UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio De La Infraestructura De Red Informática De La Subzona De Los Ríos, Comando Babahoyo.

EGRESADA:

Diana Mabel Alvarado Carrasco

TUTOR:

Ing. Hugo Guerrero Torres, MGRT.

AÑO 2018

INTRODUCCIÓN

La infraestructura de red es el mecanismo compuesto por diversos elementos y equipos activos que cumplen el propósito de establecer el medio de transmisión y comunicación para de esta forma garantizar el correcto traslado de la información de un extremo a otro sin importar cuan lejano este el punto de destino al que deben arribar los datos; de esta premisa nace lo que hoy en día se conoce como *Tecnología de la información (IT)* que a su vez es una rama que se encuentra totalmente intrínseca en todo lo referente al Networking (*Concepto que revoluciona y reinventa todo lo que se conoce a través de la implementación de aplicaciones y plataformas orientadas a la nube con una estrategia de integración* "*Voz, Datos y Video*").

Sin embargo esto no es un término nuevo ni exclusivo de la era digital; todo lo contrario, el Networking nace del comportamiento del ser humano en el instante en que siente la necesidad de mejorar sus habilidades y destrezas y producto de ello sufre cambios y modificaciones desde el punto de vista social, económico, cultural y psicológico; es así que el mismo comportamiento se observa en las redes de datos ya que cada equipo informático constituye un nodo (*punto de intersección, unión de varios elementos que convergen en un mismo lugar*) con un alto grado de valor dentro de los parámetros de ponderación el cual es controlado por el administrador de la red.

Debido a este criterio anteriormente detallado, se pretende realizar un estudio de la infraestructura de red informática del comando policial de la Provincia de los Ríos acantonado en la ciudad de Babahoyo, para ello se elabora un caso de estudio en el cual

se apliquen los conocimientos necesarios a fin de determinar y sugerir las directrices que permitan mejorar el funcionamiento y rendimiento de la red objeto de estudio.

Es así que mediante el método de la observación directa se evidencia de manera enfática múltiples deficiencias en la infraestructura de la red informática del comando policial, se demuestran las continuas caídas del servicio de internet sin que haya mayor tipo de explicación, las comunicaciones internas colapsan en determinados instantes del día y no se han tomado en cuenta los conceptos básicos para la implementación de un sistema de cableado estructurado, no obstante se evidencia que no existen registros o un ente controlador del domino interno de la red, de tal forma que todos los equipos se encuentra directamente conectados al mundo sin ningún tipo de protección contra posibles intrusiones.

Por lo anteriormente expuesto y en base a los lineamientos mandatorios de lo que dictamina la *Tecnología de la Información (IT) "Planear, organizar, difundir, evaluar y vigilar el desarrollo de la actividad en lo referente al uso de tecnologías de la información y comunicaciones conforme a las necesidades institucionales y en cumplimiento de los programas y políticas aprobadas; así mismo, promoverá el aprovechamiento de las nuevas tendencias en tecnologías"*; se decide realizar a través del desarrollo de esta investigación el aporte de una guía que indique como se resolverán los problemas actuales mediante el respectivo estudio en el que se cree prudente se enmarque los aspecto más relevantes y técnicos con relación a la problemática (*Diseño de red mediante capas, sistema de cableado estructurado orientado a una red de servicios, equipos activos orientados al control interno y*

perimetral de la red de datos, y la definición de los protocolos adecuados a fin de evitar futuras caídas del servicio de red en general).

DESARROLLO

Esta investigación se ambienta en las instalaciones de la sub zona del comando policial de la Provincia de Los Ríos en la ciudad de Babahoyo; se realiza un estudio de su infraestructura de datos y a la vez se pretende realizar un esbozo de un modelo práctico para la administración de todos los recursos informáticos del comando policial.

Este modelo se refuerza en la estrategia de 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 (observación directa y descriptiva), se verifica que las instalaciones del comando policial no prestan las adecuaciones necesarias para el normal despliegue de una red da datos, ya que la estructura del edificio obedece a un modelo de construcción con una antigüedad que supera los 40 años.

Para el caso de la investigación mediante la observación directa, se procede a la visita técnica y de forma guiada por toda la instalación a fin de identificar de manera visual y posterior constatación del estado mediante pruebas inmediatas de funcionamiento y estado de error a través del uso del protocolo *Address Resolution Protoco (ARP)* y *Simple Network Management Protocol (SNMP),* ambos proporcionan las herramientas para el respectivo diagnóstico de las comunicaciones internas de la red.

Para el caso de la investigación por medio de la observación descriptiva se procede a partir del diagnóstico obtenido en el proceso de observación directa; esta información permite tener una visión más amplia del comportamiento del objeto de estudio mediante el registro de las incidencias en formato no mecanizado.

Adicionalmente se establece a través de una matriz de información elaborada especialmente para la especificación el 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 este propósito se toma en cuenta el criterio definido por Gaston Toth quien es Licenciado en Ciencias de la Computación y especialista en metodologías, guías y normas existentes relacionadas con la Seguridad de la Información. (Toth, 2014).

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

Tabla 1 *Criterios para la recopilación de datos y realización del estudio.*

Autora: Diana Alvarado

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.

Tabla 2 *Definición e interpretación de los resultados según la matriz informativa.*

Autora: Diana Alvarado

Es así como con la ayuda de la matriz informativa se logra evidenciar los detalles técnicos y todos los pormenores que en la actualidad aquejan al rendimiento de la red de datos del comando policial.

De acuerdo con las tablas anteriores se define un estudio basado en la recopilación de información a partir de una serie de criterios contenidos en la aplicación del estándar *IT Incident Management Help Desk SLA;* lo cual colabora en la detección de las amenazas y vulnerabilidades de la infraestructura de red del comando policial.

Por tal razón a continuación se demuestra los datos obtenidos con relación al estudio realizado:

`					SENSIBILIDAD DE LOS ACTIVOS					
PROCESO	ACTIVO	PROPIETARIO	UBICACIÓN	CLASIFICACIÓN	C	I	D	TOTAL1	VALOR1	VALOR2
1	20	Eset	Bby	URG	5	10	10	25	Alto	3
1	20	Microsoft	Bby	URG	0	3	10	13	Alto	3
2	20	CNT	Bby	URG	1	10	10	21	Alto	3
2	20	Comando Policial	Bby	URG	2	10	10	22	Alto	3
3	20	Comando Policial	Bby	URG	3	10	10	23	Alto	3
3	20	Comando Policial	Bby	URG	4	10	10	24	Alto	3
3	20	Comando Policial	Bby	URG	5	10	10	25	Alto	3
2	20	Comando Policial	Bby	URG	1	10	10	21	Alto	3
2	20	Comando Policial	Bby	URG	4	10	10	24	Alto	3
2	20	Comando Policial	Bby	URG	6	10	10	26	Alto	3
2	20	Comando Policial	Bby	URG	3	10	10	23	Alto	3
2	20	Comando Policial	Bby	URG	4	10	10	24	Alto	3
2	20	Comando Policial	Bby	URG	7	10	10	27	Alto	3
1	20	Comando Policial	Bby	URG	2	10	10	22	Alto	3
1	20	Comando Policial	Bby	URG	9	10	10	29	Alto	3
3	20	Comando Policial	Bby	URG	1	10	10	21	Alto	3
3	20	Comando Policial	Bby	URG	8	10	10	28	Alto	3

Tabla 3 *Matriz de riesgo*

Autora: Diana Alvarado

A través de esta matriz se puede identificar el impacto causado en toda la infraestructura de red del citado lugar, también se logra identificar las carencias y vulnerabilidades informáticas en el ámbito de la seguridad, así como la distribución e integridad de los equipos que forman parte activa de la red.

Con este indicio se busca el fortalecimiento de la plataforma tecnológica por medio del siguiente análisis sobre las condiciones en las que operan los sistemas de comunicaciones, red de navegación, red telefónica y demás elementos que forman parte del sistema informático de la sub zona; tanto así que los valores trascendentales en las diferentes lecturas coinciden con lo expresado por el premio Nobel de la Paz, el señor

Kofin Annan, que durante la fase de investigación e interpretación son muy claros los acontecimientos y dejan expuestos que los niveles de intrusión y tiempos de caída del servicio en general son muy altos. (Kofi, 2013).

ESTADO ACTUAL DE LA RED DE DATOS E INFRAESTRUCTURA

Para la identificación y visualización del estado actual de la red de datos e infraestructura de comunicaciones se emplea el método de OSSTMM (*Manual de la Metodología Abierta de Testeo de Seguridad*) este proceso permite obtener de forma concreta el análisis de los niveles de seguridad de la información; con esto se verifica la seguridad operativa, así como los canales de comunicación entre los distintos usuarios de la red como lo explica la siguiente tabla.

ÁMBITO DE OSSTMM				
Seguridad Física		**Seguridad de Espectro**	**Seguridad de Comunicaciones**	
Humano	***Físico***	***Comunicaciones inalámbricas***	***Telecomunicaciones***	***Redes de Datos***
Comprende todos los integrantes humanos que intervienen diariamente en la red de comunicación.	*Comprende todos los elementos tangibles que aportan con seguridad en el interior y exterior de la red de comunicaciones.*	*Comprenden todas las comunicaciones electrónicas, y todo tipo de propagación de señales radio eléctricas a través del radio espectro.*	*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.*

Tabla 4 *Ámbitos de OSSTMM, definición de las áreas de estudio según su impacto en la red de datos e infraestructura.*

Fuente: Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM, adaptado de la versión original al propósito de esta investigación.

Los resultados en base a la evaluación efectuada al talento humano se orientan en su mayor parte a los niveles de acceso y relación de confianza que se proporciona en la seguridad de la información; para este fin se aplican las pruebas de observación

directa y al mismo tiempo el uso de los conceptos básicos de ingeniería social, obteniendo posteriormente información vital que compromete de una u otra forma la integridad de la información del comando policial.

Entre los resultados obtenidos se reflejan las falencias en la seguridad operacional, en el uso y mantenimiento de los equipos informáticos, tal como lo indica Juan Gómez, quien se destaca por ser especialista en sistemas de seguridad y control de intrusiones; en el mantenimiento de los equipos de comunicación, en el tendido del medio de comunicación, de igual forma se toma en cuenta la carencia de políticas y procedimientos para una posible evaluación de resultados en el comportamiento de la infraestructura de red informática. (Gómez, 2015)

Los controles y mecanismos de seguridad que se encuentran en funcionamiento, de cierta forma remedian y protegen en algo el estado del sistema de comunicaciones, aunque no en su totalidad, la mayor prioridad la tienen los procesos manuales y mecanizados llevados a cabo en el área financiera y no se le da el interés adecuado al área de tecnologías del comando policial.

La Academia Cisco define que con relación al canal físico la evaluación efectuada se enfoca al nivel de acceso al cuarto de equipos y a la disponibilidad de los diferentes equipos de interconexión interno-externo a la red de datos, el tiempo de respuesta a las múltiples incidencias y eventualidades del sistema frente a posibles intrusiones maliciosas y negaciones de servicios. (Academy Cisco Networking, 2014)

Los resultados se demuestran a través de ilustraciones, las mismas que son producto de la tabulación de los datos obtenidos según los parámetros definidos para la toma de muestras en el escenario de investigación.

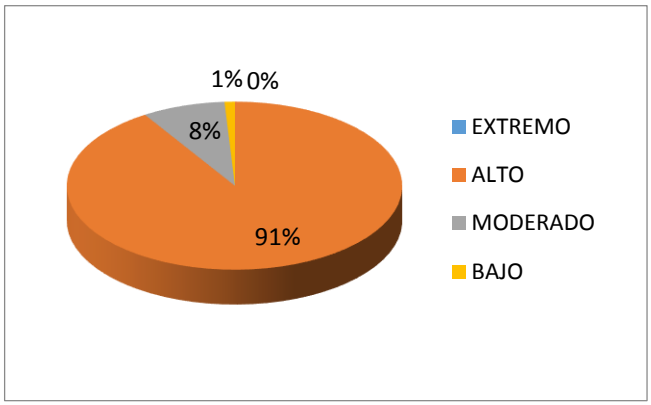


Gráfico 1 Riesgo Residual en la Infraestructura del comando policial
Autora: Diana Alvarado

En la gráfica anterior se observa los niveles alarmantes con relación al riesgo en forma residual a toda la infraestructura de red del comando policial de la sub zona de la Provincia de los Ríos, esto se da como producto a la mala gestión de los recursos y en la forma como se administran los diferentes insumos para el trabajo diario en la red de datos, el 91% representa le nivel de intrusiones y ataques detectados luego de haberse implementado una política de control de infecciones por código malicioso, incidencias por Adware, Malware, Trojan Horse, Ransomware y demás características propias de un ataque de virus en grado 1, 2 y 3. (M.S., 2014)

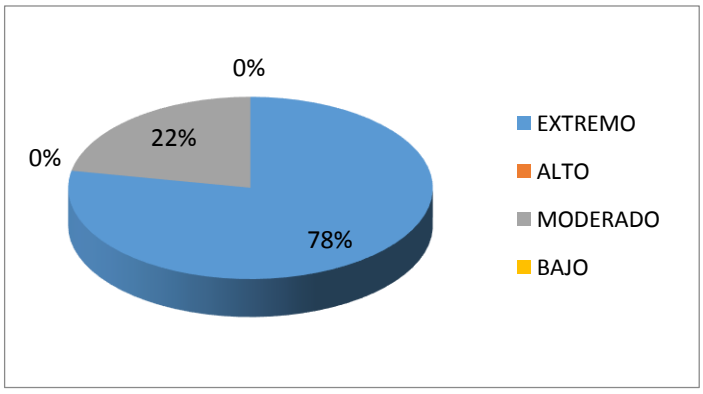


Gráfico 2 Riesgo Inherente, potenciales niveles de ataques a la infraestructura del comando policial
Autora: Diana Alvarado

Con relación a este punto se logra describir que el 78% representa la presencia de amenazas y causas producidas por la carencia de elementos de control interno, la falta de seguridad perimetral es un factor clave en el elevado porcentaje de riesgo en toda la infraestructura, dejando totalmente vulnerables todos los equipos que se encuentran directamente conectados a la red de datos.

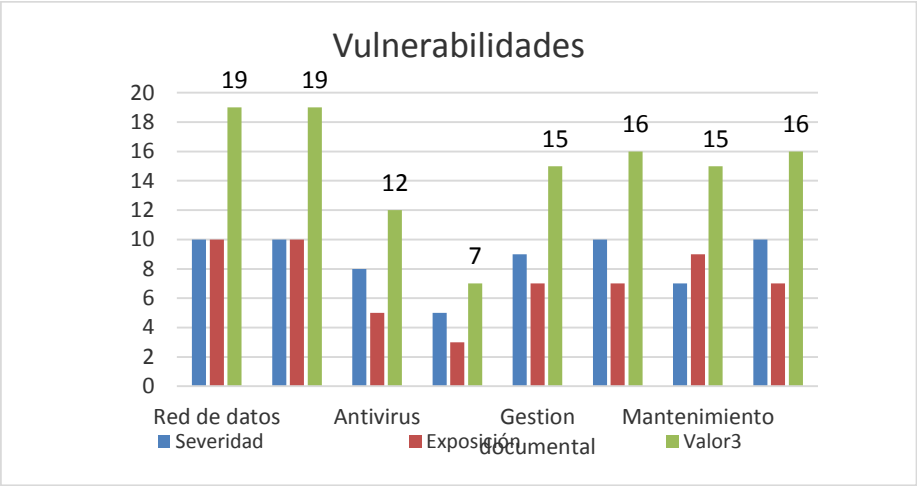


Gráfico 3 *Vulnerabilidades detectadas en la Infraestructura del comando policial.*
Autora: Diana Alvarado

En el grafico 3 se define mediante la esquematización por columnas cuales son los niveles de incidencias en la red de datos a nivel de infraestructura de comunicación, Luis Fernando Acevedo, especialista en control de intrusiones de código malicioso afirma que las vulnerabilidades creadas a raíz de contar con un sistema de antivirus que no cumplen los requisitos mínimos para una correcta defensa de las amenazas que provienen del internet, la gestión documental no se encuentra centralizada; a su vez es administrada de forma distribuida en cada equipos conectado a la red y como respaldo se hace la extracción por medio de memorias USB las mismas que a menudo se infectan por la promiscuidad entre las conexiones con los demás equipos informáticos de la red anfitriona o equipos ajenos a la red. (Acevedo, 2016)

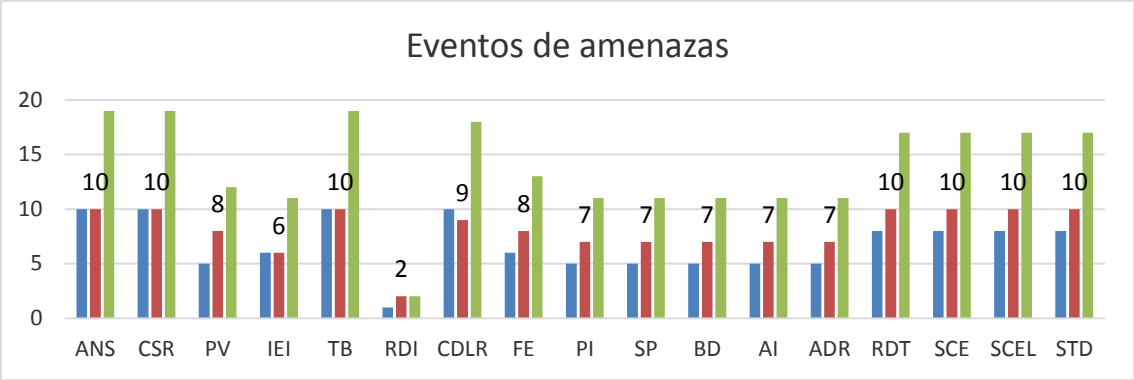


Gráfico 4 *Amenazas detectadas a partir de incidencias registradas en la red de datos*
Autora: Diana Alvarado

En la gráfica 4 se demuestra los niveles de amenazas tan solo en un día de verificación de eventualidades en el comando policial de Babahoyo, de tal forma que los valores en un reporte semanal, mensual o anual son verdaderamente abrumadores.

Un reconocido especialista en control de ataques por suplantación de identidad como lo es el señor Thomas Demuth, indica de forma categórica que las limitaciones se ponderan de manera individual, luego se las relaciona directamente con su causa y se elabora una matriz de seguimiento de tal forma que este proceso permite la identificación de cualquier anomalía o cambio en el comportamiento de la infraestructura de red del comando policial, posteriormente se procede con el respectivo cálculo de limitaciones del recinto y de la red objeto de estudio y de esta manera se logra obtener el estado real y actual de la infraestructura en términos generales y específicos. (Thomas Demuth, 2014)

MODELO DE SEGURIDAD

Dentro de lo abarcado en este estudio realizado a la infraestructura de red del comando policial de la sub zona de la Provincia de los Ríos, se esboza un diseño de un

sistema de defensa basado en redes definidas por software y a su vez con rutinas de control basadas en la norma ISO/IEC 27001:2013 (*Information technology - Security techniques - Information security management systems Requirements*), esta norma es la que indica cómo gestionar la seguridad de la información en su última revisión en el 2013.

Se define un modelo de defensa para los niveles en los cuales actúan los usuarios de la red de voz, dato y video a través de una segmentación de funciones con técnicas conocidas como IDS, IPS, Firewall, Proxy, Routing y Switching en ambiente de código abierto sobre plataforma de comunicaciones Linux. **Ver Anexo 1.**

Juan Rodrigo Paredes, reconocido investigador en el área de programación en redes y seguridad de la información en este sentido coincide con lo siguiente; se logrará educar a los usuarios de la red mediante las normas y procedimientos como base en el primer nivel de seguridad del modelo que se propone para apalear la situación actual de la infraestructura; en segunda instancia se obtendrá la adecuada gestión y la prioridad necesaria a la gestión de la información y la minimización de los niveles de riesgo de la seguridad de la información y por último se agregará una estructura vertical para la administración de los recursos así como el acceso a la información. (Paredes, 2013):

- Política de seguridad.
- Organización documental y acceso a la información.
- Gestión de los equipos informáticos.
- Seguridad y recurso humano.
- Seguridad física del entorno.
- Gestión de comunicaciones y operaciones.

- Control de acceso
- Adquisición, desarrollo y mantenimiento de equipos y sistemas informáticos.
- Gestión, monitoreo y activación del sistema de incidentes en la seguridad de la información.

DEFENSA PERIMETRAL

Para la defensa perimetral se describen las características y funciones del software ideal para que cumpla con la función de mantener totalmente cubierta la red de voz, datos y video de cualquier amenaza interna o externa a la infraestructura; de esta forma el especialista en Tecnología de la Información, Técnicas de la Seguridad y Código de Práctica para la Gestión de la Seguridad de la Información Rodrigo Aranza Watter introduce el concepto y utilización de los mecanismos IDS/IPS sobre software libre definiendo su comportamiento de acuerdo con las configuraciones establecidas en la estructura de la red de datos. (Watter, 2014)

Un profesional de la seguridad informática como lo es Andrew Tompson quien basado en su propia experiencia indica que para minimizar aún más el riesgo de infección o ataque a los equipos primarios de la red se contempla la adición de una *zona desmilitarizada (DMZ)* con el objetivo de proveer un mayor servicio en cuanto a las conexiones entre los distintos equipos hacia la red interna y conexiones externas. (Tompson, 2013)

Al hablar de *Intrusion Detection System (IDS)* como el sistema de *Intrusion Prevention System (IPS),* básicamente se tiene que tomar en cuenta el criterio del profesional más respetado en el ámbito de las redes de computadoras en todo el mundo como lo es el señor Andrew Tanenbaum graduado del *Instituto Tecnologico de Massachusetts (MIT)* quien aborda el uso de soluciones ya sean propietarias o de libre distribución con la salvedad que entre toda la gama de software disponible existen diferencias mínimas y máximas en cuanto a la cobertura que se provee en el monitoreo de intrusiones que pueden llegar a burlar el firewall, pueden llegar a detectar a tiempo o tardíamente los ataques dirigidos a los servidores de datos, permite en forma global o especifica o a su vez no permitir el escaneo de ataques comunes. (Tanembaum, 2013).

Para ello la solución va enmarcada al uso y aplicación de un sistema de defensa y control basado en redes definidas por software sobre plataforma de comunicaciones y operaciones Linux, distribución CentOS 7 de 64 Bits y una Suite de soluciones de alto rendimiento orientadas al análisis, estudio y control de infraestructuras de redes de datos. **Ver Anexo 2.**

MODELO DE RED

Carlos Estrada famoso ingeniero de seguridad de la empresa telefónica España plantea un modelo de tres capas en topología estrella extendida la misma que permitirá que la red sea escalable, confiable y tolerante a errores con tiempos de respuesta totalmente bajos, se prevé la minimización de las incidencias y en su defecto se garantiza alta disponibilidad del medio de transmisión. (Carlos Estrada, 2015).

En base al diseño propuesto López Martínez especialista en Penetración y Testeo en infraestructura de redes describe un comportamiento estable y sin cambios o caídas en las comunicaciones debido a la segmentación de la red; este efecto permite aislar de manera menos invasiva la propagación de malestar en la infraestructura de red del comando policial. (Martinez, 2015).

Juan Carlos Tori especialista en Sistema de defensa y escalamiento por segmentación define que Los usuarios se mantendrán agrupados acorde los recursos que utilizan y a las funciones que desempeñan diariamente mediante la separación lógica de los ambientes y conexiones; este concepto toma el nombre de *Red de Área Local Virtual (Vlan).* (Juan Carlos Tori, 2016).

Y el nivel de comportamiento de la red de dato se mantendrá totalmente controlada en todos los aspectos. **Ver Anexo 3.**

CONCLUSIÓN

Un especialista de Seguridad de la Información como lo es Alfred Bertolin catedrático de Seguridad en redes de datos y sistemas distribuidos para la Universidad de Milano ,evidencia que para la implementación y puesta a punto del sistema de cableado estructurado y demás componentes de la red de datos del comando policial en la mayor parte fue realizada de manera empírica por parte de contratistas y mano de obra no calificada para el objeto de contratación; siguiendo la misma línea de investigación se comprueba que en iguales condiciones se desarrolló la puesta a punto de los equipos informáticos, adecuación de la suite de ofimática, antivirus y demás aditamentos para el trabajo diario de cada dependencia, el sistema telefónico se constata que no cumple con un estándar básico de instalación y despliegue en un edifico de múltiples oficinas. (Bertolin, 2016)

Se realizó un estudio en forma acuciosa a la infraestructura de red informática del comando policial de la sub zona de la Provincia de los Ríos, a través del estudio se evidencia que el estado actual de la infraestructura de red de datos, telefonía y video vigilancia no cumplen con los requisitos mínimos para el normal funcionamiento de un sistema de comunicación institucional, puesto que se evidencia un total descuido en cuanto a la importancia que amerita el sistema de cableado estructurado, el sistema eléctrico, el servicio de internet, el ambiente regulado y controlado de las comunicaciones, las políticas de acceso y control de la información, el sistema de antivirus, la suite de ofimática y demás programas y utilitarios que son necesarios en el desarrollo de las actividades diarias de cada uno de los usuarios activos en la red informática del comando policial.

La institución no posee un ambiente regulado y climatizado para el cuarto de equipos o el cuarto de telecomunicaciones, tal es el caso que los equipos se encuentran agrupados en condiciones no estandarizadas y no recomendables; por consiguiente, se constata que el área en la que se encuentran los dispositivos es compartida con la sala de fisiatría y terapia física. **Ver Anexo 4.**

Adicionalmente es necesario indicar que el estudio realizado ha colaborado para el diseño de seguridad por medio de un modelo multicapas el mismo que se basa en la defensa de cada uno de los segmentos definidos en la configuración de la red informática del comando policial, para ello se procedió con el respectivo levantamiento de la información por medio del Manual de la *Metodología Abierta de Testeo de Seguridad (OSSTMM),* como una metodología practica de penetración en escenarios hostiles para la identificación de riesgos, amenazas y vulnerabilidades en el entorno del objeto de estudio.

Se realizaron pruebas de simulación de tráfico y ataques en base a los objetivos de hacking ético en las diferentes capas de modelo OSI poniendo a prueba el funcionamiento del sistema de IDS/IPS obteniéndose posteriormente los resultados demostrados en el desarrollo de esta investigación.

Se concluye que el comando policial de Babahoyo debe adoptar una política de responsabilidad técnico-social en la cual predomine el objetivo de adecuar, escalar y estabilizar los servicios que se encuentran actualmente en funcionamiento en sus instalaciones así también debe realizar las modificaciones necesarias contenidas en esta

investigación de carácter urgente para así evitar y garantizar que la integridad de la información almacenadas en sus servidores no será blanco fácil de cualquier intrusión o ataque dirigido su infraestructura informática.

BIBLIOGRAFÍA

Academy Cisco Networking. (2014). Exploration 4.0 Comunicaciones, ataques comunes. *CISCO*.

Acevedo, L. F. (2016). Virus y Malware, una amenaza de Internet. *Repositorio Universitario de la DGTIC*, 87-94.

Bertolin. (2016). Seguridad de la Información. *Parainfo*.

Carlos Estrada. (2015). Seguridad por niveles. *España Telecomunicaciones*.

Gómez, J. (2015). Sistema de Detección de Intrusiones. *Seguridad Informática*, 79-81.

Juan Carlos Tori. (2016). Sistemad de defensa y escalamiento por segmentación. *Comuicaciones y Telemática*.

Kofi, A. (2013). *Discurso Inaugural de la Primera Fase de la WSIS. Ginebra. .* Ginebra: WSIS.

M.S., A. (2014). Analisis y Diseño de Sistemas de Información . *OSSTMM*, 38-53.

Martinez, L. (2015). Modelos en defensa, Penetración y testeo. *Editex*.

Paredes, J. R. (2013). Cultura en la Red Informática . *Seguridades en Linea , Internet y Datos*, 23.

Tanembaum. (2013). Redes de Computadoras y Seguridad. *Pearson*.

Thomas Demuth. (2014). ARP Spoofing y Poisoning, TRUCOS DE TRÁFICO. *ACL Security*.

Tompson, A. (2013). DMZ una solución a los problemas de seguridad. *Seguridad en Redes* , 52.

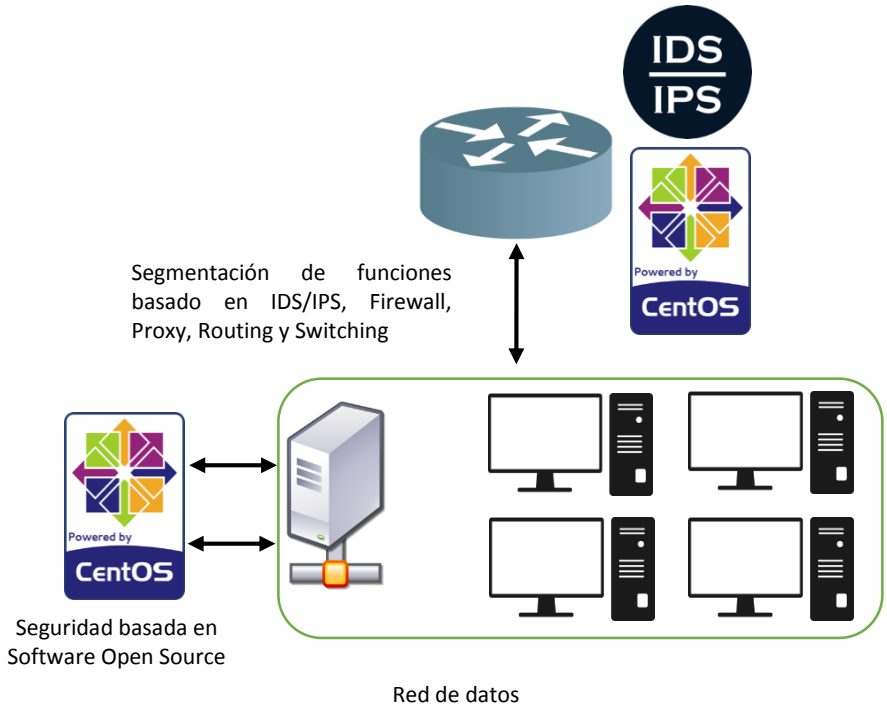
Toth, J. &. (2014). Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM. *Neuquén*, 94-98.

Watter, R. A. (2014). Tecnología de la Información- Técnicasde la Seguridad - Códifo de Práctica para la Gestión de la Seguridad de la Información. *INEN*.

ANEXOS

Anexo 1.

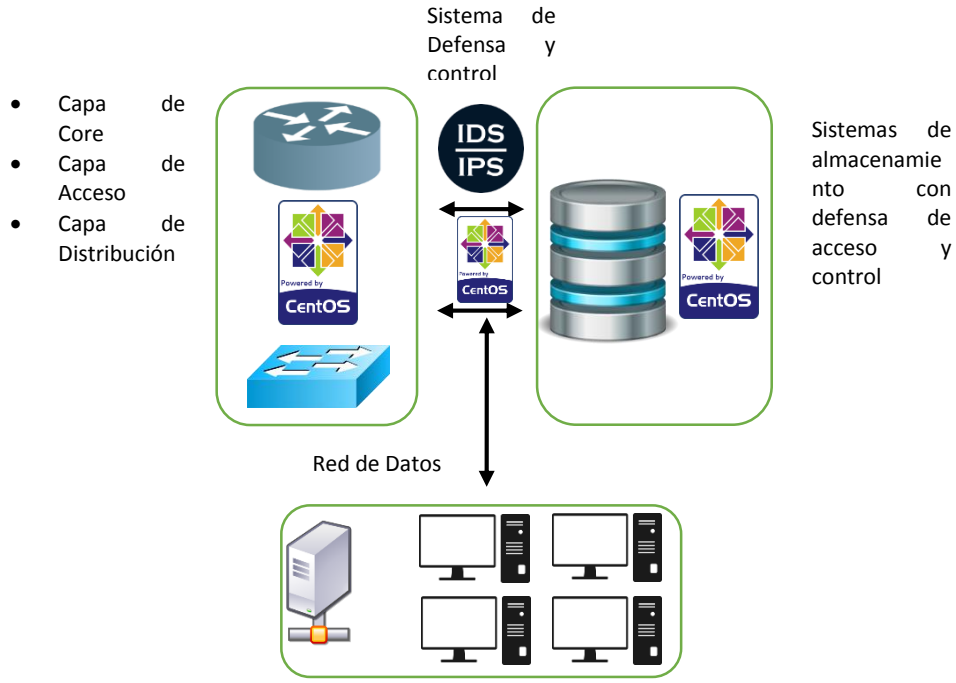
Se define un modelo de defensa para los niveles en los cuales actúan los usuarios de la red de voz, dato y video a través de una segmentación de funciones con técnicas conocidas como IDS, IPS, Firewall, Proxy, Routing y Switching en ambiente de código abierto sobre plataforma de comunicaciones Linux.



Autora: Diana Alvarado

Anexo 2.

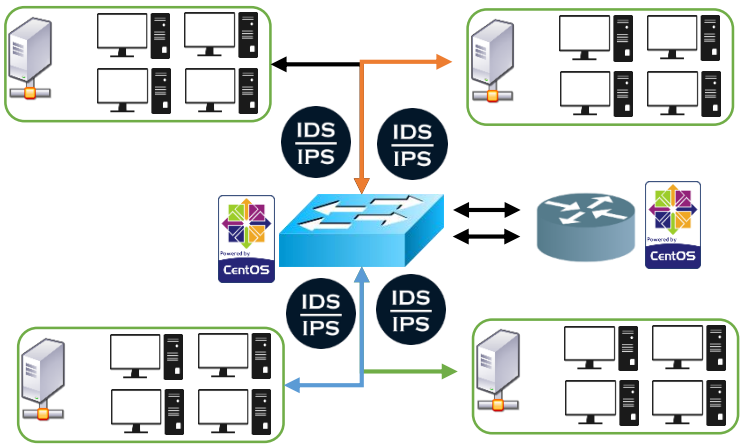
Para ello la solución va enmarcada al uso y aplicación de un sistema de defensa y control basado en redes definidas por software sobre plataforma de comunicaciones y operaciones Linux, distribución CentOS 7 de 64 Bits y una Suite de soluciones de alto rendimiento orientadas al análisis, estudio y control de infraestructuras de redes de datos.



Autora: Diana Alvarado

Anexo 3.

Y el nivel de comportamiento de la red de dato se mantendrá totalmente controlada en todos los aspectos, se define un ambiente controlado en el cual se impone un esquema open source para la detección de intrusiones.



Autora: Diana Alvarado

Anexo 4.

La institución no posee un ambiente regulado y climatizado para el cuarto de equipos o el cuarto de telecomunicaciones, tal es el caso que los equipos se encuentran agrupados en condiciones no estandarizadas y no recomendables; por consiguiente, se constata que el área en la que se encuentran los dispositivos es compartida con la sala de fisiatría y terapia física.

Autora: Diana Alvarado

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS