UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

Mayo 2018 – Octubre 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRACTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA

ANÁLISIS DE LA SEGURIDAD INFORMÁTICA DE LA RED DE LA GOBERNACIÓN DE LA PROVINCIA DE LOS RÍOS.

EGRESADO

FRANKLIN ARMANDO ASITUMBAY ALUCHO

TUTOR

MAGISTER. MIGUEL ZUÑIGA

Babahoyo – Los Ríos – Ecuador

2018

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN.

La capacidad de prevenir, responder y recuperarse de cualquier tipo de incidencia provocada por algún factor que sea de tipo natural o provocada por el ser humano así como los distintos desastres naturales en función de la afectación provocada en la sociedad con relación a la seguridad local y provincial; Siendo la Gobernación de La Provincia de Los Ríos una institución gubernamental encargada de fomentar la seguridad ciudadana donde la tecnología a más de cumplir un rol importante se convierte en un aliado estratégico para enfrentar problemas adverso; así también mantener la capacidad de coordinar una correcta comunicación con las demás entidades y estamentos del estado Ecuatoriano a fin de proveer las soluciones inmediatas a las vicisitudes del momento.

Por esta razón se procede a realizar un análisis de la seguridad informática de la red de la Gobernación de la Provincia de Los Ríos con el objetivo de identificar los puntos neurálgicos así también las áreas críticas y sectores vulnerables de la red de datos de la entidad que es objeto de estudio.

Adicionalmente se pretende aportar con un caso de estudio en el cual se demuestre la importancia de mantener un ambiente controlado con sistemas y canales de comunicación para una perfecta coordinación con elementos y ayuda externa ya sean locales, estatales, no gubernamentales y voluntarias; con lo cual se obtiene una mayor explotación y aprovechamiento de los recursos y capacidades disponibles de la infraestructura de la institución.

De acuerdo a la observación en primera instancia, se verifica que la entidad no posee una herramienta general que permita la colaboración en línea con otras instituciones del mismo nivel jerárquico relacionadas a controlar las incidencias informáticas así como el análisis y mitigación de riesgo en la Provincia de Los Ríos; de la misma forma se observa claramente que entre la principal problemática en relación al análisis de la red de datos de la Gobernación no cuenta con una metodología que permita elegir una mejor opción, política o regla de seguridad para la integridad de los datos que reposan en los equipos informáticos de las distintas dependencias de la entidad entre ellos servidores, central de comunicación, computadores de escritorio y demás equipos necesarios para el desarrollo de actividades propias.

En términos generales la Gobernación de la Provincia de Los Ríos presenta serios inconvenientes con la presencia de elementos nocivos tales como virus informático en todo el parque informático, aplicaciones provenientes de internet que agregan lentitud en los procesos ejecutados, libre ejecución de programa de descarga directa lo cual satura el ancho de banda y estropea el servicio de internet en todo el edificio; todo ello debido a la ausencia de un sistema de seguridad perimetral lo cual a su vez seria el mecanismo ideal para resolver los problemas actuales.

DESARROLLO

El desarrollo de las habilidades de los profesionales informáticos va de la mano con la implementación e implantación de los sistemas de seguridad ya sea estos orientados a la información, la comunicación, la conexión y la administración; es así como mediante el presente caso de estudio se logra abordar los lineamientos que determinan el correcto funcionamiento de los sistemas de seguridad informática con énfasis a la red de datos de la Gobernación de La Provincia de Los Ríos, Ecuador.

Para el desarrollo de este estudio de caso se revisado los conceptos básicos sobre seguridad y con el mismo indicio se entabla los parámetros necesarios para descubrir las vulnerabilidades, amenazas y posibles intrusiones las mismas que son un producto derivado de los factores antes mencionados.

Al hablar de amenazas y vulnerabilidades se refiere a “la posibilidad de que ocurra cualquier tipo de evento o acción que produzca a su vez un daño mayor ya sea tangible o intangible lo cual afecta en mayor grado a la seguridad informática de cualquier red de datos” (Erb, 2014).

Las intrusiones en una red de datos son evento que en su mayoría ocasionan una serie de inserciones anómalas en la red de datos anfitriona, “Según Albert Lockhart en una red de datos es vital poseer un sistema de protección ya sea basado en Software o en Hardware que evite la inserción de datos no autorizados en la estructura de la red, de no contar con este mecanismo, los resultados suelen ser catastróficos” (Lockhart A., 2016).

Por tal razón se procede a realizar el planteamiento de la investigación mediante la observación directa en conjunto con la descripción de los hechos y acontecimientos que existen en la Red de Datos de la Gobernación de La Provincia de Los Ríos; para ello se aplica al escenario de investigación los conceptos básicos sobre seguridad y se logra demostrar que no existe de manera directa o indirecta un correcto control de amenazas o elementos nocivos en la red de datos, tal es el caso que la protección contra virus informáticos se encuentra en estado de obsolescencia, la conexión hacia el Internet no se encuentra protegida, adicionalmente se verifica que los equipos de cómputo no cuentan con un plan de contingencia para el respaldo de archivos y elementos de valor de la institución.

La institución se encuentra a su vez conformada por el siguiente orden orgánico funcional:

- Gobernador.
- Asesoría Jurídica.
- Planificación.
    - Planificación e Inversión.
    - Información, Seguimiento y Control.
- Comunicación Social.
- Dirección Administrativa.
    - Talento Humano.
    - Tecnología de la Información y Comunicación.
    - Secretaria.

    - Financiero.
- Dirección de Gestión, Política y Conflictos.
    - Jefatura Política
    - Tenencia Política.
- Dirección de Garantías Democráticas.
    - Protección de derechos.
    - Comisaria de la mujer y la familia.
- Dirección de Seguridad Ciudadana.
    - Control y Seguridad Ciudadana.
    - Intendencia Política.
    - Intendencia de la Policía.
    - Comisaría de Policía.

Adicionalmente como antecedente se sabe que la institución a través de su ente regulador tiene por deber y cumplimiento asesorar y asistir al señor presidente del Ecuador para adopción y ejecución de políticas y acciones que permitan obtener un mayor despliegue de soluciones a las problemáticas e incidencias que se suscitan a diario en todo el territorio de la Provincia de los Ríos.

Continuando con la revisión y observación en el sitio se detecta que el activo más valioso de la institución objeto de estudio, así como la red de datos no se encuentran respaldada y no cuenta con los mecanismos que le provean de la seguridad necesaria para evitar posibles anomalías e incidencias; se observa un sistema de cableado estructurado en categoría 6 el mismo que no cuenta con la certificación que valide su correcto funcionamiento; el sistema está pensado para albergar comunicaciones de voz

y datos así también video vigilancia, los equipos de interconexión son equipos de gama baja lo cual implica que no son administrables y por ende no permiten agregar niveles de seguridad en capa 2 y capa 3.

Los dispositivos y demás equipos activos se encuentran ubicados en el cuarto de computo dentro del área asignada al departamento de Tecnología de la Información y la Comunicación, para el efecto están empernados en un rack de piso de tipo abatible el cual es totalmente recomendado para realizar cualquier tipo de manteamiento preventivo y correctivo en la red informática de la Gobernación.

De acuerdo a las pruebas establecidas en el departamento de Tecnologías de la Información y Comunicación se hace un descubrimiento de los servicios que actúan sobre la red como es el caso de un servidor de dominio o DNS el mismo que está configurado con sistema operativo Microsoft Windows Server 2012 Enterprise Edition, un servidor de archivos con plataforma SharePoint de Micrososft Windows Server 2012 R2.

Al hablar de Microsoft como plataforma de servicios para el despliegue de servidores de dominio o DNS y de servidores de documentación e intranet como es el SharePoint se refiere a “herramientas colaborativas que ofrecen una tecnología de complementos que permiten compartir, administrar, editar, agrupar, interactuar, transformar y escalar la red informática de tal forma que se pueda construir una intranet con elementos de conocimiento colectivo. (Micrsoft, 2016).

Gráfico 1 Centro de Computo, núcleo de la Red Informática de la Gobernación de Los Ríos.
Fuente: El Autor

El Core de la red se encuentra construido por un equipo de capa 3 el mismo que se encuentra configurado por el proveedor de internet para el acceso a los servicios de internet hacia la red local, en cascada se encuentran acondicionados un equipo de capa 2 para las conexiones de datos entra cada computador y un distribuidor de comunicaciones telefónicas que se encarga de llevar extensiones analógicas a cada puesto de trabajo mediante los ductos de red.

Al hablar del Core de la red, se refiere básicamente “al núcleo o la capa encargada de proporcionar la conectividad entre los distintos puntos de acceso ya sean Router conocido como equipo de capa 3, Switch conocidos como equipo de capa 2 con la finalidad de enlazar todos los servicios que operen en la red; así lo indica Sebastián Criamer en su artículo de enlaces y conectividades para la Academia Cisco” (Criamer, 2017).

La red de datos de la Gobernación de Los Ríos está configurada en un segmento de Clase C “se entiende por redes de Clase C a la numeración de Protocolos de Internet apropiada para escenarios menores a 254 computadoras directamente conectadas a la red; lo cual significa que este tipo de redes son las de menor impacto por ser consideradas de uso doméstico, tal como lo indica Alejandro Llagua en su libro de Direccionamiento y Segmentación de Red” (Llagua, 2016).

Se evidencia que el sistema telefónico de la entidad es 100% analógico basado en una solución propietario con una edad promedio de 23 años de operatividad, por ende, La Gobernación de la Provincia de los Ríos se encuentra en extrema urgencia al momento de realizar conexiones y seguimientos a los distintos sucesos ocurridos en los diferentes cantones de la provincia depende únicamente las comunicaciones que realiza a través de *la Public Switched Telephone Network (PSTN)*.

A continuación, se visualiza a través del grafico 2 el estado actual y funcionamiento de la red de datos de la institución antes mencionada.

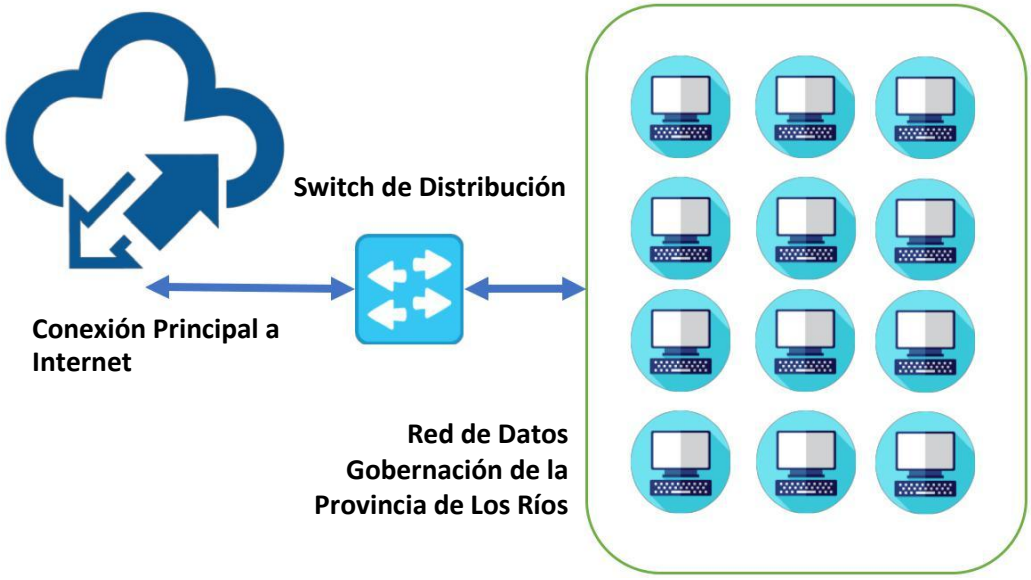

Gráfico 2*Diagrama de la Red de Datos de la Gobernación de la Provincia de Los Ríos.*
Fuente: El Autor.

La problemática se define como una instancia controlable ya que se ajusta a un modelo de control estándar el mismo que contempla estrategias para definir una Infraestructura Tecnológica (IT) para mejorar los parámetros de control de la actual red de datos; de acuerdo con el método de investigación empleado se verifica que las instalaciones de la Gobernación la Provincia de Los Ríos prestan las adecuaciones necesarias para el normal despliegue de una red da datos, ya que la estructura del edificio ha sido totalmente remodelada sobre la infraestructura principal.

Adicionalmente se construye una matriz de información perfilada necesariamente para la descripción del estado actual del parque informático, equipos de interconectividad, estado del enlace principal a internet y por ende el estado en el que se encuentra el medio de transmisión tal como se indica en la tabla 1, 2 y 3.

Para ello se toma en cuenta el principio de la seguridad informática lo cual es totalmente recomendable para escenarios no mayor a 50 usuarios directamente conectados a la red, es así como se utiliza OSSTMM “es una metodología abierta de comprobación de seguridad informática, esta herramienta permite detectar errores de seguridad y vulnerabilidades en todos los ámbitos de la red informática según lo define Andrew Lockhart en su libro sobre seguridad y análisis informático” (Lockhart A. , 2016).

Tabla 1

Criterios de Recopilación y Evaluación de Datos

No.	Proceso
1	Gestión de la documentación, antivirus, ofimatica, mantenimiento
2	Seguridad Perimetral, Red de Datos, Internet, Cableado estructurado
3	Identificación y acceso a la red de datos, intrusiones, control

En esta tabla se especifican los criterios requeridos para la recopilación de datos y posterior estudio de estos.

Tabla 2

Definición e interpretación de resultados Según matriz de datos.

Valor	Descripción
1	La brecha puede resultar en poca o nula pérdida o daño.
2	La brecha puede resultar en una pérdida o daño menor.
3	La brecha puede resultar en una pérdida o daño serio, y los procesos del modelo IT pueden verse afectados negativamente.
4	La brecha puede resultar en una pérdida o daño serio, y los procesos del modelo IT pueden fallar o interrumpirse.
5	La brecha puede resultar en altas pérdidas. Los procesos del modelo de IT fallarán.

En esta tabla se definen la interpretación otorgada a cada criterio de investigación de acuerdo con la matriz de información.

Tabla 3
Matriz de Riesgo en Función de la Seguridad Informática.

`							SENSIBILIDAD DE LA SEGURIDAD IN	
PROCESO	**% ACTIVIDAD**	**FABRICANTE**	**UBICACIÓN**	**CLASIFICACIÓN**	**CRÍTICO**	**NO CRÍTICO**	**INTERVENCÓN INMEDIATA**	**N IM**
20	0%	Eset	Planta Baja	URGENTE	Actualizaciones		Si	
13	0%	Eset	Planta Alta	URGENTE	Actualizaciones		Si	
33	100%	CNT	Sistemas	URGENTE	Navegación no Controlada		Si	
20	100%	Microsoft	Planta Baja	URGENTE	Actualizaciones		Si	
13	100%	Microsoft	Planta Alta	URGENTE	Actualizaciones		Si	
17	100%	Panasonic	Edificio Principal	ALTA	Upgrade o Reemplazo	No		
52	80%	Cableado Estructurado	Edificio Principal	ALTA	No tiene Certificación	No		
2	100%	Servidores	Sistemas	URGENTE	Configuración Básica		Si	
33	0%	Equipos Clones	Edificio Principal	URGENTE	No hay respaldo de información en tiempo real		Si	
0%	0%	Proxy	Edificio Principal	URGENTE	Servicio no Existente		Si	
0%	0%	Firewall	Edificio Principal	URGENTE	Servicio no Existente		Si	
0%	0%	Router	Edificio Principal	URGENTE	Servicio no Existente		Si	
0%	0%	Segementación	Edificio Principal	URGENTE	Servicio no Existente		Si	
0%	0%	NAS Backup	Sistemas	URGENTE	Servicio no Existente		Si	

A través de esta matriz se logra evidenciar el estado actual de la seguridad informática de La Gobernación de Los Ríos, se evidencia estado de obsolescencia de las protecciones a nivel de software y a carencia de protección a nivel de hardware.

De acuerdo con los datos obtenidos en la matriz anterior, se procede a definir un estudio análisis de la seguridad informática de la red de la Gobernación de la Provincia de Los Ríos; análisis que se encuentra ambientado en la recopilación de información la misma que se representa mediante una serie de criterios contenidos en el estándar *IT Incident Management Help Desk SLA (ITIL).*

Al hablar de ITIL se refiere a “el conjunto de buenas prácticas basado en la gestión de servicios tecnológicos orientados a la administración de procesos y operaciones para determinar el tipo de control que se debe aplicar en los escenarios de trabajo donde existan amenazas o elementos que alteren el orden de la red de datos; así lo define la Academia Cisco en su libro de seguridad informática 4ta. Edición” (Cisco, 2017).

Al referirse a este estándar en particular se logra determinar y detectar de forma acuciosa las amenazas y vulnerabilidades informáticas que puedan existir en la infraestructura de red de la entidad anteriormente citada, “es así como la matriz OSSTMM permite identificar el impacto causado en toda la infraestructura de red ya sea voz, datos o video: con ello en termino general se pretende garantizar un fortalecimiento institucional a través de la repotenciación de la plataforma tecnológica de la entidad a nivel de comunicaciones internas del edificio tal como lo indica Marcos Bustos en su libro de Seguridad y Amenazas en ambientes controlados ” (Bustos, 2016).

La hablar del estándar ISO/IEC 27001 se refiere a “la acción que permite agregar los niveles de seguridad que sean requeridos en función del mejoramiento de la infraestructura de red, a ello se asocia una matriz basada en el *Open Source Security Testing Methodology Manual (OSSTMM);* es así como Randolf Trevor evalúa de forma concreta los niveles de seguridad así como la información almacenada en las diferentes estaciones de trabajo según su publicación sobre las metodologías aplicables para garantizar la operatividad y canales de comunicación de los usuarios en una red informática” (Trevor, 2015).

Tabla 4

Ámbitos del OSSTMM, Análisis y verificación de los niveles de seguridad

ÁMBITO DE OSSTMM						
Seguridad Física	**Seguridad de la Información**	**Organización de la Información**	**Gestión de Activos**		**Seguridad del recurso Humano**	**Gestión de Operaciones y Comunicaciones**
Información	Acceso Físico y Lógico	Almacenamiento y Distribución	Telecomunicaciones	Redes de Datos	Grupo de Trabajo	Distribución y Acceso
Comprende todos los elementos tangibles que aportan con seguridad en el interior y exterior de la red de comunicaciones	Comprende todos los elementos considerados necesarios para el establecer los permisos de lectura, escritura o ejecución así como también la movilidad y transporte de un extremo a otro de la red.	Comprenden los mecanismos informáticos que permiten almacenar y dimensionar la cantidad necesaria en espacio y tiempo en un escenario controlado para administrar la información de forma adecuada.	Comprende todas las redes de Telecomunicaciones ya sean digitales o analógicas	Comprende todos los sistemas electrónicos y redes de datos incluidas las que integran voz, datos y video	Comprende todos los integrantes humanos que intervienen diariamente en la red de comunicaciones	Comprende todas las comunicaciones electrónicas y todo tipo de propagación de señales radio eléctricas a través del radio espectro

Se definen las áreas de mayor impacto según el análisis efectuado a la infraestructura de datos, se considera un método eficaz en la detección de incidencias y eventos no controlados.

Los resultados obtenidos en base al análisis efectuado a la seguridad informática de la Gobernación de Los Ríos fueron extrapolados a través de la herramienta informática NPM Summry del fabricante Solarwinds, esta esa aplicación que se encuentra orientada a la observación, monitorización y reporte de las incidencias ocurrida en un periodo de tiempo; para lo cual es necesario ejecutarlo de forma directamente conectado a la red a través de un equipo anfitrión con sistema operativo Microsoft, tal como se indica en el gráfico 2 y 3.

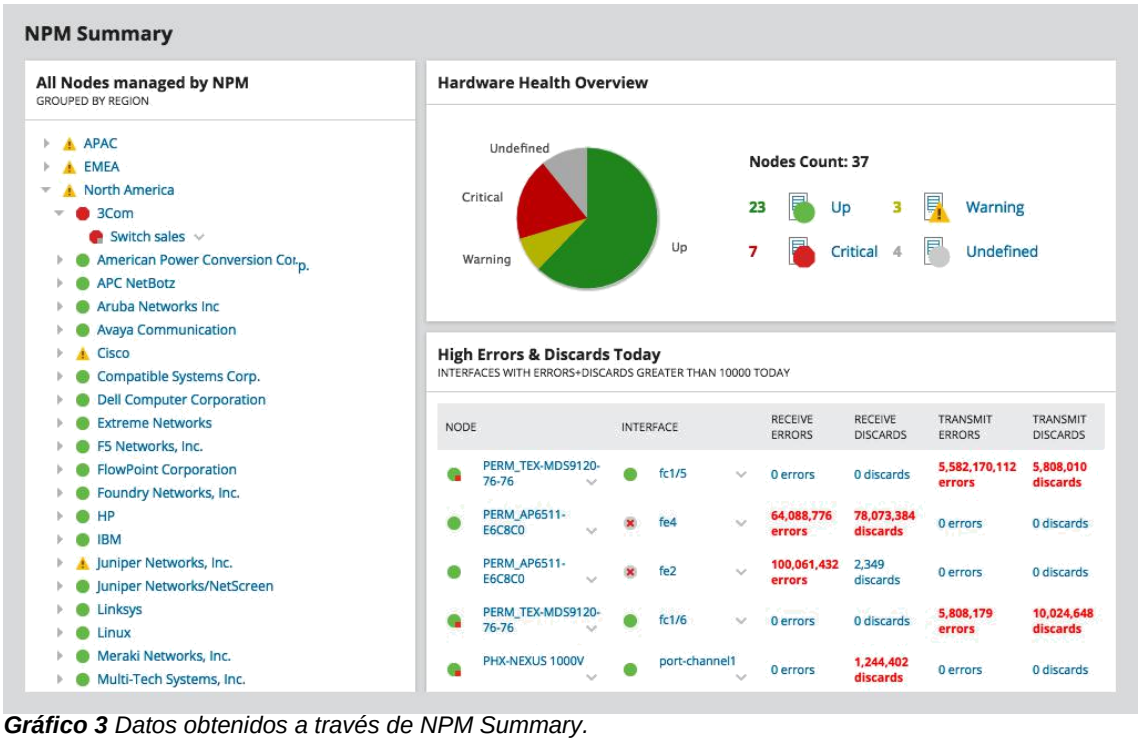

Gráfico 3 *Datos obtenidos a través de NPM Summary.*
Fuente: El Autor.

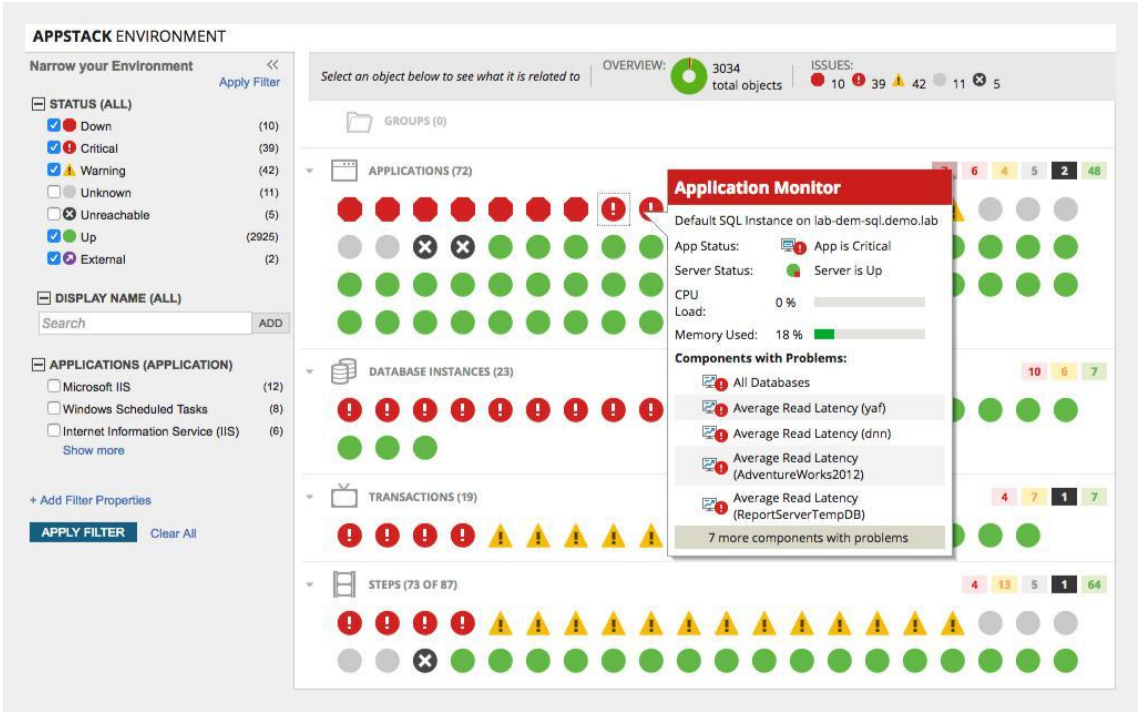

Gráfico 4 *Amenazas y vulnerabilidades que afectan a la seguridad informática de la red de la Gobernación de Los Ríos.*
Fuente: El Autor.

De acuerdo con las gráficas anteriores se observan incidencias al interior de la red informática, las mismas que se basan en la detección de conexiones maliciosas a causa de la presencia de virus informáticos los cuales han detectado que la mayoría de los puertos de comunicación se encuentran desprotegidos; afectando de forma critica las comunicaciones entre los usuarios debido a la ocupación de la memoria principal del equipo.

También se observan que las comunicaciones externas se ven colapsadas en determinados instantes de la jornada laboral, en consecuencia, se evidencia a través de la herramienta de monitoreo que las aplicaciones maliciosas hacen uso de todo el canal principal; lo cual provoca una saturación en el ancho de banda de subida y de bajada, dejando sin tiempo de respuesta a la institución.

En contraparte se hace uso de una herramienta complementaria cuya única misión es detectar y controlar las comunicaciones internas y externas a fin de evidenciar el uso real del ancho de banda “se define al ancho de banda como la conexión establecida hacia el internet desde el equipo instalado al usuario final, mediante el cual se configura el mínimo y el máximo del tráfico total de voz, datos y video que el usuario puede consumir en un tiempo determinado ya sea en una red de área local o en una red de uso personal” (Cisco A. , 2017)

Para la demostración de lo antes mencionado se representa las conexiones comprometidas en estado de criticidad a través de la herramienta WhatsUP Gold del fabricante IPSWITCH y el PRTG del fabricante PAESSLER, ver los gráficos 4, 5 y 6.

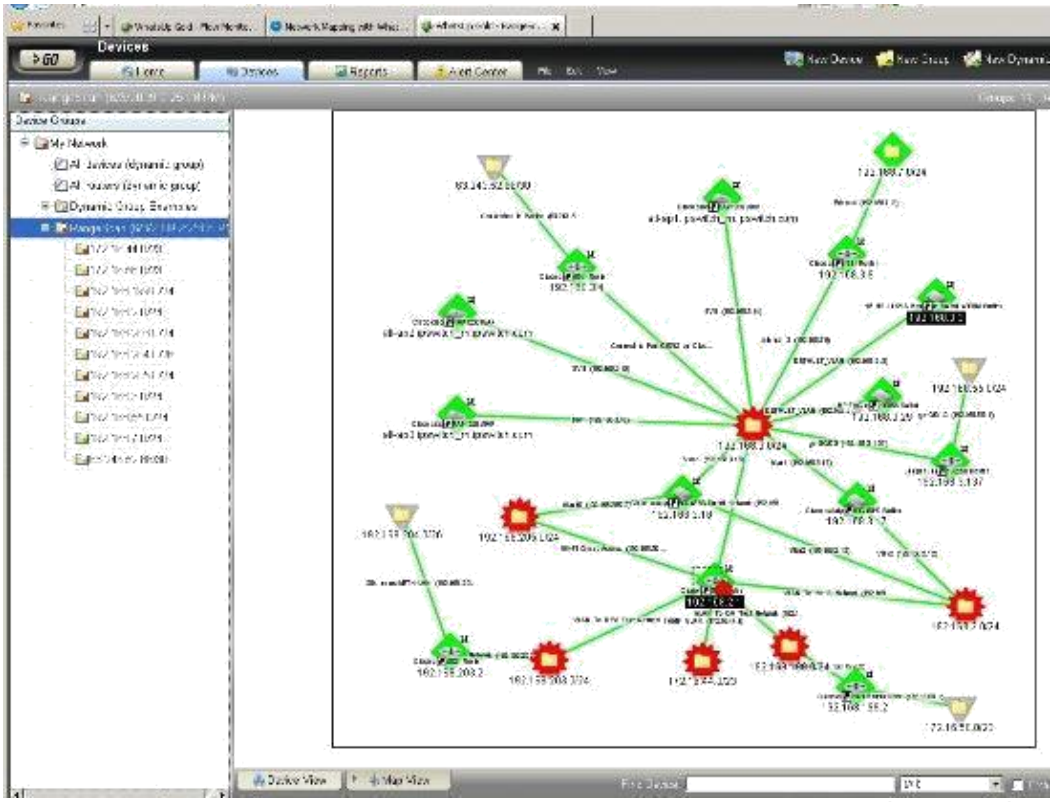

Gráfico 5 *Esquema de conexiones entrantes y salientes en la red de datos de la Gobernación de Los Ríos.*
Fuente: El Autor.

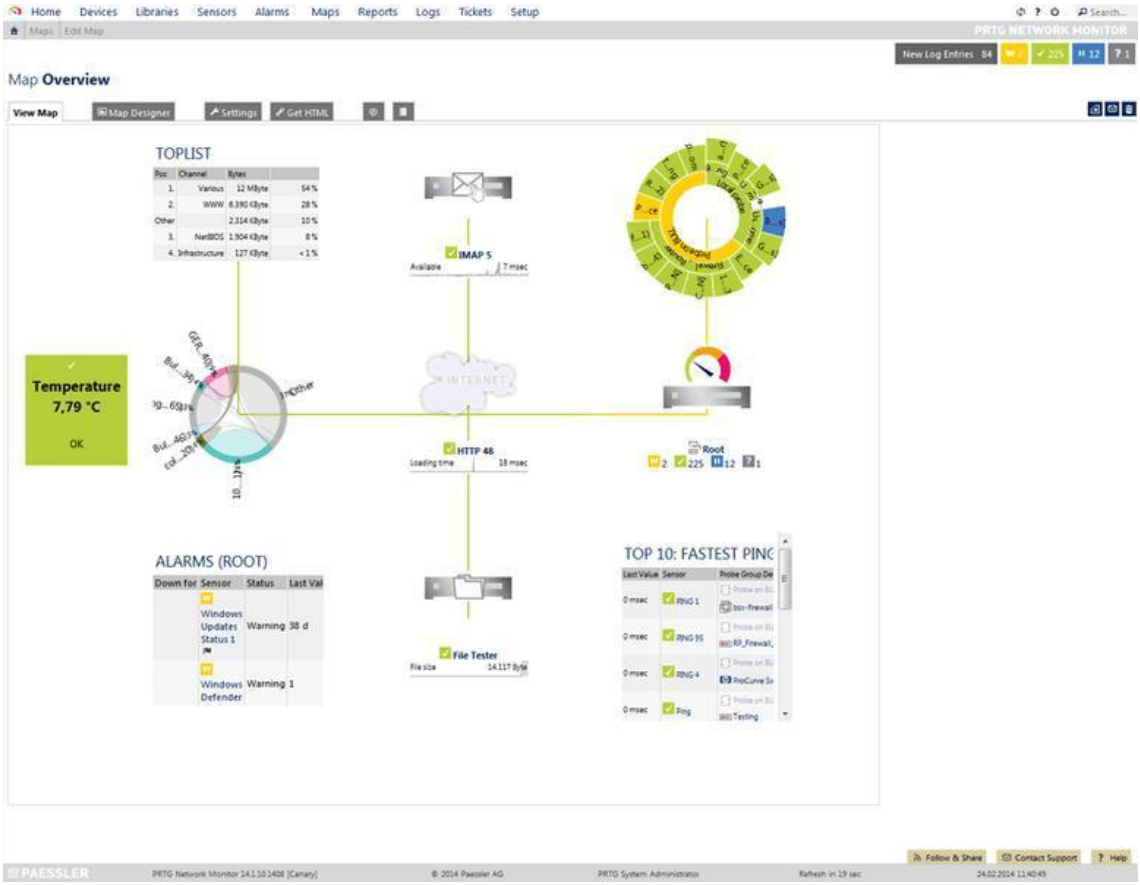

Gráfico 6 *Mapa de incidencia de la red, conexiones entrantes y salientes, Uso del monitor de comunicaciones PRTG.*
Fuente: El Autor.

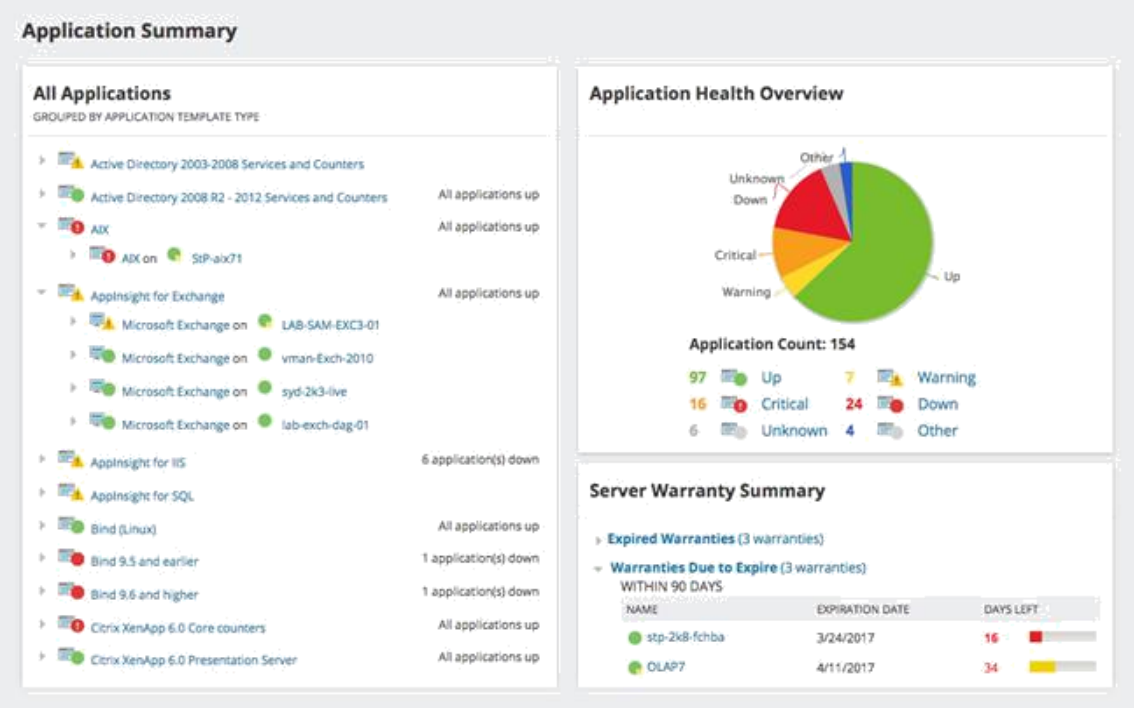

Gráfico 7 *Monitoreo de amenazas y vulnerabilidades en la red de datos de la Gobernación de Los Ríos.*
Fuente: El Autor.

Según las evidencias recopiladas a través de las diferentes herramientas instaladas en la red de datos de la Gobernación de Los Ríos, se determina que el 83% de la red se encuentra afectada por la presencia de Malwares, Adwares, Crackers, Trojan Horse y Ransomware; el 17% restante se encuentra afectado por la desactualización de los sistemas operativos y aplicaciones de ofimática instaladas en los equipos.

Al referirse a la presencia de Malwares, Adwares, Crackers, Trojan Horse y Ransomware se define que “son amenazas informáticas o software hostil cuya única función es infiltrase a los niveles más profundos del sistema operativo y desde ahí iniciar un evento en cadena en el cual se modifican los archivos y librerías nativas del sistema base con el objetivo de desestabilizar la plataforma y entorpecer los procesos dentro del computador para luego distribuirse de forma automática por la red de datos en ausencia de un sistema de protección tal como lo indica Ana Muñoz en el libro de seguridades en ambientes hostiles” (Muñez, 2017).

Por tal razón para determinar el nivel de impacto en el análisis de la seguridad informática de la red de la Gobernación de la Provincia de los Ríos se complementa con el analizador de tráfico y comunicaciones a nivel de protocolos como es el Wireshark; Wireshark se puede definir que es el analizador de protocolo de red más importante y ampliamente utilizado en todo el mundo.

En términos generales es una herramienta que “permite visualizar lo que está sucediendo en el interior de la red a un nivel microscópico y es el estándar de facto en la mayoría de los escenarios de trabajo, cabe indicar que esta herramienta es sin fines de lucro y por lo tanto es considerado el analizador de protocolos con la capacidad de determinar, analizar y solucionar los problemas que se lleguen a suscitar en una red informática, es así como lo define Geral Combs en su libro sobre Wireshark más que una herramienta de monitoreo (Combs, 2016).

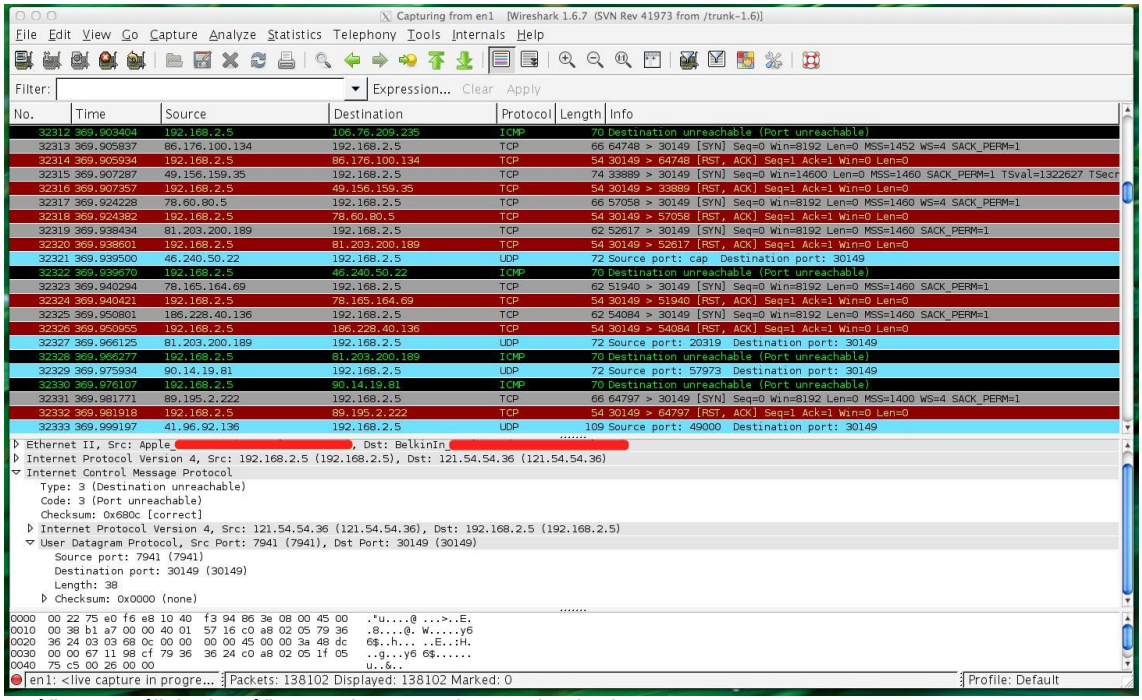

Gráfico 8 Análisis de tráfico con la Herramienta Wireshark.
Fuente: El Autor.

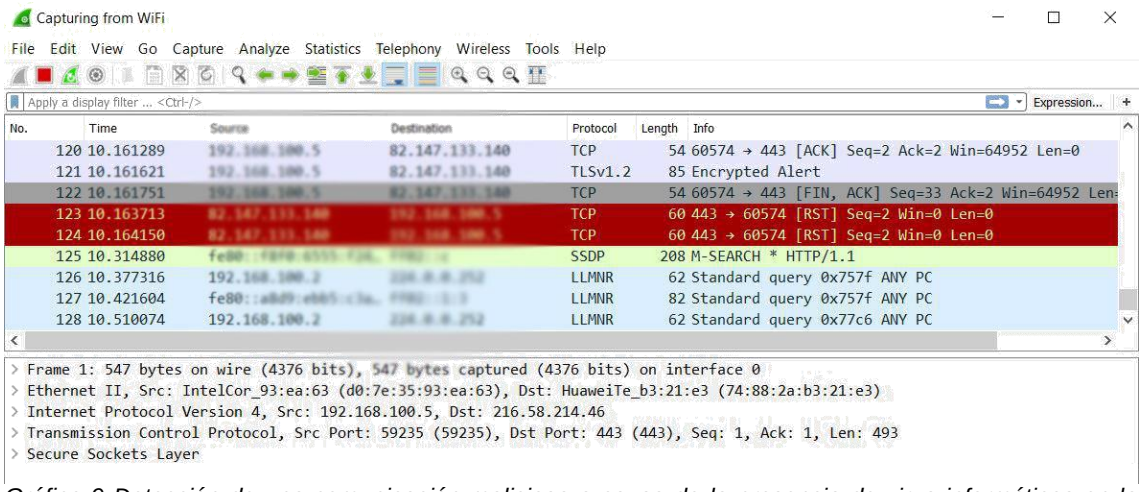

Gráfico 9 Detección de una comunicación maliciosa a causa de la presencia de virus informáticos en la red de datos.
Fuente: El Autor.

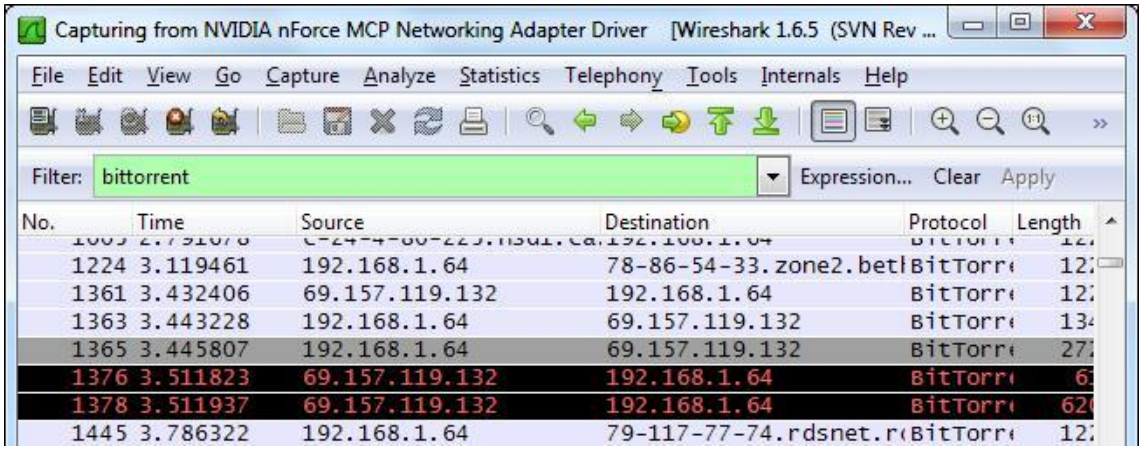

Gráfico 10 Análisis de tráfico, detección de comunicaciones no permitidas, la presencia de Software P2P como Bittorrent causan saturación en el ancho de banda de la red institucional y provocan latencia en el servicio de internet de la Gobernación de los Ríos.
Fuente: El Autor.

De acuerdo con las gráficas anteriores se observa que en el análisis efectuado a la seguridad informática de la red anfitriona, existen comunicaciones no controladas las cuales a su vez causan trastornos en los servicios locales, existe saturación en el servidor principal en la Gobernación de los Ríos, saturación en los procesos ejecutados en memoria principal de la mayor parte de los equipos de cómputo de la entidad, el dominio local no cuenta con las directivas que permitan regular las instalaciones de aplicaciones de terceros o en su defecto de aplicaciones de dudosa procedencia.

El procedimiento adecuado para la presente investigación se basa en la dotación de un sistema de control perimetral basado en Sistema Operativo Open Source Linux, con Distribución CentOS 7 de 64 Bits, se potencializa una solución informática con una suite multipropósito la cual va enmarcada en el aprovisionamiento de seguridad perimetral con servicios de enrutamiento, segmentación y cifrado de información a nivel de protocolos de comunicación.

CONCLUSIÓN

Para lograr obtener un correcto análisis de la seguridad informática de la red de la Gobernación de la Provincia de Los Ríos se utilizó como metodología de trabajo el estándar ISO/IEC 27001 de la cual se desprende la matriz de Open Security Testing Metodología Manual (OSSTMM); para el efecto fue necesario contar con la presencia del profesional responsable del área de Tecnologías de la Información y Comunicación de la entidad, cabe indicar que los datos obtenidos fueron tratados en su momento con el jefe de TIC con el objetivo de colaborar con un criterio más elaborado desde el punto de vista externo a los hechos.

La implementación de políticas de seguridad informáticas en la Gobernación de la Provincia de Los Ríos es una solución integral que asegura la protección y preservación de la información administrada en toda la entidad; con ello se proporciona un método de prevención y control de daños e incidencias que afecte al correcto desempeño de la red de datos y demás equipos activos directamente conectados a la red.

Se considera necesario que las personas encargadas del área de TIC reciban la respectiva capacitación sobre todo lo concerniente a seguridad informática de tal forma que se logre aplicar el conocimiento en las diferentes actividades que encierran las fortalezas y debilidades en cuanto a la protección requerida por la Gobernación de la Provincia de Los Ríos.

La implementación de una solución de bajo costo la misma que está totalmente integrada y orientada al control, prevención y regulación de los entornos de red de datos; cuya misión y función es la de rechazar conexiones a servicios comprometidos o de extraña procedencia, permitir solo el tráfico establecido como correos institucionales, sitios de confianzas y demás aplicaciones o herramientas que se crean de uso oficial o laboral, proporcionar un único punto de acceso externo, dirigir el tráfico entrante y saliente a través de los servicios de la intranet o SharePoint, ocultar sistemas o servicios vulnerables de la red, auditar el tráfico entrante y saliente con énfasis a la protección de ataques de negación de servicios, ocultar la información como nombres de los equipos, topología de la red, tipos de dispositivo, cuentas de usuarios internos a través del servidor de dominio de la Gobernación de la Provincia de Los Ríos.

La solución para todo lo antes expuesto debe estar complementada sobre Sistema Operativo Linux Distribución CentOS 7 de 64 bits en la cual se deberá instalar una solución informática de tipo Unified Threat Management (UTM); lo cual quiere decir que el computador donde se instale la solución se convertirá de forma inmediata en un Router Administrable con funciones integrada de Firewall y Proxy, IDS e IPS; al referir el termino IDS e IPS se destaca la intensión de establecer un sistema de protección basado en detección de intrusos mediante el uso de programas de código abierto para la detección de accesos no autorizados tal como se indica en el anexo 1.

BIBLIOGRAFÍA

Lockhart, A. (2016). Security in Data Networks. *Stanford University*, 28-32.

Fagioni, S. (2016). Seguridad y Modelos de Encriptación. *Universidada de Belgrano*, 44-46.

Esquiezabal, M. M. (2017). Análisis Críticos. *Universidad de Valladolid*, 31-34. Barzola, M. (2014). Modelos de Control en la Seguridad Informática. *Gupo Santander Latinoamérica*, 54-57.

Manjarrez, J. c. (2015). Control y Análisis Informático a la Seguridad de los Datos en Tránsito. *Cisco Security*, 12-17.

Bustos, M. (2016). Seguridad y Amenazas en ambientes controlados. *Chile Seguridad*, 12-14.

Annan, K. (2014). Seguridad, Acceso e Información Libre. *Cumbre de La Naciones Unidas*, 23-29.

Trevor, R. S. (2015). Open Source Security Testing Methology Manual. *Security Method and Analitic*, 32-38.

Arizábal, C. (2016). Métodos y Herramientas de Monitoreo. *Cisco Security*, 32-41.

Combs, G. (2016). Wireshark, más que una herramienta de monitoreo. *Ciencia y Tecnoligía*, 31.

Lockhart, A. (2016). Seguridad de Redes, Los Mejores Trucos. *ANAYA*.

Lockhart, A. (2016). Open Source as a Security Method in a LAN Network. *Open Source Security*, 35-37.

Erb, M. (2014). Gestión de Riesgo en La Seguridad Informática. *Creative Commons* , 21.

Micrsoft. (2016). Tu intranet móvil e inteligente. *Microsoft*, 13.

Lockhart, A. (2016). Security and computer analysis. *Informatic Security*, 35.

Cisco. (2017). Seguridad Informática 4ta Edición. *Cisco Security*, 21.

Criamer, S. (2017). La Capa de Core como un Modelo de Enlace. *Cisco*, 2-3.

Llagua, A. (2016). Direccionamiento y Segmentación de Red. *Perú Tecnológico*, 26-27.

Cisco, A. (2017). Service Quality Configuration. *Cisco Academy*, 4-6.

Muñez, A. (2017). Seguridades en Ambientes Hostiles. *Computer Hoy*, 12.

ANEXOS

Figura 1 Edificio de la Gobernación de la Provincia de Los Ríos.

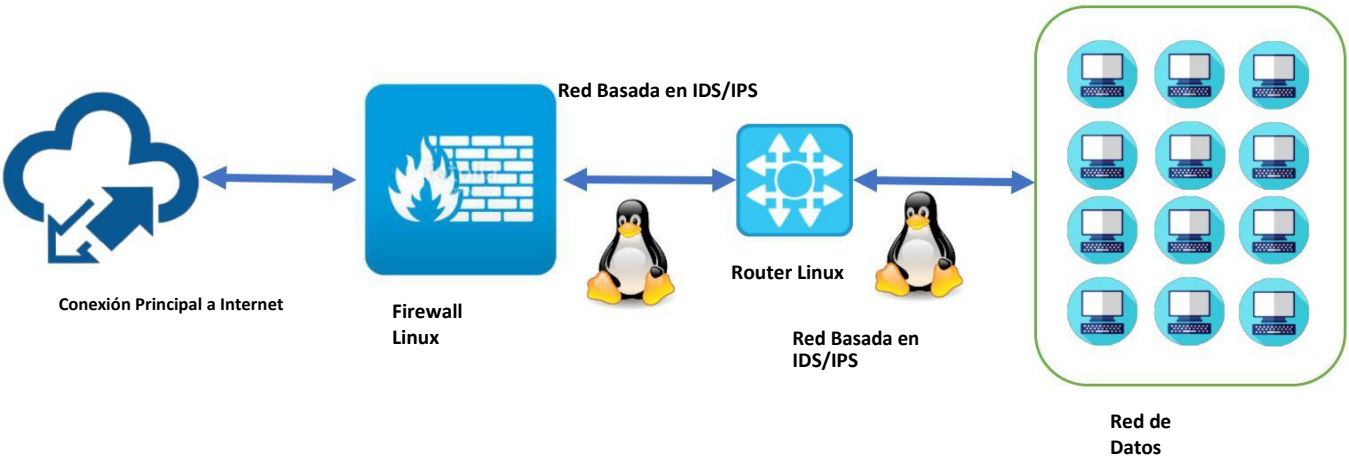

Figura 2 Solución UTM basado en Linux como método de seguridad para la red de datos de la Gobernación de la Provincia de Los Ríos.
Fuente: EL Autor