.com/products/platforms/appliances. [Último acceso: 5 Marzo 2016].

[34] F5 Networks Inc, «BIG-IP System Hardware Datasheet,» 2015.

[35] F5 Networks Inc., «F5 Silverline. Web Application Firewall. Overview,» 2016.

[36] Fortinet., «FortiGate/FortiWifi 90D Series.,» 2016.

[37] AVFirewalls, «www.avfirewalls.com,» [En línea]. Available: http://www.avfirewalls.com/FortiGate-90D.asp. [Último acceso: 5 Marzo 2016].

[38] Fortinet, «FortiAP Wireless Access Points,» 2015.

[39] Fortinet, «FortiClient,» [En línea]. Available: http://forticlient.com/. [Último acceso: 6 Marzo 2016].

[40] Fortinet, «Network Authentication,» [En línea]. Available: http://www.fortinet.com/products/network-authentication/. [Último acceso: 8 Marzo 2016].

[41] Fortinet, «Ethernet Access and Data Center Switches - FortiSwitch,» [En línea]. Available: http://www.fortinet.com/products/fortiswitch/. [Último acceso: 9 Marzo 2016].

[42] PaloAlto Networks, «Guia para el comprador de firewall,» 2012.