UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TEMA:

"LA SEGURIDAD PERIMETRAL Y SU INCIDENCIA EN LA CALIDAD DE SERVICIO DE LA RED INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI"

Trabajo de Titulación

Previo a la obtención del Grado Académico de Magíster en Informática

Autor: Ingeniero Manuel Fernando Defaz Calvopiña

Director: Ingeniero David Omar Guevara Aulestia, Magister.

Ambato – Ecuador

2015

Al Consejo de Posgrado de la Universidad Técnica de Ambato.

El tribunal de defensa del trabajo de titulación presidido por el Ingeniero José Vicente Morales Lozada, Magister, Presidente del Tribunal e integrado por los señores: Ingeniero Javier Vinicio Salazar Mera, Magister, Ingeniero Franklin Oswaldo Mayorga Mayorga, Magister, Ingeniera Blanca Rocío Cuji Chacha, Magister; Miembros del Tribunal de Defensa, designados por el Consejo de Posgrado de la Universidad Técnica de Ambato, para receptar la defensa oral del trabajo de titulación con el tema: "LA SEGURIDAD PERIMETRAL Y SU INCIDENCIA EN LA CALIDAD DE SERVICIO DE LA RED INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI", elaborado y presentado por el señor Ingeniero Manuel Fernando Defaz Calvopiña, para optar por el Grado Académico de Magister en Informática.

Una vez escuchada la defensa oral, el Tribunal aprueba y remite el trabajo de titulación para uso y custodia en las bibliotecas de la UTA.

Ingeniero José Vicente Morales Lozada, Magister
Presidente del Tribunal de Defensa

Ingeniero Javier Vinicio Salazar Mera, Magister
Miembro del Tribunal

Ingeniero Franklin Oswaldo Mayorga Mayorga, Magister
Miembro del Tribunal

Ingeniera Blanca Rocío Cuji Chacha, Magister
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de titulación con el tema: “LA SEGURIDAD PERIMETRAL Y SU INCIDENCIA EN LA CALIDAD DE SERVICIO DE LA RED INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI”, le corresponde exclusivamente al: Ingeniero Manuel Fernando Defaz Calvopiña, autor bajo la Dirección del Ingeniero David Omar Guevara Aulestia, Magister, Director del trabajo de titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

---	---
Ing. Manuel Fernando Defaz Calvopiña	*Ing. David Guevara Aulestia, Mg.*
Autor	Director

DERECHOS DEL AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este trabajo de titulación como un documento disponible para su lectura, consulta y proceso de investigación.

Cedo los Derechos de mi trabajo de titulación, con fines de difusión pública a demás autoriza su reproducción dentro de las regulaciones de la Universidad.

_____

Ing. Manuel Fernando Defaz Calvopiña

C.C. 0501780282

AGRADECIMIENTO

A mis Hijos Rafaela, Emilio y Paulo, a mi esposa Victoria; por tener la paciencia y el tiempo para soportar esta etapa de mi vida.

A todos mis hermanos quienes de una u otra manera me apoyaron para alcanzar este esta meta.

Fernando

DEDICATORIA

A mi madre en el cielo, porque siempre serás mi fuente de inspiración, tú me enseñaste a nunca rendirme en los momentos difíciles, con todo tu amor y cariño me diste fuerzas para mantenerme constante en conseguir mis metas, por inculcarme todos los valores desde mi infancia para ser una persona de bien, por depositar en mi toda tu confianza y apoyo, por aconsejarme diariamente para de esta manera disfrutar de esta nueva etapa de mi vida. Para ti mi amor.

Fernando

ÍNDICE GENERAL

PORTADAI
AUTORÍA DE LA INVESTIGACIÓN II
DERECHOS DEL AUTOR III
AGRADECIMIENTO IV
DEDICATORIA V
ÍNDICE GENERAL VI
ÍNDICE DE TABLAS VIII
ÍNDICE DE FIGURAS IX
RESUMEN EJECUTIVO X
EXECUTIVE SUMMARY XI
CAPÍTULO I 1
EL PROBLEMA DE INVESTIGACIÓN 1
1.1 TEMA: 1
1.2. PLANTEAMIENTO DEL PROBLEMA 1
1.2.1. CONTEXTUALIZACIÓN 1
1.2.2. ANÁLISIS CRÍTICO 3
1.2.3. PROGNOSIS 4
1.2.4. FORMULACIÓN DEL PROBLEMA 4
1.2.5. PREGUNTAS DIRECTRICES 4
1.2.6. DELIMITACIÓN DEL OBJETO DE INVESTIGACIÓN 5
1.3. JUSTIFICACIÓN 5
1.4. OBJETIVOS 6
1.4.1. OBJETIVO GENERAL 6
1.4.2. ESPECÍFICOS 6
CAPÍTULO II 7
MARCO TEÓRICO 7
2.1. ANTECEDENTES INVESTIGATIVOS 7
2.2. FUNDAMENTACIÓN FILOSÓFICA 9
2.3. FUNDAMENTACIÓN LEGAL 10
2.4. CATEGORÍAS FUNDAMENTALES 11
2.4.1. VISIÓN DIALÉCTICA DE CONCEPTUALIZACIONES QUE SUSTENTAN LAS VARIABLES DEL PROBLEMA 11
2.5. HIPÓTESIS 33
2.6. SEÑALAMIENTO VARIABLES 33

CAPÍTULO III **34**

METODOLOGÍA **34**

3.1. ENFOQUE 34
3.2. MODALIDAD BÁSICA DE LA INVESTIGACIÓN 35
3.2.1. INVESTIGACIÓN DE CAMPO 35
3.2.2. INVESTIGACIÓN BIBLIOGRÁFICA-DOCUMENTAL 36
3.3. NIVEL O TIPO DE INVESTIGACIÓN 37
3.3.1. INVESTIGACIÓN EXPLORATORIA 37
3.3.2. INVESTIGACIÓN DESCRIPTIVA 37
3.3.3. INVESTIGACIÓN ASOCIACIÓN DE VARIABLES (CORRELACIONAL) 38
3.4. POBLACIÓN Y MUESTRA 38
3.4.1. POBLACIÓN 38
3.4.2. MUESTRA 39
3.5. OPERACIONALIZACIÓN DE LAS VARIABLES 40
3.5.1. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE 41
3.5.2. OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE 42
3.6. RECOLECCIÓN DE INFORMACIÓN 43
3.6.1. PLAN PARA LA RECOLECCIÓN DE INFORMACIÓN 43
3.6.2. PLAN DE PROCESAMIENTO DE INFORMACIÓN 45
3.6.3. PLAN DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 47

CAPÍTULO IV **48**

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS **48**

4.1. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 48
4.2. VERIFICACIÓN DE LA HIPÓTESIS. 57

CAPÍTULO V **62**

CONCLUSIONES Y RECOMENDACIONES **62**

5.1. CONCLUSIONES 62
5.2. RECOMENDACIONES 62

CAPÍTULO VI **64**

PROPUESTA **64**

6.1. DATOS INFORMATIVOS 64

TEMA: ANÁLISIS DE SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA EL GADPC. **64**

6.2. ANTECEDENTES DE LA PROPUESTA 64
6.3. JUSTIFICACIÓN 65
6.4. OBJETIVOS 66
6.4.1. OBJETIVO GENERAL 66

6.4.2. ESPECÍFICOS 66
6.5. ANÁLISIS DE FACTIBILIDAD 66
6.5.1. FACTIBILIDAD OPERATIVA 67
6.5.2. FACTIBILIDAD TÉCNICA 67
6.5.3. FACTIBILIDAD ECONÓMICA 69
6.6. FUNDAMENTACIÓN 69
6.7. METODOLOGÍA, MODELO OPERATIVO 76
6.7.1. MODELO OPERATIVO 76
6.7.2. METODOLOGÍA 78
6.7.3. APLICACIÓN DE LA METODOLOGÍA DE SOLUCIÓN DE SEGURIDAD PERIMETRAL EN EL GADPC. 82
6.8. ADMINISTRACIÓN 127
6.9. PREVISIÓN DE LA EVALUACIÓN 127

ÍNDICE DE TABLAS

Tabla 1: Población 39
Tabla 2: Muestra 40
Tabla 3. Operacionalización de la Variable Independiente 41
Tabla 4. Operacionalización de la Variable Dependiente 42
Tabla 5. Procedimiento de recolección de información 44
Tabla 5. Procedimiento de recolección de información (continuación) 45
Tabla 6. Título con idea principal de la pregunta 46
Tabla 7: Vulnerabilidad Informática 48
Tabla 8: Detección de virus en el computador 49
Tabla 9: Herramientas de detección de intrusos en la red en la red informática 50
Tabla 10: Sistema operativo con mejor seguridad 51
Tabla 11: La seguridad informática vs. la calidad de servicio 52
Tabla 12: Inconvenientes en la red informática 53
Tabla 13: Calidad del servicio Informático 54
Tabla 14: Acceso a los sistemas informáticos 55
Tabla 15: Servicio de Internet 56
Tabla 16: Frecuencias observadas 59
Tabla 17: Resumen de procesamiento de casos 60
Tabla 18: Tabulación cruzada 60
Tabla 19: Valores de chi-cuadrado y probabilidad asociada. 60
Tabla 20: Elementos tecnológicos pasivos 69
Tabla 21: Modelo Operativo 77
Tabla 22: Planificación para la solución de seguridad perimetral para el GADPC 80
Tabla 22: Planificación para la solución de seguridad perimetral para el GADPC (continuación) 81
Tabla 23: Resumen de Activos 82
Tabla 23: Resumen de Activos (continuación) 83
Tabla 24: Servidores. Características y Funciones 85

Tabla 25: Amenazas y sus Consecuencias 90
Tabla 26: Requerimientos de seguridad de cada activo 92
Tabla 27: Identificación de componentes claves 96
Tabla 28: Direcciones IPs 99
Tabla 29: Requerimientos 104
Tabla 30: Servidores con la función que desempeñan 112
Tabla 31: Comparación de tecnologías de seguridad perimetral 124
Tabla 31: Comparación de tecnologías de seguridad perimetral (continuación) 125
Tabla 32: Matriz de análisis de evaluación 128

ÍNDICE DE FIGURAS

Figura 1: Árbol de Problemas 3
Figura 2: Superordinación conceptual 11
Figura 3: Subordinación conceptual 12
Figura 4: Calidad de Servicio *(QoS)* 16
Figura 5: Zona Desmilitarizada (*DMZ*) 27
Figura 6: Gestión Unificada de Amenazas 33
Figura 7. Título con idea principal de la pregunta 46
Figura 8: Análisis de Vulnerabilidad Informática 48
Figura 9: Análisis de la detección de virus en el computador 49
Figura 10: Análisis de Herramientas de detección de intrusos en la red informática 50
Figura 11: Análisis del Sistema operativo con mejor seguridad 51
Figura 12: La seguridad informática vs. la calidad de servicio 52
Figura 13: Inconvenientes en la red informática 53
Figura 14: Calidad del servicio Informático 54
Figura 15: Análisis del Acceso a los sistemas informáticos 55
Figura 16: Servicio de Internet 56
Figura 17: Distribución de chi cuadrado 61
Figura 18: Computadores por dirección 68
Figura 19: Tipos de computadores 68
Figura 20: Estructura de *ISO* 27001 70
Figura 21: Zona Desmilitarizada (*DMZ*) 73
Figura 22: Gestión Unificada de Amenazas (*UTM)* 75
Figura 23: Diagrama de la red informática actual del GADPC 98
Figura 24: Escaneo con *ZENMAP*. Servidor web. 186.46.92.162 - GADPC 100
Figura 25: Escaneo con *NESSUS*. Servidor web 186.46.92.162 - GADPC 101
Figura 26: Reporte *NESSUS*. Servidor de web 186.46.92.162 - GADPC 102
Figura 26: Reporte *NESSUS*. Servidor de web 186.46.92.162 – GADPC (continuación) 103
Figura 27: Gestión Unificada de amenazas. *UTM (Unified Threat Management)* 108
Figura 28: Diseño de seguridad perimetral para la red informática del GADCP 110
Figura 29: Cuadrante Mágico de *Gartner* para *Enterprise Network Firewalls* 122

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TEMA: "LA SEGURIDAD PERIMETRAL Y SU INCIDENCIA EN LA CALIDAD DE SERVICIO DE LA RED INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI".

AUTOR **:** Ingeniero Manuel Fernando Defaz Calvopiña

DIRECTOR : Ingeniero David Guevara Aulestia, Magister

FECHA : 15 de enero del 2015

RESUMEN EJECUTIVO

La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad etc., en la presentación de sus servicios los gobiernos autónomos descentralizados emprenderán un proceso progresivo de aplicación de los sistemas de gobierno y democracia digital, aprovechando de las tecnologías disponibles. De esta manera poder brindar un mejor servicio a la ciudadanía en general. Tomando en cuenta factores esenciales como los avances en la tecnología, creación de redes informáticas, intercambio de información, vulnerabilidad de las redes, se pone en manifiesto la necesidad de implementar un sistema seguridad perimetral que cubra los requerimientos del GADPC.

En la investigación realizada se presenta una solución de seguridad perimetral, que en su primera parte se describe el estado actual de la institución, los riesgos, amenazas contra la integridad de los activos del sistema informático y las contramedidas que pueden ser adoptadas. En segunda instancia se explica el escenario de trabajo, sus requerimientos y sus necesidades de seguridad presentando los criterios que fueron tomados en consideración para la selección de la solución más idónea, se desarrollan los controles de acceso lógico y las política de seguridad que debe ser aplicada en la solución seleccionada, para finalmente presentar las conclusiones que se desprenden del esquema de seguridad perimetral planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado.

DESCRIPTORES: eficacia, eficiencia, calidad, gobiernos, descentralizados, tecnologías, riesgos, amenazas, seguridad, perimetral

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN INFORMÁTICA

THEME: "THE PERIMETER SECURITY AND ITS IMPACT ON THE QUALITY OF SERVICE OF INFORMATION NETWORK FOR THE HOME GOVERNMENT OF THE PROVINCE OF DECENTRALIZEDCOTOPAXI".

AUTHOR: Ingeniero Manuel Fernando Defaz Calvopiña.

DIRECTED BY : Ingeniero David Guevara Aulestia, Magister**.**

DATE: January 15, 2015.

EXECUTIVE SUMMARY

The civil service is a service to the community governed by the principles of effectiveness, efficiency, quality etc., in presenting its services decentralized autonomous governments undertake a gradual process of implementing digital systems of governance and democracy, building of available technologies. Thus to provide better service to the general public. Taking into account key factors such as advances in technology, computer networking, information sharing, vulnerability of networks is underlined the need to implement a perimeter security system that meets the requirements of GADPC.

In research conducted perimeter security solution, which in its first part the current status of the institution, risks, threats to the integrity of the assets of the computer system and countermeasures that can be taken is described occurs. Secondly stage work, its requirements and security needs presenting explains the criteria that were considered for the selection of the most suitable solution, the logical access controls and security policy to be applied develop in the selected solution, and finally present the findings from the raised perimeter security scheme as well as recommendations for maintaining an adequate level of safety.

DESCRIPTORS: effectiveness, efficiency, quality, governments, decentralized technologies, risks, threats, security, perimeter.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 TEMA:

“La seguridad perimetral y su incidencia en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi”.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Contextualización

En el estudio sobre el estado del arte de la seguridad y sus necesidades reales, realizado por **Solórzano Cadena &Rezabala Triviño (2013),** describe que:

> Hoy en día las grandes empresas corporativas están ya pensando e invirtiendo en movilidad, en virtualización, en computación en la nube,…, lo que mejorará la productividad de las empresas y la gran mayoría optarán por contar estos productos y como ya hemos dicho contar con un buen sistema de seguridad informática no será una opción sino una obligación para estas empresas.

Por tal razón es de conocimiento que los ataques informáticos a un sistema se encuentran en constante crecimiento, debido principalmente al significativo aumento de la conectividad de dispositivos electrónicos a redes privadas, públicas o *internet*. A efecto de este crecimiento, los indicadores de seguridad de un sistema también se incrementan en la medida en que se

implementan controles y herramientas específicas para solucionar problemas relacionados a la seguridad de sistemas, redes y usuarios.

En el estudio realizado por **Solórzano Cadena &Rezabala Triviño (2013)** concluye:

> Las estadísticas nos indican que en el Ecuador ITIL (Biblioteca de Infraestructura de Tecnologías de Información), es el estándar y las buenas prácticas que están en las áreas de la seguridad de la información en los departamentos de tecnología, eso se debe a que ITIL independientemente del modelo de negocio ayuda a las organizaciones a lograr la calidad y la eficiencia en las operaciones de TI (tecnología de información).

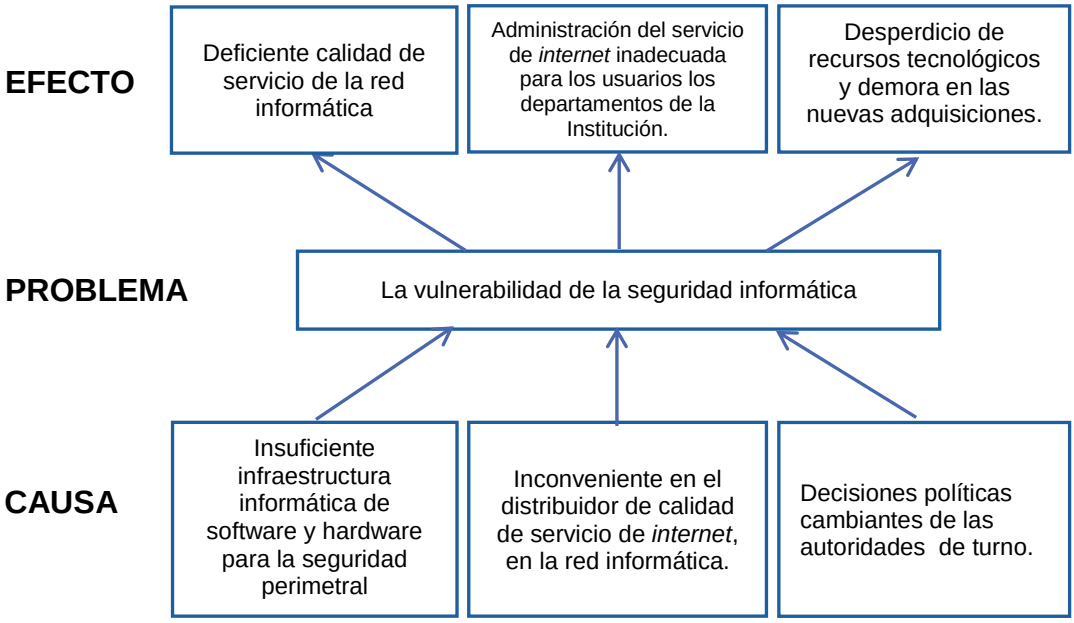
Aun así Ecuador es un lugar que se presta para el espionaje informático, los organismos oficiales desconocen la manera de cómo manejar estos casos de inseguridad informática, la mayoría de las personas no saben y ni se imaginan que es exactamente el espionaje informático y como se lleva a cabo todo esto. En los gobiernos autónomos descentralizados, existe muy poca o ninguna protección a las fuentes de información, a tal punto que tienen cuentas de correo electrónico en fuentes comunes sin conocer la vulnerabilidad de su información.

El Gobierno Autónomo Descentralizado de la Provincia de Cotopaxi (GADPC) no es la excepción, en la actualidad cuenta con una red para la gestión administrativa y operativa, esta no posee un *firewall* para su salida a *internet* y que en total suman casi 160 computadores, lo que ha ocasionado algunos inconvenientes, al ser el servidor *proxy* el único que proporciona la salida a *Internet* convirtiéndose en un cuello de botella y en un punto crítico ya que de presentarse daños o inconvenientes toda la institución se queda sin servicio de *internet* por períodos de tiempo indeterminados. No se dispone de una infraestructura de *firewall* que posibilite el crecimiento y

administración centralizada de las subredes, y que al momento solo presta el servicio de *internet* para ciertos usuarios. Con la infraestructura existente no puede crecer ni dotar del servicio a más redes ya que no existe un estudio técnico especializado, lo que ha ocasionado algunos problemas al momento de querer expandir o mejorar algún servicio de los que ya se tiene asignados en la actualidad.

1.2.2. Análisis Crítico

1.2.2.1. Árbol de Problemas



FUENTE: GADPC.
ELABORADO POR: Fernando Defaz.

Figura 1: Árbol de Problemas

La gran mayoría del personal del GAD, usa aplicaciones a través de internet, además de la trasmisión de datos como medio de comunicación entre sus diferentes instancias. Este uso masivo de la red de datos indica que la seguridad informática es una pieza fundamental para su desarrollo ya que sin la misma sería muy vulnerable la red.

El acceso a internet, es una de las principales causas en problemas de seguridad informática, es difícil poder controlar en su totalidad el acceso ya

que son los usuarios los que deciden que paginas visitar, es por esta razón que se cuenta con muy pocas políticas que minimizan el acceso a páginas no seguras que puedan atentar contra la seguridad de la red.

Esto hace que se tenga que cumplir con ciertas normas de seguridad, que permitan describir un conjunto de procedimientos de gestión, ideados para lograr la calidad y eficiencia en las operaciones de tecnología de información y poder mejorar la calidad del servicio informático.

Otro aspecto negativo a considerar son las decisiones políticas cambiantes de las autoridades del GAD las que ocasionan demora en las adquisiciones tecnológicas.

1.2.3. Prognosis

La seguridad perimetral informática es un factor de vital importancia dentro de la transformación de la nueva era digital y en los rápidos cambios tecnológicos que están tomando lugar en la sociedad, ya que sin las adecuadas medidas de seguridad, se seguirá teniendo una red informática vulnerable, los sistemas de información expuestos a terceros y la administración de internet inadecuada por el uso descontrolado del ancho de banda, llegando a la saturación de la misma, dejando sin Internet a ciertos grupos de usuarios y el riesgo que los paquetes no lleguen íntegros a su destino, en el caso de las redes inalámbricas.

1.2.4. Formulación del Problema

¿Es la insuficiente infraestructura de seguridad perimetral la principal causa de vulnerabilidad de la seguridad informática, lo que conllevó a una deficiente calidad de servicio de la red informática en los años 2013 – 2014 en el GADPC?

1.2.5. Preguntas directrices

- ¿Cuáles son las técnicas y tecnologías que permitirán garantizar la información que se genera en el GADPC?

- ¿Cuáles son los beneficios de contar con un *firewall* y un medidor de calidad de servicio en la GADPC?
- ¿Cómo mejorar las seguridades y el servicio de *internet* optimizando aspectos económicos?

1.2.6. Delimitación del objeto de Investigación

Campo: Informática
Área: Seguridades
Aspecto: Vulnerabilidad de la seguridad informática
Temporal: Período fiscal 2013 – 2014
Espacial: Gobierno autónomo descentralizado de la provincia de Cotopaxi (ver Anexo 2, RUC).

1.3. JUSTIFICACIÓN

En primer lugar se debe destacar la **importancia** primordial que debe darse a la protección de los sistemas y de los entornos de red y más teniendo en cuenta el incremento masivo de los ataques que se está produciendo en la actualidad. Mantener los recursos de información y telecomunicaciones protegidos, es una de las principales prioridades para el GAD.

De esta forma, se pretende realizar un estudio sobre las distintas tecnologías de seguridad perimetral, analizando sus características y su funcionamiento. Para posteriormente elegir uno de los sistemas de detección propuestos.

La investigación cobra mayor relevancia al presentar un esquema de seguridad en un entorno de red real, que en este caso será para el GAD de la provincia de Cotopaxi, con un conjunto de herramientas disponibles que podrán ser utilizadas para mejorar el rendimiento y obtener una configuración más adecuada del sistema. Con la propuesta de seguridad perimetral en este entorno, se pretende identificar posibles usos y penetraciones no autorizados, que informen de actividad maliciosa destinada hacia la red que se pretende proteger.

De lo expuesto anteriormente, es importante mencionar los beneficios que se pueden obtener de este estudio: crecimiento de la red institucional organizado, optimizando recursos y costos, contar con una infraestructura de red segura y con tolerancia a fallas, administración centralizada y controlada del servicio de *internet*, con mayores velocidades de acceso a la información.

1.4. OBJETIVOS

1.4.1. Objetivo General

Analizar la seguridad perimetral y su incidencia en la calidad de servicio de la red informática, para el mejoramiento de la comunicación en el GADPC.

1.4.2. Específicos

- Diagnosticar la calidad de servicio de la red informática para la determinación de las vulnerabilidades de los sistemas informáticos.
- Identificar las diferentes tecnologías de seguridad perimetral para la determinación de una solución adecuada para el GADPC.
- Proponer un diseño de seguridad perimetral para la mitigación de la vulnerabilidad informática en la red de datos del GADPC.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES INVESTIGATIVOS

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. En nuestro país, son reconocidas las empresas que ofrecen soluciones de seguridad perimetral con calidad de servicios, las que trabajan con estándares y protocolos propietarios, convirtiendo a estas soluciones en poco amigables.

Es por esta razón que existen registros sobre estudios similares en otros países e incluso en el nuestro, pero concretamente en la revisión efectuada en el consorcio de bibliotecas universitarias del Ecuador (COBUEC) y en el buscador *google* académico de *internet*, se han encontrado las siguientes tesis que guardan relación con el tema en mención:

En la investigación realizada por **Flores Saltos (2007:05)**,"pretende dotar a la red informática del Hospital Millennium de las principales seguridades que permitan confidencialidad y seguridad de la información".

Tomando como referencia el trabajo de tesis de **Reyes Mena (2010:06),** en el cual realiza,

> El análisis de las tecnologías de calidad de servicio y alta disponibilidad utilizadas en el diseño de los sistemas de comunicaciones, los mismos que constituyen un conjunto de medidas, técnicas y mecanismos tendientes a garantizar la disponibilidad y calidad de los servicios de comunicaciones en las empresas.

En la tesis de **Baltazar Gálvez & Campuzano Ramírez (2014: *Internet*),** mencionan que:

> Mantener la información integra, disponible y de manera confidencial es de gran importancia para cualquier organización, ya que de ello depende que dicha organización cumpla con sus objetivos establecidos. Por otro lado, no es posible garantizar la seguridad global, pero si es posible disminuir los riesgos dentro de una red de área local, ¿cómo lograrlo?, existen distintas formas aunque como se mencionó, no necesariamente existe un camino, es decir, se pueden tener distintos esquemas de seguridad de acuerdo con las necesidades de cada organización.

En el estudio de investigación de **Robalino Peña (2011:04),** su tesis se profundiza en,

> El estudio nivel de seguridad en la transmisión de datos (*VoIP*) que proporcionan los protocolos adyacentes a esta tecnología. En la actualidad podemos encontrar mucha información sobre la transferencia de la voz sobre *IP* (*VoIP*) y de cómo implementar esta tecnología, pero poca información de cómo lograr que estas trasmisiones sean seguras o de cómo se podría mejorar su calidad. El énfasis se centra en la selección del mejor Protocolo que incremente la seguridad en la transmisión de Voz sobre *IP*.

Mientras que en el trabajo de **Pullutaxi Achachi (2012),** como una investigación complementaria muestra, “el uso de la tecnología de detección de ataques para ayudar a la Institución a tener un soporte sobre administración y monitoreo de la red”.

Una vez realizada la revisión bibliografía relacionada con este proyecto de investigación se determina que las seguridades perimetrales con calidad de servicio, es una temática no muy utilizada y aplicada en conjunto, pero que si es estudiada, considerada y aplicada independientemente y no en su totalidad, de modo que se puede concluir que estos temas ya han llamado la atención de otros investigadores que han realizado estudios, publicaciones y recomendaciones preliminares sobre la aplicación de estas tecnologías, lo cual va aportar enormemente al proceso de investigación, análisis y elaboración del diseño de un esquema de seguridad perimetral para la red de comunicaciones del GADPC.

2.2. FUNDAMENTACIÓN FILOSÓFICA

El uso de sistemas de información y de redes electrónicas, incluida el *Internet* ha adquirido importancia en el desarrollo del ser humano, permitiendo la realización y concreción de múltiples necesidades que facilitan la vida de las personas. Por eso es necesario impulsar el acceso de la población a los servicios informáticos que se generan por y a través de diferentes medios electrónicos, siendo el proyecto seguridades perimetrales y *QoS* el que permita garantizar su utilización, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura, por lo que en lo filosófico es conveniente enfocarlo dentro del paradigma positivista ya que hablamos de los problemas sociales en los que se ve involucrado el ser humano.

La Investigación se apoyará en el hecho de que la vida social es dialéctica, por tanto su estudio, debe abordarse desde la dinámica del cambio social. Es importante entender que los servicios electrónicos seguros a través de

las redes de Información deban ser concebidos como una tecnología cambiante y en forma acelerada y no como un producto final.

2.3. FUNDAMENTACIÓN LEGAL

La Constitución de la República del Ecuador establece en el Art 227 que la Administración Pública constituye un servicio a la colectividad que se rige con principios de eficacia, calidad, desconcentración, descentralización, coordinación, planificación, trasparencia, etc. En tal virtud la **Secretaría Nacional de la Administración Pública (2013: 1,2)**, establece:

> E importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad de la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública central, Institucional y que depende de la función ejecutiva.
>
> Que la administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica de los denominados ataque cibernéticos.
>
> Que las tecnologías de Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter-institucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información

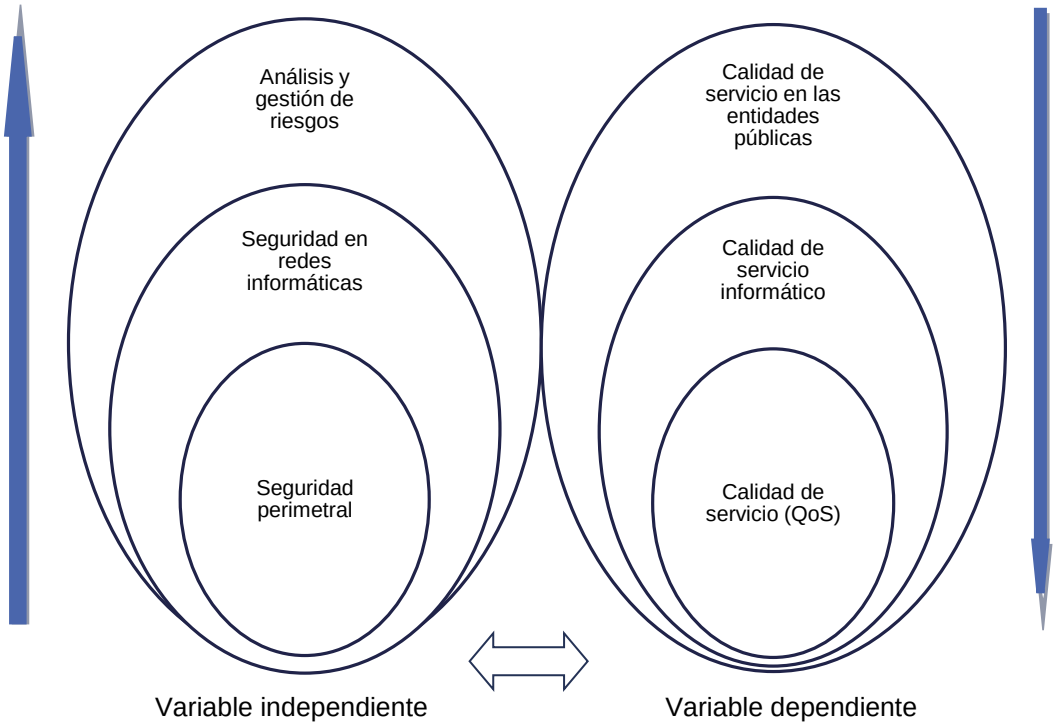
La implementación de un esquema de gestión de seguridad de la información (EGSI), se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, y recursos.

2.4. CATEGORÍAS FUNDAMENTALES

2.4.1. Visión dialéctica de conceptualizaciones que sustentan las variables del problema

2.4.1.1. Gráficos de inclusión interrelacionados

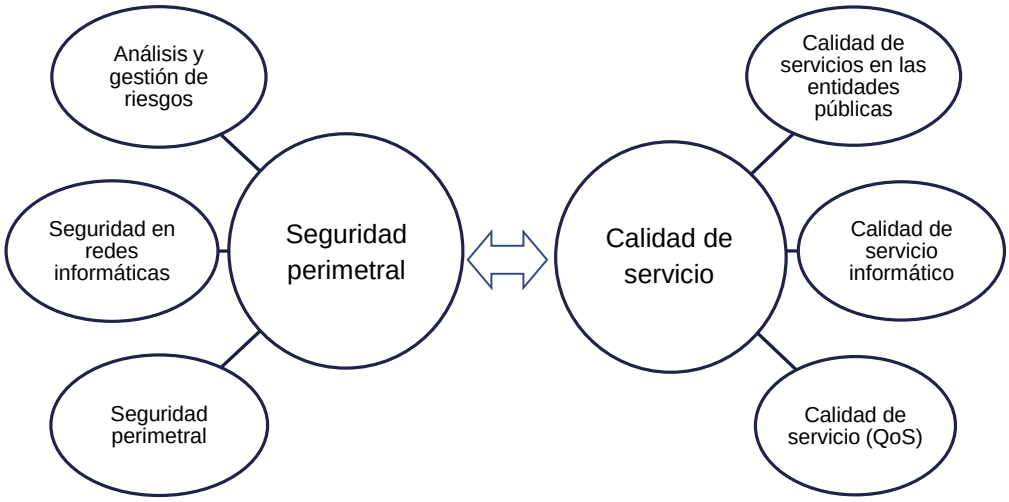
- **Superordinación conceptual**



Fuente: Investigación de campo
Elaborado por: Fernando Defaz

Figura 2: Superordinación conceptual

- **Subordinación conceptual**



Fuente: Investigación de campo
Elaborado por: Fernando Defaz

Figura 3: Subordinación conceptual

2.4.1.2. Marco conceptual variable dependiente.

✓ **Calidad de servicio en las entidades públicas.**

Los gobiernos autónomos descentralizados provinciales.- son niveles de gobierno de carácter provincial que se encargan de planificar y ejecutar obras públicas, además de otros servicios. Son personas jurídicas de derecho público, con autonomía política, administrativa y financiera.

Entre sus responsabilidades es el de promover el desarrollo sustentable de su circunscripción territorial provincial para garantizar la realización del buen vivir a través de la implementación de políticas públicas provinciales, en el marco de sus competencias constitucionales y legales.

Competencias de los GAD provinciales:

1. Planificar el desarrollo provincial y formular los correspondientes planes de ordenamiento territorial, de manera articulada con la planificación nacional, regional, cantonal y parroquial.
2. Planificar, construir y mantener el sistema vial de ámbito provincial, que no incluya las zonas urbanas.
3. Ejecutar, en coordinación con el gobierno regional, obras en cuencas y micro cuencas.
4. La gestión ambiental provincial.
5. Planificar, construir, operar y mantener sistemas de riego.
6. Fomentar la actividad agropecuaria.
7. Fomentar las actividades productivas provinciales.
8. Gestionar la cooperación internacional para el cumplimiento de sus competencias.

Según **Granja Galindo (2006:121), "**El servicio público, consiste en toda actividad directa o indirecta de la Administración Pública, regulado por la ley, cuyo objetivo esencial es la satisfacción continua de las necesidades, a favor de la colectividad"

Calidad de Servicio público.- se denomina a toda actividad basada en sus competencias, que lleva a cabo una entidad u organismo público que además cumpla con estándares internacionales de calidad; con la finalidad de satisfacer la necesidad de interés general.

La calidad en los servicios públicos es una exigencia constitucional y es una obligación de la Administración Pública. Es además el recurso con que cuenta un estado para compensar las desigualdades de la población a la que sirve, porque es la posibilidad real de que el conjunto de ciudadanos reciba los mismos servicios.

Dentro de los objetivos a cumplir por el GAD, es la consecución de su misión y la producción de servicios de calidad con eficiencia, siendo uno

de los indicadores principales la satisfacción del cliente. Si el sector público se presenta como una empresa de servicios, los ciudadanos actúan como clientes, ejerciendo una mayor presión por alcanzar mayores niveles de eficacia y eficiencia del sistema.

Al efecto se requiere implementar, dentro de las herramientas comunes de trabajo, las tecnologías de información más adecuadas y se requiere un mayor control y seguridad de la información generada en las actividades propias de la administración pública provincial.

- ✓ **Calidad del servicio informático**

Para **Díaz M. (2009: Internet), "**la calidad del servicio informático,

> Es el conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades explícitas o implícitas".

Principales características que hacen a un servicio informático de calidad:

1. **Control de calidad:** Es el conjunto de técnicas y actividades de carácter operativo, utilizadas para verificar los requerimientos relativos a la calidad del producto o servicio.

2. **Garantía de calidad:** Es el conjunto de acciones planificadas y sistemáticas necesarias para proporcionar la confianza adecuada de que un producto o servicio que satisfaga los requerimientos dados sobre calidad.

3. **Gestión de la calidad:** Este es el aspecto de la función de gestión que determina y aplica la política de la calidad, los objetivos y las responsabilidades y que lo realiza con medios tales como la planificación de la calidad, el control de la calidad, la garantía de calidad y la mejora de la calidad.

Calidad del software

Según **IEEE (2012: internet),"**La calidad de software es todo el conjunto de cualidades que lo caracterizan determinando su eficiencia y utilidad, satisfaciendo las necesidades tanto implícitas como explícitas del cliente".

Las principales características que hacen a un software de calidad son:

Mantenibilidad: el software debe ser diseñado de tal manera, que permita ajustarlo a los cambios en los requerimientos del cliente.

Confiabilidad: incluye varias características además de la confiabilidad, como la seguridad, control de fallos, etc.

Eficiencia: tiene que ver con el uso eficiente de los recursos que necesita un sistema para su funcionamiento.

Usabilidad: el software debiera ser utilizado sin un gran esfuerzo por los usuarios para los que fue diseñado, documentado, etc.

Calidad del Hardware

Según **Rodríguez y Martínez** (2008),

> Es la base del funcionamiento de cualquier sistema. Cierto es que sin el software, el hardware no puede realizar mucho, pero también es cierto que el hardware es el que provee la presencia física para que el proceso ocurra. La escogencia del software va muy ligada a la del hardware, ya que muchas de las características especiales del software son dadas indirectamente por el hardware del que se sustenta.

- **Calidad de servicio (*QoS*)**

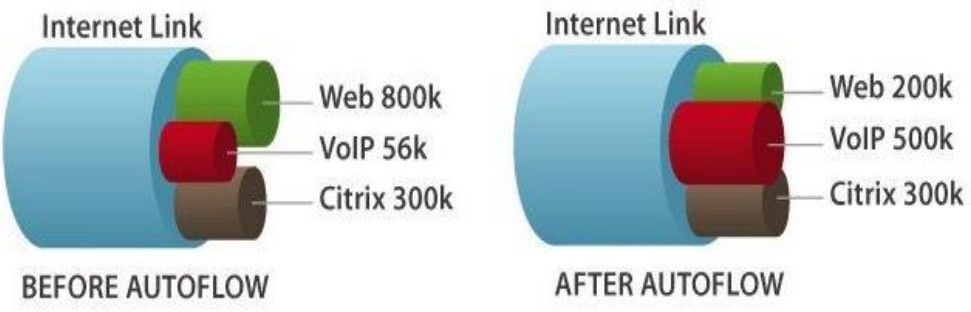
Según **García F. (2009:140)**, menciona que:

> Una solución es hacer que los *Reuters* y los *Switch*es de red funcionen de maneras distintas para cada tipo de servicio (voz, datos, video) del tráfico de la red. Al utilizar la calidad de Servicio, distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada ancho de banda de las otras.

Para tener una idea más clara de *QoS*, **Maldonado (2011:45)** menciona,

> Las ventajas principales de una red sensible a la *QoS* son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y tenemos una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda.

El término calidad de servicio hace referencia a una cantidad de tecnologías, que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío.



Fuente: Jiménez, (2014).
Elaborado por: Fernando Defaz

Figura 4: Calidad de Servicio *(QoS)*

Información digital.- Se transmite en forma de paquetes. Para verlo más claro con un ejemplo, cuando entramos en una página web, nuestro router crea uno o más paquetes virtuales que contienen la petición para ver dicha web. Una vez que el servidor que alberga la web deseada recibe la petición, descompone el código fuente de la página web en los paquetes que sean necesarios y nos envía a nuestro router y posteriormente a nuestro navegador, para que los una y conforme la web tal como la vemos habitualmente.

Pérdida de algunos paquetes.- Es el no recibir los paquetes en el orden adecuado, ya sea porque cada uno ha tomado una ruta distinta para llegar hasta su destino o por el retardo a la hora de enviarlos, como por ejemplo, cuando la imagen de una página web no se ha cargado, o la carga de la misma parece que se queda a medias. En ciertos casos puede ser un problema, sobre todo cuando hablamos de información que debe ser procesada secuencialmente como una conexión de *VoIP* (voz sobre IP).

QoS es un sistema disponible en casi todos los routers actuales, dispositivos de comunicación que permiten ofrecer una garantía en la transmisión de cierto tipo de información así como establecer prioridades en los flujos de la misma.

2.4.1.3. Marco conceptual variable independiente

- **Análisis y gestión de riesgos**

Se analizará la confianza que merecen los sistemas de información con los que trabajamos, ya que se depende de ellos en actividades personales, empresariales o en la administración si un día fallan, no podemos improvisar. Cuando tenemos un incidente es demasiado tarde para evitarlo y podríamos ser culpables de negligencia.

Cuando uno no puede anticiparse a los hechos, lo profesional es preparar planes de acción para mitigar los incidentes y establecer soluciones alternativas.

Análisis de impacto y análisis de riesgos

Se llama análisis de impacto al ejercicio de imaginarse las consecuencias de que haya un incidente, accidental o deliberado; la estimación del impacto es un dato de entrada del análisis de riesgos.

Tras inventariar activos y amenazas, hay que calificar cada escenario posible para conocer su impacto y su riesgo. El impacto es de lo que hablamos antes: las consecuencias para el negocio. El riesgo va un paso más allá y ordena los incidentes según la probabilidad de que ocurran. Con esas estimaciones podemos priorizar los riesgos y concentrarnos en aquellas cosas más probables y que traigan las peores consecuencias.

A veces se llaman indicadores del estado de seguridad y sirven para tomar decisiones. El impacto mide lo que puede pasar. El riesgo mide lo que probablemente pase.

Gestión de riesgos

Típicamente tienes 4 formas de afrontar los riesgos.

1. **Evitar la situación.-** Se debe preguntar si necesitamos todo lo que tenemos. Por ejemplo, poner un servidor Web público en el servidor de bases de datos puede ser una forma de dar un excelente servicio a los clientes, pero también abre la puerta a que haya una fuga o un robo de información. Podemos separar el servidor de base de datos del de acceso público y así el escenario de riesgo es otro.
2. **Mitigar el peligro.-** El riesgo se mitigas con medidas preventivas. Por ejemplo, si se tiene copias de seguridad de la información, no se impide que se pierda un archivo o que se averíe el servidor de bases

de datos, pero se sabe que se recupera rápidamente la información y se sigue trabajando.

3. **Aceptar riesgos.-**Muchas actividades consisten en buena medida en asumir riesgos para alcanzar ciertos beneficios. Lo que el análisis de riesgos proporciona es la información para saber qué nos estamos jugando y tomar decisiones informadas. No las puede tomar un técnico, las tiene que tomar la dirección. Por ejemplo, el comercio electrónico.
4. **Pasárselo a otro.-** Contratar un seguro es pasarle el riesgo a la aseguradora.

Es una cuestión de gestión de recursos: técnicos, humanos y económicos. La decisión se toma a la vista de las consecuencias y del costo de la solución. El análisis de riesgos califica las consecuencias y por otra parte es determinante cuántos recursos pueden justificarse para la solución. Al final hay que llegar a un equilibrio. Se debe tomar en cuenta que el costo de las medidas de protección no puede superar el bien protegido.

- **Seguridad en redes informáticas**

En lo referente a las seguridades de red **Trillo (2005:45)** menciona, “Seguridad en una red es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado”.

De acuerdo **Stallings W. (2004:262)**,

> La definición y el objetivo de la seguridad en las redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos

basados en una política de seguridad tales que permitan el control de lo adecuado.

Actualmente las redes informáticas se utilizan para comunicar no sólo a individuos sino que tienen una gran utilidad en las comunicaciones empresariales, bancarias, estatales, diplomáticas, militares, entre ciudadanos con la administración pública, etc. Mucha información, en algunos casos sensible, circula por estas redes. Existe un riesgo real de que personas no autorizadas intenten tener acceso ilegítimo a ella.

Las redes informáticas presentan muchas vulnerabilidades y es necesario protegerlas. En este sentido se define la seguridad en redes como todo aquel conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o los problemas derivados de procesar la información en ellos contenida. Se trata de conseguir que el costo de la consecución indebida de un recurso sea superior a su valor. Con esta idea en mente se diseñan mecanismos de seguridad.

- **Tipos de seguridad**

  Seguridad Física

  La seguridad física está relacionada con los recursos y el espacio físico utilizados para la protección de los elementos que conforman los sistemas de información dentro de la empresa

  Seguridad Lógica

  La seguridad lógica está relacionada con los procedimientos y recursos lógicos utilizados para proteger los sistemas de información dentro de la empresa

- **Servicios de seguridad**

  Autenticidad

  Garantiza que una entidad es quien dice ser. El servicio de autenticidad protege del ataque de suplantación de personalidad.

Integridad

El objetivo de este servicio es garantizar que los datos y recursos no han sido alterados y sean fiables.

Disponibilidad

El objetivo de esta propiedad es garantizar que la información y los servicios no sean interrumpidos y permanezcan accesibles en forma permanente.

Confidencialidad

El objetivo de esta propiedad es garantizar que la información no sea revelada a personas no autorizadas

- **Beneficios de la seguridad**

  Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

  Aumento de la productividad. El hecho de implementar políticas de seguridad, tales como: Acceso restringido a *Internet*, Uso correcto de usuarios y claves, etc.; hace que el personal utilice los recursos adecuadamente logrando un aumento de la productividad.

  Compromiso con la misión de la compañía. Brinda confiabilidad al usuario final, lo cual se refleja en la buena imagen de la Institución.

- **Delitos Informáticos**

  Los delitos informáticos son los actos que perjudican a personas, entidades o instituciones y son ejecutados por medio del uso de computadoras a través de *Internet* o directamente por dispositivos electrónicos sofisticados.

  Algunos de los más conocidos delitos informáticos son:

Propagación de Virus informáticos

Los servicios de *Internet* más comúnmente empleados para la propagación masiva de virus, son el correo electrónico con archivos adjuntos, mensajería instantánea, http es decir visitando páginas web con códigos malignos previamente configuradas, el servicio Telnet, el mismo que aprovecha las vulnerabilidades de los sistemas operativos, e ingresa a los sistemas con generadores de contraseñas o forzando al sistema.

Estafas y Fraudes

Las estafas y fraudes se han convirtiendo en prácticas habituales por quienes se aprovecharse del descuido, negligencia o ingenuidad del resto de usuarios que utilizan el *Internet* no solo como vía de consulta o uso de sus servicios, sino también para adquirir productos en línea.

Pishing

El pishing consiste en falsificar una página web que simula pertenecer a un Portal de Pagos o hasta de un Banco y al cual el usuario, previo mensaje de correo electrónico conminatorio es convencido a ingresar los datos de su tarjeta de crédito, con el propósito de una supuesta regularización, a causa de un supuesto error.

Esta información es posteriormente utilizada para realizar compras ilegales a través de *Internet*.

Scamming

El Scamming es la típica labor que conduce a una estafa. Usualmente empieza con una carta enviada en forma masiva con el nombre del destinatario, y en la cual le pueden ofrecer una serie de oportunidades al usuario como ganar dinero, premios, préstamos a bajo interés, oportunidad del cobro, etc.

- **Otros delitos informáticos**
  - ✓ El envío masivo de correo no deseado o SPAM.

- ✓ Los troyanos son programas potencialmente peligrosos, se ocultan dentro de otro para evitar ser detectado e instalarse de forma permanente en el sistema, permiten el acceso a usuarios externos, a través de una red local o de *Internet*, con el fin de recabar información
- ✓ Uso de Rootkits para los mismos fines anteriores y daños irreversibles. Un rootkits es una herramienta usada para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema.
- ✓ Ataques a servidores con el objeto de sabotearlos, conocidos como Cracking o Defacing. Cracking es el ataque o intromisión no autorizada desde el exterior al equipo. Sucede al tener una conexión permanente a la *Internet*, sobre todo con direcciones IP fijas.
- ✓ Interceptación de paquetes de datos enviados por *Internet* o Sniffing que es un tipo de ataque en el cual se busca recabar información para posteriormente analizar el tráfico de red y obtener información confidencial

Dada la complejidad de los delitos informáticos y los de alta tecnología no es fácil establecer un marco legal apropiado y eficiente. Pero es esencial conocer cuáles son y cómo funcionan para brindar soluciones a la organización que permitan proteger y precautelar la seguridad de la información.

- **Políticas de Seguridad**

Las Políticas de Seguridad son las normas y procedimientos que reglamentan la forma en que una organización protege y maneja su información, además de prevenir y protegerla ante los diversos tipos de ataques informáticos.

El objetivo de la definición de políticas de seguridad es notificar al mayor detalle a los usuarios, empleados y gerentes acerca de las reglas y

mecanismos que se deben efectuar, cumplir y utilizar para proteger los recursos y componentes de los sistemas de la empresa u organización, en especial la información.

Los componentes que una política de seguridad debe contemplar son:

- ✓ Política de privacidad
- ✓ Política de acceso
- ✓ Política de autenticación
- ✓ Política de contabilidad
- ✓ Política de mantenimiento para la red
- ✓ Política de divulgación de información.

Otros aspectos muy importantes a incorporar en la política de seguridad son

- ✓ Procedimientos para reconocer actividades no autorizadas.
- ✓ Definir acciones a tomar en caso de incidentes.
- ✓ Definir acciones a tomar cuando se sospeche de actividades no autorizadas.
- ✓ Conseguir que la política sea refrendada por el estamento más alto posible dentro de la organización.
- ✓ Divulgar la política de forma eficiente entre los usuarios y administradores.
- ✓ Articular medidas de auditoría de nuestro propio sistema de seguridad.
- ✓ Establecer plazos de revisión de la política en función de resultados obtenidos.

- **Estándares internacionales**

A pesar de que no existe una guía específica la cual se deba seguir fielmente para implementar algún esquema de seguridad en redes debido a que las necesidades para cada institución o empresa son distintas, sin embargo, existen estándares internacionales a seguir además de recomendaciones de organizaciones expertas en el área de

La propuesta de la investigación se basará en la serie ISO 27000, por describir un esquema de gestión de seguridad de la información y que paulatinamente se irán implementando en las entidades de la administración pública del gobierno Ecuatoriano como se describe en la fundamentación legal.

La serie *ISO/IEC* 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e *IEC* (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

ISO 27000 es una lista de estándares, en la cual se manejan ciertos rangos que van desde 27000 a 27019 y de 27030 a 27044, entre los que destacan *ISO* 27001, estándar cuyo objetivo es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (*SGSI*).

- **Seguridad perimetral**

Según **Staff U. (2011:23)**,"La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de aseguración en el perímetro externo de la red y a diferentes niveles".

La labor responsable de seguridad **Álvarez M. (2007:65)** comenta que,

> Su filosofía se basa en la protección de todo el sistema informático de una empresa desde fuera, es decir componer una coraza que proteja todos los elementos sensibles de ser atacados dentro de un sistema informático. Esto implica que cada paquete de tráfico trasmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para nuestra red.

Según las anteriores conceptualizaciones, tenemos que definir niveles de seguridad, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, aplicaciones y denegando cualquier tipo de acceso a otros, esto nos lleva a concluir que sin una política de seguridad, la seguridad perimetral no sirve de mucho.

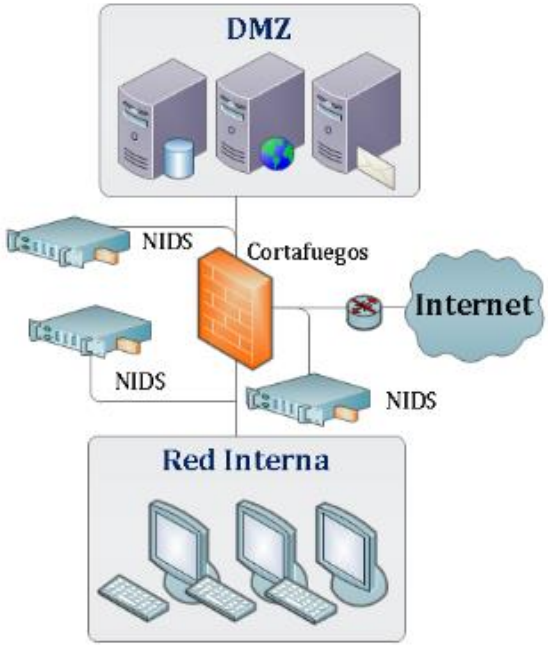
La solución de seguridad perimetral protege a las redes de ataques informáticos como *crackers*, ataques de negación de servicio (*Denied of Service-DoS*), virus, gusanos, troyanos, *spam*, contenido malicioso en correos y páginas *web*, protegiendo a la red en todos los enlaces, puntos de conexión o perímetro de la misma, incluyendo *VPN´s* y enlaces a *Internet*.

Zona Desmilitarizada (*DMZ*)

Una *DMZ* o zona desmilitarizada (*Demilitarized Zone*) es una subred situada entre la red interna, como puede ser una *LAN*, y entre una red externa, por ejemplo *Internet*.

Usualmente la *DMZ* contiene servicios accesibles desde *Internet*, como pueden ser el acceso a contenidos de páginas web, transferencia de archivos mediante servidor *FTP*, servicios de dominio de nombres DNS, etc. El objetivo de la *DMZ* es permitir las conexiones desde la red interna y la externa a la *DMZ*, pero las conexiones desde la *DMZ* sólo se permiten a la red externa, es decir que los equipos en la *DMZ* no pueden

conectarse con la red interna, por lo tanto pueden dar servicios a la red externa y además protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. La zona desmilitarizada brinda confianza a la red interna y está protegida de la red externa.



Fuente:Ramos Fraile (2011)
Elaborado por: Fernando Defaz

Figura 5: Zona Desmilitarizada (*DMZ*)

El Firewall

Un *Firewall* en *Internet* es un sistema o grupo de sistemas que impone una política de seguridad entre la red privada de una organización y el *Internet*. Es una colección de elementos, tanto software como de hardware, destinado a filtrar todo el tráfico desde la *Internet* hacia nuestra red.

El *firewall* o cortafuegos actúa a modo de barrera que se interpone entre el servidor e *Internet*, examinando todos los paquetes de datos que entran o salen de su servidor.

El *firewall* funciona mediante la definición de políticas de seguridad.

Posteriormente el propio *firewall* se encargará de verificar que todos y cada uno de los paquetes con destino al servidor se cumplan, descartando aquellos que no lo hagan.

Las políticas de seguridad se basan sobre todo en reglas utilizadas para:

- Impedir el acceso a los puertos del servidor (excepto a los que vayan a utilizarse) para evitar que un intruso pueda tomar el control del servidor aprovechando vulnerabilidades de aplicaciones de comunicaciones o un puerto abierto por un virus o gusano.

- Parar los ataques de denegación de servicio para evitar que un ataque basado en una gran cantidad de peticiones al servidor (fuerza bruta) pueda llevarlo al colapso. El firewall detectaría el intento y cortaría el flujo de datos sin dejar que llegase al servidor. También se detectan y cortan muchos más tipos de ataques sofisticados cuya intención es colapsar los servicios de red del servidor.

Un *firewall* contiene usualmente ya configuradas las principales políticas de seguridad generales para cualquier organización sin embargo le permite definir sus propias reglas de seguridad.

Arquitecturas básicas de un firewall

Los elementos para la construcción de un *firewall* son innumerables, sin embargo existen algunos elementos esenciales que se deben tomar en cuenta al seleccionar los tipos de *firewall*.

1. Control de daños
2. Zonas de riesgo
3. Modo de fallo
4. Facilidad de uso
5. Políticas de seguridad por defecto

6. Manejo de *Stateful inspection*
7. Sistema de Prevención contra Intrusiones (*IPSInstrusion Protection System*).
8. Anti-*spam*
9. Filtrado w*eb*
10. Protección Anti-*malware* (bloquea toda clase de amenazas de contenidos (virus, gusanos, troyanos, *spyware*, intentos de *phishing*, etc.)
11. Soporte de *VPN* (Redes privadas virtuales)
12. Sistema de detección de intrusos (*IDSInstrusion Detection System*), entre otros.

- **Tipos de *Firewall***

  ***Firewalls* basados en filtrado de paquetes**

  Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), dejan pasar a una red a través de paquetes IP en función de unas determinadas reglas. Estos *firewall*s conceptualmente trabajan a nivel de red, y son capaces de filtrar tráfico en función de direcciones de *IP*, protocolos, y números de puerto de *TCP o UDP*.

  Firewalls* basados en *proxies

  Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), no dejan pasar a una red a través de paquetes *IP*. La comunicación se produce por medio de proxies, que se ejecutan en el *firewall*.

  ***Firewall*s con transparencia o de tercera generación**

  La característica primordial de estos sistemas es que admiten paquetes no destinados a ellos mismos, de forma similar a como lo hacen los *routers*, y en función de una serie de reglas y configuraciones, son

capaces de arrancar los proxies correspondientes automáticamente y conectar con el destinatario inicial.

Aparentemente para el usuario, se ha conectado con el servidor final, aunque realmente lo ha hecho con el *proxy*, que le devuelve los paquetes con dirección IP origen la del servidor final. Esto implica, que el programa cliente del usuario no requiere ningún tipo de configuración. En definitiva, se trata de *firewall*s basados en proxies, pero con apariencia y funcionalidad similar a los basados en filtrado de paquetes.

- **Seguridad en profundidad en la red externa**

  Las medidas fundamentales tomadas en el perímetro exterior se pueden resumir en:

  - Reducción al mínimo de los servicios *TCP/IP* ofrecidos por cada sistema.
  - Reducción al mínimo de los usuarios en cada uno de los sistemas.
  - Uso extensivo de *tcp-wrappers* en los servicios necesarios.
  - Monitorización de *routers* en alerta de tráfico sospechoso.
  - Escaneos periódicos de todo el perímetro en busca de posibles problemas.
  - Sincronización de relojes en todos los sistemas para poder hacer un seguimiento fiable de logs en el caso de posibles incidentes.

- **Seguridad en profundidad en la red interna**

  En cuanto a la red interna se puede clasificar los problemas provocados por usuarios internos o por intrusiones realizadas desde puntos no controlados de nuestra una red.

  Contra este tipo de problemas, se debe aplicar medidas parecidas a las del perímetro externo, añadiendo el uso de programas de chequeo de la seguridad de las contraseñas elegidas por los usuarios.

Otra medida fundamental para prevenir accesos desde el exterior por puntos no controlados de una red, es establecer la prohibición del uso de módems con capacidad de llamada entrante. Si este uso fuese inevitable, como norma, debe utilizarse para ello, sistemas no conectados físicamente a la red o realizarse bajo la estricta vigilancia del administrador de red responsable.

- **Procedimientos generales de Seguridad**

  Las normas dictadas en la elaboración de la política de seguridad, en algunos casos de forma concreta y en otros de forma más abstracta, pero igualmente concluyentes, deben materializarse en una serie de procedimientos y normas a seguir en la operación y mantenimiento de las tareas diarias, sobretodo en cuanto a lo relacionado con las actividades que de una forma u otra tienen que ver con uso del *Internet*.

- **Restricciones en el Firewall**

  La parte más importante de estas tareas se realiza en el *firewall*, conjuntamente con la tarea de permitir o denegar determinados servicios en función de los distintos usuarios y su ubicación. Se definen tres grupos de usuarios:

  1. Usuarios internos con permiso de salida para servicios restringidos
  2. Resto de usuarios internos con permiso de salida para servicios no restringidos.
  3. Usuarios externos con permiso de entrada desde el exterior

  Las prioridades asignadas a cada grupo deben al igual que las políticas de seguridad de la empresa, iniciarse analizando esencialmente el nivel de prioridad que corresponde a cada grupo acorde a las necesidades de los usuarios. Sin embargo existen se pueden definir algunas políticas generales para la seguridad de cualquier *firewall*. La política de seguridad debe basarse en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación de la organización. Si no se dispone de la información detallada de la política a seguir, aunque sea un

firewall esmeradamente desarrollado y armado, se estará exponiendo la red privada a un posible atentado.

- **Limitaciones del *firewall***

  Un *firewall* no puede protegerse contra los ataques que se efectúen fuera de su punto de operación o fuera de su área de alcance.

  El *firewall* no puede protegerse ante amenazas a las que esta sometidas debido a usuarios inconscientes. No puede prohibir, por ejemplo, que los usuarios copien datos importantes en medios magnéticos o tarjetas PCMCIA y substraigan estas de la organización.

  El *firewall* no se puede proteger contra los ataques de la "Ingeniería Social", por ejemplo los comúnmente llamados hackers. Es por ello que los empleados deben ser informados acerca de los varios tipos de ataque social que pueden suceder, así como de sanciones en caso de la situación lo amerite. En base a esto la organización debe crear políticas en cuanto al uso de nombre de usuario y contraseñas.

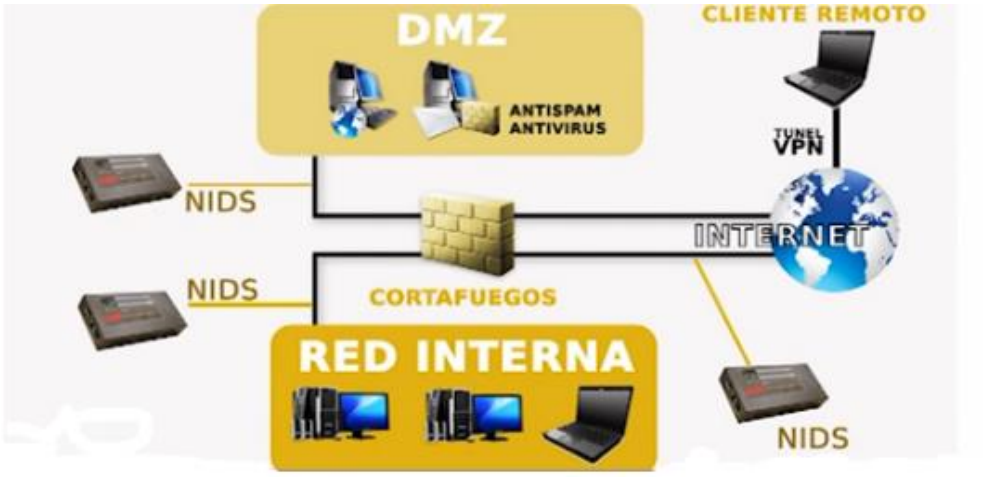
  El *firewall* no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software obtenidos del *Internet* por sistemas operativos al momento de comprimir o descomprimir archivos binarios, esto debido a que el *firewall* de no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él. La solución consiste en la utilización de software anti-viral en cada uno de los equipos.

  Además, el *firewall* de *Internet* no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

La seguridad que provea un *firewall* debe ser completada con políticas de seguridad generales para todos los grupos de usuarios y sus respectivos equipos.

- **Gestión Unificada de Amenazas**

La organización después de estudiar costos, deberá adquirir un sistema de Gestión Unificada de Amenazas *UTM (Unified Threat Management)*, un único equipo que incluye múltiples características de seguridad: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus y anti spam y redes privadas virtuales.



Fuente:Ramos Fraile (2011)
Elaborado por: Fernando Defaz

Figura 6: Gestión Unificada de Amenazas

2.5. HIPÓTESIS

La incorporación de la seguridad perimetral mejorará la calidad de servicio de la red informática del gobierno autónomo descentralizado de la provincia de Cotopaxi.

2.6. SEÑALAMIENTO VARIABLES

- **Variable independiente:** La seguridad perimetral
- **Variable dependiente:** Calidad de servicio

Unidad de observación: El gobierno autónomo descentralizado de la provincia de Cotopaxi**.**

CAPÍTULO III

METODOLOGÍA

3.1. ENFOQUE

Para **Abril (2010: *Internet*)**, en el documento paradigmas de investigación, en el tema definiciones y conceptualización comenta que,

> La palabra paradigma viene del griego paradigma que significa modelo, patrón. (…), es un ejemplo o un esquema básico de interpretación de la realidad, que ha sido verificado por un proceso de investigación científica, es decir aplicando leyes, teorías, modelos, métodos y técnicas, aplicando e instrumentando; y, sobre la base de este ejemplo se proporcionan modelos científicos. (…). La investigación educativa responde al paradigma (…) positivista (…); que se conecta con la corriente filosófica del realismo.

De igual forma **Abril (2010: *Internet*),** conceptualiza a la,

> Investigación cuantitativa como la clásica o tradicional, dentro de lo cual se ubica la mayoría (si no todos) los tipos de investigación, se manifiestan entre otras, las siguientes características:
>
> **a.** Los objetivos y el proceso de investigación solo es conocido por los técnicos y los investigadores.

b. Las decisiones para actuar son tomadas solo por los técnicos.

c. La población es pasiva y es considerada únicamente como un depósito de información.

d. La población no tiene que reaccionar frente a la investigación o a la acción decidida.

e. Los resultados del estudio son destinados exclusivamente a los investigadores y al organismo o centro de investigación. La población no tiene que conocerlos ni discutirlos.

La investigación a realizar es predominantemente cuantitativa basada en el paradigma positivista, porque que se conecta con la corriente filosófica del realismo, es decir es decir proyecta la calidad de los servicios de la red informática en función de la cantidad de personas que la utilizan, entre las principales tenemos las autoridades, el departamento informático y comunicaciones, el personal administrativo operativo, lo que permitirá efectuar un acercamiento a la realidad de la seguridad informática.

En el presente estudio, se utilizará para estudiar las propiedades y fenómenos cuantitativos y sus relaciones para proporcionar la manera de establecer, formular, fortalecer y revisar la teoría existente.

3.2. MODALIDAD BÁSICA DE LA INVESTIGACIÓN

3.2.1. Investigación de campo

Es la investigación que se realiza en el lugar de los hechos *"in situ",* utilizando fuentes primarias de información.

El trabajo de campo o recopilación de datos según **Armijos & Armijos (2009:04),**

> Se realizará de una forma u otra en función de la metodología escogida. En el caso de una encuesta la realización del trabajo de campo implica necesariamente llevar a cabo un proceso de selección, formación y control de los entrevistadores. Esta etapa tiene una importancia clave para que la investigación resulte eficaz y se justifique su costo: los errores producidos en la misma pueden invalidar la investigación, a pesar de que posteriormente se utilicen las técnicas más sofisticadas de análisis de la información.

El estudio se basa en la investigación de campo que permita evidenciar la vulnerabilidad de la seguridad informática en la red de datos del GADPC lugar donde ocurre el problema y que los datos sean tomados del personal que trabaja en este organismo del estado.

3.2.2. Investigación bibliográfica-documental

Es la investigación que se realiza en depositorios de información, utilizando fuentes secundarias de información.

Una de las modalidades básicas de investigación según **Meléndez Tamayo (2013:10)**,

> Se basa en el estudio que se realiza a partir de la revisión de diferentes fuentes bibliográficas o documentales (literatura sobre el tema de investigación). En esta modalidad de la investigación debe predominar, el análisis, la interpretación, las opiniones, las conclusiones y recomendaciones del autor o los autores

Es primordial para este efecto realizar la documentación de los requisitos y expectativas de cada uno de los temas y subtemas que conciernan al proyecto, para posteriormente realizar el análisis de la información recolectada; por medios bibliográficos, *internet* y sitios web especializados.

3.3. NIVEL O TIPO DE INVESTIGACIÓN

A continuación se establecerá el grado de profundidad con que se abordará la investigación.

3.3.1. Investigación exploratoria

Meléndez Tamayo (2013:16), manifiesta que,

> Este nivel está dirigido a tener un conocimiento general o aproximativo de la realidad. Comúnmente, se emplea este tipo de investigación en el inicio de cualquier proceso científico, cuando se quiere explorar algún tópico que ha sido tratado escasamente, por no tener mucha información sobre el o porque no se dispone de medios para llegar a mayor profundidad.

Que permita conocer el nivel de seguridad y calidad de servicio que existe en la red informática del GADPC.

3.3.2. Investigación descriptiva

Para **Meléndez Tamayo (2013:17)**, la investigación descriptiva trata de,

> Obtener información acerca de un fenómeno o proceso, para describir sus implicaciones, sin interesarse mucho (o muy poco) en conocer el origen o causa de la situación.

Fundamentalmente está dirigida a dar una visión de cómo opera y cuáles son sus características.

En la presente investigación se describirá temas como el tipo de tecnología de red, los sistemas, aplicaciones y servicios de red, dar una visión de cómo opera y cuáles son sus características y vulnerabilidades.

3.3.3. Investigación asociación de variables (correlacional)

Este tipo de investigación según **Meléndez Tamayo (2013:17)**, tiene como objetivo, “encontrar las relaciones de causa-efecto que se dan entre los hechos a objeto de conocerlos con mayor profundidad”.

Se explicará la seguridad perimetral aplicando calidad de servicios y su forma de incidir en la comunicación de la red de datos.

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

El desarrollo de la investigación se la realizará en las dependencias del GADPC, la misma que cuenta con ciento sesenta empleados distribuidos en las oficinas administrativas, operativas, en la que se incluye al personal del área informática y sus autoridades. Con los cuales se va a realizar un trabajo de campo.

El siguiente cuadro muestra cómo se encuentra distribuida la población para nuestra investigación:

Tabla 1: Población

POBLACIÓN	FRECUENCIA	PORCENTAJE
Autoridades del GADPC	5	3,125%
Dpto. Informática y Telecomunicaciones	5	3,125%
Personal Administrativo, Operativo	150	93,75%
TOTAL	160	100,00%

FUENTE: GADPC
ELABORADO POR: Fernando Defaz

3.4.2. Muestra

Cálculo de la muestra:

N=160

α=5%

Para un Nivel de confianza del 95%, **Z=**1,96

2p=0,25

$$\boldsymbol{n} = \frac{\mathbf{0.25}\boldsymbol{N}}{\left(\frac{\boldsymbol{\alpha}}{\boldsymbol{Z}}\right)^{\mathbf{2}}(\boldsymbol{N}-\mathbf{1})+\mathbf{0.25}} = 113$$

Dónde:

N: es el tamaño de la población

α: alfa es el valor del error tipo 1

Z= Es un valor tipificado, indica el valor del número de unidades de desviación estándar para una prueba de dos colas con una zona de rechazo igual alfa.

p= Probabilidad a favor o en contra.

2p= Máximo número de valor de error estándar.

n= Tamaño de la Muestra

Explicación de la fórmula: 0.25 es el valor de 2p que produce el máximo valor de error estándar, esto es p = 0.5. El valor del error alfa, es del 5 % (0.05) con un nivel de confianza de 95% (0.95) lo que equivale a un valor z de 1.959963985 (a nivel práctico1.96).

Tabla 2: Muestra

POBLACIÓN	FRECUENCIA	PORCENTAJE
Autoridades del GADPC	4	3,540%
Dpto. Informática y Telecomunicaciones	4	3,540%
Personal Administrativo, Operativo	105	92,920%
TOTAL	113	100,00%

FUENTE: GADPC
ELABORADO POR: Fernando Defaz

3.5. OPERACIONALIZACIÓN DE LAS VARIABLES

Es un proceso, por medio del cual se pasa del plano abstracto de la investigación, a un plano concreto, transformando la variable a categorías, las categorías a indicadores y los indicadores a ítems, lo que facilitará la recolección de información por medio de un proceso de deducción lógica.

3.5.1. Operacionalización de la variable independiente

Tabla 3. Operacionalización de la Variable Independiente

VARIABLE	DEFINICIÓN CONCEPTUAL	INDICADORES	ÍTEM BÁSICO	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
SEGURIDAD PERIMETRAL	Es una protección de todo el sistema informático de una empresa desde fuera. Esto implica que cada paquete de tráfico trasmitido debe ser diseccionado, analizado y aceptado o rechazado en función de su potencial riesgo de seguridad para la red informática del GADPC.	Crecimiento anual de usuarios en los últimos dos años. Eficiencia de la red de datos. Periodicidad de problemas en la red de datos Eficiencia de los sistemas internos	¿De cuánto es el crecimiento anual de usuarios en la red en los últimos dos años? ¿Dentro del Plan Estratégico Institucional, cual es la proyección Informática en lo referente a Seguridad en la red y Calidad de Servicio? ¿El presupuesto asignado para el departamento de Sistemas, cubre las expectativas para el crecimiento tecnológico Informático? ¿Cómo se controla el acceso a la red e *internet* para que la información que fluye sea segura? ¿Con qué frecuencia cree que los inconvenientes en la red ocurren? ¿En relación al acceso a los sistemas internos del GADPC cómo considera el servicio? ¿Qué sistema operativo brinda mejor seguridad a sus aplicaciones? ¿Ha sufrido algún tipo de vulnerabilidad ya sea por virus, terceras personas u otro tipo de amenaza?	**Técnica:** Entrevista al Jefe de servicios informáticos **Instrumento:** Cuestionario (ver Anexo 4). **Técnica:** Encuesta aplicada a autoridades, personal del Dpto. informático, administrativo, operativo. **Instrumento:** Cuestionario (ver Anexo 3).

FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz

3.5.2. Operacionalización de la variable dependiente

Tabla 4. Operacionalización de la Variable Dependiente

VARIABLE	DEFINICIÓN CONCEPTUAL	INDICADORES	ÍTEM BÁSICO	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN
CALIDAD DE SERVICIO	Es la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, así tenemos una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso.	Eficiencia de los servicios de *internet*.	¿Cómo califica la calidad de servicio informático? ¿Cree que mediante una adecuada seguridad en la red se pueda mejorar la calidad de servicio informático? ¿Cómo considera el servicio de *internet*? ¿De qué forma se distribuye el ancho de banda para las aplicaciones que tienen mayor prioridad de uso?	**Técnica:** Encuesta aplicada a autoridades, personal del Dpto. informático, administrativo, operativo. **Instrumento:** Cuestionario (ver Anexo 3).

FUENTE: Investigación de campo

ELABORADO POR: Fernando Defaz

3.6. RECOLECCIÓN DE INFORMACIÓN

3.6.1. Plan para la recolección de información

Este plan contempla estrategias metodológicas requeridas por los objetivos (ver Pág. 18) e hipótesis de investigación (ver Pág. 26), de acuerdo con el enfoque escogido que para el presente estudio es predominantemente cuantitativo (ver Pág. 27), considerando los siguientes elementos:

- **Definición de los sujetos: personas u objetos que van a ser investigados**.

  Profesionales que se encuentra laborando actualmente en el gobierno autónomo descentralizado de provincial de Cotopaxi y que podemos distinguirlos en la siguiente clasificación: Autoridades políticas asignadas por mandato popular, personal administrativo y operativo, de informática y telecomunicaciones; como se puede visualizar en la población y/o muestra de estudio (ver Pág. 10).

- **Selección de las técnicas a emplear en el proceso de recolección de información**.

  Para conceptualizar la técnica de encuesta **Palencia Avendaño (2013: *Internet*)** define como un “Sondeo efectuado en la opinión pública o privada para indagar su juicio sobre cierto hecho o fenómeno. El listado de las preguntas o enunciados se conoce como protocolo de la encuesta.”
  De similar forma **Palencia Avendaño (2013: *Internet*)** también define a la entrevista como: “La técnica para la obtención de información en el que se mantiene una conversación entre dos o más personas. En la entrevista se puede usar como instrumento un listado de preguntas o asuntos a ser interrogados o protocolo de la entrevista.”

- **Instrumentos seleccionados o diseñados de acuerdo con la técnica escogida para la investigación**.

  Para aplicar las técnicas mencionadas en el los párrafos anteriores según **Palencia Avendaño (2013: *Internet*)** se debe utilizar un instrumento para obtener la información, al que lo define como un "Artificio utilizado para efectuar algún trabajo, en este caso mediciones o registros, pueden corresponder a protocolos, cuestionarios, listas de chequeo, etc."

  Para la presente investigación se realizará una entrevista al jefe del departamento informático por ser la persona que conoce en detalle el funcionamiento de la red de datos (ver Anexo 4) y una encuesta al resto del personal (ver Anexo 3)

- **Explicitación de procedimientos para la recolección de información, cómo se va a aplicar los instrumentos, condiciones de tiempo y espacio, etc**.

Tabla 5. Procedimiento de recolección de información

TÉCNICAS	PROCEDIMIENTO
ENCUESTA	**¿Cómo?** • Realizando una encuesta al personal del GADPC, mediante la aplicación de un cuestionario con la única finalidad de recolectar información que será importante para nuestra investigación.
	¿Dónde? • En el gobierno autónomo descentralizado de la provincia de Cotopaxi.

Fuente: Investigación de campo
Elaborador por: Fernando Defaz

Tabla5. Procedimiento de recolección de información (continuación)

TÉCNICAS	PROCEDIMIENTO
	¿Cuándo? • Primera semana de septiembre del 2014
ENTREVISTA	¿Cómo? • Realizando una entrevista al jefe del departamento informático, mediante la aplicación de un cuestionario de entrevista, de la misma manera que en la técnica anterior para recolectar información que será importante para nuestra investigación.
	¿Dónde? • En el gobierno autónomo descentralizado de la provincia de Cotopaxi.
	¿Cuándo? • Segunda semana de septiembre del 2014

Fuente: Investigación de campo
Elaborador por: Fernando Defaz

3.6.2. Plan de procesamiento de información

- **Revisión crítica de la información recogida.** Es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, etc.

- **Repetición de la recolección**. En ciertos casos individuales, para corregir fallas de contestación.

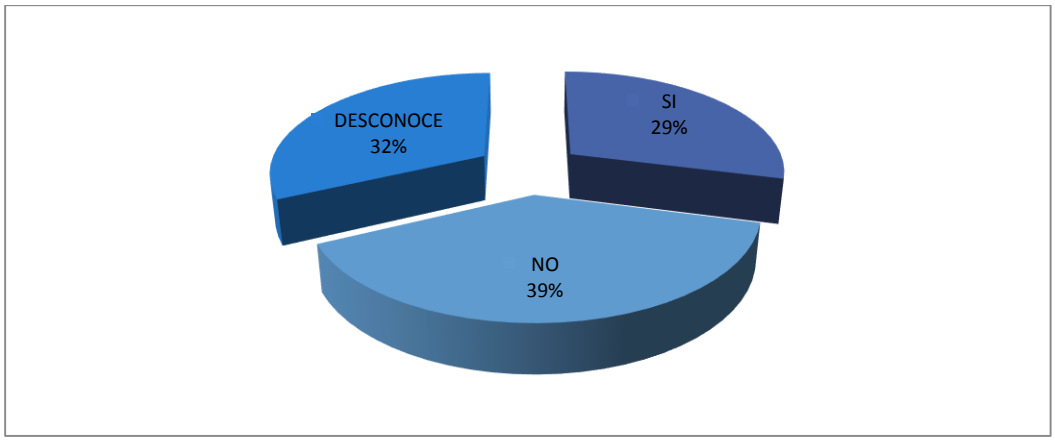
- **Tabulación o cuadros según variables de cada hipótesis:** Manejo de información, estudio estadístico de datos para presentación de resultados. Ejemplo de tabla a ser utilizada para la cuantificación de los resultados obtenidos con los instrumentos de recolección de información primaria (de campo).

Tabla6. Título con idea principal de la pregunta

OPCIONES	CANTIDAD	FRECUENCIA, %
SI	54	81
NO	13	19
TOTAL	67	100

Fuente: Investigación de campo
Elaborador por: Fernando Defaz

- **Representaciones gráficas.** Ejemplo de figura a ser utilizada para la presentación visual porcentual de los resultados cuantificados en la tabla anterior.



Fuente: Investigación de campo
Elaborador por: Fernando Defaz

Figura7. Título con idea principal de la pregunta

3.6.3. Plan de análisis e interpretación de resultados

- **Análisis de los resultados estadísticos**. Destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis (lectura de datos).

- **Interpretación de los resultados***.* Con apoyo del marco teórico, en el aspecto pertinente.

- **Comprobación de hipótesis**. Explicar el posible método estadístico de comprobación de hipótesis (H_1) a ser utilizado en el desarrollo de la investigación, con sus respectivos pasos, incluyendo la cita de texto y su utilidad, teniendo en cuenta el enfoque (cuantitativo o cualitativo) de la hipótesis de trabajo; así como, del tamaño de la población (finita o infinita, $N \leq 100 \geq N$) y/o muestra.

- **Establecimiento de conclusiones y recomendaciones**. Explicación del procedimiento de obtención de las conclusiones y recomendaciones. Las conclusiones se derivan de la ejecución y cumplimiento de los objetivos específicos de la investigación. Las recomendaciones se derivan de las conclusiones establecidas. A más de las conclusiones y recomendaciones derivadas de los objetivos específicos, si pueden establecerse más conclusiones y recomendaciones propias de la investigación.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis e Interpretación de resultados

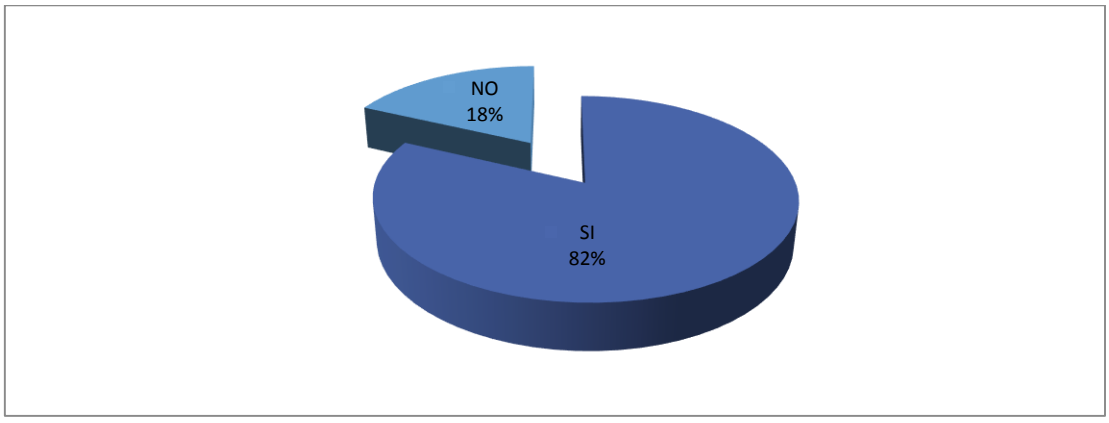
Encuesta aplicada al personal administrativo, operativo, autoridades del GAD, departamento informática y telecomunicaciones.

1. **¿Ha sufrido algún tipo de vulnerabilidad Informática ya sea por virus, terceras personas u otro tipo de amenazas?**

Tabla7: Vulnerabilidad Informática

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
SI	93	82%
NO	20	18%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 8: Análisis de Vulnerabilidad Informática

Análisis: Se observa quede 113 personas que representan el 100% de la muestra, el 82% manifiesta que ha sufrido algún tipo de vulnerabilidad ya sea por virus, terceras personas u otro tipo de amenaza y solo el 18% señala que no ha sufrido ningún tipo de vulnerabilidad.

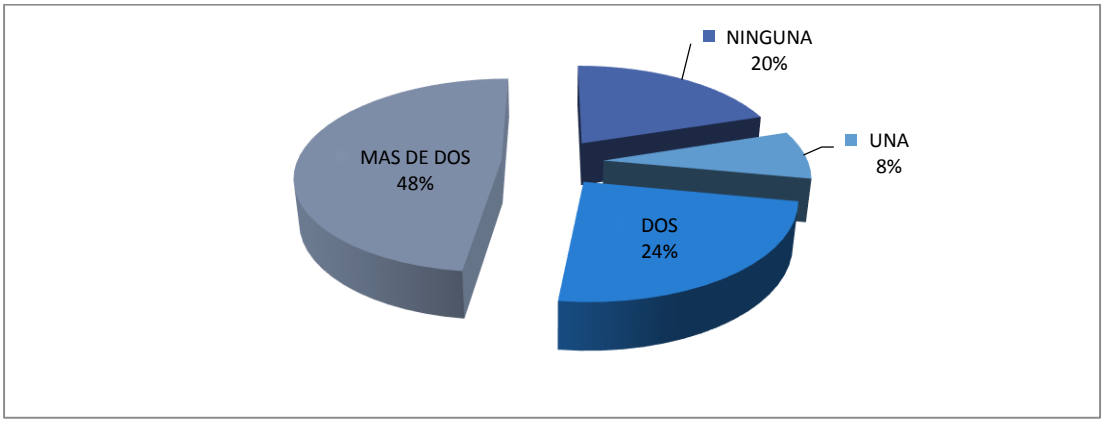
Interpretación: La mayoría de los encuestados afirman que sí existen vulnerabilidades, lo que evidencia la necesidad de mejorar la seguridad perimetral y la calidad del servicio (*QoS*) informático del GADPC.

2. ¿Cuántas veces se han detectado virus en su computador en los dos últimos años?

Tabla8: Detección de virus en el computador

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
NINGUNA	22	20%
UNA	8	8%
DOS	26	24%
MAS DE DOS	57	48%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 9: Análisis de la detección de virus en el computador

Análisis: La investigación indica que de 113 personas que representan el 100% de la muestra o personal encuestado, el 20% manifiesta que nunca o ninguna vez se han detectado virus en su computador en los dos últimos años, el 8% señala que solo una vez, el 24% de la unidad de estudio que dos veces y el 48% declara que más de dos veces se le han detectados virus en su computador en los dos últimos años.

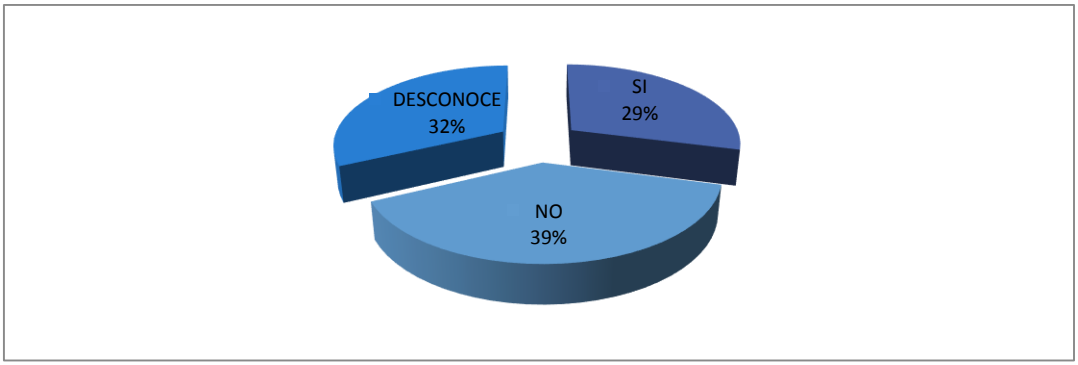
Interpretación: La mayor parte de los encuestados manifiestan que más de dos veces se han detectado virus en su computador en los dos últimos años, lo que evidencia que existen brechas en la Seguridad Perimetral de la red.

3. **¿Dispone el GAD de herramientas o sistemas que detecten los intentos de acceso a la red de datos de la institución?**

Tabla9: Herramientas de detección de intrusos en la red en la red informática

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
SI	32	29%
NO	43	39%
DESCONOCE	38	32%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 10: Análisis de Herramientas de detección de intrusos en la red informática

Análisis: La investigación indica que de 113 personas que representan el 100% de la unidad de estudio, el 29% de los encuestados manifiestan que el GAD dispone de herramientas o sistemas que detecten los intentos de acceso a la red de datos de la institución, el 39% señala que no dispone de estos recursos y el 32% de la unidad de estudio desconoce si el GAD dispone o no de los mismos.

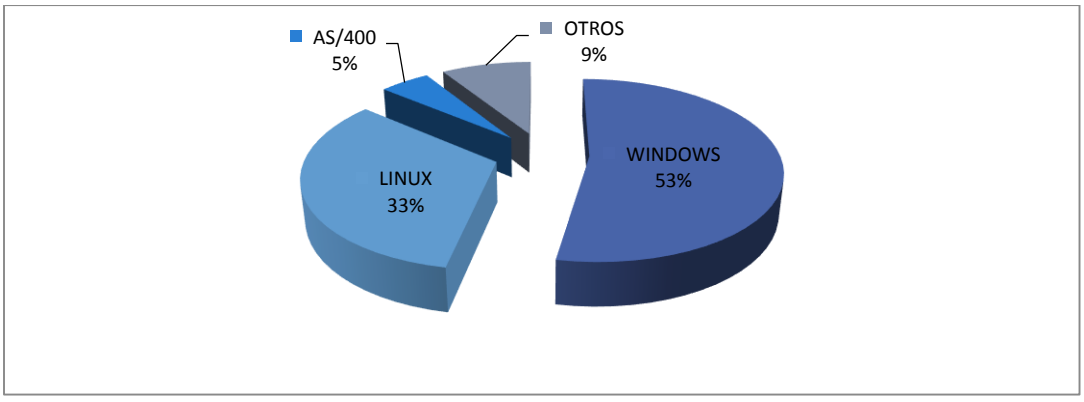
Interpretación: La mayoría de los encuestados plantean que el GAD no dispone de Herramientas o Sistemas que detecten los intentos de acceso a la red de datos de la institución, donde se evidencia la baja calidad de la red perimetral y los servicios informáticos.

4. ¿Qué sistema operativo brinda mejor seguridad a sus aplicaciones?

Tabla 10: Sistema operativo con mejor seguridad

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
WINDOWS	59	53%
LINUX	37	33%
AS/400	7	5%
OTROS	10	9%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 11: Análisis del Sistema operativo con mejor seguridad

Análisis: Se observa que el 53% de los encuestados manifiestan que el sistema operativo Windows brinda mejor seguridad a sus aplicaciones, el 33% señala que es Linux, el 9% de la unidad de estudio que son otros sistemas operativos los que les brinda mejor seguridad a sus aplicaciones y solo el 5% declara que es AS/400.

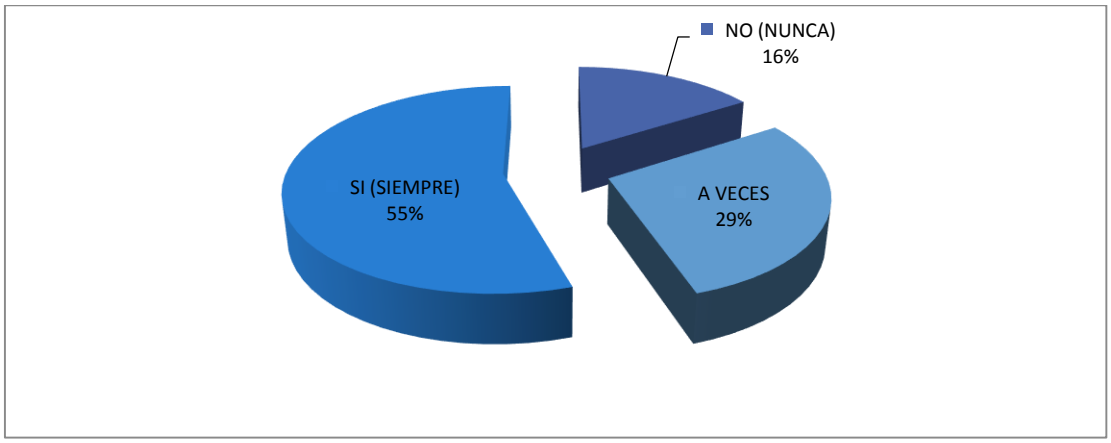
Interpretación: Se aprecia que en gran medida los encuestados manifiestan que en su opinión el sistema operativo Windows brinda mejor seguridad a sus aplicaciones en comparación con otros programas.

5. **¿Cree que mediante una adecuada seguridad en la red se pueda mejorar la calidad del servicio informático?**

Tabla11: La seguridad informática vs. la calidad de servicio

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
NO (NUNCA)	17	16%
A VECES	32	29%
SI (SIEMPRE)	64	55%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 12: La seguridad informática vs. la calidad de servicio

Análisis: En este caso el 55% de los encuestados manifiestan que consideran que mediante una adecuada seguridad en la red se pueda mejorar la calidad del servicio informático, el 29% señala que a veces y el 16% de la unidad de estudio que no.

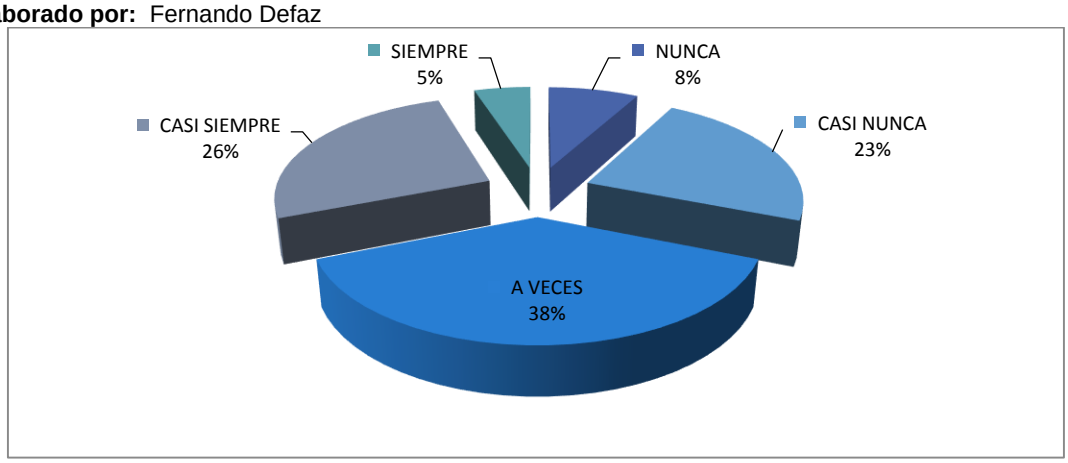
Interpretación: Los encuestados en su gran mayoría coinciden en que mediante una adecuada seguridad en la red se pueda mejorar la calidad del servicio informático, lo que pone en evidencia la necesidad de buscar alternativas por parte del servicio informático del GAD para realizar estas mejoras.

6. ¿Con qué frecuencia cree que ocurren inconvenientes en la red?

Tabla12: Inconvenientes en la red informática

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
NUNCA	9	8%
CASI NUNCA	25	23%
A VECES	42	38%
CASI SIEMPRE	29	26%
SIEMPRE	8	5%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 13: Inconvenientes en la red informática

Análisis: Se observa quede 113 personas que representan el 100%, el 8% de los encuestados manifiestan que nunca ocurren inconvenientes en la red, el 5% que siempre,, el 23% señala que casi nunca ocurren estos inconvenientes, el 26% que casi siempre ocurren y el 38% de la unidad de estudio cree que a veces si ocurren.

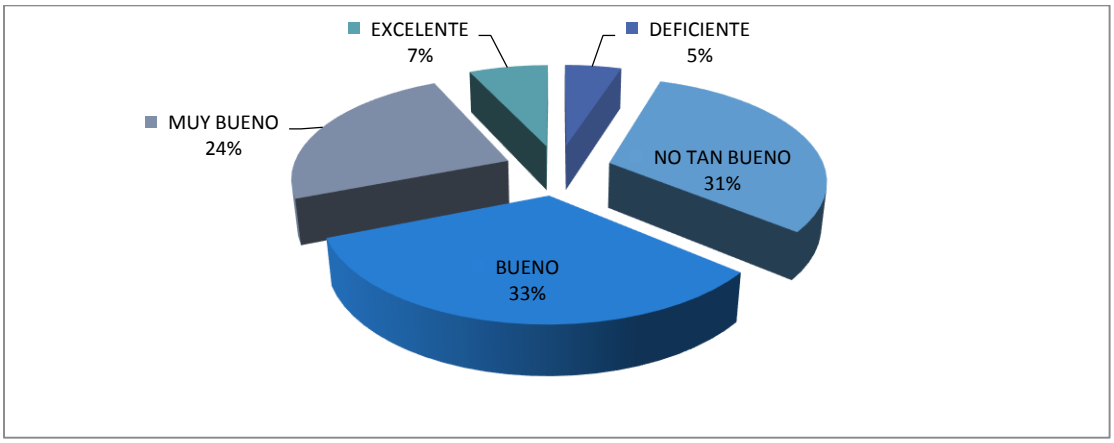
Interpretación: La mayor cantidad de los encuestados manifiestan que a veces ocurren inconvenientes en la red, lo que hace que constituya una necesidad actualizar y modernizar la Seguridad Perimetral.

7. ¿Cómo califica la calidad del servicio informático?

Tabla13: Calidad del servicio Informático

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
DEFICIENTE	5	5%
NO TAN BUENO	35	31%
BUENO	37	33%
MUY BUENO	26	24%
EXCELENTE	10	7%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 14: Calidad del servicio Informático

Análisis: De la población total de 113 personas que representan el 100% de la muestra, el 33% manifiesta que califica como bueno el servicio informático, el 24% como muy bueno, el 31% lo califica como no tan bueno, solo el 7% como excelente y el 5% califica como deficiente el servicio informático.

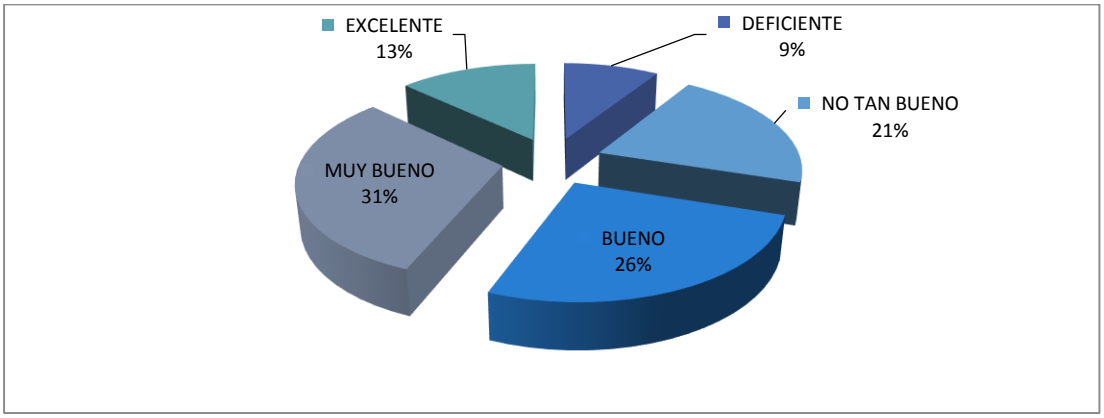
Interpretación: Se aprecia que la mayor cantidad de los encuestados coinciden y manifiestan como bueno y no tan bueno, lo que evidencia la insuficiente calidad en este servicio y la necesidad de mejorarlo.

8. ¿En relación al acceso a los sistemas informáticos internos del GADPC, cómo considera el servicio?

Tabla14: Acceso a los sistemas informáticos

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
DEFICIENTE	10	9%
NO TAN BUENO	23	21%
BUENO	29	26%
MUY BUENO	34	31%
EXCELENTE	17	13%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 15: Análisis del Acceso a los sistemas informáticos

Análisis: La investigación demuestra que de 113 personas que representan el 100%, el 9% manifiesta que califica o considera el servicio como deficiente, solo el 13% de los encuestados lo consideran excelente, como bueno lo califica el 26%, el 21% lo considera no tan bueno, y el 31% lo califica como muy bueno el servicio con relación al acceso a los sistemas internos del GADPC.

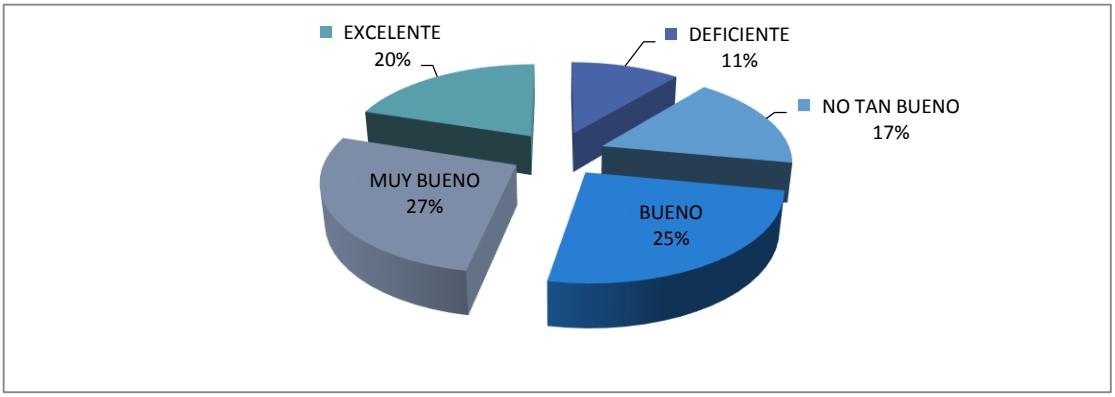
Interpretación: La mayoría de los encuestados consideran como muy bueno el servicio de acceso a los sistemas internos del GAD, esto evidencia que el acceso a los sistemas internos del GAD es bueno.

9. ¿Cómo considera el servicio de *Internet*?

Tabla15: Servicio de Internet

RESPUESTA	FRECUENCIA	PORCENTAJE (%)
DEFICIENTE	12	11%
NO TAN BUENO	19	17%
BUENO	28	25%
MUY BUENO	30	27%
EXCELENTE	24	20%
Total	**113**	**100%**

Fuente: GADPC
Elaborado por: Fernando Defaz



Fuente: GADPC
Elaborado por: Fernando Defaz

Figura 16: Servicio de Internet

Análisis: El 11% manifiesta que considera el servicio de *internet* como deficiente, el 17% de los encuestados lo consideran como no tan bueno, como bueno lo califica el 25%, el 20% lo considera excelente, y el 27% califica o considera como muy bueno el servicio de *internet*.

Interpretación: La mayoría de los encuestados plantean que el servicio de *internet* es muy bueno, en este caso se demuestra que el servicio de *internet* es estable y satisfactorio, además de cubrir todas las posibles necesidades.

4.2. Verificación de la Hipótesis.

Consiste en evaluar la hipótesis entre sus dos variables categóricas, mediante la utilización del método estadístico denominado Chi- cuadrado.

- **Las variables que interviene en la hipótesis:**

  Variable independiente: La seguridad perimetral

  Variable dependiente: Calidad de servicio

- **Formulación de la Hipótesis Nula (Ho) y la Hipótesis alternativa (H1)**

  Modelo Lógico.

  Ho:

  La seguridad perimetral no incide en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.

  H1:

  La seguridad perimetral si incide en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.

Modelo Estadístico.

Para la comprobación de la hipótesis se escogió la prueba Chi cuadrado, cuya fórmula es la siguiente:

$$\chi^2 = \sum \left(\frac{(O - E)^2}{E} \right)$$

Simbología

χ^2	=	Chi cuadrado
$\sum$	=	sumatoria
O	=	frecuencia observada
E	=	frecuencia esperada

- **Determinación del nivel de significación o de riesgo**

  La presente investigación tendrá un nivel de confianza del **0,95** (95%), por tanto un nivel de riesgo es del 5%, es decir α **= 0.05**de probabilidad de rechazo.

- **Calculo de chi-cuadrado**

  ✓ **Elección de la prueba estadística**

  En lo referente a la elaboración de la matriz de tabulación se toma en cuenta tres preguntas del cuestionario aplicado al personal en la investigación.

  1. ¿Con qué frecuencia cree que ocurren inconvenientes en la red?
  2. ¿Cómo califica la calidad del Servicio Informático?
  3. ¿En relación al acceso a los sistemas internos del GADPC, cómo considera el servicio?

✓ **Frecuencia observada**

Tabla 16: Frecuencias observadas

La seguridad perimetral y la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi	ALTERNATIVAS					
	DEFICIENTE	NO TAN BUENO	BUENO	MUY BUENO	EXELENTE	TOTAL
1. Inconvenientes en la red	5	35	37	26	10	113
2. Calidad del Servicio Informático	10	23	29	34	17	113
3. Acceso a los sistemas internos	12	19	28	30	24	113
TOTAL	27	77	94	90	51	339

Fuente: Investigación de Campo
Elaborado por: Fernando Defaz

✓ **Grados de libertad (gl)**

$\mathbf{gl} = (\mathrm{f} - 1) \times (\mathrm{c} - 1)$ $\mathbf{gl} = (3 - 1) \times (5 - 1)$ $\mathbf{gl} = (3 - 1) \times (5 - 1)$ $\mathbf{gl} = 8$

La cantidad de filas y columnas se toman de la tabla 16, frecuencias observadas

✓ **Pruebas de Chi-Cuadrado**

Para la comprobación de Hipótesis se utilizará el Software SPSS, según **Freire (2014), "**es un paquete estadístico especialmente diseñado para resolver problemas en el área de la estadística".

Procedimiento:

1. Ingreso de los datos en el programa SPSS, basado en la tabla 3. De Frecuencias observadas
2. Seleccionar en el menú datos, seguidos de la opción ponderar casos mediante la frecuencia cantidad.
3. Seleccionamos en el menú Estadísticos descriptivos, tablas cruzadas, estadísticos y seleccionamos chi-cuadrado.

4. Resultados.

Tabla 17: Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Preguntas de Encuestas * Respuestas de los Encuestados	339	100.0%	0	0.0%	339	100.0%

Fuente: Software SPSS
Elaborado por: Fernando Defaz

Tabla 18: Tabulación cruzada

		Respuestas de los Encuestados					Total
		Deficiente	No tan Bueno	Bueno	Muy Bueno	Excelente	
Preguntas de la Encuesta	**Inconvenientes en la Red Informática**	5	35	37	26	10	113
	Calidad del Servicio Informático	10	23	29	34	17	113
	Acceso los Sistemas de Información	12	19	28	30	24	113
Total		27	77	94	90	51	339

Fuente: Software SPSS
Elaborado por: Fernando Defaz

Tabla 19: Valores de chi-cuadrado y probabilidad asociada.

	Valor	gl	Sig. asintótica
Chi-cuadrado de Pearson	16.676	8	.034
Razón de verosimilitud	16.894	8	.031
Asociación lineal por lineal	3.694	1	.055
N de casos válidos	339		

Fuente: Software SPSS
Elaborado por: Fernando Defaz

Donde podemos observar:

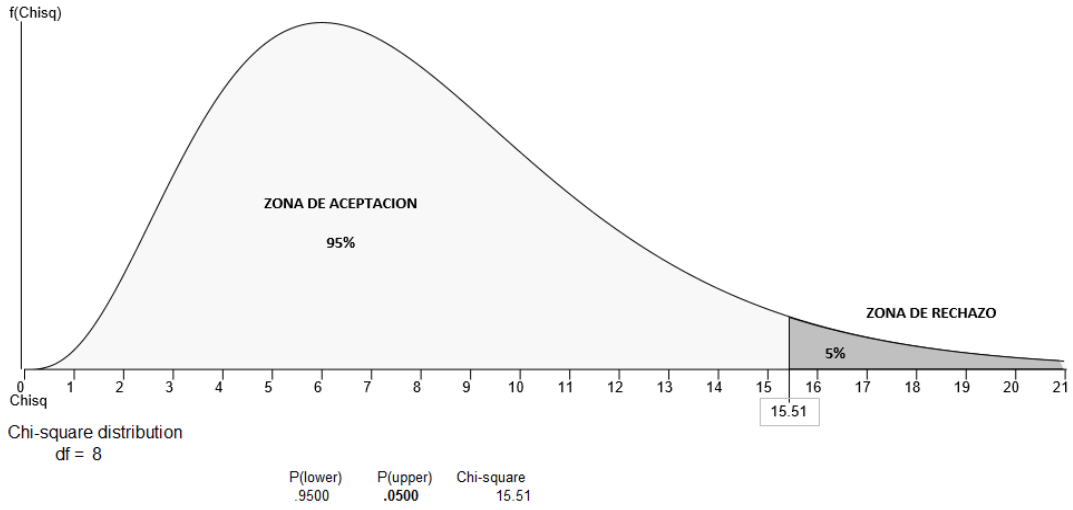
Chi-cuadrado de Pearson con el valor de 16.676, se encuentra en la zona de rechazo de acuerdo a la figura de distribución de chi cuadrado.

Con el valor de p=0.034, que es la probabilidad de rechazo (Significancia asintótica) podemos establecer la siguiente regla de decisión.

✓ **Regla de decisión:**

Si p<0.05. Hay diferencia significativa entre Ho y H1

Si p>=0.05. No hay diferencia significativa entre Ho y H1



Fuente: Investigación de Campo. Calculado con el software MegaStat
Elaborado por: Fernando Defaz

Figura 17: Distribución de chi cuadrado

- **Decisión**

Como: p es menor que 0.05; se rechaza la hipótesis nula y se acepta la hipótesis alternativa, con lo cual se confirma que: La seguridad perimetral si incide en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

En base a la información analizada se deducen las siguientes conclusiones:

- El GAD no dispone de herramientas o sistemas que detecten los intentos de acceso a la red de datos de la institución, por lo que se puede determinar la baja protección de la red y de los servicios informáticos.
- Existen vulnerabilidades en los sistemas de información y en la red informática, lo que evidencia la necesidad de mejorar la seguridad y la calidad del servicio informático del GADPC.
- Si bien la mayoría los servicios informáticos son buenos no se los puede calificar como excelentes, puesto que existen problemas de seguridad y ocasionalmente demora en el flujo de datos y por tanto la red Informática necesita mejoras.
- Los problemas que se han producido en la red interna del GAD, han sido por no contar con políticas de seguridad y procedimientos, que permitan que los procesos sean optimizados en tiempo y costo.

5.2. Recomendaciones

En base a la información analizada se deducen las siguientes recomendaciones:

- Se recomienda utilizar herramientas de monitoreo, para realizar escaneos de seguridad sobre la red, los diversos sistemas operativos y aplicaciones, que evalúen vulnerabilidades específicas y auditen el nivel de seguridad de los sistemas.

- Identificar vulnerabilidades en los activos críticos de la red y proponer una solución de seguridad perimetral para el gobierno autónomo descentralizado de la provincia de Cotopaxi.

- Mejorar la calidad de servicio informático, al ofrecer una garantía en la transmisión de cierto tipo de información, que provea a la red la capacidad de identificar, priorizar los tráficos críticos y mejorar la transmisión de internet.
- Establecer políticas de seguridad informática en el GAD, para definir lo que se puede hacer y lo que está prohibido dentro de los sistemas de información y la red de datos.

CAPÍTULO VI

PROPUESTA

ANÁLISIS DE SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI

6.1. DATOS INFORMATIVOS

Tema: Análisis de solución de seguridad perimetral para el GADPC.

Institución: Gobierno Autónomo Descentralizado de la Provincia de Cotopaxi.

Provincia: Cotopaxi

Cantón: Latacunga

Sostenimiento: Estatal

Dirección: Calle General Proaño y calle Quito

Autoridades del GADPC: 5

Dpto. Informática y Telecomunicaciones: 5

Personal Administrativo, Operativo: 150

6.2. ANTECEDENTES DE LA PROPUESTA

Como bien se planteó al inicio de este proyecto los ataques informáticos a un sistema se encuentran en constante crecimiento, debido principalmente al significativo aumento de la conectividad de dispositivos electrónicos a redes privadas, públicas o *internet*. A consecuencia de este crecimiento, los indicadores de seguridad de un sistema también se incrementan en la medida en que se implementan controles y herramientas específicas para solucionar problemas relacionados a la seguridad de sistemas, redes y usuarios.

Evidentemente el GADPC no es la excepción, en la actualidad cuenta con una red para la gestión administrativa y operativa, esta no posee un *Firewall* para su salida a *internet* y que en total suman casi 160 computadores, lo que ha ocasionado algunos inconvenientes al ser el servidor *proxy* el único que proporciona la salida a *Internet* convirtiéndose en un cuello de botella y en un punto crítico ya que de presentarse daños o inconvenientes toda la institución se queda sin servicio de *internet* por períodos de tiempo indeterminados. No se dispone de una infraestructura de *firewall* que posibilite el crecimiento y administración centralizada de las subredes, y que al momento solo presta el servicio de *internet* para ciertos usuarios. Con la infraestructura existente no puede crecer ni dotar del servicio a más redes ya que no existe un estudio técnico especializado, lo que ha ocasionado algunos problemas al momento de querer expandir o mejorar algún servicio de los que ya se tiene asignados actualmente.

6.3. JUSTIFICACIÓN

Es necesario reconocer la importancia que tiene la protección de los sistemas y de los entornos de red, considerando el incremento masivo de los ataques que se producen cotidianamente. Mantener los recursos de información y telecomunicaciones protegidos, es una de las principales prioridades para el GADPC.

En este proyecto se pretende realizar un estudio sobre las distintas Tecnologías de Seguridad Perimetral, analizando sus características y su funcionamiento para posteriormente elegir uno de los sistemas de detección propuestos.

La investigación cobra mayor relevancia al presentar un diseño de seguridad en un entorno de red real, desarrollada para el GAD de la provincia de Cotopaxi, con un conjunto de herramientas disponibles que podrán ser utilizadas para mejorar el rendimiento y obtener una configuración más adecuada del sistema. Con la propuesta de seguridad perimetral en este entorno, se pretende

identificar posibles usos y penetraciones no autorizados, que informen de actividad maliciosa destinada hacia la red que se pretende proteger.

De todo lo antes expuesto, es conveniente reconocer y mencionar los beneficios que se pueden obtener de este estudio: crecimiento de la red institucional organizado, optimizando recursos y costos, contar con una infraestructura de red segura y con tolerancia a fallas, administración centralizada y controlada del servicio de *internet*, con mayores velocidades de acceso a la información.

6.4. OBJETIVOS

6.4.1. Objetivo General

Realizar un análisis de solución de seguridad perimetral y la relación con la calidad de servicio del gobierno autónomo descentralizado de la provincia de Cotopaxi

6.4.2. Específicos

- Diagnosticar la calidad de servicio de la red informática del GADPC, para la determinación de las vulnerabilidades de los sistemas informáticos.
- Identificar las diferentes tecnologías de seguridad perimetral para la determinación de una solución adecuada para el GADPC.
- Proponer una solución de seguridad perimetral para la mitigación de la vulnerabilidad informática en la red de datos del GADPC.

6.5. ANÁLISIS DE FACTIBILIDAD

El desarrollo de este proyecto ayudará a reforzar la red ya existente, eliminando las vulnerabilidades, propiciando una adecuada administración de *internet*.

Se protegerá con *firewall*, lo cual evitará el pirateo de datos confidenciales y no confidenciales por parte de intrusos, se evitaran además violaciones de códigos de seguridad, logrando conservar no solo la confianza de las instituciones que tienen informaciones importantes, sino de la provincia de Cotopaxi y el país.

Con la instalación y uso de un distribuidor de ancho de banda, se eliminará la sobre utilización de algunos usuarios, mejorando y estabilizando considerablemente la velocidad de *Internet*, y a su vez mejorando también la calidad del servicio.

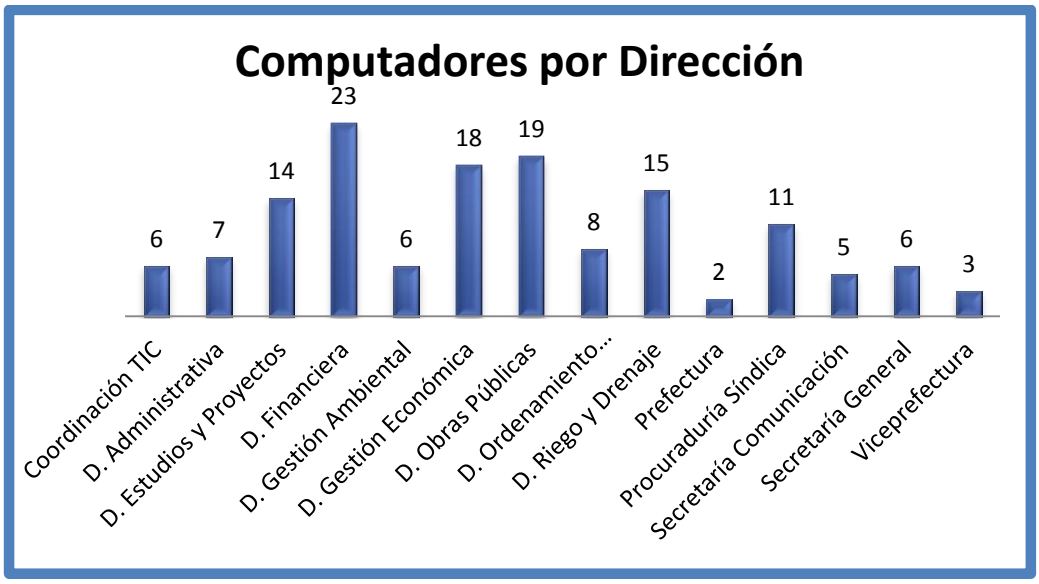
6.5.1. Factibilidad operativa

Para el desarrollo de este proyecto se cuenta con el apoyo del gobierno autónomo descentralizado de la provincia de Cotopaxi, facilitando la información, equipos y herramientas necesarias para el efecto y lo más importante, la autorización para que el personal del área de sistemas participe en el proyecto.

6.5.2. Factibilidad técnica

El GAD cuenta con elementos tecnológicos, para el cumplimiento de sus actividades y funciones diarias de trabajo, base fundamental poner en marcha nuestra investigación.

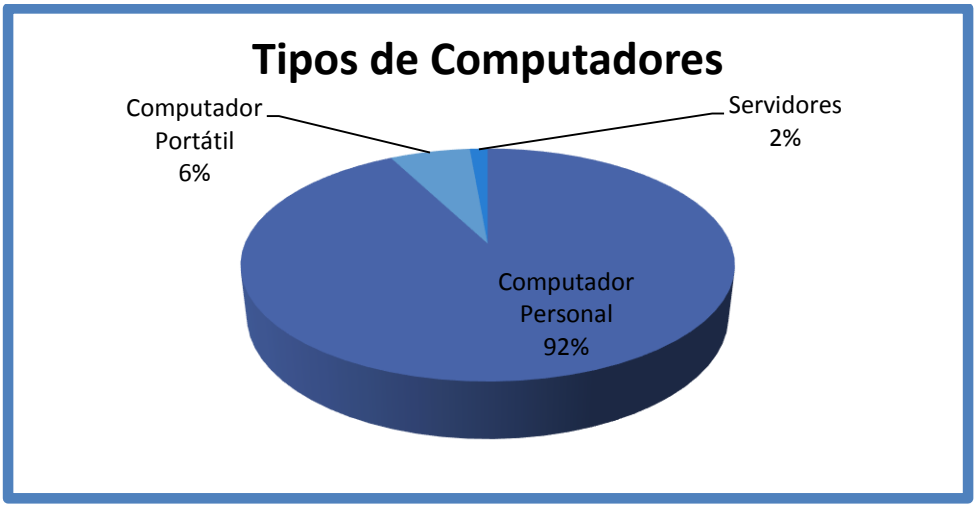
Son 143 computadores distribuidos de la siguiente forma:



Fuente: Investigación de Campo.
Elaborado por: Fernando Defaz

Figura 18: Computadores por dirección

De acuerdo al tipo de computador, el parque informático de la Institución está compuesto por:



Fuente: Investigación de Campo.
Elaborado por: Fernando Defaz

Figura 19: Tipos de computadores

Elementos que permiten la comunicación de la red interna e internet y las impresoras del GAD.

Tabla 20: Elementos tecnológicos pasivos

Activos importantes	Cantidad
***Switch*s: (3com)**	4
Router (Cisco CISCO877-M)	3
Access Point	10
Impresoras láser en red	8

Fuente: Investigación de campo
Elaborado por: Fernando Defaz

6.5.3. Factibilidad económica

El GAD provincial, cuenta con un presupuesto para cada uno de los proyectos que emprende, el departamento de sistemas, tiene asignado un presupuesto para proyectos de desarrollo encaminados a mejorar el servicio tecnológico. Este financiamiento consta en el presupuesto anual de la institución.

6.6. FUNDAMENTACIÓN

- **Norma *ISO* 27001**

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (*ISO*) y describe cómo gestionar la seguridad de la información en una empresa. Proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

Fuente: Investigación de Campo. 27001 Academy (2013)
Elaborado por: Fernando Defaz

Figura 20: Estructura de *ISO* 27001

- **Análisis de impacto y análisis de riesgos**

Mañas José (2011) comenta que:

> Tras inventariar activos y amenazas, hay que calificar cada escenario posible para conocer su impacto y su riesgo.
>
> Se llama análisis de impacto al ejercicio de imaginarse las consecuencias de que haya un incidente o acción deliberada.
>
> El riesgo va un paso más allá y ordena los incidentes según la probabilidad de que ocurran. Con esas estimaciones podemos priorizar los riesgos y concentrarnos en aquellas cosas más probables y que traigan las peores consecuencias.

A veces se llaman indicadores del estado de seguridad y sirven para tomar decisiones. El impacto mide lo que puede pasar. El riesgo mide lo que probablemente pase.

- **Gestión de riesgos**

Para**Mañas José (2011)** existen 4 formas de afrontar los riesgos:

> **Evitar la situación.-** Se debe preguntar si necesitamos todo lo que tenemos. Por ejemplo, poner un servidor Web público en el servidor de bases de datos puede ser una forma de dar un excelente servicio a los clientes, pero también abre la puerta a que haya una fuga o un robo de información. Podemos separar el servidor de base de datos del de acceso público y así el escenario de riesgo es otro.
>
> **Mitigar el peligro.-** El riesgo se mitigas con medidas preventivas. Por ejemplo, si se tiene copias de seguridad de la información, no se impide que se pierda un archivo o que se averíe el servidor de bases de datos, pero se sabe que se recupera rápidamente la información y se sigue trabajando.
>
> **Aceptar riesgos.-**Muchas actividades consisten en buena medida en asumir riesgos para alcanzar ciertos beneficios. Lo que el análisis de riesgos proporciona es la información para saber qué nos estamos jugando y tomar decisiones informadas. No las puede tomar un técnico, las tiene que tomar la dirección. Por ejemplo, el comercio electrónico.
>
> **Pasárselo a otro.-** Contratar un seguro es pasarle el riesgo a la aseguradora.

- **Seguridad Informática**

De acuerdo **Stallings W. (2004:262)**,

La definición y el objetivo de la seguridad en las redes es mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.

- **Tipos de seguridad**
  - ✓ **Seguridad Física**

    La seguridad física está relacionada con los recursos y el espacio físico utilizados para la protección de los elementos que conforman los sistemas de información dentro de la empresa

  - ✓ **Seguridad Lógica**

    La seguridad lógica está relacionada con los procedimientos y recursos lógicos utilizados para proteger los sistemas de información dentro de la empresa

- **Servicios de seguridad**

  - ✓ **Autenticidad**

    Garantiza que una entidad es quien dice ser. El servicio de autenticidad protege del ataque de suplantación de personalidad.

  - ✓ **Integridad**

    El objetivo de este servicio es garantizar que los datos y recursos no han sido alterados y sean fiables.

  - ✓ **Disponibilidad**

    El objetivo de esta propiedad es garantizar que la información y los servicios no sean interrumpidos y permanezcan accesibles en forma permanente.

- ✓ **Confidencialidad**

  El objetivo de esta propiedad es garantizar que la información no sea revelada a personas no autorizadas

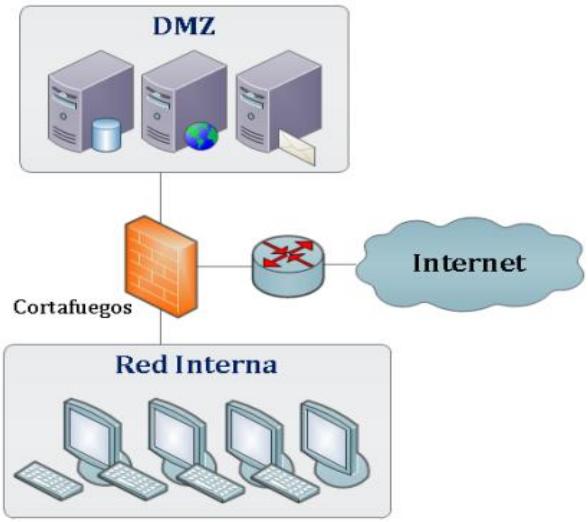
- **Seguridad perimetral**

Para Staff (2011) La solución de seguridad perimetral,

> Protege las redes de ataques informáticos como *crackers*, ataques de negación de servicio (*Denied of Service -DoS*), virus, gusanos, troyanos, *spam*, contenido malicioso en correos y páginas *web*, protegiendo a la red en todos los enlaces, puntos de conexión o perímetro de la misma, incluyendo *VPN´s* y enlaces a *Internet*.

- **Zona Desmilitarizada (*DMZ*)**

De acuerdo a lo descrito por**Ramos Fraile (2011)**, "Una *DMZ* o zona desmilitarizada (*Demilitarized Zone*) es una subred situada entre la red interna, como puede ser una *LAN*, y entre una red externa, por ejemplo *Internet"*.



Fuente: Ramos Fraile (2011)
Elaborado por: Fernando Defaz

Figura 21: Zona Desmilitarizada (*DMZ*)

- **Características de una *DMZ*:**
  - ✓ Diseño de una red local ubicada entre la red interna y la red externa (p. ej. Internet).
  - ✓ Utilizada para servicios públicos: correo electrónico, *dns, web, ftp*, que serán expuestos a los riesgos de seguridad.
  - ✓ Creada mediante uno o dos cortafuegos que restringe el tráfico entre las tres redes.
  - ✓ Desde la DMZ no se permiten conexiones a la red interna.

- **El *Firewall***

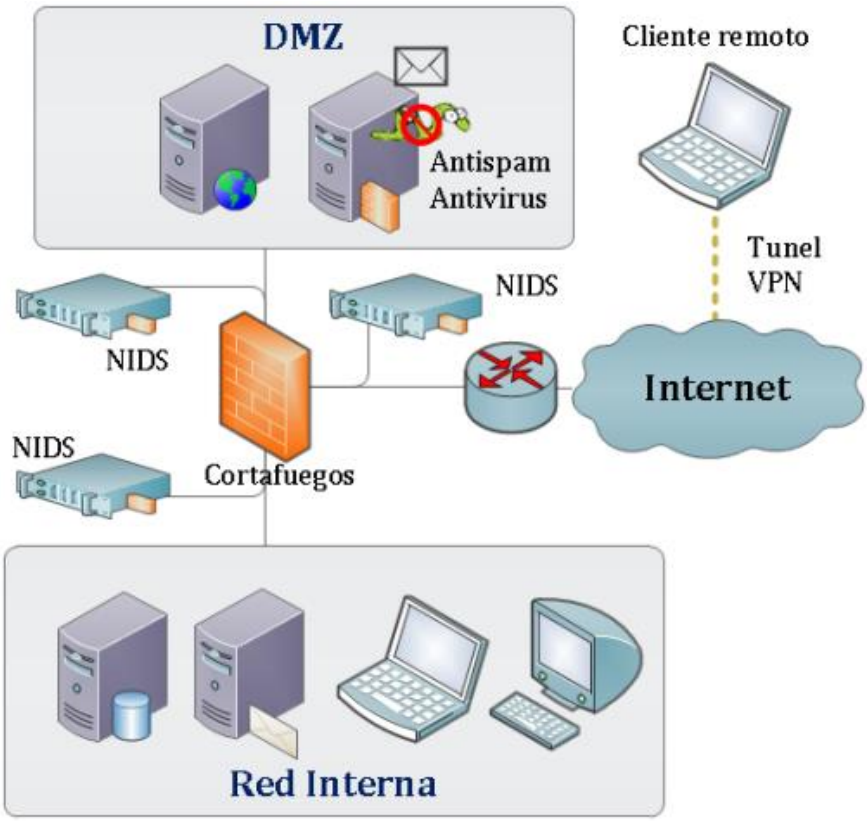
Contreras Vega (2004)lo define como, "un sistema o grupo de sistemas que impone una política de seguridad entre la red privada de una organización y el *Internet*. Es una colección de elementos, tanto software como de hardware, destinado a filtrar todo el tráfico desde la *Internet* hacia nuestra red".

Posteriormente el propio *firewall* se encargará de verificar que todos y cada uno de los paquetes con destino al servidor se cumplan, descartando aquellos que no lo hagan.

Un *firewall* contiene usualmente ya configuradas las principales políticas de seguridad generales para cualquier organización sin embargo le permite definir sus propias reglas de seguridad.

- **Gestión Unificada de Amenazas**

Según el curso de **Intypedia (2014) "**Un sistema de Gestión Unificada de Amenazas *UTM (Unified Threat Management)*, es un único equipo que incluye múltiples características de seguridad: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus y anti spam y redes privadas virtuales".



Fuente: Ramos Fraile (2011)
Elaborado por: Fernando Defaz

Figura 22:Gestión Unificada de Amenazas (*UTM)*

- **Calidad de servicio QoS**

El término calidad de servicio hace referencia a una cantidad de tecnologías, que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío.

Según **García F. (2009:140)**,

> Es hacer que los Reuters y los Switches de red funcionen de maneras distintas para cada tipo de servicio (voz, datos, video) del tráfico de la red. Al utilizar la calidad de Servicio, distintas

aplicaciones de red pueden coexistir en la misma red sin consumir cada ancho de banda de las otras.

6.7. METODOLOGÍA, MODELO OPERATIVO

6.7.1. Modelo Operativo

La siguiente tabla muestra el modelo operativo para la ejecución de solución de seguridad perimetral para el GADPC.

Tabla 21: Modelo Operativo

OBJETIVO	META	ACTIVIDADES	RESULTADOS	PLAZO (DIAS)
PLANIFICACIÓN				
Realizar la planificación de solución de seguridad perimetral basado en el estándar 27001.	Establecer una serie de pasos sistemáticos que determinen la metodología de seguridad perimetral para el gobierno autónomo descentralizado de la provincia de Cotopaxi.	Determinar las fases y procesos para: • Análisis de riesgos • Diseño de seguridad para el GADPC. • Políticas de seguridad. • Tecnología de seguridad perimetral.	• Planificación de la solución de seguridad perimetral para el GADPC	7
SOCIALIZACIÓN				
Socializar el plan solución de seguridad perimetral, su funcionamiento y aplicación.	Dar a conocer a las autoridades del gobierno autónomo descentralizado de la provincia de Cotopaxi, de qué manera se pretende dar solución al problema de inseguridad de la red informática de la institución,	Explicación de las fases a desarrollarse en la aplicación de la metodología de seguridad informática. • Diálogos • Exposición	• Aprobación de las autoridades para continuar con la ejecución de la propuesta	2
EJECUCIÓN				
Aplicar la metodología de seguridad perimetral	Identificar las vulnerabilidades de la red informática y proponer una solución de seguridad perimetral.	Ejecutar las fases y procesos para: • Análisis de riesgos • Diseño de seguridad para el GADPC. • Políticas de seguridad. • Tecnología de seguridad perimetral.	• Solución de seguridad perimetral para el gobierno autónomo descentralizado de la provincia de Cotopaxi	40
EVALUACIÓN				
Realizar una continua revisión de evaluación, basado en una estricta vigilancia durante el desarrollo de la propuesta**.**	Mejorar la seguridad del acceso a la información, datos y recursos informáticos del gobierno autónomo descentralizado de la provincia de Cotopaxi.	Verificación de vulnerabilidades con herramientas de software disponibles en internet, sin fines comerciales para: escaneo de seguridad, auditar los niveles de seguridad de los sistemas y proponer sugerencias de solución de seguridad.	Solución de seguridad perimetral para el gobierno autónomo descentralizado de la provincia de Cotopaxi	

Fuente: Investigación campo
Elaborado por: Fernando Defaz

6.7.2. Metodología

Con el objetivo de alcanzar una *LAN* efectiva con una adecuada seguridad perimetral y calidad de servicio, capaz de satisfacer las necesidades de la red informática del GADPC y por tanto de sus usuarios, es esencial cumplir con una serie planificada de pasos sistemáticos, basados en el estándar *ISO* 27001, adaptado a las necesidades de la institución. A continuación se realiza una breve descripción de la planificación de la metodología.

- **Análisis de riesgos**

Este es un método que está basado en un conjunto de criterios, los cuales definen los elementos esenciales para la evaluación del riesgo de seguridad.

Comprende básicamente 3 grandes fases:

1. **Identificación de activos – Perfiles de Amenazas.-** En esta fase, se debe recoger: Información de activos existentes, requerimientos de seguridad, áreas de interés, estrategias de protección actuales y vulnerabilidades existentes.

2. **Identificación de Vulnerabilidades en la Infraestructura.-** Enfoca a las vulnerabilidades tecnológicas que afectan a los activos críticos y componentes de infraestructura que soportan a estos activos.

3. **Define los riesgos asociados con los activos críticos y crea planes de mitigación para esos riesgos.**

- **Diseño de seguridades**

Es una guía para asegurar las redes, ya que ellas seguirán ofreciendo todos los servicios que el usuario espera de la red.

Se basa en un enfoque modular por dos motivos importantes.

1. El diseño relaciona la seguridad entre los distintos bloques funcionales de la red

2. Permite diseñar la seguridad módulo a módulo en lugar de hacerlo generalmente.

- **Políticas de seguridad**

Para la elaboración de políticas se utilizará como guíala NORMA ISO 177999, tanto para la seguridad física como lógica de la red, que tratan de promover sistemas de calidad para la seguridad del usuario.

- **Tecnología de seguridad perimetral**

A fin de considerar los dispositivos más apropiados para el desarrollo del proyecto, se vuelve necesario comparar y caracterizar las tecnologías que más se ajusten a las necesidades, condiciones y régimen de trabajo que demanda la red ya existente, lo cual se realizará basados en la técnica del cuadrante mágico de GARTNER, en aras de hacer una buena elección y con el objetivo de eliminar las vulnerabilidades y elevar la calidad del servicio informático del GADPC.

La siguiente tabla describe una serie de pasos sistemáticos que determinan la metodología de seguridad perimetral para el gobierno autónomo descentralizado de la provincia de Cotopaxi.

Tabla 22: Planificación para la solución de seguridad perimetral para el GADPC

OBJETIVO	META	ACTIVIDADES	RESULTADOS	PLAZO (DIAS)
ANÁLISIS DE RIESGOS				
Identificar las amenazas que un sistema de información y su entorno pueden tener. Cuantificar las consecuencias e impacto generado por los ataques y amenazas concretados.	Identificar activos y perfiles de amenazas.	Recopilación de la información de activos existentes, requerimientos de seguridad, áreas de interés, estrategias de protección actuales y vulnerabilidades existentes.	• Activos existentes. • Requerimientos de seguridad. • Estrategias de protección actuales. • Vulnerabilidades existentes	7
	Identificar vulnerabilidades en la infraestructura.	Identificar las vulnerabilidades tecnológicas que afectan a los activos críticos y componentes de infraestructura que soportan a estos activos.	• Principales causas de amenazas. • Consecuencias. • Requerimientos de seguridad. • Identificación del sistema de seguridad actual. • Creación de perfiles de amenazas. • Identificación de componentes claves • Evaluación de vulnerabilidades en la red	7
	Realizar el análisis de resultados. Realizar la determinación de requerimientos.	Analizar resultados. Determinar requerimientos	• Análisis de resultados. • Requerimientos de seguridad	5
DISEÑO DE SEGURIDAD PARA EL GADPC				
Diseñar la seguridad física.	Proteger los activos informáticos del GAD de los riesgos de desastres naturales, actos accidentales o mal intencionados.	Proponer un diseño que relacione la seguridad entre los distintos bloques funcionales de la red.	• Diseño de la seguridad física	4
	Minimizar la pérdida de información y garantizar la recuperación de la misma.			
	Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.			

Fuente: Investigación campo
Elaborado por: Fernando Defaz

Tabla 22: Planificación para la solución de seguridad perimetral para el GADPC (continuación)

OBJETIVO	META	ACTIVIDADES	RESULTADOS	PLAZO (DIAS)
Diseñar la seguridad lógica.	Definir y controlar los permisos y accesos a los programas y archivos	Proponer un diseño que relacione la seguridad entre los distintos bloques funcionales de la red.	• Diseño de la seguridad lógica	4
	Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos.			
	Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento.			
	Asegurar que la información trasmitida sea recibida por el destinatario al cual fue enviada y que la información sea la misma.			
POLÍTICAS DE SEGURIDAD				
Elaborar políticas de seguridad	Elaborar una guía de políticas.	Establecer políticas de seguridad informática.	• Guía de políticas de seguridad	4
TECNOLOGÍA DE SEGURIDAD PERIMETRAL				
Analizar las tecnologías de seguridad perimetral	Seleccionar la tecnología adecuada	Comparación de tecnologías de seguridad perimetral aplicando el diagrama mágico de Gartner	• Tecnología de seguridad para el GADPC	3

Fuente: Investigación campo
Elaborado por: Fernando Defaz

6.7.3. Aplicación de la metodología de solución de seguridad perimetral en el GADPC.

La aplicación de la metodología de seguridad informática en el GAD permitió la obtención de los siguientes resultados en cada etapa:

6.7.3.1. Análisis de riesgos

Definición de Riesgo

Es la probabilidad de que una amenaza o ataque ocurra y provoque un efecto negativo en la red. El riesgo es mayor mientras mayor es el valor del activo y mayor su grado de exposición a amenazas.

El riesgo no puede eliminarse por completo, pero si se puede reducir.

Objetivos del Análisis de Riesgos:

Identificar las amenazas que un sistema de información y su entorno pueden tener.

Cuantificar las consecuencias e impacto generado por los ataques y amenazas concretados.

- **Identificación de los activos**

Tabla 23: Resumen de Activos

ACTIVOS IMPORTANTES	DESCRIPCIÓN
INFORMACIÓN	
Bases de datos Magan (Funcionando en una PC de Escritorio)	Almacena Información: • Contable • Financiera • Activos Fijos e Inventario
Base de datos Vehicular	Almacena Información: • Control Vehicular • Gastos Movilidad • GPS (en construcción)

Fuente: GADPC
Elaborado por: Fernando Defaz

Tabla 23: Resumen de Activos (continuación)

ACTIVOS IMPORTANTES	DESCRIPCIÓN
Software	
Sistema Integrado Megan	Sistema para el control Vehicular, en lo que se refiere a gastos de movilidad, ubicación de las unidades, combustible, inventario, repuestos etc.
Sistema Integrado Megan	Sistema para la administración de activos fijos e inventarios, y la parte Financiera Contable.
Hardware	
PCs: (200)	Estaciones de trabajo de cada usuario de la red donde almacenan información de las actividades que desempeñan
Servidor IBM Centos:(1)	Utilizado para la base de datos Vehicular. Actualmente en mantenimiento.
Servidor Blade:(1)(No en Funcionamiento)	PROCESADOR: Familia de productos E5-2600 con procesador Intel Xeon, con hasta ocho cores y procesamiento de hasta 16 subprocesos simultáneos MEMORIA: 32 GB a 1333 MHz DIMM; Double Data Rate (DDR)3 con detección y corrección de errores (ECC) de perfil muy bajo (VLP), a 1333 o 1600 MHz, duplicación de memoria y asistencia de recambios DISCOS DUROS: 2 de 146GB 2.5” SFF Slim-HS 15K 6Gbps SAS HDD
*Switch*s: (3com)(4)	Equipo mediante el cual se establece la comunicación al interior de la intranet y son parte fundamental del backbone de la red
Router (Cisco CISCO877-M)(3)	Equipo mediante el cual se establece la conexión hacia el exterior de la red.
Access Point: (10)	Componentes Wireless
Laptops(5)	Equipos utilizados en reuniones o comisiones de trabajo donde almacenan información y son utilizados en su mayoría como estaciones de trabajo
Impresoras láser en red: (8)	Compartidas en red para el uso exclusivo del personal interno.

Fuente: GADPC
Elaborado por: Fernando Defaz

- **Activos Críticos**
  - ✓ **Información**

Dentro de este grupo tenemos como principal activo a la Base de Datos MEGAN, que contiene la información medular del GAD, esto es información financiera de la Institución como son los salarios, gastos, cuentas contables, activos e inventarios.

La base de datos Vehicular, es otro activo crítico ya que en ella se almacena Información del Control Vehicular, Gastos Movilidad, GPS (en construcción), que la actualidad dejo de funcionar por inconvenientes administrativos.

  - ✓ **Software**

Dentro de este grupo tenemos como activo importante el sistema integrado MEGAN, mediante el cual se tiene acceso y se manipula la información de la base de datos antes descrita, es un sistema desarrollado en la misma institución bajo la plataforma Windows con My SQL y PHP.
El Sistema Vehicular es otro activo importante ya que maneja toda la información vehicular de mucha importancia para la institución, desarrollado en PHP con PostgreSQL.

  - ✓ **Hardware**

Se considera como activos críticos de hardware a los equipos que son importantes en el procesamiento, almacenamiento y transmisión de la información crítica descrita anteriormente.

    - ➢ **Servidores**

En la siguiente tabla se describen las características y funciones de cada Servidor.

Tabla 24: Servidores. Características y Funciones

TOTAL	MODELO	CARACTERÍSTICAS	FUNCIÓN
1	Servidor IBM	• Core-Doble IntelÃ‚Â® XeonÃ‚Â® Processor 5130 hasta 2.0 GHz y hasta 1333 MHz front-side bus orQuad-Core Intel Xeon Processor E5335 hasta 2.0 GHz • 1 GB/32 GB FullyBuffered DIMM 667 MHz a través de 8 ranuras DIMM • 4.0 TB hot-swap SATA, 2.4 TB hot-swap SAS, or 3.0 TB simple-swap SATA • Numero de Procesadores 1/2 • L2 2×2 MB (doble-core) o 2×4 MB (quad-core)	• Servidor con Sistema Operativo Linux Centos 6.4 • Base de datosVehicular desarrollado en Postgres SQL.
1	Servidor Blade	• PROCESADOR: Familia de productos E5-2600 con procesador Intel Xeon, con hasta ocho cores y procesamiento de hasta 16 subprocesos simultáneos • MEMORIA: 32 GB a 1333 MHz DIMM; Double Data Rate (DDR)3 con detección y corrección de errores (ECC) de perfil muy bajo (VLP), a 1333 o 1600 MHz, duplicación de memoria y asistencia de recambios • • DISCOS DUROS: 2 de 146GB 2.5” SFF Slim-HS 15K 6Gbps	• En Mantenimiento

Fuente: GADPC
Elaborado por: Fernando Defaz

- **Router Cisco 877-M**

Características:

32 MB Flash

64 MB DRAM

Cisco IOS IP Software Feature

Funcionalidades de voz

Interfaces WAN son incluidas por separado

- ***Switchs 3COM***

Características

24 ports 10/100 Mbps Nway auto-negociables

Auto MDI-II/MDI-X ports (todos los puertos son Up-link con cualquiercable)

Integrate address Look-Up Engine, supports up to 8 K absolute MAC address

2.5 Mb internal RAM for frame buffering

Modo de Transmisión Full/Halfduplex para cada Puerto (200 Mbps)

Tazas Wire-speed filtering/forwarding

Control de flujo IEEE 802.3x flow para modo Full-duplex

Control de flujo Back pressure para modo Full-duplex

Método Store-and-forward switching

Extensivefront-panel diagnosticLEDs

- **Cableado:** UTP Categoría 5e

- **PCs.**

Según el inventario realizado, se resume lo siguiente:

Se cuenta con 200 equipos personales

El 90% de los usuarios almacenan la información en los respectivos discos duros de los equipos a su cargo. Estos discos duros tienen una capacidad de almacenamiento de alrededor de 40 GB.

El 30%, esto es 60 equipos, tienen licencias para el sistema operativo, aplicaciones y herramientas de oficinas.

Los equipos personales son Clones, con sistema operativo Windows XP, Windows 2000 Profesional, con 512 MB en RAM, 40 GB en Disco duro como mínimo.

Utilizan como aplicaciones principales: Office 2000 Profesional, WinZip, *Internet* Explorer.

- **Portátiles**

  Según el inventario realizado se concluyó que:

  Existen 5 computadores portátiles, cada uno configurado para acceder a la red de la intranet

  El 90% de los equipos son utilizados como máquinas de escritorio y adicionalmente son empleados para reuniones o comisiones de trabajo fuera de la institución.

  En la mayoría de discos duros se almacena información institucional por utilizarlas como equipos personales.

- **Servicio de web hosting**

  Además de los equipos que se encuentran en la intranet, se tiene un Web hosting, donde se encuentra almacenadas algunas aplicaciones como: La página web del GAD, Proyectos de Sociales etc., además se cuenta con un espacio para bases de datos.

- **Seguridades físicas**

  Las instalaciones físicas del GAD, consisten en un edificio de tres pisos, los cuales son custodiados por guardias, los lugares donde se encuentran los servidores tienen acceso restringido y se encuentran cerradas generalmente con llave que posee el administrador de la red.

  Se cuenta con una unidad UPS que provee energía eléctrica en caso de un cese de fluido eléctrico a los servidores, con el objeto de salvaguardar los equipos y los datos de posibles daños.

- **Seguridades lógicas**

  En el siguiente resumen dado por los técnicos del servidor se detalla la seguridad con la que cuenta.

El servidor cuenta con un sistema operativo Linux Centos 6.4 en el caso de existir algún servicio innecesario es removido del sistema para disminuir el número de programas que necesitarían seguridad. Los puertos que son comúnmente usados por los hackers para atacarlos son protegidos por *firewall*s.

Todos los password son cambiados con palabras seguras, no adivinables.

El software que es usado en el sistema es actualizado o parchado apropiadamente contra las vulnerabilidades de seguridad cuando son descubiertos.

En los servidores se ejecutan programas de seguridad para detectar programas sospechosos, si uno es descubierto se envía mensajes a los técnicos para revisar los servidores de esta manera la actividad en la red es monitoreada.

Cada usuario posee un USERNAME y PASSWORD tanto para el personal técnico como para los operarios de las PCs.

El administrador del sistema, en este caso el responsable del proceso de informática, es quien crea las cuentas a cada usuario.

Para seguridad de los datos y de la red de posibles accesos no deseados no poseen un *firewall*, y no hay mecanismos adicionales de autentificación, tampoco perfiles o políticas de acceso para usuarios.

- **Respaldo de datos**

No se realiza respaldo diario de las BDDs.

- **Seguridades legales**

  La institución no cuenta con todas las licencias requeridas por la ley, ya que solo se tienen 60 licencias para Microsoft Windows y existen alrededor de 200 terminales con este producto.

- **Identificación de vulnerabilidades existentes**

Como se mencionó anteriormente la propuesta se basa en la norma ISO 27001, luego de la identificación de activos, se debe identificar las amenazas de los activos, las áreas que son afectadas, sus causas y consecuencias.

- **Principales causas de amenazas**

  - ✓ **Acción deliberada o accidental por parte de personas.-** Este grupo incluye a personas que son parte del GAD, así como a personas que no pertenecen a él, quienes pueden tomar acción deliberada sobre los activos.
  - ✓ **Problemas de Sistemas.-** Estos problemas son por ejemplo defectos de hardware, defectos de software, no disponibilidad de los sistemas, virus, código malicioso, y otros problemas relacionados.
  - ✓ **Otros Problemas.-** Estos son problemas que están fuera de algún control. Esto puede incluir desastres naturales.

- **Consecuencias de las Amenazas**

  - ✓ Revelación u observación de información.
  - ✓ Modificación de información importante.
  - ✓ Destrucción o pérdida de la información, hardware o software importante.
  - ✓ Interrupción de acceso a la información, software, aplicaciones o servicios.

En la siguiente tabla se detalla las amenazas y sus consecuencias para cada activo, tanto de información, así como de hardware y software.

Tabla 25: Amenazas y sus Consecuencias

ACTIVO	CAUSAS DE AMENAZAS			CONSECUENCIA			
	Acción deliberada o accidental por parte de personas	Problemas de sistemas	Otros Problemas	Revelación	Modificación	Destrucción y/o pérdida	Interrupción
INFORMACIÓN							
Base de datos MEGAN	X	X		X	X	X	X
Base de datos Vehicular	X	X		X	X	X	X
HARDWARE							
Servidor IBM	X	X				X	X
Servidor Blade	X	X				X	X
Router		X				X	X
Switchs		X				X	X
SOFTWARE							
Sistema MEGAN	X	X		X	X	X	X
Sistema Vehicular	X	X		X	X	X	X

Fuente: GADPC
Elaborado por: Fernando Defaz

- **Análisis de las amenazas**

✓ **Información**

Como muestra la tabla, la Información tiene como fuente de amenaza la acción deliberada o accidental de personas que se encuentran dentro o

fuera del GAD, debido a que muchos usuarios confían sus contraseñas a otras personas. Adicionalmente no existe mucha seguridad en las oficinas y los usuarios dejan aplicaciones abiertas. Esto puede ocasionar la revelación, modificación o pérdida de la información

✓ **Hardware**

Una amenaza para el hardware, es el robo de portátiles y por ende el robo de la información existente en dichos equipos.

Se puede tener también problemas de sistemas debido a hardware defectuoso.

Adicionalmente el hardware está expuesto a otro tipo de amenazas como desastres naturales, cortocircuitos.

Como consecuencia de estas amenazas se tiene la suspensión del servicio que brindan las aplicaciones del GAD.

✓ **Software**

Una fuente de amenaza para el software del GAD, son básicamente los problemas del sistema, que se describen A continuación:

- Cuellos de botella
- Códigos Maliciosos
- Retardos en las Aplicaciones
- Aplicaciones no disponibles

Como consecuencia de estas amenazas, se tiene la interrupción del servicio de las aplicaciones del GAD.

- **Requerimiento de seguridad**

En la siguiente tabla se identifica los requerimientos de seguridad para los activos críticos.

Tabla 26: Requerimientos de seguridad de cada activo

ACTIVO	REQUERIMIENTO DE SEGURIDAD
INFORMACION	
Base de datos MEGAN	• Disponibilidad • Acceso a la información es requerida las 24 h. • Integridad • Los nuevos ingresos y la modificación deben ser realizados por personas autorizadas • Confidencialidad • Puede ser conocido
Base de datos Vehicular	• Disponibilidad • Acceso a la información las 24 h. • Integridad • Esta información debe ser manejada por personas autorizadas de cada área • Confidencialidad • Solamente el área puede conocer la información respectiva
HARDWARE	
Servidor de Correo Servidor Web Servidor MEGAN Servidor Vehicular Router *Switch*s	• Disponibilidad • Acceso a la información las 24 h. • Integridad • Administrado solo por el personal de sistemas • Confidencialidad
SOFTWARE	
Servidor MEGAN	• Disponibilidad • Acceso a la información las 24 h. • Integridad • Solo manipulado por el personal autorizado • Confidencialidad • Solo conocido por personal autorizado
Servidor Vehicular	• Disponibilidad • Acceso a la información 24 h. • Integridad • Solo manipulado por el personal autorizado • Confidencialidad • Solo conocido por el personal autorizado

Fuente: GADPC
Elaborado por: Fernando Defaz

Según la tabla anterior, se resume lo siguiente:

- ✓ **Información**

  Disponibilidad: Las bases de datos deben estar disponibles las 24 h., por consultas o por trabajos fuera de horario.

  Integridad: Todos los ingresos y modificaciones deben ser realizados por personas autorizadas de las áreas correspondientes.

  Confidencial: Solo por el personal autorizado.

- ✓ **Hardware**

  Disponibilidad: El hardware tiene que estar disponible todo el tiempo de manera que permita el funcionamiento óptimo de la red.

  Integridad: Solo puede ser administrado por el departamento de sistemas.

- ✓ **Software**

  Disponibilidad: Las aplicaciones tienen que estar disponible las 24 h. para brindar los diferentes servicios al personal autorizado.

  Integridad: Las actualizaciones o modificaciones a los sistemas deben ser realizadas por el departamento de informática.

  Confidencialidad: Conocido solo por el departamento de informática.

- ▪ **Identificación del Sistema de Seguridad actual en el GAD**

Según las reuniones con el coordinador sistemas, se han obtenido los siguientes resultados:

- ✓ Existen estrategias de seguridad basadas en los objetivos del GAD, sin embargo éstos no son documentados ni revisados periódicamente.
- ✓ El GAD no da a conocer sobre la responsabilidad que el personal debe tener con la seguridad de la información, pues en los contratos laborales no existe una cláusula que indique aquello.
- ✓ Adicionalmente existe poco interés para invertir en soluciones de seguridad.
- ✓ No existe ninguna documentación sobre políticas de seguridades, ni un plan de contingencia en la organización.
- ✓ No existen políticas de seguridad ni procedimientos para controlar el acceso físico al personal, al hardware o dispositivos de comunicación, cabe mencionar que por esta falta de políticas ya se ha tenido pérdidas.
- ✓ Existe un control de activo (hardware y equipos de oficina) por parte del departamento administrativo. No existe un plan para el mantenimiento de equipos tanto para hardware y software, cada equipo que llega a tener problemas es reparado en ese momento.
- ✓ Los respaldos de la información se guardan en otra máquina dentro de la misma organización.
- ✓ Cada usuario cuenta con una password para el ingreso al SO, y para algunas aplicaciones que manejan información.
- ✓ El monitoreo de la red son revisados frecuentemente por el administrador, pero no existe un firewall para mitigar vulnerabilidades encontradas.
- ✓ No existen procedimientos para el manejo de vulnerabilidades.

- **Creación de Perfiles de Amenazas**

Siguiendo con el estándar ISO 27001, se procederá con un perfil de amenazas:

Acceso a la Red.- Es decir, cuando se amenaza a un activo utilizando la red en una forma accidental o deliberadamente.

Acceso Físico.- Cuando se amenaza a un activo desde el espacio físico mediante un actor humano

Problemas del sistema.- Cuando se amenaza a un activo mediante problemas de software, hardware o alguna aplicación por ejemplo: Defectos de software, virus, amenazas vía *internet*, caídas del sistema, defectos de hardware.

Otros problemas.- Cuando se amenaza a un activo crítico, mediante desastres naturales, problemas con tercerizadoras, problemas de telecomunicaciones, problemas de proveedores.

- **Análisis de las amenazas cuando los actores humanos accesan a la red y al espacio físico**

Puede haber una modificación o pérdida de la información en las bases de datos causada por actores internos y externos de la organización. Actualmente se cuenta con una seguridad básica para el ingreso a los equipos que consisten en claves o perfiles de usuarios, pero no existe un documento donde se identifiquen las prácticas de seguridad para el personal, tales como: Políticas de passwords, que no se divulgue información importante, asegurar la información del cual ellos son responsables, etc.

Con respecto a los sistemas, la mayoría accesan a la información de las base de datos y por contar con servidores de poca capacidad existe en

muchas ocasiones cuellos de botella lo que ocasiona que la aplicación sea interrumpida o no esté disponible.

Con respecto al hardware, muchas veces se interrumpe el trabajo debido a algún daño en el equipo. No existe un plan de mantenimiento, uno de los problemas más frecuentes es la fuente de poder que deja de funcionar, en varias ocasiones hasta quema los demás dispositivos, lo que retrasa como mínimo un día de trabajo.

- **Análisis de las amenazas cuando el actor son los problemas del sistema y otros**

Los principales problemas son las infecciones por virus, troyanos, spam o ataques externos vía *internet*, aunque la organización cuenta con un antivirus (AVG Edición Free), la mayoría de veces no ha sido lo suficiente para arreglar los equipos.

- **Identificación de componentes claves**

Luego de la creación de perfiles de amenazas se identificó a cada activo con un valor de importancia dependiendo del daño que causarían si se perdiera dicho activo. El valor de importancia varia de 1 a 5, donde: 1 es de menor importancia y5 el de mayor importancia.

Tabla 27: Identificación de componentes claves

ACTIVO	IMPORTANCIA
Información	5
Hardware	4-3-2
Software	3-2

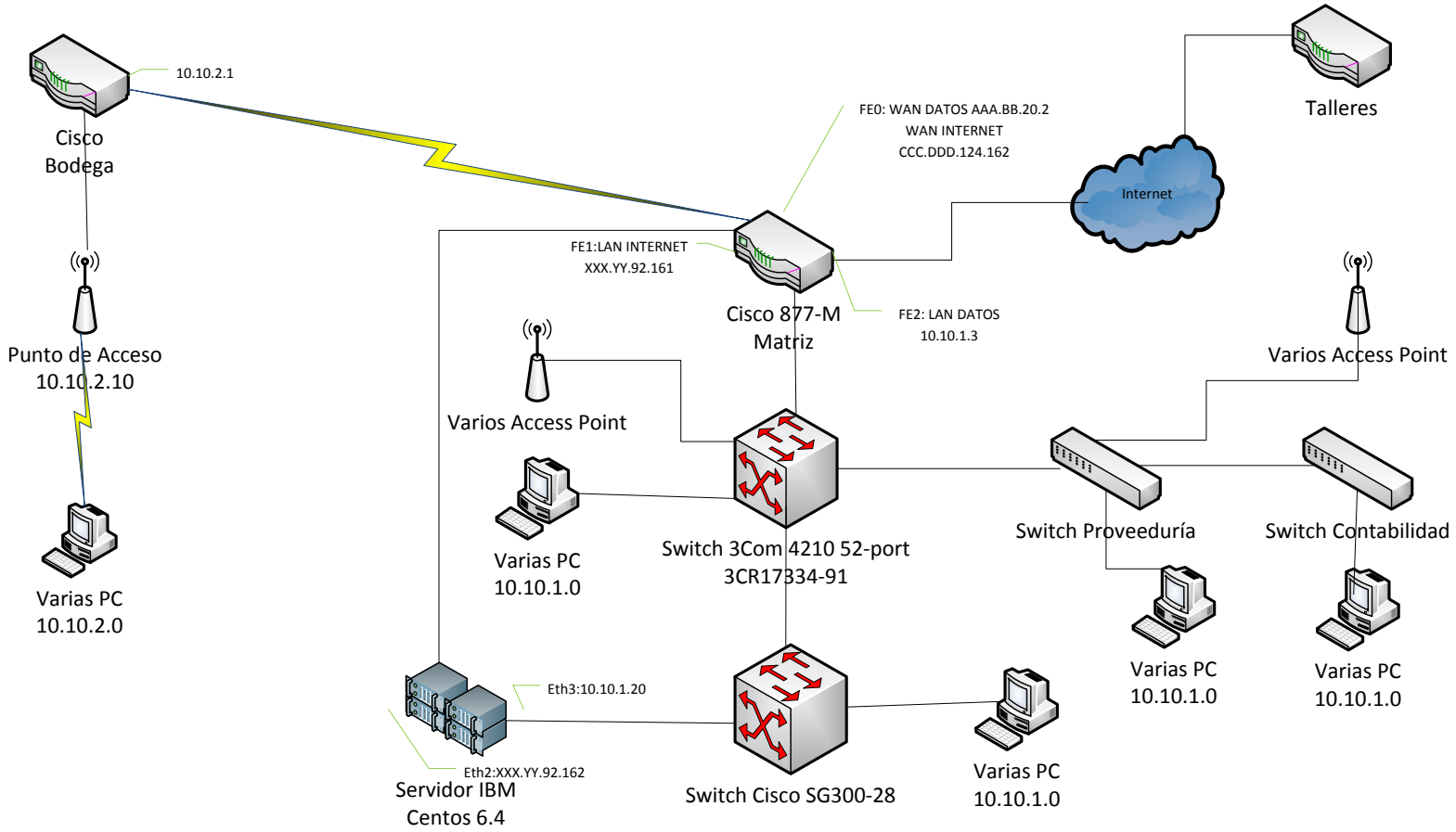
Fuente: Investigación de campo
Elaborado por: Fernando Defaz

- ✓ La Información tiene una importancia de:
  - ➢ 5 ya que en ella se encuentran las bases de datos, respaldos de las mismas, contraseñas de los usuarios.
- ✓ El Hardware tiene una importancia de:
  - ➢ 4 para servidores.
  - ➢ 3 para PCs.
  - ➢ 2 para routers y switches.
- ✓ El Software tiene una importancia de:
  - ➢ 3 aplicación y programas fuentes.
  - ➢ 2 sistemas operativos.

- **Evaluación de Vulnerabilidades en la Red**

Actualmente la Institución cuenta con la topología estrella. En la figura se ilustra la red actual del GAD.

TOPOLOGÍA SIMPLIFICADA ACTUAL DE LA RED INFORMÁTICA
DEL GOBIERNO PROVINCIAL DE COTOPAXI – AGOSTO / 2014



Fuente: GADPC.
Elaborado por: Fernando Defaz**.**

Figura 23: Diagrama de la red informática actual del GADPC

Para la evaluación de vulnerabilidades se utilizó las siguientes herramientas: *ZENMAP* 6.47 y *NESSUS* descargadas gratuitamente de internet.

Estas pruebas fueron realizadas desde una máquina externa a la red informática del GAG, al servidor web.

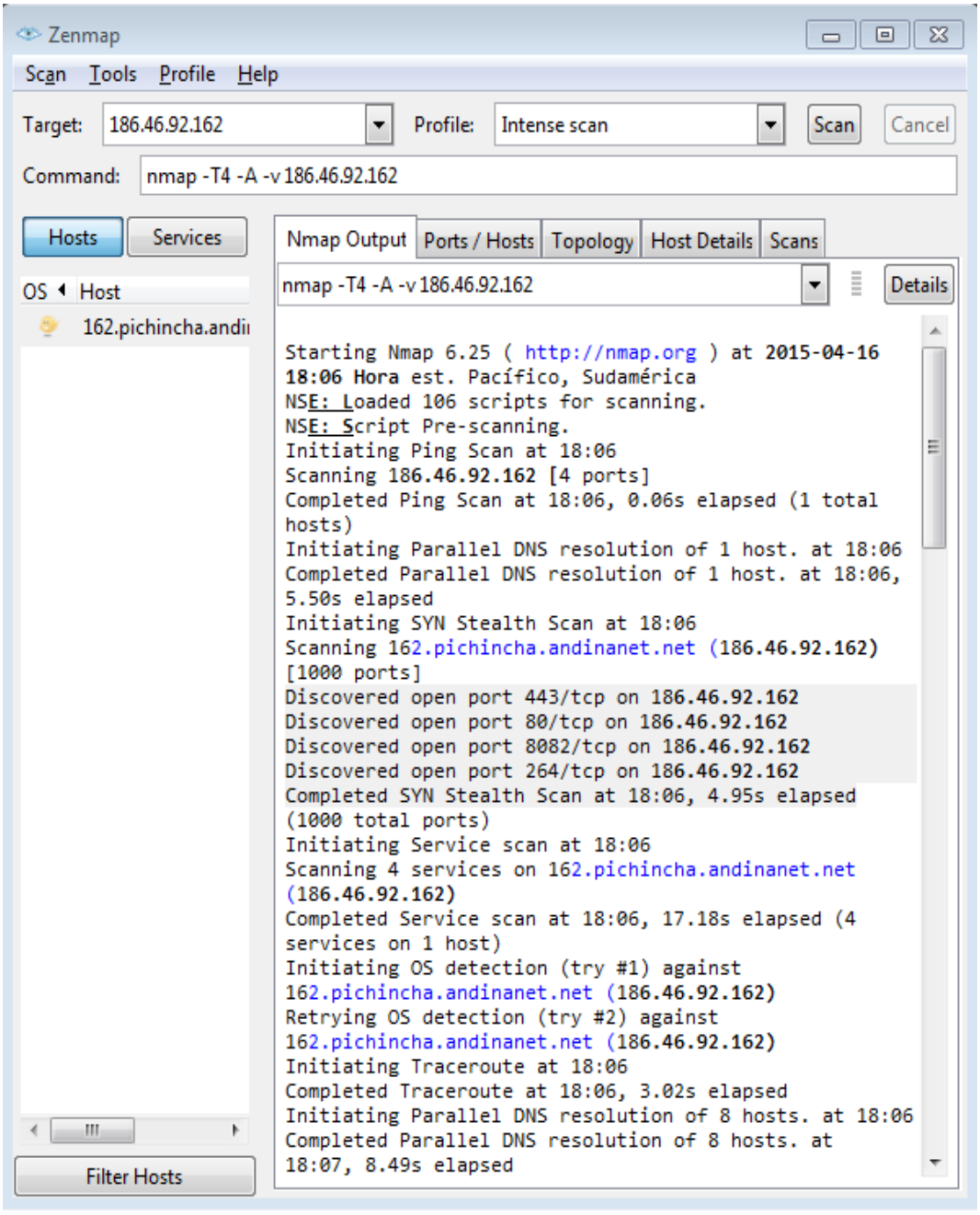
Tabla 28: Direcciones *IPs*

NOMBRE	DIRECCION IP
Servidor de Internet	186.46.92.162
PC Externa	192.168.1.7

Fuente: Investigación de campo
Elaborado por: Fernando Defaz

✓ ***ZENMAP***

Esta herramienta permite conocer los puertos abiertos y protocolos disponibles de una o un grupo de PCs, la siguiente figura es el resultado obtenido de monitorear el servidor de Internet del gobierno autónomo descentralizado de la provincia de Cotopaxi.



Fuente: investigación de campo
Elaborado por: Fernando Defaz**.**

Figura 24: Escaneo con *ZENMAP*. Servidor web. 186.46.92.162 - GADPC

En la figura se muestra que el servidor de Internet tiene abierto los siguientes puertos para el acceso remoto:

Discovered open port 443/tcp on 186.46.92.162

Discovered open port 80/tcp on 186.46.92.162

Discovered open port 8082/tcp on 186.46.92.162

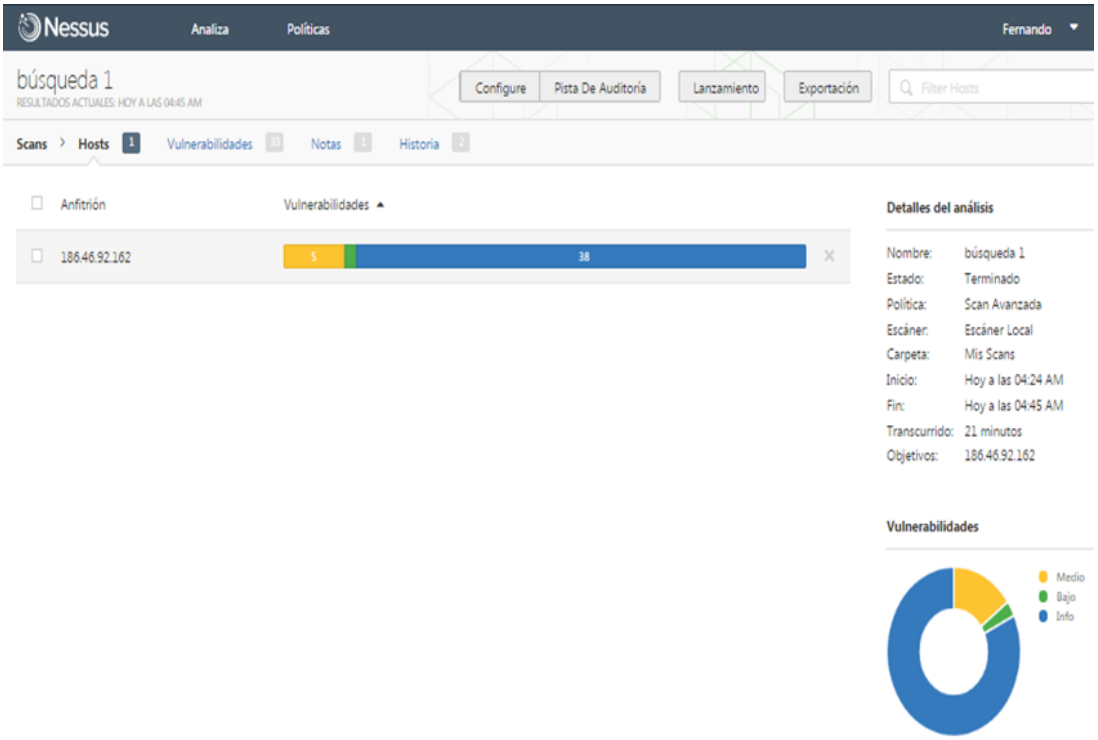
Discovered open port 264/tcp on 186.46.92.162

Esto hace que sea el servidor vulnerable a posibles ataques.

✓ **NESSUS**

Muestra la información más completa de los equipos como: Puertos abiertos, notas de seguridad, advertencias de seguridad, agujeros, sistemas operativos, parches instalados, el nivel de riesgo de la vulnerabilidad además de dar una solución a ese riesgo como por ejemplo la instalación de nuevos parches.

La siguiente figura permite conocer el nivel de riesgo que tiene el servidor web según las vulnerabilidades encontradas.



Fuente: investigación de campo
Elaborado por: Fernando Defaz.

Figura 25: Escaneo con *NESSUS*. Servidor web 186.46.92.162 - GADPC

Se observa el porcentaje de vulnerabilidades encontradas con la IP 186.46.92.162, correspondiente al servidor web del gobierno autónomo descentralizado de la provincia de Cotopaxi.

186.46.92.162

Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	27	33

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	80035	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22094	Check Point FireWall-1 ICA Service Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39521	Backported Security Patch Detection (WWW)
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address

Fuente: investigación de campo.
Elaborado por: Fernando Defaz.

Figura 26: Reporte *NESSUS*. Servidor de web 186.46.92.162 - GADPC

Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	58409	Check Point SecuRemote Hostname Information Disclosure
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

Fuente: investigación de campo.
Elaborado por: Fernando Defaz**.**

Figura 26: Reporte *NESSUS*. Servidor de web 186.46.92.162 – GADPC (continuación)

En la figura anterior se ilustra las vulnerabilidades de la red, tales como: los puertos abiertos, notas de seguridad, advertencia de seguridad y agujeros.

- **Análisis de Resultados**
  - **Riesgos asociados con los activos críticos**

Según las evaluaciones realizadas de las vulnerabilidades encontradas a la IP PUBLICA=186.46.92.162, se puede indicar que los servidores no solo tienen abierto los puertos que le corresponden, dependiendo a su función, sino que existen agujeros por donde pueden ser atacados.

Con lo que se suma también a que no existen manuales de procedimientos ni políticas de seguridad que guíen al usuario en el manejo de aplicaciones, manejo de la información, esto ha ocasionado la perdida de información tanto en forma accidental así como deliberada lo que ha generado retraso en el trabajo

No existe un adecuado control para el acceso físico a los departamentos, esto ocasiona que el trabajo sea interrumpido para atender consultas de personas externas a la Institución.

Determinación de Requerimientos

Tabla 29: Requerimientos

Requerimiento	Descripción	Prioridad
Adquisición y organización de Servidores en una sola área	Debido al incremento de usuarios en la red y por la seguridad de la misma, se deben adquirir servidores que soporten los servicios actuales; cada servidor cumplirá con máximo dos funciones para que no colapse, todos los servidores deberán estar ubicados en una sola área con sus respectivas seguridades.	**Alta**
Desarrollar políticas de seguridad de acceso físico a los equipos	Debido a la falta de políticas para el acceso físico a los equipos se han originado problemas tales como pérdida de información y pérdida o daño de dispositivos de hardware.	**Media**
Manual de políticas y procedimientos para el acceso y manejode lainformación	Se debe realizar un manual de políticas y procedimientos para el manejo de la información, donde se responsabilice al usuario del uso de ella así como de su almacenamiento seguro.	**Mediana**
Capacitación de usuarios	Planificar una capacitación a los usuarios para el uso de las aplicaciones existentes así como de las herramientas actualizadas para que puedan desempeñar mejor su trabajo.	**Media**
Desarrollar un diseño de seguridad Perimetral para la Intranet que minimice el riesgo de un ataque.	Se requiere diseñar un esquema de Seguridad Perimetral con un distribuidor del ancho de banda para la Intranet, para mejorar su rendimiento y minimizar el riesgo de un ataque	**Alta**
Plan para el Mantenimiento preventivo de Equipos	Se debe contar con un plan para el mantenimiento de equipos para prevenir posibles daños de fuentes de poder, daños de discos duros, o la infección de virus, además, contar con los sistemas operativos y aplicaciones actualizadas.	**Baja**

Fuente: GADPC
Elaborado por: Fernando Defaz

Los requerimientos con prioridad alta se recomiendan que se den solución de forma inmediata para proteger los activos críticos de la Institución.

.7.3.2. Diseño del Esquema de Seguridad para el GADPC

Para realizar el diseño de seguridad tanto Física como Lógica y para el manual de políticas y procedimientos se basaron en los lineamientos de la norma ISO 27001.

- **Diseño de la seguridad Física**

Objetivos:

- ✓ Proteger los activos informáticos del GAD de los riesgos de desastres naturales, actos accidentales o mal intencionados
- ✓ Minimizar la pérdida de información y garantizar la recuperación de la misma.
- ✓ Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

- **Áreas Seguras**

Proteger físicamente contra el acceso no autorizado o daño a la información de los sistemas a todos los departamentos del GAD especialmente donde se procesa Información.

- **Perímetro Físico**

El área de los servidores *DMZ*(Zona Desmilitarizada) debe ser cerrada adecuadamente contando con una ventilación adecuada y sus respectivas instalaciones eléctricas, donde el acceso solo será para las personas autorizadas tales como administradores de las aplicaciones, bases de datos y red.

El departamento de Sistemas junto con el departamento Administrativo deberá crear normas a seguir para acceder y modificar al hardware. Cada empleado será responsable de sus computadores personales y no

se permitirá que personas no autorizadas a los sistemas de información tengan acceso a los computadores sin autorización.

El acceso a los diferentes departamentos deberá ser controlado en primera instancia por la guardia de seguridad y segundo por la secretaria de cada departamento en horas laborables; en horas no laborables no ingresará ninguna persona no autorizada a los departamentos.

- **Controles de acceso físico**

El área de información debe estar ubicada al ingreso del edificio, de tal manera que todos los usuarios que requieran información para algún trámite la obtenga en esta área y así evitar que pasen a otro departamento si no es necesario.

Toda persona externa que ingrese a la institución por motivos específicos deberá registrar su información en un documento: nombre, hora de ingreso, departamento al que se dirige y además el guardia deberá retener algún documento de identidad.

- **Seguridad de los Equipos**

Proteger físicamente a los equipos para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Institución.

- ✓ **Ubicación y protección de los Equipos**

En cada departamento los equipos deberán ser ubicados en lugares que no afecten al mismo, por ejemplo no cerca de ventanas donde puedan ser afectados por la lluvia, polvo o por robo.

El GAD pondrá políticas sobre comer, beber o fumar cerca de las instalaciones de los equipos especialmente en el área de procesamiento de información.

Se deberá realizar por los menos dos veces al año un monitoreo de las condiciones ambientales en los departamentos especialmente en los de procesamiento de datos para prevenir cualquier problema en los equipos.

- ✓ **Suministros de Energía**

El área de los servidores debe contar con un UPS para asegurar el trabajo continuo hasta que el generador de energía sea activado. Así mismo el edificio del GAD contará con una puesta a tierra para proteger de rayos a los equipos, además, la caja donde se encuentran los interruptores de energía deben ser colocados en lugares fuera del alcance de personas externas para que no se ocasionen alguna interrupción de energía.

- ✓ **Seguridad del Cableado**

El cableado de red debe estar protegido por conductos como canaletas y ubicados en lugares que no obstruyan el paso a las personas para evitar daños al cable y que se vean interrumpidos los servicios de red.

Las instalaciones de cableado eléctrico deberá ser independiente del cableado de red para evitar interferencias.

- **Diseño de la Seguridad Lógica**

Objetivos:

- ✓ Definir y controlar los permisos y accesos a los programas y archivos
- ✓ Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos

- ✓ Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento
- ✓ Asegurar que la información trasmitida sea recibida por el destinatario al cual fue enviada y que la información sea la misma.

Para el diseño de la seguridad de la red se consideró que el GAD después de estudiar costos, deberá adquirir un sistema de Gestión Unificada de Amenazas *UTM (Unified Threat Management)*, un único equipo que incluye múltiples características de seguridad: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus y anti spam y redes privadas virtuales.

Fuente:Ramos Fraile (2011). Seguridad perimetral
Elaborado por: Fernando Defaz

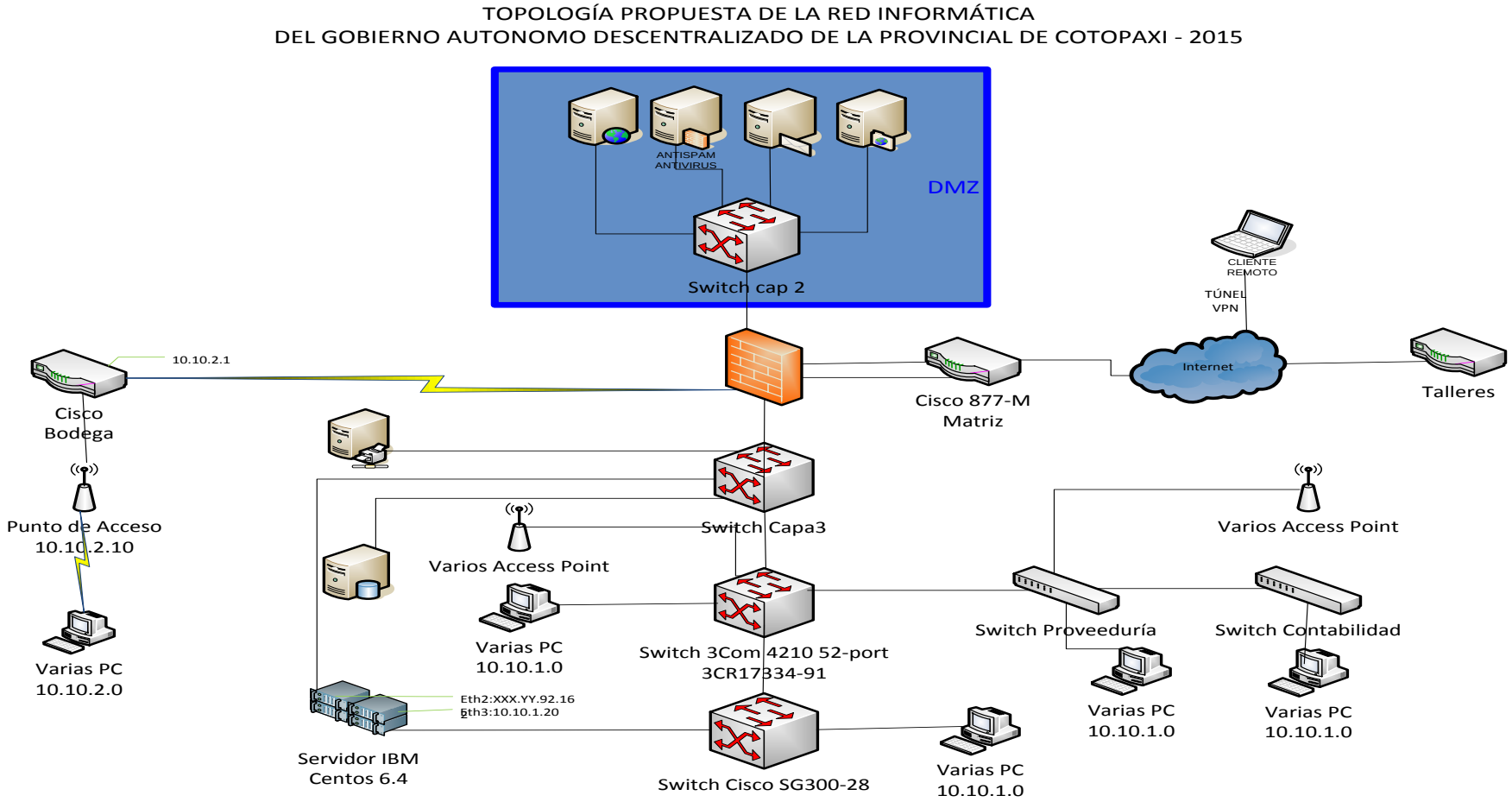
Figura 27: Gestión Unificada de amenazas. *UTM (Unified Threat Management)*

Estos elementos son muy útiles para centralizar soluciones.

Es importante, configurar el cortafuegos, segmentando los servicios Web y la pasarela de correo en la *DMZ* con una política restrictiva. Luego se debe configurar el sistema de detección y prevención de intrusos, escuchando las interfaces instaladas para conocer todos los ataques posibles. Es recomendable que el servidor de base de datos se quede en la red interna inaccesible desde *Internet* y que todos los trabajadores y dependencias se

conectan usando una VPN. Con lo que tendremos una arquitectura mucho más segura.

La figura muestra el diseño de seguridad perimetral para la red GAD, basada en un sistema de Gestión Unificada de Amenazas *UTM (Unified Threat Management).*



Fuente: Investigación de campo
Elaborado por: Fernando Defaz

Figura 28: Diseño de seguridad perimetral para la red informática del GADCP

- **Componentes del nuevo diseño**

La red de datos del GAD estará conformada por los equipos que se mencionan a continuación definidas en respuesta a los requerimientos establecidos anteriormente:

✓ **Modulo Internet DMZ**

Dentro del Módulo de *Internet* se necesitarán los siguientes dispositivos:

- Router
- *Firewall*s

  IDS

  IPS

  Optimizador de Ancho de banda
- Servidor HTTP
- Servidor SMTP
- Servidor DNS
- Servidor *FTP*
- *Switch* capa 3

✓ **Modulo Campo**

Dentro del Módulo de Campo se necesitarán los siguientes dispositivos:

- Servidor de base de datos
- Servidor de Aplicaciones y Archivos
- Servidor de Impresoras (Se configurará en uno ya existente)
- Switch capa 2
- Switch capa 3
- PCs (se utilizaran los existentes)

A continuación en la tabla se describe las funciones para los nuevos equipos del diseño propuesto.

Tabla30: Servidores con la función que desempeñan

EQUIPO	FUNCION
Servidor de Base de Datos (nuevo)	• Cuenta con 4 discos • Predominará la BDDSQL Server y como secundaria Oracle

Servidor de Aplicaciones y Archivos (nuevo)	• Cuenta con 4 discos.
	• Aplicaciones:
	  ◦ Sistema MEGAN
	  ◦ Sistema Vehicular
	• Archivos: Usuarios

Servidor: web, correo, *FTP*, *proxy*	• Sistema Académico
Servidor de Impresoras	• Uno existente solo para ese servicio

Fuente: GADPC
Elaborado por: Fernando Defaz

- ✓ **Control de Acceso Lógico**
  - ➢ **Requerimientos para el control de acceso**

Controla el acceso a la información mediante requerimientos de seguridad, además de políticas de autorización y difusión de la información

Políticas de Control de accesos

El GAD deberá definir y documentar políticas de acceso para cada sistema de información dependiendo de los requerimientos de seguridad para el acceso.

Las políticas de acceso deberán estar relacionadas con la clasificación de información para cada departamento.

El departamento de Sistemas deberá ubicar a cada usuario bajo un perfil dependiendo de la categoría del puesto de trabajo.

El departamento de Sistemas documentará dentro de las políticas de acceso que está permitido y que no, que debe imponerse y que reglas serán optativas o condicionales, como por ejemplo, páginas web y servicios de red.

- **Administración de accesos de usuarios**

Tiene como objetivo impedir el acceso no autorizado a los sistemas de información implementando procedimientos de asignación para el acceso a estos sistemas.

Dentro de estos procedimientos se deberá tomar en cuenta desde el inicio de un nuevo usuario hasta la finalización del mismo cuando ya no requiera acceso a los sistemas de información.

Registro de Usuarios

El departamento de Sistemas creará para cada usuario un identificador personal para el acceso de cada sistema, esto permitirá que cada usuario sea responsable por sus acciones.

Administración de contraseñas

Se responsabilizará a cada usuario por mantener su password o contraseña en secreto.

El departamento de Sistemas proporcionará al usuario nuevo o al usuario que olvidó su clave, una contraseña provisional. Esta contraseña provisional será dada personalmente al usuario, sin hacer uso de correos electrónicos o de terceras personas.

El departamento de Sistemas verificará que el usuario tenga permisos para el uso del sistema de información, además debe contar con la autorización del Director del departamento para el acceso del sistema al usuario requerido.

El departamento de Sistemas deberá asignar los privilegios mínimos a cada usuario dependiendo de la necesidad de uso de los sistemas.

- **Responsabilidades del usuario**

Objetivo principal es concientizar a los usuarios su responsabilidad para el acceso a los sistemas de información, entre ellas el uso de las contraseñas y la seguridad de los equipos que están bajo su cargo.

- **Control de acceso a la red**

El objetivo es garantizar la seguridad de los servicios de red tanto interna como externa, evitando interfaces inadecuadas entre la Institución y otras organizaciones, protegiendo la red y los servicios de red con mecanismos de autenticación y con controles de acceso a los usuarios para el uso de los servicios de información.

Políticas para utilizar los servicios de red

El departamento de sistemas deberá crear políticas y procedimientos para el acceso de los usuarios a los servicios de red dependiendo del perfil de cada usuario.

Enrutamiento Forzado

El departamento de Sistemas deberá aplicar reglas para evitar que los usuarios escojan rutas fuera de la trazada entre su computador personal y los servicios de red a los que tienen acceso tales como conexiones automáticas de los puertos al *firewall*, imponer el uso del *firewall* a todos los usuarios externos a la Institución que necesiten tener acceso a nuestra red, además controlar las comunicaciones autorizadas internas a externas o viceversa mediante *firewall*s.

Control de conexión a la red

El departamento de Sistemas deberá implementar políticas de acceso para limitar las conexiones de los usuarios a las aplicaciones que

están dentro y fuera de la Institución a través de un *firewall*, por ejemplo, el correo electrónico y transferencia de archivos en ambas direcciones.

- **Monitoreo del Acceso y uso de los Sistemas**

La Finalidad es detectar actividades no autorizadas, además permitirá medir la eficacia de los controles adoptados con las políticas de acceso.

Registro de eventos

Se deberá llevar y almacenar por un período determinado un registro de auditoría que contará con su respectiva seguridad y que deba contener la identificación del usuario, fecha y hora de inicio y terminación, registro de intentos exitosos y fallidos del acceso al sistemas y a los datos para posibles investigación de algún fraude, para esto todos los computadores tendrán una configuración sincronizada de relojes.

Monitoreo del uso de los sistemas

El departamento de sistemas deberá monitorear el uso de los sistemas de información con el fin de controlar que solo los usuarios que tengan autorización a ella sean los que estén utilizándolas.

Trabajo remoto

El departamento de sistemas deberá desarrollas políticas e implementar la protección para el acceso al trabajo remoto de usuarios que deban trabajar fuera de la Institución, además este trabajo deberá ser autorizado y controlado.

.7.3.3. Políticas de seguridad para la red del GADPC

- **Adquisición e instalación de equipos**

La adquisición de nuevos equipos será revisada y analizada por el departamento de Sistemas para justificar el pedido.

La instalación de los equipos será realizada por el departamento de sistemas siguiendo los procedimientos para la configuración e instalación de los programas permitidos en la empresa y en conocimiento del departamento de Activos fijos para asignar a un responsable del activo.

- **Seguridad física del equipo**

El usuario responsable del equipo deberá notificar al departamento de sistemas y al departamento de activo fijo si el equipo será asignado a otra persona, ubicado en otra área o parte de él será reemplazado por un hardware nuevo.

Todo equipo que sale de la institución debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la institución, motivo y responsable del equipo, además notificar al departamento de sistemas si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

Las portátiles deberán estar aseguradas por alguna empresa externa.

- **Mantenimiento de equipos**

El departamento de sistemas estará a cargo del mantenimiento preventivo de los servidores y computadoras personales además será realizado cada seis meses previo a una calendarización y deberá ser registrado en una bitácora.

Cualquier problema de falla del equipo deberá reportarse inmediatamente al departamento de sistemas porque podría ocasionar pérdida de la información o interrupción de los servicios.

El departamento de sistemas estará a cargo del mantenimiento correctivo de los equipos y de la red supervisado por el Jefe de Sistemas.

El departamento de sistemas se responsabilizará de mantener la adecuada instalación de la infraestructura de red.

- **Políticas de seguridad del software**

  - **Adquisición, instalación y actualización**

    El departamento de sistemas será quien instale software adicional a los equipos si es necesario para el usuario.

    El departamento de sistemas será el encargado de la actualización de software y de los parches de seguridad periódicamente.

    Todo software que se necesite comprar para el departamento de sistemas tendrá su previa justificación y aprobación de las autoridades para su adquisición.

    Todo software adquirido será registrado en el departamento de activo fijo.

- **Políticas de seguridad para el control de acceso a los sistemas de información**

  - **Acceso Físico**

    Los equipos deberán estar ubicados bajo condiciones que ofrezcan seguridad física, eléctricas y además que permitan el acceso físico sin ninguna restricción al personal del departamento de sistemas.

El departamento de sistemas será quien tenga acceso al cuarto deservidores sin ninguna restricción y en caso urgente pueden acceder las autoridades del GAD.

- **Acceso a la información**

El departamento de sistemas no será responsable de la información personal de los usuarios que se encuentre en los discos duros de cada computador.

Si el usuario detectara la presencia de algún virus en el equipo, deberán notificar inmediatamente al departamento de sistemas y desconectar al equipo de la red hasta solucionar el problema.

Cada usuario deberá cerrar la sesión en su computador personal cuando no lo esté utilizando.

Se deberá responsabilizar al personal de contrato sobre el manejo de información a través de sus contratos.

- **Respaldos y Recuperación de archivos, aplicaciones y bases de datos**

El departamento de sistemas será responsable para realizar los backups de la información.

El departamento de sistemas garantizará la seguridad de la información de los usuarios que se encuentra almacenada en los servidores de archivos, servidores de bases de datos, servidores de aplicaciones.

El departamento de sistemas será quien garantice la protección dela información asegurando su integridad, disponibilidad de acuerdo a sus normas establecidas.

El departamento de sistemas garantizara la seguridad de las bases de datos, los respaldos de las mismas y la restauración si hubiera la necesidad.

- **Acceso a los servicios de red**

El acceso del personal a los servicios de red y de la información en horas no laborables será con previa autorización del responsable del área y coordinado con el departamento de sistemas para asignar los permisos.

El departamento de sistemas será quien otorgue permisos a los empleados para el acceso a la información y los servicios de la red dependiendo de su perfil.

El departamento de sistemas será quien controle que el acceso a la red y a la información esté disponible y no sea interrumpido las 24 horas del día, los 365días del año.

El departamento de sistemas será quien asegure la disponibilidad de los servicios para los usuarios de acceso remoto, con previa autorización de las autoridades. El departamento de sistemas se responsabilizará dela administración de las IPs públicas y privadas.

El departamento de sistemas será quien realice el monitoreo de la red y si encontrara alguna actividad sospechosa ocasionado por un computador personal, lo desconectará de la red hasta solucionar el problema.

El departamento de sistemas se responsabilizará de la administración, operación y correcto funcionamiento de los servicios de red.

- **Administración de usuarios**

El departamento de sistemas será quien cree la cuenta al nuevo usuario en la red con su respectiva identificación y autenticación.

Cada usuario en su primer ingreso podrá cambiar su contraseña que será única e intransferible, es decir, queda prohibido que el usuario comparta su contraseña a los compañeros.

El departamento de sistemas administrara el tiempo útil de la clave.

El departamento de sistemas creará cuentas temporales con el respectivo control de acceso y dependiendo al perfil solicitado.

El departamento de sistemas será quien elimine las cuentas de las personas que ya no laboran en la institución.

El departamento de sistemas será quien modifique las cuentas de los usuarios con previa autorización del jefe del departamento solicitante.

- **Correo electrónico e Internet**

El departamento de sistemas será quien administre la información que ingresa por el correo electrónico.

El departamento de sistemas será quien controle la navegación de los usuarios y limite el acceso a páginas de internet que no tienen ningún vínculo con las funciones del GAD.

El departamento de sistemas definirá que tamaño de archivos podrá enviar y recibir cada usuario dependiendo de las normas del departamento. El usuario no abrirá correo electrónico enviado por un remitente que no conoce, no responderá el mensaje ni mucho menos ejecutará archivos adjuntos en dichos correos.

- **Políticas de seguridad para el desarrollo de software**

Todo Software desarrollado en el departamento de sistemas tendrá su respectiva documentación (manual de usuario, instalación y programación).

Todo software desarrollado en el departamento de sistemas deberá seguir una metodología con sus respectivas normas y procedimientos seleccionados por el departamento de sistemas.

Toda modificación de algún software deberá tener su pedido formal dando su justificación y estará guiada por el Jefe de Sistemas.

- **Políticas de seguridad para contingencia**

El departamento de sistemas debe contar con planes de contingencia que pueda garantizar la recuperación de la información por algún desastre sin el mayor número de pérdidas y a un bajo costo.

Para el caso de un colapso total de aplicaciones o de bases de datos, se deberá definir un procedimiento de restauración de los respaldos de las mimas.

- **Políticas de seguridad para la capacitación del personal**

El departamento de sistemas deberá contar con un plan de capacitación al personal de la empresa del software existente.

El departamento de sistemas deberá tener la posibilidad de capacitarse en lenguajes para el desarrollo de software, nuevas aplicaciones que faciliten el trabajo de los usuarios, de administración de la red y mantenimiento de equipos y red.

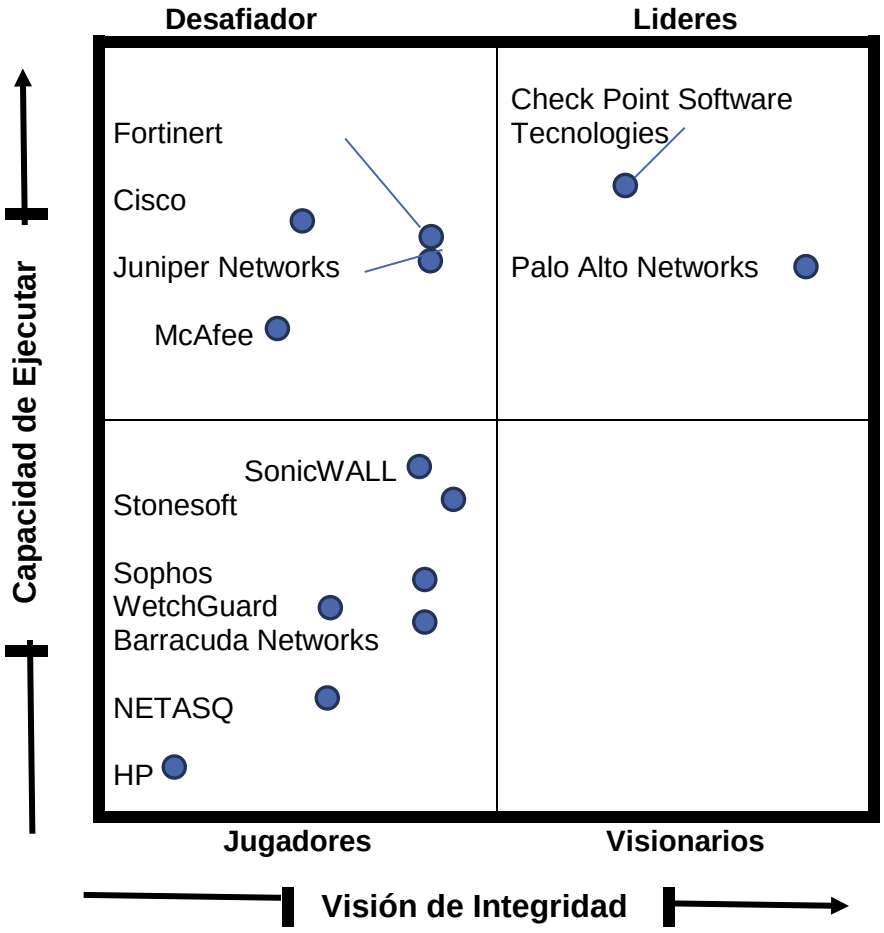
6.7.3.4. Tecnologías de seguridad perimetral

- **Diagrama de *Gartner***

  Se define al cuadrante mágico como un eje cartesiano que divide el plano en cuatro cuadrantes, a cada fabricante se le puntúa en base a una serie de ítems que terminan por colocarlo en una de las cuatro partes.

- **Posicionamiento de los vendedores en el cuadrante**

El cuadrante para el año 2015está distribuido de la siguiente manera:



Fuente: Serrano (2014: Internet). Cuadrante mágico de Gartner
Elaborado por: Fernando Defaz

Figura 29: Cuadrante Mágico de *Gartner* para *Enterprise Network Firewalls*

Se clasifica a cada vendedor de diferentes formas:

Líderes: Representa al vendedor que sabe lo que se lleva entre manos y que en general es una apuesta relativamente segura.

Desafiadores (o aspirante): Es aquella clasificación de un vendedor que va por el buen camino pero que por diversas razones su solución no llega a

abarcar todo lo que se espera de un líder, y por tanto se lo etiqueta como aspirante.

Visionarios: Se clasifican así a aquellos proveedores que han sido capaces de identificar de manera astuta las necesidades del mercado y ofrecen productos para cubrirla, pero que no disponen de algunas otras funcionalidades que resultan imprescindibles.

Jugadores: Son aquellos que se encuentran en el cuadrante abajo-izquierda que no tienen los recursos para llegar a ser un Challenger ni la versatilidad en sus soluciones para ser considerado un Visionarie, pero que sin embargo han destacado de manera especial durante el año pasado como para hacerse un hueco en el cuadrante.

Gartner incluye entre sus clientes a algunas de las más grandes empresas, agencias de gobierno, empresas tecnológicas y agencias de inversión como BT, CV, The Wall Street Journal, etc. La empresa se concentra en la investigación, programas ejecutivos, consultas y eventos.

- **Análisis de las tecnologías de Seguridad Perimetral**

Tabla 31: Comparación de tecnologías de seguridad perimetral

TECNOLOGÍA	DESCRIPCIÓN	CARACTERÍSTICAS GENERALES	EJEMPLOS
Check point	Líder mundial en seguridad de *Internet*, ofrece a los clientes protección contra todo tipo de amenazas, reduce la complejidad de la seguridad y el coste total de propiedad. (Calificado como el número uno por el Diagrama de *GARTNER*)	Automatiza en forma inteligente la gestión de políticas complejas del *firewall*, sus cambios de política, de planes y optimiza los conjuntos de reglas así como identifica normas de riesgo para asegurar la correcta configuración de los *firewall*s. Reduce el tiempo de preparación de auditoría. Gestión unificada de amenazas, incluyen todo lo necesario para asegurar la red. Cada dispositivo posee la gestión centralizada integrada, junto con las actualizaciones de seguridad completas, hardware y soporte al cliente. • Genera informes automatizados de auditoría y de cumplimiento. • Limpia y optimiza las reglas del *firewall*. • Descubre y mitiga los riesgos de esas reglas. • Monitorea los cambios de políticas de seguridad de la red. • Soluciona efectivamente problemas de la red.	*Algo Sec Firewall Analyzer* *Check Point UTM*-1 Appliance Check Point Smart Dashboard R77.10 Standar
Palo Alto *net works*	Las aplicaciones tradicionales cliente/servidor corriendo en puertos únicos permitían clasificarlas en base al tráfico. Las aplicaciones actuales de Palo Alto net works evaden la detección de los *firewall*s existentes porque su diseño de protección está basado en el número de puerto TCP/UDP. (Calificado como número dos por *GARTNET*)	• Clasificar el tráfico basándose en la identificación exacta de la aplicación no sólo información de Puerto/Protocolo (AppID™ traffic classification technology). • Clasificar, controlar e inspeccionar aplicaciones y tráfico encriptadas (AppID™ traffic classification technology with SSL forward *proxy*). • Visualización gráfica de qué aplicaciones están corriendo en la red con información de usuario, grupo y red, categorizado, asimismo por sesiones, bytes, puertos, amenazas y tiempo (ACC – Application Command Center). • Protección en tiempo real con baja latencia contra virus, spyware y vulnerabilidades de aplicaciones gracias a un motor de prevención de amenazas (FlashMatch™ Real-Time Threat Prevention Engine). • Tres diferentes opciones de implementación. • Reducción de costos capitales al reducir los pasivos y costos de operación provocados por un aumento.	PA 4000 Series para empresas grandes PA 2000 Series para empresas medianas

Fuente: Personal.
Elaborado por: Fernando Defaz

Tabla 31: Comparación de tecnologías de seguridad perimetral (continuación)

TECNOLOGÍA	DESCRIPCIÓN	CARACTERÍSTICAS GENERALES	EJEMPLOS
• ***FORTINET***	• Fabricante pionero y líder de soluciones de Seguridad Integral de redes en tiempo real. Sus plataformas de seguridad con aceleración ASIC ofrecen protección multinivel integrando todas las aplicaciones de seguridad esenciales, como firewalling, VPN IPSec y SSL, antivirus, IDS/IPS, filtrado de contenidos web, antispam y calidad de servicio. Fortinet dispone del más completo porfolio de seguridad, tanto integral de redes como específica de aplicaciones (correo electrónico, bases de datos, etc.) que satisfacen los requerimientos más exigentes con funcionalidades líderes en el mercado y con el mayor de los rendimientos. Fortinet es el único proveedor que ofrece seguridad integral con virtualización para grandes empresas, MSSPs y operadores de telecomunicaciones a través de una plataforma de alto rendimiento con integración de ocho funcionalidades y con gestión centralizada de múltiples dominios. Estrategia centrada en redes inalámbricas. • La línea de productos FortiAP es el primer fruto de la estrategia de Fortinet centrada en la seguridad en redes locales inalámbricas de carácter empresarial. Como primeros productos dentro de la gama FortiAP, FortiAP-210 con single-radio/banda dual y FortiAP-220 con banda dual y radio dual, ofrecen cobertura fiable, alto rendimiento y un precio competitivo de alto valor comparado con productos similares de su clase. • La línea FortiAP puede ser utilizada para ofrecer acceso a la red inalámbrica a empleados, locales comerciales, almacenes, puntos de venta o hotspots para el uso de invitados.	• FortiAP Seguridad redes Wireless. • wifi, Seguridad, Inalámbrica. • Protección de Redes Wireless utilizando dispositivo FortiGate como controladora. • Autenticación: la autenticación más fuerte con WPA2 y un portal cautivo integrado para el acceso de invitados. • Inspección profunda de la capa 7: permite la priorización de ancho de banda inalámbrico para aplicaciones críticas. • Política de cumplimiento: políticas de identidad-conocimiento, junto con la detección de puntos y presentación de informes, control granular endpoint, informes de auditoría, análisis específicos y mensurables. • Bajo TCO: opciones de despliegue y capacidad flexibles para aprovechar la base instalada de FortiGate, una plataforma común de gestión centralizada y sin derechos de licencia especiales reducen aún más el coste total de propiedad. • Modos de despliegue del proxy inverso en línea, transparente y fuera de línea. • Perfiles de auto aprendizajes automáticos. • Escáner de vulnerabilidades Web. • Prevención de fugas de Datos. • Auditoria de seguridad.	• FortiAP 210 • FortiAP 220

Fuente: Personal.
Elaborado por: Fernando Defaz

- **Selección de la tecnología para el GADPC**

  Debido a las necesidades de la red informática del gobierno autónomo descentralizado de la provincia de Cotopaxi, su régimen de trabajo y vulnerabilidades detectadas, se determina escoger la tecnología Check Point, por ser la que más se ajusta en la solución de los problemas, cumple con la mayoría de los requerimiento de la red, con la ventaja además de ser la más completa y la número uno escogida por el cuadrante mágico de Gartner.

  - **Check Point.**

    Comercializa productos de seguridad informática, estos son los más demandados por las empresas debido a su adaptabilidad, la facilidad de despliegue y la dirección unificada del cliente con la seguridad de los puestos de trabajo.

    Los productos de Check Point dan seguridad a los datos, blindan totalmente la información en las empresas, además de ser las herramientas de cifrado líderes de la industria, las soluciones de Check Point requieren una mínima administración y participación del usuario final, reduciendo así los gastos operacionales de los clientes.

    En el Anexo 5 se puede ver la demostración para mitigación de las vulnerabilidades para el gobierno autónomo descentralizado de la provincia de Cotopaxi, utilizando *Check Point SmartDashboard.*

- **Conclusiones y recomendaciones de la demostración**

  Conclusiones:

  ✓ La configuración de seguridad en un firewall, se lo realiza de acuerdo a las políticas que se vayan implementar, las que se seleccionan en función de lo que se desee proteger.

- ✓ Existen un sinnúmero de herramientas que pueden monitorear, detectar y proteger vulnerabilidades, pero lamentablemente las que brindan mejores posibilidades tienen un costo para utilizarlas.

Recomendaciones:

- ✓ Elaborar una guía de procedimientos para implementar políticas de seguridad en el firewall, lo que permitirá conocer que activos se desea proteger y con qué tipo de restricciones.

- ✓ Se recomienda la adquisición de un firewall que tenga las características de ser un sistema de Gestión Unificada de Amenazas *UTM (Unified Threat Management)*, que es un único equipo que incluye múltiples características de seguridad: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus, anti spam y redes privadas virtuales.

6.8. Administración

Las personas que intervienen en la administración y aplicación de la metodología de seguridad perimetral estará conformada por:

- Prefecto provincial
- Jefe informático
- Jefe de talento humano.

6.9. Previsión de la evaluación

El realizar la previsión de la evaluación en el marco de una estricta vigilancia durante el desarrollo de la propuesta, permitirá verificar si se ha logrado mejorar la seguridad del acceso a la información, datos y recursos informáticos del gobierno autónomo descentralizado de la provincia de Cotopaxi, para que las autoridades puedan ejecutar de mejor manera la evaluación se ha diseñado la siguiente matriz.

Tabla 32: Matriz de análisis de evaluación

ASPECTOS PARA EL PLAN DE EVALUACIÓN	ELEMENTOS O RECURSOS PARA EL PROCESO DE EVALUACIÓN
¿Quién solicita evaluar?	Prefecto provincial, jefe de talento humano, jefe informático.
¿Por qué evaluar?	Es importante conocer y comprobar si la propuesta de solución de seguridad perimetral satisfacen los objetivos planteados en la investigación y si alcanzan los resultados esperados de seguridad.
¿Para qué evaluar?	Para identificar las posibles vulnerabilidades en la red informática y prevenir inseguridades en la implementación del sistemas de seguridad.
¿Que evaluar?	La aplicación de la metodología de seguridad y los resultados obtenidos.
¿Cuándo evaluar?	Cuando la propuesta se haya desarrollada.
¿Cómo evaluar?	Identificando los activos críticos (hardware, software) y sus vulnerabilidades.
¿Con qué evaluar?	A través del criterio de las autoridades, profesional en el área de sistemas o afines y mediante la aplicación de la metodología de seguridad.

Fuente: Personal.
Elaborado por: Fernando Defaz

BIBLIOGRAFIA

Álvarez Marañón, G. (2007). *Cómo protegernos de los peligros de Internet.* Buenos Aires, Argentina: csic-csic Pres.

Caballero, J. (1998). *Redes de banda ancha.* Barcelona: Libri Mundi.

Hadnagy, C. (2011). *Ingeniería social. El arte del hacking personal.* Barcelona: Libri Mundi.

Maciá Pérez, F. (2010). *Administración de servicios de Internet: De la teoría a la práctica.* Alicante: Libri Mundi.

Philippe, F. (2008). *Recursos Informáticos Windows Server 2008 - Administración y explotación.* Alicante: eni.

Ramos Fraile, A. (02 de 2011). *Seguridad perimetral*. Obtenido de Seguridad perimetral: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

27001, A. (2013). *Norma ISO 27001*. Obtenido de Cómo funciona la ISO 27001: http://www.iso27001standard.com/es/que-es-iso-27001/

Abril Porras, V. (19 de Julio de 2014). Paradigmas. Ambato, Tungurahua, Ecuador.

Baltazar Gálvez, J. M., & Campuzano Ramírez, J. C. (22 de Julio de 2014). *Universidad Nacional Autonoma de México*. Obtenido de Facultad de Ingeniería: www.portalacademico.cch.unam.mx

CISCO. (2014). *Cisco CCNA3*. Obtenido de Cisco CCNA3: http://www.cisco.com/web/learning/netacad/demos

Colectivo de Autores. (2008). Gobiernos descentralizados. Quito, Ecuador.

Congreso Nacional. (17 de IV de 2002). *Registro Oficial 557-S, 17-IV-2002 según la Ley 2002-67*. Obtenido de LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS: www.asambleanacional.gob.ec

Constitucion del Ecuador. (2008). *Administración pública* (segunda edicion ed.). Ecuador.

Constitucion Politica, C. (Viernes de Agosto de 2014). *Calidad de Servicios Públicos*. Obtenido de Marco Normativo: www.oas.org/es/sap/dgpe/gemgpe/ecudor/calidad.asp

Contreras Vega, G. (2004). *Curso.* Obtenido de Introducción a la seguridad en internet y aplicaciones: http://www.capacinet.gob.mx/Cursos/Tecnologia%20amiga/desarrolladordesoftware/Seguridad_Internet_SE.pdf

Cootad en el Registro Oficial. (2010). Gobierno y Democracia Digital. *Cootad en el Registro Oficial*. Recuperado el 2010

Diego, G. (2005). *Derecho Municipal: Autonomía y Regioanalización Asociativa.* Buenos Aires: Ediar.

Flores Saltos, F. G. (2007). Tesis. *Estudio, Administración e Implementación de Políticas de Seguridad en la Red Informática del Hospital Millennium de la ciudad de Ambato*. Ambato, Tungurahua, Ecuador.

Freire, E. s. (Agosto de 2014). Manual de SPSS Aplicado a proyectos de fin de titulación. Ecuador.

GADPC. (20 de 12 de 2014). *Gobierno Autónomo Descentralizado de la Provincia de Cotopaxi*. Obtenido de Mision: http://www.cotopaxi.gob.ec

García Mata, F. (2009). *Videovigilancia: CCTV usando videos IP.* Malaga: Vertice.

GFI Languard NSS. (2014). *SOTI*. Obtenido de GFI Languard NSS: http://www.isoftland.com/software/gfi/languard

Granja Galindo, N. (2006). *Fundamentos de Derecho Administrativo.* Quito: Editorial Jurídica.

Hernández, R. (2003). *La administracion de la funcion informatica; una nueva profesión.* Balderas, Mexico: Limusa.

Huidrobo Moya, J., A. S., & Calero, J. (2000). *Redes de Area Local.* Madrid: Libri Mundi.

IEEE. (2012). *Calidad del Software*. Obtenido de Calidad del Software: http://www.ecured.cu/index.php/Calidad_de_Software

Jiménez, E. (29 de 12 de 2014). *Conoce tu router*. Obtenido de Calidad del servicio (QoS): http://www.xatakaon.com/modems-y-routers/conoce-tu-router-viii-calidad-del-servicio-qos

Maldonado Ampuero, A. (2011). *Medición de calidad de servicio (QoS) en telefonía IP para distintos medios de acceso.* Concepcion Chile: Universitaria.

Mañas, J. A. (2011). *ANÁLISIS Y GESTIÓN DE RIESGOS.* Madrid, España: Creative Commons. Obtenido de http://www.criptored.upm.es/intypedia/docs/es/video11/GuionIntypedia011.pdf

Nmap Network Scanning. (2014). *Nmap Network Scanning*. Obtenido de Guia de referencia de Nmap: http://nmap.org/man/es/index.html#man-description

Pablo, A. S. (2009). Calidad. Madrid: Paraninfo.

Pullutaxi Achachi, W. L. (2012). Tesis. *Sistemas MULTI-AGENTE para la detección de ataques en los entornos dinámicos y distribuidos de la empresa importadora REPCOPY*. Ambato, Tungurahua, Ecuador.

R, S. P. (2009). Creación y dirección de Pymes. Madrid: Diaz de santos. SA.

Registro Oficial. (21 de Enero de 2014). *Suplemento* . Obtenido de Registro Oficial Nº 166 : http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/114e7f21-be5c-4412-a75a-03980d5643d0/Registro%20Oficial%20166%20Ley%20Reformatoria%20al%20Cootad.pdf

Revision, C. (2009). Autonomia. En *United State Commision to Revise and Compile the of Puerto Rico.* Puerto Rico.

revision, C. o. (2009). Autonomia. En *United State Commision to Revise and Compile the of Puerto Rico.* Puerto Rico.

Reyes Mena, J. L. (2010). Tesis. *Rediseño de la Red de Comunicaciones Administrativa de Hidropastaza S. A. aplicando Tecnologías de Calidad de Servicio y Alta Disponibilidad para solucionar los problemas de Comunicaciones de la Empresa*. Ambato, Tungurahua, Ecuador.

Robalino Peña, F. (2011). Tesis. *Los protocolos de VoIP inciden en la seguridad de la transmisión de datos en la F.I.S.E.I. de la U.T.A. en el primer semestre del año 2010.* Ambato, Tungurahua, Ecuador.

Salud, G. a. (2008). Temario Comúm.e-book. España: MAD. S. L.

Sarubbi, J. (2008). *Seguridad informatice Tecnicas de defensa comunes bajo variantes del sistema operativo Unix.* Luján, Buenos Aires: Libri Mundi.

Saydam, T., & Magedanz, T. (1996). *From Networks and Network Management into Service and Service Management.* Mexico: Universitaria.

Secretaría Nacional de la Administración Pública. (09 de 2013). *Acuerdo No. 166.* Obtenido de CRISTIAN CASTILLO PEÑAHERRERA SECRETARIO NACIONAL DE LA ADMINISTRACIÓN PUBLICA CONSIDERANDO:: http://www.deloitte.com/assets/Dcom-Ecuador/Local%20Assets/Documents/ERS/Acuerdo_166%2023-sep-2013.pdf

Serrano, L. (2014). *Cuadrante Mágico de Gartner para Enterprise Network Firewalls*. Obtenido de Cuadrante Mágico de Gartner para Enterprise Network Firewalls: http://www.computing.es/seguridad/tendencias/1037053002501/gartner-cuadrante-magico-firewalls.1.html

Solórzano Cadena, L., & Rezabala Triviño, J. (23 de 05 de 2013). *REPOSITORIO DE ESPOL.* Obtenido de Estudio sobre el estado del arte de la seguridad informática en el Ecuador y sus necesidades reales: http://www.dspace.espol.edu.ec/handle/123456789/24298

Staff, U. (2011). *Hacking.* Buenos Aires: Fox Andina.

Stallings, W. (2004). *Fundamentos de seguridad en redes: aplicaciones y estándares.* Madrid: Pearson Educacion.

T, D. M. (2009). Formación a través de internet: evaluación de la calidad. barcelona: UOC.

T, D. M. (Viernes de Agosto de 2014). *Formación a través de internet*. Obtenido de Evaluación de la calidad: http://dmi.uib.es/~bbuades/calidad/tsld010.htm

Trillo Sáez, B. (2005). *Cuaderno de prácticas, Redes locales.* Madrid España: Vision Libros.

Ujat, D. (2007). *Avances en Informática y Sistemas Computacionales Tomo II (CONAIS 2007).* Tabasco, México: Libri Mundi.

Villoria Mendieta, M. (1996). *La modernización de la administración como instrumento al servicio de la democracia.* Madrid: Libri Mundi.

William, R. N. (2008). Planificación Y Evaluación de Proyectos Informáticos. Costa Rica: Universisas a Distancia.

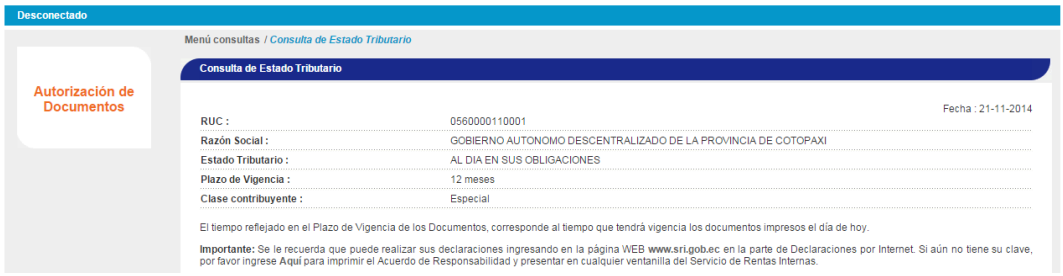
Anexos

Anexo 1

MATRIZ DE ANÁLISIS DE SITUACIONES			
Situación actual real negativa	**Identificación del problema a ser investigado**	**Situación futura deseada positiva**	**Propuesta de solución al problema planteado**
• **Necesidad que se mejore la velocidad de *internet*.** • **Correos electrónicos no deseados.** • **Infección de los servicios informáticos causados por virus, gusanos, troyanos, *spyware*, intentos de *phishing*, etc.** • **No se dispone de una infraestructura de *firewall* que posibilite el crecimiento y administración centralizada de las subredes.** • **Con la infraestructura de seguridad existente, no puede crecer ni dotar del servicio de *internet* a más redes.**	• La vulnerabilidad de la seguridad informática	• Mejorar el ancho de banda para el uso de *internet*, de acuerdo a la importancia y prioridad de cada usuario. • Sistemas informáticos funcionando en forma eficiente, libre de infecciones maliciosas informáticas. • Crecimiento de las subredes en forma controlada y centralizada, a través de un *firewall*.	• Administrador de ancho de banda con calidad de servicio. • Un esquema de seguridad perimetral informática para el GADPC.

FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz.

Anexo 2



FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz.

Anexo 3

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE ESTUDIOS DE POSGRADO
CUESTIONARIO DE ENCUESTA

DIRIGIDO A: Autoridades, Personal Administrativo, Operativo.

PROYECTO: La seguridad perimetral y su incidencia en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.
OBJETIVO: Obtener información sobre la seguridad y la calidad de servicio de la red informática en el GADPC.
MOTIVACIÓN: Saludos cordiales, le invitamos a contestar con la mayor seriedad el siguiente cuestionario a fin de obtener información valiosa y confiable, que será de uso oficial y de máxima confidencialidad, con miras a mejorar la calidad de servicio informático en el GADPC.
INSTRUCCIONES: Seleccione la respuesta adecuada a su modo de pensar o su opinión según el caso. Procure ser lo más objetivo y veraz.

1. ¿Su computador ha sufrido algún tipo de vulnerabilidad informática ya sea por virus, terceras personas u otro tipo de amenaza?

SI ☐ NO ☐

La opción es SI, especifique el tipo: ……

2. ¿Cuántas veces se han detectado virus en su computador en los dos últimos años?

NINGUNA ☐ UNA ☐ DOS ☐ MÁS DE DOS ☐

3. ¿Dispone el GAD de herramientas o sistemas que detecten los intentos de acceso a la red de datos de la Institución?

SI ☐ NO ☐ DESCONOCE ☐

4. ¿Qué sistema operativo brinda mejor seguridad a sus aplicaciones?

WINDOWS ☐

LINUX ☐

AS/400 ☐

OTRO ☐ Especifique: …….

5. ¿Cree que mediante una adecuada seguridad en la red se pueda mejorar la calidad de servicio informático?

No (nunca) ☐ A veces ☐ Si (siempre) ☐

	Equivalencia de los rangos = 1 Nunca; 5 Siempre	**1**	**2**	**3**	**4**	**5**
6.	¿Con qué frecuencia cree que los inconvenientes en la red ocurren?					
	Equivalencia de los rangos = 1 Deficiente; 5 Excelente	**1**	**2**	**3**	**4**	**5**
7.	¿Cómo califica la calidad de servicio informático?					
8.	¿En relación al acceso a los sistemas informáticos internos del GADPC, cómo considera el servicio?					
9.	¿Cómo considera el servicio de *internet*?					

¡GRACIAS POR SU COLABORACIÓN!
ESPACIO RESERVADO PARA ENCUESTADORES Y SUPERVISORES DE LA UTA

	Encuesta personal	**Vía Telefónico**	**E-mail**
Fecha (día/mes/año)			
Hora inicio (hr/min.)			
Hora término (hr/min.)			
Nombre y Apellido del Encuestador:	**Observaciones:**		
SUPERVISIÓN: Visita conjunta ◯ Control Telefónico ◯ Revisión cuestionario ◯			
FIRMA ENCUESTADOR	**FIRMA SUPERVISOR**		

Anexo4

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE ESTUDIOS DE POSGRADO

CUESTIONARIO DE ENTREVISTA

DIRIGIDO A: Director Informático.

PROYECTO: La seguridad perimetral y su incidencia en la calidad de servicio de la red informática para el gobierno autónomo descentralizado de la provincia de Cotopaxi.
OBJETIVO: Obtener información sobre la seguridad y la calidad de servicio de la red informática en el GADPC.
MOTIVACIÓN: Saludos cordiales, le invitamos a contestar con la mayor seriedad las siguientes preguntas de la entrevista a fin de obtener información valiosa y confiable, que será de uso oficial y de máxima confidencialidad, con miras a mejorar la calidad de servicio informático en el GADPC.
INSTRUCCIONES: Conteste las preguntas a su modo de pensar o su opinión según el caso.

1. ¿De cuánto es el crecimiento anual de usuarios en la red en los últimos dos años?
2. ¿Dentro del Plan Estratégico Institucional, cual es la proyección Informática en lo referente a Seguridad en la red y Calidad de Servicio?
3. ¿Cómo se controla el acceso a la red e *internet* para que la información que fluye sea segura?
4. ¿De qué forma se distribuye el ancho de banda para las aplicaciones que tienen mayor prioridad de uso?
5. ¿El presupuesto asignado para el departamento de Sistemas, cubre las expectativas para el crecimiento tecnológico Informático?

¡GRACIAS POR SU COLABORACIÓN!
ESPACIO RESERVADO PARA EL ENTREVISTADOR DE LA UTA

Entrevista personal		
Fecha (día/mes/año)		**Observaciones:**
Hora inicio (hr/min.)		
Hora término (hr/min.)		

Nombre y Apellido del Entrevistador:		
SUPERVISIÓN: Visita conjunta ◯ Control Telefónico ◯ Revisión Entrevista ◯		
FIRMA ENTREVISTADOR	**FIRMA SUPERVISOR**	

Anexo5

Demostración para la mitigación de las vulnerabilidades en el GADPC.

Check Point SmartDashboard.- Es una consola a través de la cual se pueden integrar y configurar firewalls. La funcionalidad del firewall se determinará a través de la implementación políticas de seguridad de acuerdo a los perfiles del host o grupo de hosts que vamos a proteger.

Para la mitigación de vulnerabilidades en la red del GAD se establecerá políticas de prevención de amenazas que están basadas en:

Protección: Antivirus, anti spam, anti bot.

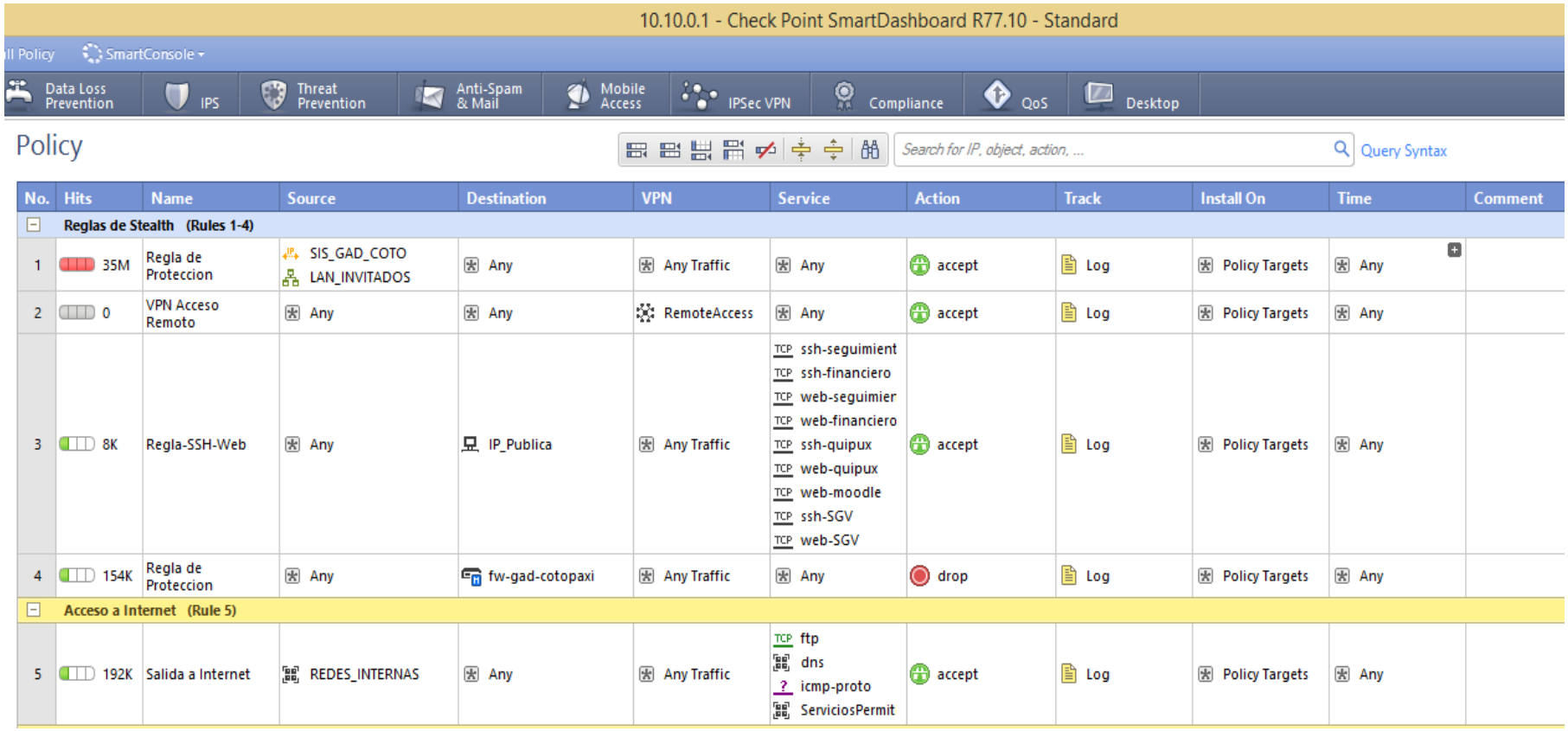
Rango a proteger: Servidor web con IP=186.46.92.162

Acción tomada: Prevent, es decir cortar el enlace.

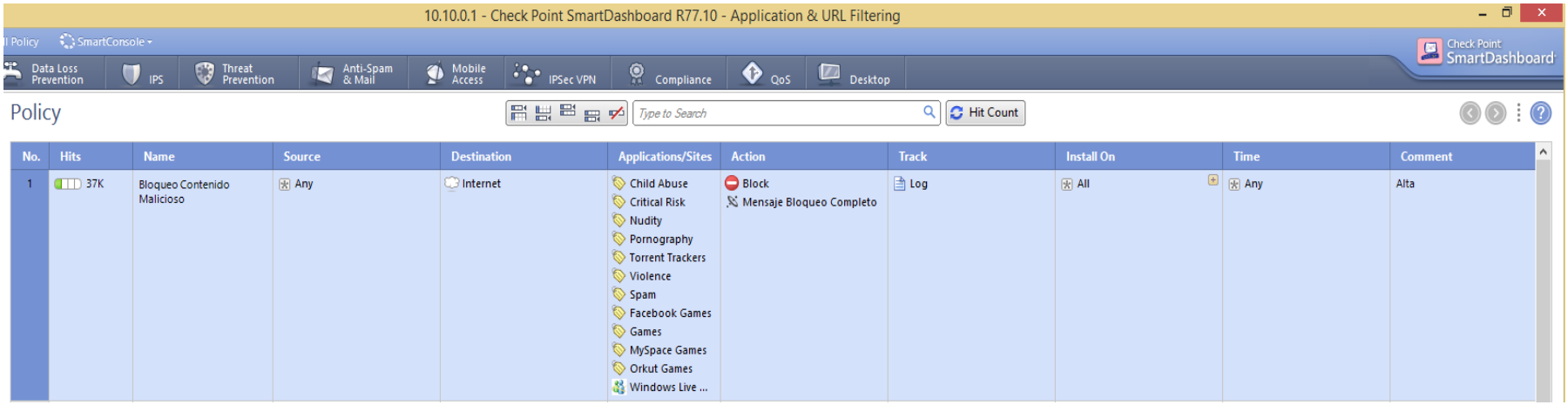
Manera de informar: Alert, alerta de la acción maliciosa.

Excepciones: Ninguna.

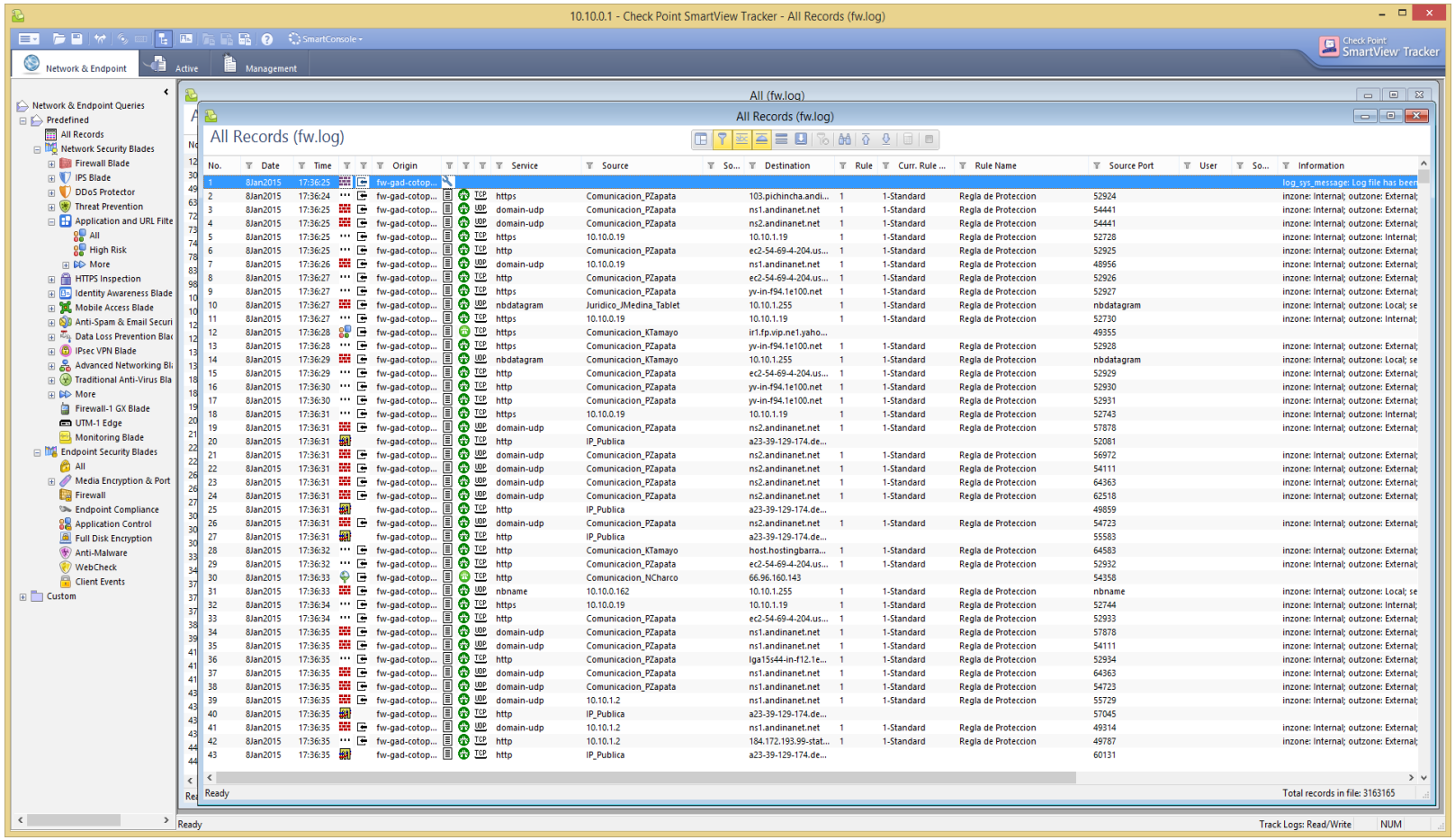
Resultados obtenidos:



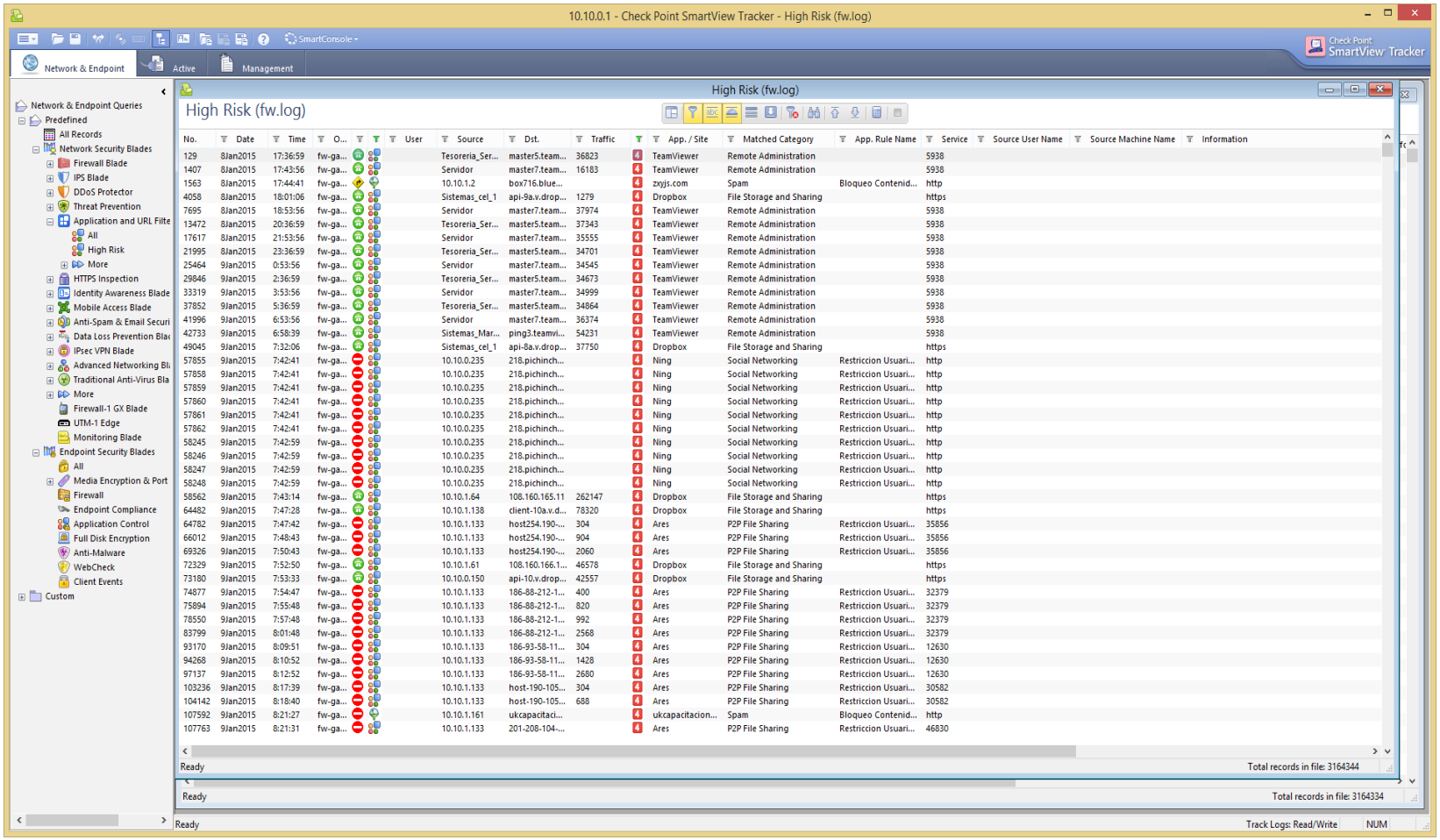
FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz



FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz



FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz



FUENTE: Investigación de campo
ELABORADO POR: Fernando Defaz

Algunas protecciones vienen configuradas por defecto.

Además podemos observar que las amenazas vienen visualizadas con colores de acuerdo a cada un nivel de actividad maliciosa así: bajo=verde, medio=amarillo, alto=rojo.
Por lo que la red informática del gobierno autónomo descentralizado de provincia de Cotopaxi quedaría protegida contra virus, spam, bot.

Anexo6

REQUERIMIENTOS TÉCNICOS DE ACTIVOS

DESCRIPCIÓN	ESPECIFICACIONES MÍNIMAS SOLICITADAS
1. PARTES PARA CHASIS IBM BLADE CENTER HS23	
Switch LAN 1 Gbps capa 3	
Cantidad	1
Marca	Especificar
Modelo	Especificar
Puertos *Ethernet* 10/100/1000	24
Administrable	Requerido
Factor de forma: Fixed, Rack Mountable 1U, Stackable/Clustering	Requerido
Número máximo apilamiento	>=8
Routing Protocol: RIP-1, RIP-2, HSRP, static IP routing, RIPng	Requerido
Remote Management Protocol: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, T*FTP*, SSH, CLI	Requerido
Authentication Method: Kerberos, Secure Shell (SSH), RADIUS, TACACS+	Requerido
Características: Hot swap module replacement, Layer 3 *switch*ing, Layer 2 *switch*ing, dynamic IP address assignment ,DHCP support, auto-negotiation, ARP support, trunking, *VLAN* support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, traffic shaping, *Broadcast* Storm Control, High Availability, Multicast Storm Control, Unicast Storm Control, Rapid Spanning Tree Protocol (RSTP) support, DHCP snooping, Dynamic Trunking Protocol (DTP) support, Port Aggregation Protocol (PAgP) support, Access Control List (ACL) support, Quality of Service (*QoS*), Jumbo Frames support, MLD snooping, Dynamic ARP Inspection (DAI), Per-*VLAN* Spanning Tree Plus (PVST+), EIGRP Stub Routing	Requerido
Estándares: IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1ae	Requerido

Memoria DRAM	256 MB
Memoria Flash	128 MB Flash
Lucesindicadoras LED: Port status, link activity, port transmission speed, port duplex mode, power, system	Requerido
Interfaces: 24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 **USB : 1 x 4 PIN USB Type A** **1 x console - mini-USB Type B - management** **1 x RS-232 - RJ-45 - management** **1 x 10Base-T/100Base-TX - RJ-45 - management** **Network stackdevice : 2 x**	Requerido
Rack Mounting Kit	Requerido
Powerredundancy	Especificar
Alimentación eléctrica: AC 120/230 V (50/60 Hz)	Requerido
Default AC Power Supply Rating with Dual Modular Slots: 350W	Especificar
StackPower	Requerido
MTBF	>=189,000 hour(s)
Software incluido: IOS IP Base	Requerido
Garantía	3 años
Instalación y puesta en marcha	Requerido
Incluye configuración del hardware	Requerido
2. SERVIDORES BLADE	
Cantidad	3
Marca	De la misma marca del Chasis Blade
Modelo	Blade
El servidor blade debe ser nuevo de fábrica, no re-manufacturado (no refurbished), ni reparado, ni re-acondicionado en ninguna de sus partes ni componentes	Requerido
Procesador	
Marca	Intel
Tecnología: Xeon 8 Core	Requerido
Velocidad Mínima	>= 2.6 Ghz / 1600 MHz
Núcleos: 8	Requerido
Cache L3 por procesador	>= 20 MB
Número de Procesadores Soportados	>=2
Número de Procesadores Instalados: 2	Requerido
Memoria	
Marca	De la misma marca del servidor ofertado

Crecimiento máximo en memoria	>=192 GB
Memoria Instalada: 32 GB en módulos de 8GB	Requerido
Tipo de Memoria: PC3-12800 CL11 ECC DDR3 VLP RDIMM o mejor	Requerido
Velocidad de la Memoria	>=1600 MHz
Pantalla	
Marca	Especificar
Modelo	Especificar
Diseño: Ultradelgado	Requerido
Tipo: LED	Requerido
Tamaño: 23"	Requerido
Resolución: 1920x1080	Requerido
Tiempo de respuesta:	<= 5 ms
Controlador de disco interno	
Tipo	SAS / HotSwap
Almacenamiento interno	
Marca	De la misma marca del servidor ofertado
Capacidad de cada disco: 300 GB	Requerido
Cantidad de discos instalados: 2 por cada servidor blade	Requerido
Velocidad: 15,000 rpm / 6Gbps	Requerido
Tamaño: 2.5in	Requerido
Tipo: Small Form Factor (SFF HS SAS HDD)	Requerido
Sistema de Administración	
Módulo Integrado de Administración	Requerido
Monitoreo del Sistema	Requerido
Registro de eventos de falla	Requerido
Alerta de fallas	Disco Duro, Memoria, Procesador
Capacidad de interacción con el módulo de administración del chasis	Requerido
Sistemas Operativos Soportados	
Microsoft Windows Server, Linux, Vmware	Requerido, Especificar
Sistemas Operativos con Acceso a la Unidad de Almacenamiento (Storage)	
Microsoft Windows, Linux, Vmware	Requerido, Especificar
Servicios y garantía	
El oferente debe incluir instalación, configuración de equipos, transferencia de conocimientos, actualización de firmware en infraestructura IBM	Requerido
Garantía: 3 años	Requerido
3. SOLUCIÓN DE ALMACENAMIENTO NAS (STORAGE)	
Cantidad	1

Marca	Especificar
Modelo	Especificar
Hardware	
Storage de rack	Requerido
Procesador núcleo cuádruple	Requerido
Frecuencia CPU	>=3.3 GHz
Punto flotante	Requerido
Motor de cifrado de hardware	Requerido
Memoria instalada: 16 GB DDR3	Requerido
Memoria ampliable	>=32 GB
Disco duro intercambiable en caliente	Requerido
LAN: Gigabit x4	Requerido
Soporte Link Aggregation	Requerido
Despertar con LAN/WAN	Requerido
Puerto expansión para tarjeta de 10 Gb	Especificar
External HDD Interface : Puerto USB 2.0 X 2, 1 Puerto expansión , Puerto USB 3.0 X 2	Requerido
Kit de montaje para rack	Requerido
Energia y voltaje	
Fuente redundante	Requerido
Nivel de ruido	<= 55dB(A)
Gestión de Almacenamiento	
10 discos Enterprise de 4 TB / HGST SATA 6 Gb/s 64 MB caché configurados en RAID 5 más 2 discos SSD Entreprise para caché, total 40TB	Requerido
Receptáculos de unidad máx. con la unidad de expansión	>=34
Tipo de unidad: 3.5" SATA(III) / SATA(II) HDD 2.5" SATA(III) / SATA(II) HDD 2.5" SATA(III) / SATA(II) SSD	Especificar
Receptáculos de unidades SSD de caché dedicadas	>=2
Tamaño max. del sistema de archivos:	>= 108 TB
Número máx. de volumen interno	>=1024
iSCSI Target máximo	>=128
iSCSI LUN máximo	>=512
Niveles de raid	
Soporte para niveles 0, 1, 5, 6, 10	Requerido
Migración de RAID: 1-5 / 5-6	Requerido
Expansión dinámica de volúmenes lógicos	

Expansión de volumen con unidades de disco duro más grandes	Especificar
Expansión de volumen añadiendo una unidad de disco duro	Especificar
Capacidad de uso compartido de archivos	
Cuentas de usuario máx:	>= 4096
Grupos máx:	>= 512
Carpetas compartidas máx:	>= 512
Tareas máx. de sincronización de carpetas compartidas:	>= 32
Conexiones CIFS / AFP / *FTP* simultáneas	>= 1024
Compatibilidad con lista de acceso a Windows (ACL)	Requerido
Sistemas operativos compatibles que accesan al Storage	
Linux	Requerido, especificar
Windows	Requerido, especificar
Otros	Especificar
Virtualización Compatible	
VmwarevSphere 5	Requerido
Microsoft Hyper-V	Requerido
Citrix	Especificar
Especificar otros	Especificar
Software de administración	
El tipo de licenciamiento debe ser perpetuo	Requerido
Se deberá incluir el soporte y mantenimiento de todo el software incluido en la solución de almacenamiento para un período de un año como mínimo	Requerido
Software de administración propietario incluído con la solución	Requerido
Tipo de acceso desde computador cliente, especificar implementación	Requerido

Aplicaciones: Monitor de recursos, File Station, Unidad virtual, Carpeta remota, Copias de seguridad, Sincronizaciones, Servidor DNS, DHCP, *FTP*, correo, VPN, Directorio LDAP, multimedia, Web Station, host virtual, PHP/MySQL, Time Backup, Cloud Station, Multimedia DLNA certificado, restauración instantánea de archivo, virtualización, cuota de usuario personalizada, Compatibilidad con aplicaciones de terceros, compatibilidad de múltiples subredes, conexión SSL, compatibilidad de *VLAN*, administrador de conexión, administración de disco duro	Requerido
Servicios, Garantía	
La unidad de almacenamiento debe quedar instalada, configurada y funcionando correctamente en conjunto con el chasis blade y los servidores blade, debe quedar integrada con nuevos servicios de nube en los usuarios, tareas de backup e instancias de respaldo, DNS/DHCP/*FTP*/CLOUD STATION/APLICACIONES MÓVILES	Requerido
El oferente deberá entregar la solución configurada y funcionando, debe incluir todos los elementos y accesorios para su correcto funcionamiento	Requerido
Garantía del Storage	>=3 años estándar, brindada por el fabricante
Garantía de discos	>=1 años estándar, brindada por el fabricante
4. *FIREWALL*	
Marca	Especificar
Modelo	Especificar
Orientado a	Empresa de mediano tamaño
Factor de Forma	De rack, incluir accesorios para montar en rack
Ocupación en rack	1U
Puertos: 10 x GE RJ45 ports (including 8 x FortiASIC-accelerated ports, 2 x management ports)	Requerido
Tipo interfaces: 10/100/1000	Requerido
Puertos USB	>=2
Puerto de consola: serial RJ45	>=1
Alamcenamiento interno	>= 32 GB
DC power supply + Hardware plus	Requerido

1 year 8x5 Forticare and FortiGuard Bundle	Requerido
***Firewall*Throughput (1518 byte UDP)**	>= 8 Gbps
***Firewall*Throughput (512 byte UDP)**	>= 8 Gbps
***Firewall*Throughput (64 byte UDP)**	>= 8 Gbps
***IPS*ec VPN Throughput (512 byte packet)**	>= 4.5 Gbps
***IPS*Throughput**	>= 1.2 Gbps
***Proxy*-based Antivirus Throughput**	>= 200 Mbps
Flow-based Antivirus Throughput	>= 550 Mbps
Client-to-Gateway *IPS*ec VPN Tunnels	>= 10,000
Gateway-to-Gateway *IPS*ec VPN Tunnels (System / VDOM)	>= 6,000 / 3,000
SSL-VPN Users (Recommended Max)	>= 500
SSL-VPN Throughput	>= 200 Mbps
ConcurrentSessions (TCP)	>= 1,000,000
New Sessions/Sec (TCP)	>= 35,000
***Firewall*Policies (Max)**	>= 10,000
UnlimitedUserLicenses	Requerido
Virtual Domains (VDOMs)	>= 10
High AvailabilityConfigurations	Active/Active, Active/Pasive, Clustering - Especificar
Mobile Access	Especificar
AdvancedNetworking&Clustering	Especificar
IdentityAwareness	Especificar
Application Control	Requerido
Data LossPrevention	Especificar
URL Filtering	Requerido
Antivirus & Anti-malware	Requerido
Anti-spam	Requerido
Software de administración propietario incluído con la solución	Requerido
Certificaciones: ICSA Labs: *Firewall*, SSL, VPN, *IPS*, Antivirus	Requerido
5. MEJORAMIENTO DE LA INFRAESTRUCTURA DE RED	
Switch administrable Gigabit *Ethernet*capa 3	
Cantidad	1
Marca	Especificar
Modelo	Especificar
Puertos Gigabit *Ethernet*: 26 + 2	Requerido
Capacidad en millones de paquetes por segundo (de 64 bytes): 41,67 mpps	Requerido
Capacidad de *switch*ing: 56 Gbps	Requerido
Puertos de expansión: 2 ranuras mini GBIC combinadas	Requerido

Protocolo de árbol de expansión (STP): Compatibilidad con el estándar 802.1d Árbol de expansión **Convergencia rápida mediante 802.1w (árbol de expansión rápida [RSTP, Rapid Spanning Tree]), activada en forma predeterminada** **8 instancias compatibles** **Instancias de árbol de expansión múltiple mediante 802.1s (MSTP)**	Requerido
Agrupación de puertos: Compatibilidad con protocolo de control de agregación de enlaces (LACP) versión IEEE 802.3ad **●** **Hasta 8 grupos** **●** **Hasta 8 puertos por grupo con 16 posibles puertos por cada agregación (dinámica) de enlaces 802.3ad**	Requerido
***VLAN*: Soporte para un máximo de 4096 redes *VLAN* simultáneamente** ***VLAN* basadas en puertos y en etiquetas 802.1Q** ***VLAN* basada en MAC** ***VLAN* de administración** **Perímetro de *VLAN* privada (PVE), también conocido como puertos protegidos, con varios uplinks** ***VLAN* de usuarios temporales** ***VLAN* no autenticada** **Asignación de *VLAN* dinámica por medio del servidor Radius junto con 802.1x autenticación del cliente *VLAN* CPE**	Requerido
***VLAN* de voz: El tráfico de voz se asigna automáticamente a una *VLAN* específica de voz y se trata con los niveles apropiados de *QoS*. Las capacidades de voz automáticas proporcionan implementación sin intervención en toda la red de los terminales de voz y dispositivos de control de llamadas.**	Requerido
***VLAN* de multidifusión TV**	Requerido
***VLAN* perimetral (Q-in-Q)**	Requerido

Protocolo genérico del registro de la *VLAN* (GVRP)/Protocolo genérico del registro de atributos (GARP)	Requerido
Retransmisor de protocolo de configuración dinámica de host (DHCP) en capa 2	Requerido
Detección del Protocolo de administración de grupos de *Internet* (IGMP) versiones 1, 2 y 3	Requerido
Protocolo de detección de Cisco (CDP)	Requerido
Función de consulta de IGMP	Requerido
Bloqueo de cabecera (HOL)	Requerido
Tramas gigantes: Hasta 9K (9216) bytes	Requerido
Direcciones MAC de hasta 16K (16384)	Requerido
Routing de paquetes IPv4 a velocidad de cable / Hasta 512 rutas estáticas y 128 interfaces IP	Requerido
Routing entre dominios sin clase (CIDR)	Requerido
Retransmisor DHCP en capa 3	Requerido
Retransmisor de protocolo de datagramas de usuario (UDP)	Requerido
Servidor DHCP	Requerido
Seguridad RADIUS/TACACS+	Requerido
Protocolo Secure Shell (SSH)	Requerido
Capa de sockets seguros (SSL)	Requerido
IEEE 802.1X (función de Autenticador)	Requerido
Enlace de puertos IP/Mac (IPMB)	Requerido
Secure Core Technology (SCT)	Requerido
Protección de IP de origen (*IPSG*)	Requerido
Inspección ARP dinámica (DAI)	Requerido
Flash	>= 16 MB
Memoria CPU	>= 128 MB
Buffer de paquetes	>= 8 Mb
Vigilantes de tráfico entrante; modelado y control de tráfico saliente; por *VLAN*, por puerto y basado en el flujo	Requerido
Compatible con red Cisco Small Business FindIT y Cisco OnPlus	Requerido
Interfaz de usuario web	Requerido
Access Point Wireless Empresarial	
Cantidad	10
Marca	Especificar
Modelo	Especificar

Tipo:	Punto de acceso interior de radio doble
Wi-Fi Estándar IEEE802.11n	Requerido
Wi-Fi a/b/g/n Certificado	Requerido
Puertos **1 puerto RJ-45 10/100/1000 de detección automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T)** **Dúplex: 10BASE-T/100BASE-TX: mitad o completo** **1000BASE-T: solo completo** **1 puerto serie para consola RJ-45**	Requerido
Dual band 2,4 GHz y 5 GHz	Requerido
Modos de operación Radio: Clientaccess, Local mesh, Packet capture	Requerido
Modos de operación AP: Autónomo y controlado	Requerido
Velocidad de transmisión wireless	>= 300 Mbps
ISM Band / UNII Band	Requerido
Rango frecuencia ISM	2.41 GHz - 2.46. GHz
Rango frecuencia UNII	5.18 GHz - 5.70 GHz
Número de antenas: 6	Requerido
Ganancia antenas: 4dBi, 7 dBi	Requerido
Tipo de antena: Omnidireccional	Requerido
Admite la alimentación a través de *Ethernet* (PoE) IEEE 802.3af	Requerido
MDIX automático	Requerido
Soporta *VLAN*S	Requerido

Seguridad Wireless: Security filter IP filter EAP-SIM EAP-FAST EAP-TLS EAP-TTLS PEAP RADIUS AAA EAP-MD5 PAP CHAP MS-CHAPv2 WPA WPA2 AES TKIP TLS TTLS	Requerido
MIMO Technology Quality of Service (*QoS*)	Requerido
Prensas para montaje en el techo: 2	Requerido
IEEE 802.3af PoE compliant for Gigabit *Ethernet*	Especificar
Dual core @ 800 MHz, 128 MB flash, 256 MB SDRAM	Especificar
Administración: SNMP v1, 2c, v3 DHCP HP RF Manager Embedded HTML management	Requerido
Impresora láser B/N	
Cantidad	2
Marca	Especificar
Modelo	Especificar
Tipo: Multifunción B/N	Requerido
Velocidad de copia:	>= 20 ppm
Proceso de copia: Escaneo por rayo láser e impresión electrofotográfica	Requerido
Resolución	>= 600 dpi
Copia mútiple	Hasta 99
Tiempo de calentamiento	<= 30 segundos
Velocidad de primera impresión	<= 7.5 segundos
Zoom: 50 - 200% (en incrementos del 1%)	Requerido

Memoria: 640 MB	Requerido
Capacidad entrada papel: 1 bandeja de papel de 250 hojas	Requerido
Capacidad salida papel	>= 250 hojas
Tamaño papel: A4-A5 / A6	Requerido
Gramaje papel: 60 - 90 g/m²	Requerido
Doble cara: Estándar	Requerido
CPU: RM5231 400 MHz	Requerido
Velocidad de impresión	>= 20 ppm
Lenguaje de la impresora: PCL5e, PCL6, PostScript® 3™	Requerido
Interfaz: *Ethernet* 10 base-T/100 base-TX / USB2.0	Requerido
Memoria: 640 MB + Unidad opcional de disco duro de 80 GB	Requerido
Protocolo de red: TCP/IP (IPv4, IPv6), IPX/SPX. Appletalk, SMB	Requerido
Velocidad de escaneo a todo color	>= 10 originales por minuto
Velocidad de escaneo B/N	>= 22 originales por minuto
Formatos de salida: TIFF, PDF, JPEG	Requerido
Direcciones de destino	>= 100
Escaneo a carpeta a través de protocolo SMB, *FTP* o NCP	Requerido
Software: Web Image Monitor SmartDeviceMonitor™ DeskTopBinder™ Lite Web SmartDeviceMonitor™	Requerido
Costo por página	<= $ 0.015
Computador Desktop Todo en Uno	
Cantidad	3
Marca	Especificar
Modelo	Especificar
Tipo: All In One	Requerido
Procesador: Intel Core i5	Requerido
Velocidad de Procesador	>= 2.7 GHz
Memoria DDR3	>= 8 GB
Disco duro de 1TB	Requerido
Pantalla LED 23"	Requerido
Wi-Fi IEEE802.11n	Requerido
Teclado español / ratón	Requerido
Genuine Windows	7 o posterior
Computador Portátil	
Cantidad	1

Marca	Especificar
Modelo	Especificar
Tipo: laptop	Requerido
Procesador: Intel Core i5	Requerido
Velocidad de Procesador	>= 2.0 GHz
Memoria DDR3	>= 6 GB
Disco duro	>= 640 GB
Pantalla	>= 14"
Wi-Fi IEEE802.11n	Requerido
Teclado español / ratón	Requerido
Genuine Windows	7 o posterior
6. SOFTWARE	
Windows Server 2012	
Cantidad	1
Tipo: Win SvrStd 2012R2 OLP NL Gov 2 Proc	Requerido
Licencia Adm. Windows Server 2012	
Cantidad	1
Tipo: Win SvrCAL 2012R2 OLP NL GovDvD Cal	Requerido
Licencia Usuarios Windows Server 2012	
Cantidad	50
Tipo: WinSvrCAL 2012R2 OLP NL GovUsr Cal	Requerido
Red Hat Enterprise Linux Server	
Cantidad	1
Tipo: Standard (1-2 sockets) (Up to 1 guest)	Requerido
Red Hat Enterprise Virtualization	
Cantidad	2
Tipo: Standard (2 sockets)	Requerido
Software de Virtualización	Incluir Licencias de software de Virtualización los 4 servidores blade, incluir la consola de administración, el software de cumplir con Gestión centralizada, alta disponibilidad, recuperación de datos, Vmotion, y el vcenter es ilimitad versión Estándar
Sistema Operativo	Incluir Red Hat Enterprise Linux Server Standard (1-2 sockets) (4 guests), para 4 servidores soporte Premium
Respaldo	Incluir Sofware de Respaldo de la misma marca del fabricante de la solución de Hardware ofertado, para todos los servidores que son parte de la oferta técnica

7. CAPACITACION	
Firewall	Transferencia de conocimiento para 2 personas
Herramienta de Virtualización	Transferencia de conocimiento para 2 personas
Herramienta de Colaboración	Transferencia de conocimiento para 2 personas
Herramienta de Respaldo	Transferencia de conocimiento para 2 personas
8. GARANTIA Y SOPORTE TECNICO	
Garantía de todo el hardware y software, mínimo por tres años	Requerido
Instalación Sistema Operativo	Incluye instalación base del Sistema operativo
Soporte Técnico	50 horas de soporte técnico que podrán ser brindadas en un año a partir de la entrega de los bienes y servicios ,la modalidad puede ser en sitio, telefónica o en forma remota, de toda la solución ofertada.
Tipo de soporte del Hardware , software que es parte de la solución	Soporte del oferente 7X24
9. REQUERIMIENTOS GENERALES	
TIEMPO DE ENTREGA	
Tiempo de Entrega de los bienes: Máximo 45 días calendario a partir de la firma del contrato. 15 días adicionales para la instalación y capacitación	Requerido
ADICIONALES	
Todas las partes y piezas que conforman los equipos deben estar integrados y trabajando correctamente	Requerido
Todos los equipos deben incluir cables y conectores necesarios para su correcta operación	Requerido
Todos los equipos deben incluir manuales técnicos y de operación	Requerido
El oferente deberá entregar todos los equipos instalados, configurados y funcionando incluyendo todo el hardware, software y accesorios que permitan la instalación y operación de los requerimientos especificados.	Requerido
REQUERIMIENTOS PARA EL OFERENTE	
Todos los componentes deben cumplir o superar las especificaciones técnicas y de calidad, solicitadas en este formulario	Requerido

Todos los componentes deben ser de la misma marca u homologados por el fabricante de los equipos	Requerido
La marca de los equipos o componentes deben ser reconocidas en el mercado nacional e internacional	Requerido
Los oferentes deberán ser distribuidores directos autorizados por el fabricante.	Requerido
El fabricante deberá tener oficinas localmente	Requerido
El fabricante deberá poseer bodega de repuestos en el país	Requerido
Presentar 3 certificados de clientes en donde el oferente haya provisto de soluciones similares	Requerido
Presentar un listado de los últimos proyectos de similar magnitud como solución integral que no vayan más allá de 3 años	Requerido
Los oferentes deberán presentar certificaciones del personal técnico involucrado en la instalación y capacitación de la solución	Requerido
El oferente debe tener al menos 2 personas certificadas por el fabricante en:	
Servidore Blade, Storage	
RHCE, Red Hat Certified Engineer	Requerido
RHCI, Red Had Certified Instructor	Requerido
Red Hat Enterprise Directory Services and Authentication	Requerido
En la parte de seguridades que cuente con las certificaciones	
CEH, CertifiedEthical hacker	Requerido
CHFI, Computer Hacking Forensic Investigator	Requerido
ITIL foundations	Requerido

FUENTE: GADPC
ELABORADO POR: Fernando Defaz

Anexo 6

Lista Negra

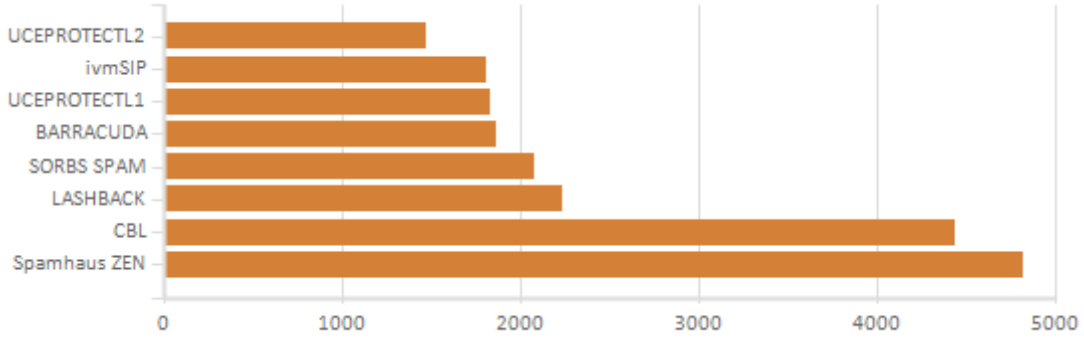
---------- Forwarded message ----------
From: **MxToolBox** <noreply@mxtoolbox.com>
Date: 2014-11-27 8:45 GMT-05:00
Subject: MxToolbox Blacklist Summary
To: Patricio Chávez <xpchavez@gmail.com>

MxToolbox Monitor Summary

11/26/2014 - 11/27/2014

Helpful Links: Dashboard Monitors Notifications History Mail Flow Settings

Global Blacklist Activityfor 11/26/2014 - 11/27/2014



SummaryInformation

AvgMxRep Score	Learn More
MxRep Change Since Last Report	Learn More
Number of Blacklist Monitors	**2**
New Listings Since Last Report	**0**
Email Frequency	daily

All Blacklist Monitors:

MxWatch is currently configured to monitor the following servers for Blacklist Activity.

IP	MxRep	Name	Current Status
186.46.92.162	Learn More	Blacklist	On CBL OnSpamhaus ZEN
186.46.92.163	Learn More	Blacklist	NotBlacklisted

Escaneo de puertos

Estado	Puerto	Nombre	Resultado	Tiempo (ms)
	21	ftp	Se intentó una operación en algo que no es un socket 186.46.92.162:21	0
	22	ssh	Se intentó una operación en algo que no es un socket 186.46.92.162:22	0
	23	telnet	Se intentó una operación en algo que no es un socket 186.46.92.162:23	0
	25	smtp	Se intentó una operación en algo que no es un socket 186.46.92.162:25	0

Estado	Puerto	Nombre	Resultado	Tiempo (ms)
✗	53	dns	Se intentó una operación en algo que no es un socket 186.46.92.162:53	0
✓	80	http	Éxito	125
✗	110	pop3	Se intentó una operación en algo que no es un socket 186.46.92.162:110	0
✗	143	imap	Se intentó una operación en algo que no es un socket 1 Comprobación **186.46.92.162** contra **89** listas negras conocidas ... 86.46.92.162:143	0
✗	139	netbios	Se intentó una operación en algo que no es un socket 186.46.92.162:139	0
✗	389	ldap	Se intentó una operación en algo que no es un socket 186.46.92.162:389	0
✓	443	https	Éxito	140
✗	587	MSA-perspectivas	Se Acabó El Tiempo	0
✗	1352	Lotus Notes	Se intentó una operación en algo que no es un socket 186.46.92.162:1352	0
✗	1433	sql server	Se intentó una operación en algo que no es un socket 186.46.92.162:1433	0
✗	3306	mi sql	Se intentó una operación en algo que no es un socket 186.46.92.162:3306	0

SMTP

smtp: 186.46.92.162 monitor Este

No se puede conectar al cabo de 15 segundos.

	Prueba	Resultado	
✗	SMTP Conectar	No se pudo conectar	

	Prueba	Resultado	

Sesión Transcripción:

```
Conexión a 186.46.92.162
1/14/2015 2:12:27 PM intento de conexión 1 - No se puede conectar al
cabo de 15 segundos. [15.05 seg] 15054ms MXTB-PWS3v2
```

Busqueda inversa

Rango: 186.46.92.160 - 186.46.92.167

Direcciones IP: 8

Máscara: 255.255.255.248 / 29

Lista negra	MxRep	Dirección IP	Nombre	DNS inversa	Detalles
Listas negras de Monitor	Aprender Más	186.46.92.160	** ** *SUBRED*	160.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.161	*Haga clic para editar*	161.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.162	*Haga clic para editar*	162.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.163	*Haga clic para editar*	163.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.164	*Haga clic para editar*	164.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.165	*Haga clic para editar*	165.pichincha.andinanet.net	

Lista negra	MxRep	Dirección IP	Nombre	DNS inversa	Detalles
Listas negras de Monitor	Aprender Más	186.46.92.166	*Haga clic para editar*	166.pichincha.andinanet.net	
Listas negras de Monitor	Aprender Más	186.46.92.167	** ** *BROADCAST*	167.pichincha.andinanet.net	

Lista Negra (evidencia)

Comprobación **186.46.92.162** contra **89** listas negras conocidas

	Lista negra	Razón	TTL	ResponseTime
OKAY	ASPEWS			62
OKAY	BACKSCATTERER			78
OKAY	BARRACUDA			125
OKAY	BBFHL1			78
OKAY	BBFHL2			62
OKAY	BLOCKLIST.DE			172
OKAY	BSB			78
OKAY	TECH QUEMADO			62
OKAY	CASA CBL			62

OKAY	CASA CBLESS			47
OKAY	CASA CBLPLUS			47
OKAY	CASA CDL			62
OKAY	CBL			78
OKAY	CYMRU bogons			62
OKAY	DAN TOR			78
OKAY	DAN TOREXIT			62
OKAY	DNS SERVICIOS			94
OKAY	DRMX			62
OKAY	DULRU			62
OKAY	EFnet RBL			62
OKAY	FABELSOURCES			62
OKAY	HIL			94
OKAY	HIL2			78
OKAY	ICMFORBIDDEN			62
OKAY	IMP SPAM			62
OKAY	IMP WORM			62

OKAY	INPS_DE			78
OKAY	InterServer			62
OKAY	ivmSIP			62
OKAY	ivmSIP24			62
OKAY	JIPPG			62
OKAY	KEMPTBL			47
OKAY	KUNDENSERVER			156
OKAY	LashBack			62
OKAY	LNSGBLOCK			62
OKAY	LNSGBULK			47
OKAY	LNSGMULTI			47
OKAY	LNSGOR			78
OKAY	LNSGSRC			62
OKAY	MADAVI			47
OKAY	Mailhosts.org IPBL			47
OKAY	Mailhosts.org SHORTLIST			62
OKAY	MAILSPIKE BL			156

OKAY	MAILSPIKE Z			172
OKAY	MEGARBL			156
OKAY	MSRBL Combinada			78
OKAY	MSRBL Imágenes			47
OKAY	MSRBL Phishing			47
OKAY	MSRBL spam			62
OKAY	MSRBL virus			62
OKAY	NETHERRELAYS			47
OKAY	NETHERUNSURE			47
OKAY	NIXSPAM			156
OKAY	NoSolicitado			62
OKAY	ORVEDB			62
OKAY	OSPAM			47
OKAY	PSBL			47
OKAY	RATAS Dyna			62
OKAY	RATAS NoPtr			62
OKAY	RATAS spam			78

OKAY	RBL JP			47
OKAY	RSBL			47
OKAY	SCHULTE			47
OKAY	SEM retrodispersión			94
OKAY	SEM NEGRO			94
OKAY	SERVICESNET			62
OKAY	BLOQUE SORBS			78
OKAY	SORBS Duhl			78
OKAY	SORBS HTTP			47
OKAY	SORBS MISC			62
OKAY	SORBS SMTP			47
OKAY	SOCKS SORBS			62
OKAY	SORBS SPAM			47
OKAY	SORBS WEB			62
OKAY	SORBS ZOMBIE			62
OKAY	SPAMCANNIBAL			47
OKAY	Spamcop			47

OKAY	Spamhaus ZEN			62
OKAY	SPEWS1			62
OKAY	SPEWS2			47
OKAY	SWINOG			62
OKAY	TRIUMF			47
OKAY	TRUNCATE			62
OKAY	UCEPROTECTL1			62
OKAY	UCEPROTECTL2			47
OKAY	UCEPROTECTL3			62
OKAY	URIBL múltiples IP			62
OKAY	VIRBL			47
OKAY	WPBL			62

Anexo 7

Autorización realización de tesis

Cotopaxi
Todos somos
PREFECTURA

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA PROVINCIA DE COTOPAXI

Oficio Nº GADPC-DAYTH-2013-075

Latacunga octubre 31, 2013

Asunto: Autorización realización de tesis

Señor
Manuel Fernando Defaz Calvopiña
Egresado de la Maestría en Informática
UNIVERSIDAD TECNICA DE AMBATO
Presente

De mi consideración:

En referencia a su solicitud para desarrollar su proyecto, debo informarle que ha sido autorizado dado la utilidad que prestaría a la institución, siendo necesario que usted presente en esta Dirección el cronograma de trabajo y desarrollo de actividades.

Vale indicar que esta aceptación no compromete remuneración alguna con el GAD Provincial de Cotopaxi.

Atentamente,

Ing. Fernando Alvarado Espinosa
DIRECTOR ADMINISTRATIVO
Y TALENTOS HUMANOS

FAE/ccm.

Todos somos Cotopaxi PREFECTURA

Dir. Tarqui Nº 507 y Quito
Teléfono: 03 2800415//
Fax. 2800415 ext. 217
mail. info@cotopaxi.gob.ec
COTOPAXI - LATACUNGA - ECUADOR