UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADASM

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO"

AUTOR: ANDREA YOMAIRA ZURA CHALÁ

DIRECTOR: MSc. EDGAR MAYA

IBARRA - ECUADOR

2015

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1 IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003193065		
APELLIDOS Y NOMBRES:	ZURA CHALÁ ANDREA YOMAIRA		
DIRECCIÓN:	AZAYA ISLA SAN CRISTÓBAL 2-08 Y AMBATO ESQUINA.		
EMAIL:	chazy_agav@yahoo.com		
TELÉFONO FIJO:	062 545 388	**TELÉFONO MÓVIL:**	0985 481 957
DATOS DE LA OBRA			
TÍTULO:	DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO		
AUTOR (ES):	ZURA CHALÁ ANDREA YOMAIRA		
FECHA:	MAYO DEL 2015		
PROGRAMA:	■ PREGRADO ☐ POSGRADO		
TITULO POR EL QUE OPTA:	INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN		
ASESOR:	MSC. EDGAR MAYA		

2 AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Zura Chalá Andrea Yomaira, con cédula de identidad Nro.100319306-5, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3 CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

.....

Firma

Nombre: Andrea Yomaira Zura Chalá

Cédula: 100319306-5

Ibarra, Mayo del 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Zura Chalá Andrea Yomaira, con cédula de identidad Nro.1003193065, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado: "DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO", que ha sido desarrollado para optar por el título de: Ingeniería Electrónica y redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Firma

Nombre: Andrea Yomaira Zura Chalá

Cédula: 100319306-5

Ibarra, Mayo del 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Andrea Yomaira Zura Chalá con cédula de identidad nro. 1003193065, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro que el presente trabajo de investigación, es de mi autoría y no ha sido realizado, ni calificado por otro profesional, para efectos académicos y legales será de mi responsabilidad.

.....

Firma

Nombre: Andrea Yomaira Zura Chalá

Cédula: 100319306-5

Ibarra, Mayo del 2015

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación “DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO.” fue desarrollado en su totalidad por la Srta. Andrea Yomaira Zura Chalá, bajo mi supervisión.

MSc. Edgar Maya
DIRECTOR DE TESIS

DEDICATORIA

Dedico este Proyecto de Titulación a mis padres; Esthela quien ha inculcado en mí su perseverancia y responsabilidad, Eddy quien m ha brindado fortaleza en cada una de mis decisiones; a ellos quienes han estado conmigo en cada una de las etapas de mi vida, entregándome apoyo incondicional su en las buenas y malas; a ellos quienes me han brindado los mejores concejos para seguir adelante, en especial me han ayudado a culminar con este objetivo alentándome a seguir siempre adelante pese a todas las caídas.

A mis tías, quienes han estado presentes en cada momento; quienes han sido un pilar fundamental en mi vida.

Especialmente dedico este trabajo a mi hijo Josue, el motor de mi vida, por quien sigo siempre adelante. A Danny, que se ha convertido en un gran compañero de vida, quien me ha ayudado y alentado en la culminación de este trabajo.

Andrea Yomaira Zura Chalá

AGRADECIMIENTOS

Agradezco, a Dios por guiar mi camino y darme perseverancia a lo largo de estos años, a mis padres y a toda mi familia por el incondicional apoyo que me han brindado en todo momento, a los docentes de la Universidad Técnica del Norte quienes con su conocimiento han aportado en mi formación profesional y personal, al MSc. Edgar Maya por haberme guiado en la culminación de este trabajo.

Andrea Yomaira Zura Chalá

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

El GAD Municipal de Otavalo proporciona distintos servicios de telecomunicaciones en beneficio de la población para ello posee una red de datos distribuida en red interna, enlaces inalámbricos y acceso a las TIC's tanto en el sector urbano como en el rural; razón por la cual es importante que su infraestructura ofrezca alta disponibilidad y calidad de servicio, soportando grandes cantidades de tráfico, además de poseer escalabilidad, flexibilidad y seguridad.

El presente trabajo plantea un diseño de modelo de seguridad multicapa, conocido como defensa en profundidad; el mismo que será aplicado en tres niveles; en el nivel de usuario se elaboró un Manual de Normas y Procedimientos de seguridad de información en base a la Norma ISO IEC 27002, el cual se socializo en conjunto con el administrador de red hacia los usuarios; en el nivel de red interna se diseñó un modelo jerárquico basado en el estudio por capas; y en la red perimetral mediante herramientas de detección de intrusos basados en motores Suricata bajo una plataforma unificada denominada SELKS.

Además mediante un presupuesto referencial se demostró que es posible migrar de una solución propietaria a una solución bajo software libre; lo que permite minimizar costos y aprovechar mejor los recursos.

ABSTRACT

The Municipal GAD Otavalo provides various telecommunications services to the benefit of people thus has a network of distributed data in internal network, wireless connections and access to TIC's both urban areas as the rural; so it is important to provide high availability infrastructure and service quality, supporting large amounts of traffic, besides having scalability, flexibility and security.

This paper presents a design of multi-layered security model, known as defense in depth; the same to be applied at three levels; at the user level a Manual of Policies and Procedures Information Security is developed based on the ISO/IEC 27002, which socialized along with the network administrator to users; in the internal network level hierarchical model based on the study was designed layered; and in the perimeter network by intrusion detection tools based on Suricata engines under a unified platform called SELKS.

Also is performed the calculation of referential budget in which it was shown that it is possible migrating from a proprietary solution to a solution under free software; enabling you to minimize costs and better use of resources.

PRESENTACIÓN

El presente proyecto de titulación consiste en la propuesta de políticas de seguridad en base a los tres pilares fundamentales como son la integridad, disponibilidad y confidencialidad de la información frente a las amenazas externas e internas a las que la red puede estar expuesta continuamente.

El proyecto inicia con la revisión de los fundamentos teóricos en el que se hará una investigación de la norma ISO/IEC 27002, la funcionalidad y aplicabilidad del Modelo de seguridad “Defensa en Profundidad”.

En el segundo capítulo se hará el levantamiento de información de la situación actual de la red de datos del GAD Municipal de Otavalo, tanto de la red física como lógica y se determinará las vulnerabilidades y amenazas a las que está expuesta.

Con la información obtenida en el levantamiento de información, a nivel de red interna se propondrá un diseño jerárquico y segmentado; en el nivel de Red Perimetral se aplicarán en el Firewall diferentes políticas de seguridad tanto para la red interna como externa; así también se considerará una Zona Desmilitarizada para los servidores, además se instalará un sistema de prevención y detección de intrusos “SURICATA” bajo software libre; en el nivel de acceso de usuarios se realizará un Manual de políticas y procedimientos de seguridad, el mismo que será socializado conjuntamente con el administrador de la red hacia los usuarios de las políticas que se establecieron durante el desarrollo de este proyecto.

Una vez terminado el diseño del sistema se realizarán pruebas de simulación de ataques siguiendo los objetivos de un hacking ético, los mismos que permiten evaluar las vulnerabilidades.

Se realizará un presupuesto referencial tomando en cuenta una comparación de tener una solución licenciada y una solución en software libre, así como también en el beneficio en cuanto a prestaciones que tienen los equipos para soportar las configuraciones frente a aquellos equipos que no.

Se efectuará las recomendaciones necesarias en los niveles de Seguridad Física, Host, Aplicación y Datos, además se mencionará las conclusiones y recomendaciones que se obtendrán a lo largo de la realización de este proyecto

CAPÍTULO I

1 FUNDAMENTOS TEÓRICOS

En este capítulo se realizará un estudio de los fundamentos de la seguridad en redes, se hará una investigación de la funcionalidad y aplicabilidad del Modelo de seguridad “Defensa en Profundidad”, se resaltará la importancia de utilizar un IDS/IPS así como también un estudio de la norma ISO/IEC 27002:2009, sin dejar de analizar los fundamentos necesarios que nos permitirán realizar la segmentación de la red mediante VLANs.

1.1 CONCEPTOS BÁSICOS DE SEGURIDAD EN REDES

Es importante tener claros varios términos que llevan a conceptualizar la seguridad de redes; términos que involucran activos, políticas, amenazas, vulnerabilidades, entre otros.

1.1.1 INFORMACIÓN

La información es uno de los activos más importantes dentro de una institución, por lo que requiere una fuerte protección aplicando diferentes medidas de seguridad para asegurar una adecuada operación y continuidad del negocio.

“La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente.” (Carlos Andrés Gil, Jonathan Martínez, Julieth Veloza & Ray Alejandro Mora, 2008)

1.1.2 SEGURIDAD DE INFORMACIÓN

Irwin Valera Romero afirma que la

Seguridad de los Sistemas de Información consiste en la protección de los sistemas de información respecto al acceso no autorizados o modificación de la información en el almacenamiento, proceso y tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas.

Cabe recalcar que no es posible una seguridad absoluta, es decir que siempre existen riesgos independiente de las medidas que se tomen.

1.1.2.1 PILARES FUNDAMENTALES DE LA SEGURIDAD DE INFORMACIÓN

La seguridad de la información según ISO 27001 se caracteriza por mantener y preservar "la integridad, confidencialidad y disponibilidad de la información".

Según La Recomendación X.800 del CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) conceptualiza estos términos así:

a. Integridad

"Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada".

b. Confidencialidad

"Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados."

c. Disponibilidad

"Propiedad de ser accesible y utilizable a petición por una entidad autorizada."

1.1.2.2 IDENTIFICACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

La identificación de riesgos según Javier Areito se define como "el proceso que se encarga de identificar y cuantificar la probabilidad que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización"

Al identificar dichos riesgos, se producen diferentes incidentes no deseados para la organización, los mismos que se presentan en la Figura 1-1.

FIGURA 1.1: Incidentes producidos en la identificación de riesgos

Fuente: (Bertolín, 2008), Pág. 8

1.1.2.2.1 AMENAZAS PARA LA SEGURIDAD DE INFORMACIÓN

Una amenaza según López en su libro Seguridad Informática, se entiende como la "presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que – de tener la oportunidad- atacarán al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad." (Pág 13)

- Clasificación de la amenazas

Se pueden encontrar diferentes clasificaciónes, de acuerdo al cirterio de los auotres, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal maera que se muetsra en la la Figura 1-2.

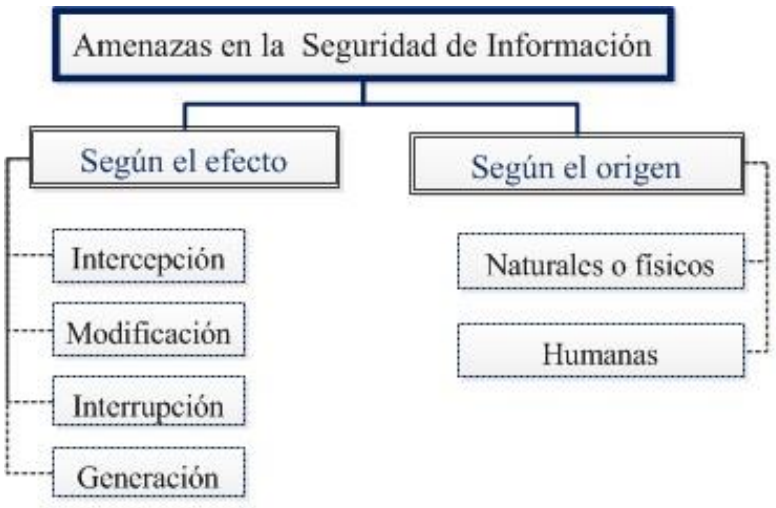


FIGURA 1.2: Clasificación de las amenazas de la seguridad de información
Fuente: Realizada por Andrea Zura

1.1.2.2.2 VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

Una vulnerabilidad no causa ningún daño por sí misma, pero provocan debilidades que pueden ser explotadas por una amenaza afectando algún activo de la entidad.

Es así que Bertolín, en su libro Seguridad de la información, describe a una vulnerabilidad como

La potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos, incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información. (2008). Pág. 23.

- Clasificación de las vulnerabilidades.

Se pueden encontrar diferentes clasificaciónes, de acuerdo al cirterio de los auotres, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal manera que se muestra en la la Figura 1-3.

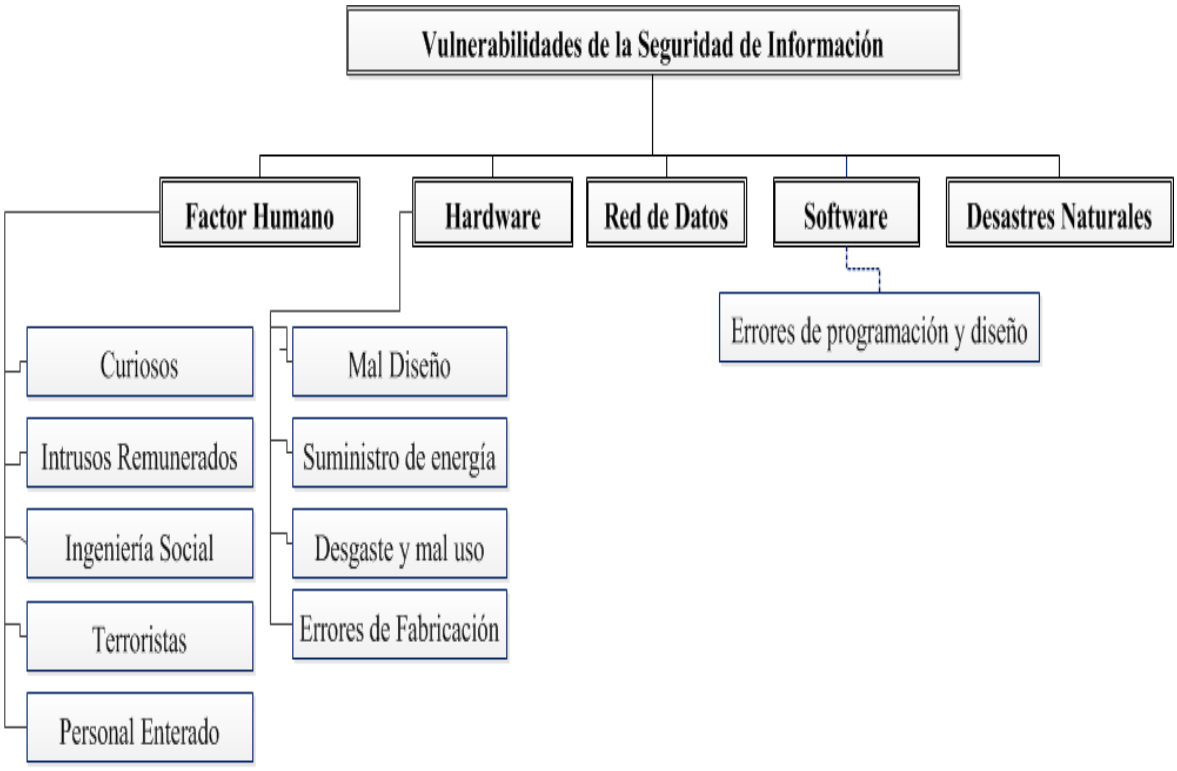


FIGURA 1.3: Clasificación de las vulnerabilidades de la seguridad de información

Fuente: Realizada por Andrea Zura

1.1.2.2.3 ATAQUES PRODUCIDOS EN LA SEGURIDAD DE LA INFORMACIÓN

Un ataque es la explotación de las vulnerabilidades encontradas en el diseño y configuración de un sistema dentro de una organización.

- Clasificación de los ataques.

Se pueden encontrar diferentes clasificaciónes, de acuerdo al criterio de los auotres, para este documento se ha tomado algunas de ellas y se las ha clasificado de tal manera que se muestra en la la Figura 1-4.

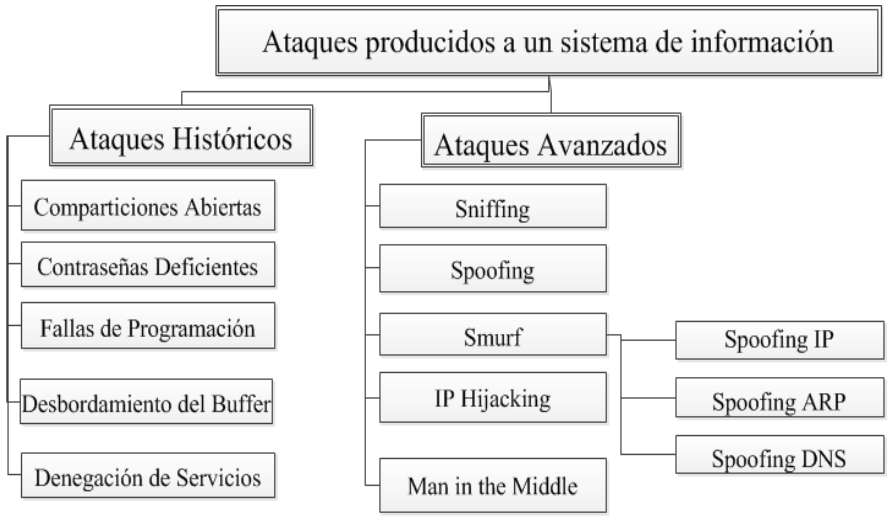


FIGURA 1.4: Clasificación de los ataques producidos en la seguridad de información

Fuente: Realizada por Andrea Zura

1.2 DEFENSA EN PROFUNDIDAD

Este modelo de seguridad está compuesto por varias líneas de defensa para la protección de uno de los activos más importantes dentro de la empresa, como es la información, modelo que viene desde entornos bélicos en los que las estratégicas militares tenían como objetivo hacer que el atacante pierda el esfuerzo inicial y en cada intento se encuentre con una barrera más por derribar. (Gadue, 2004).

Se observa en la Figura 1-5 la infraestructura de este modelo, en una serie de capas, en las que los datos son el último nivel al que el atacante podría acceder.

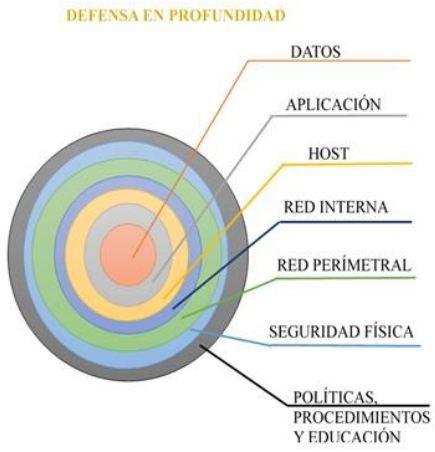


FIGURA 1.5: Capas del modelo defensa en seguridad

Fuente: Adaptado de (Montenegro).

Las capas que se muestran en el Figura 1-5, representa una barrera para el atacante en su intento de llegar a su objetivo, los datos, de tal forma que si falla cualquiera de éstas haya defensas adicionales que reduzcan las amenazas y la posibilidad de llegar a su objetivo.

1.2.1 POLÍTICAS, PROCEDIMIENTOS Y EDUCACIÓN

Es una capa dirigida a los usuarios del sistema dentro de la entidad, establece métodos para lograr concientizar a los usuarios sobre la responsabilidad y el cuidado que se debe tener con los activos de información.

En el Manual de Normas y Políticas de Seguridad informática de la Universidad de Oriente UNIVO se conceptualiza a las políticas como:

Una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Esta a su vez establece las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos. (Pág. 8)

1.2.1.1 NORMA ISO/IEC 27002

La Serie ISO/IEC 27000 fue publicada en el año 2000 y traducida al español en 2006; es un conjunto de estándares no certificables que proporcionan un marco de gestión de la Seguridad de Información, aplicable a cualquier tipo de organización, es dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información. (NTE INEN-ISO/IEC 27002)

1.2.1.1.1 ESTRUCTURA DE LA NORMA

“Esta norma contiene 11 secciones sobre controles de la seguridad que en conjunto tienen un total de 39 categorías principales de la seguridad y una sección de introducción a una evaluación y el tratamiento del riesgo” (NTE INEN-ISO/IEC 27002).

1.2.1.1.2 CLÁUSULAS

“Cada cláusula contiene una cantidad de categorías principales de la seguridad. Estas 11 cláusulas (acompañadas por la cantidad de categorías principales de la seguridad incluida en cada numeral) son:” (NTE INEN-ISO/IEC 27002).

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

De estos once dominios se derivan 39 objetivos de control que son los resultados que se esperan alcanzar mediante la implementación de los controles y 133 controles que son las prácticas, procedimientos o mecanismos que reducen el nivel de riesgo.

a. Políticas De Seguridad

Tiene como objetivo dirigir y dar soporte a la gestión de la seguridad de la información; así como también ayudar a proyectar las metas de seguridad dentro de la organización. La política de seguridad debe ser redactada, documentada, aprobada y concientizada de tal manera que sea clara y comprensible para los usuarios.

Éste posee un objetivo de control y dos controles, los que se muestran a continuación en la Figura 1-6:

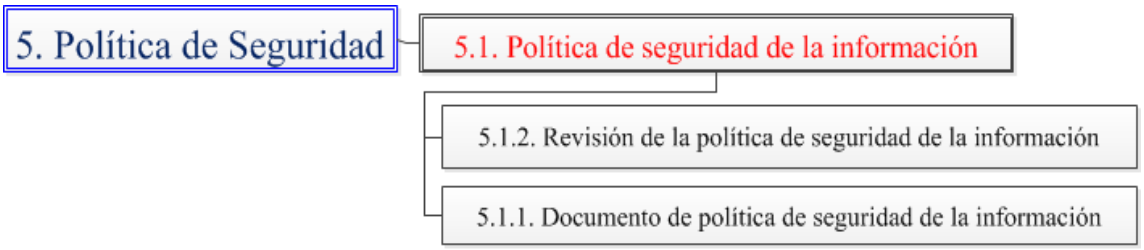


FIGURA 1.6: Esquema del 1er dominio de la Norma ISO/IEC 27002:2009
Fuente: Adaptada de NTE INEN ISO/IEC 27002

b. Aspectos organizativos de la seguridad de la información.

Su objetivo es gestionar la seguridad de la información dentro de la organización, mediante el diseño de una estructura organizativa que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma.

Éste posee dos objetivos de control y 11 controles, los que se muestran a continuación en la Figura 1-7:

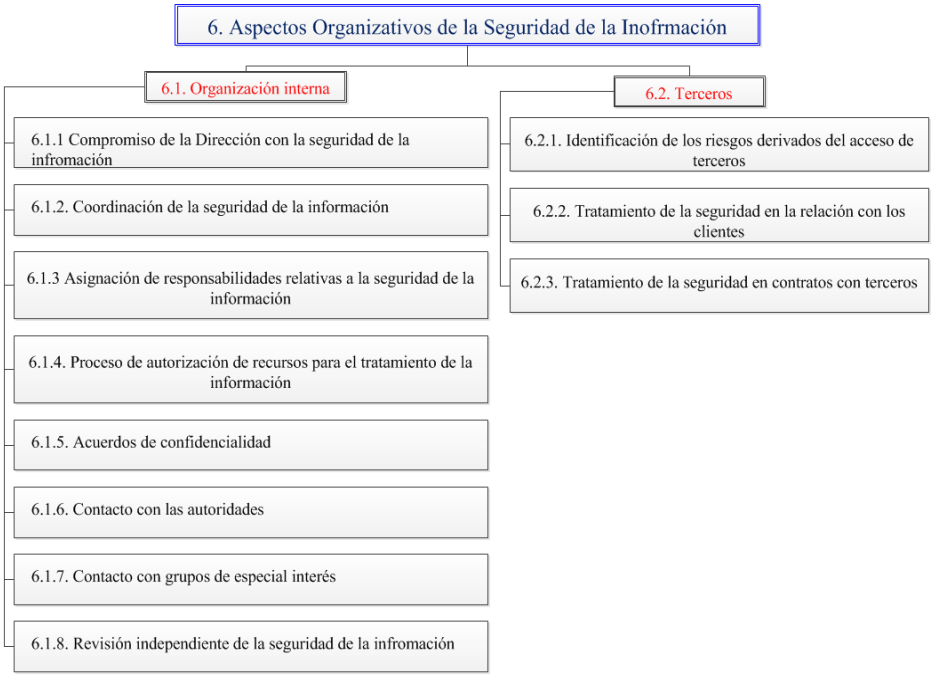


FIGURA 1.7: Esquema del 2do dominio de la Norma ISO/IEC 27002:2009
Fuente: Adaptada de NTE INEN ISO/IEC 27002

c. Gestión de activos.

El objetivo es mantener una protección adecuada sobre los activos de la organización, definiendo una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

Éste posee dos objetivos de control y 5 controles, los que se muestran a continuación en la Figura 1-8:

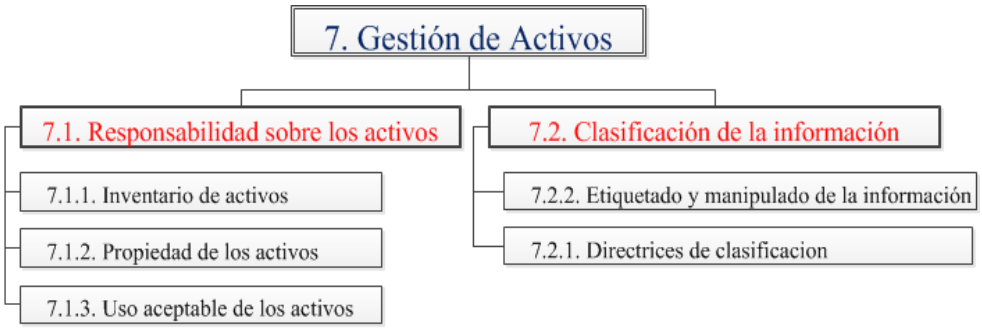


FIGURA 1.8: Esquema de 3er dominio de la Norma ISO/IEC 27002:2009
Fuente: Adaptada de NTE INEN ISO/IEC 27002

d. Seguridad ligada a los recursos humanos.

Tiene como objetivo administrar los recursos humanos de manera efectiva, mediante la evaluación y asignación de las responsabilidades de seguridad de los empleados, logrando con ello concientizarlos de los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones de los servicios.

Éste posee tres objetivos de control y 9 controles, los que se muestran en la a continuación en la Figura 1-9:

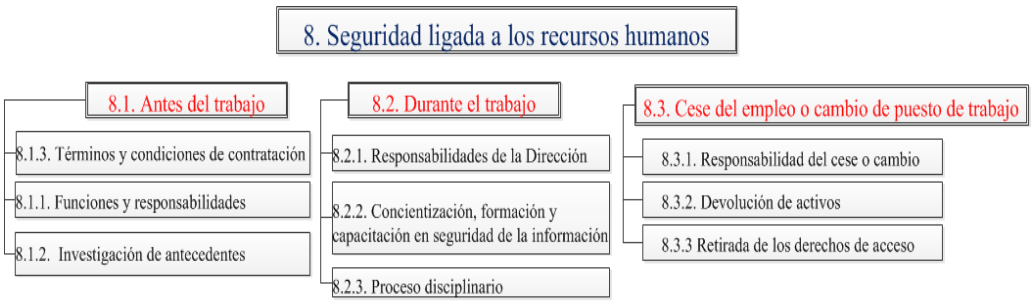


FIGURA 1.9: Esquema del 4to dominio de la Norma ISO/IEC 27002
Fuente: Adaptada de NTE INEN ISO/IEC 27002

e. Seguridad Física y del Entorno

Tiene como objetivo evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización, riesgos o robos de los recursos; mediante la organización adecuada de las áreas de trabajo y de los activos en función de su criticidad.

Éste posee dos objetivos de control y 13 controles, los que se muestran a continuación en la Figura 1-10:

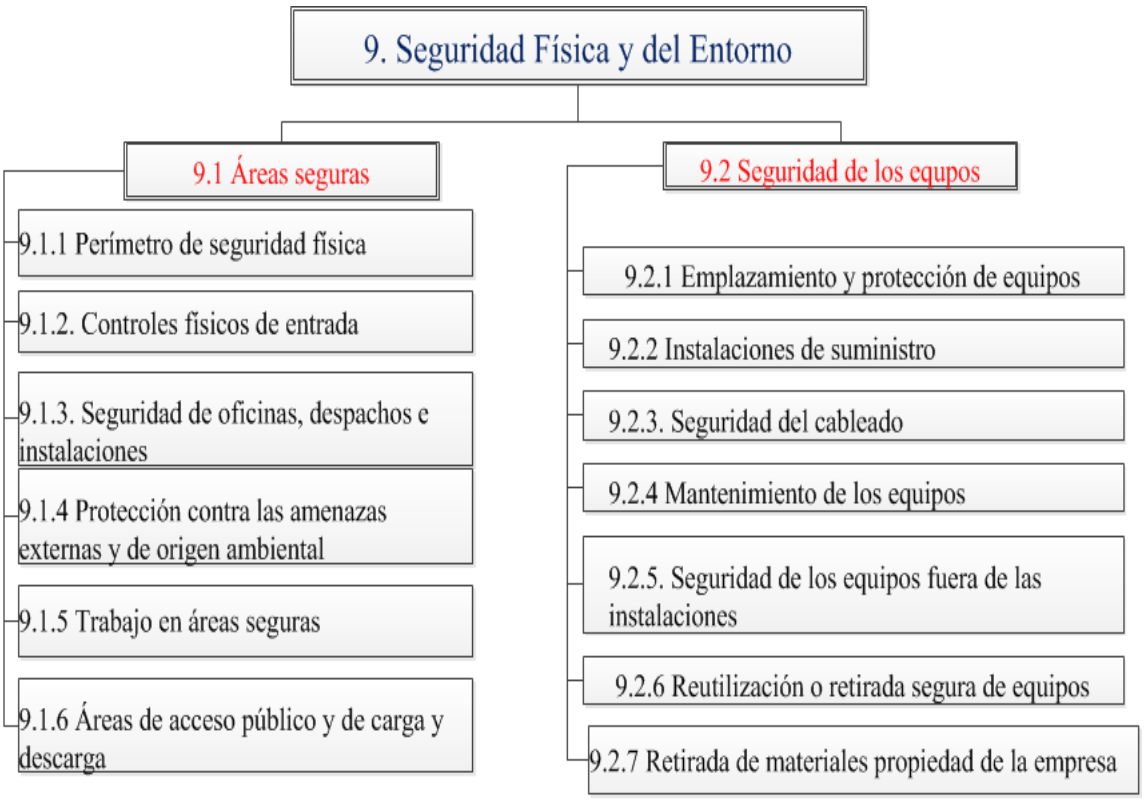


FIGURA 1.10: Esquema del 5to dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

f. Seguridad en las telecomunicaciones.

Su finalidad es mantener la integridad y disponibilidad de los servicios de información y telecomunicación, salvaguardando la información en las redes y protegiendo su infraestructura de apoyo.

Éste posee diez objetivos de control y 32 controles, los que se muestran a continuación en la Figura 1-11:

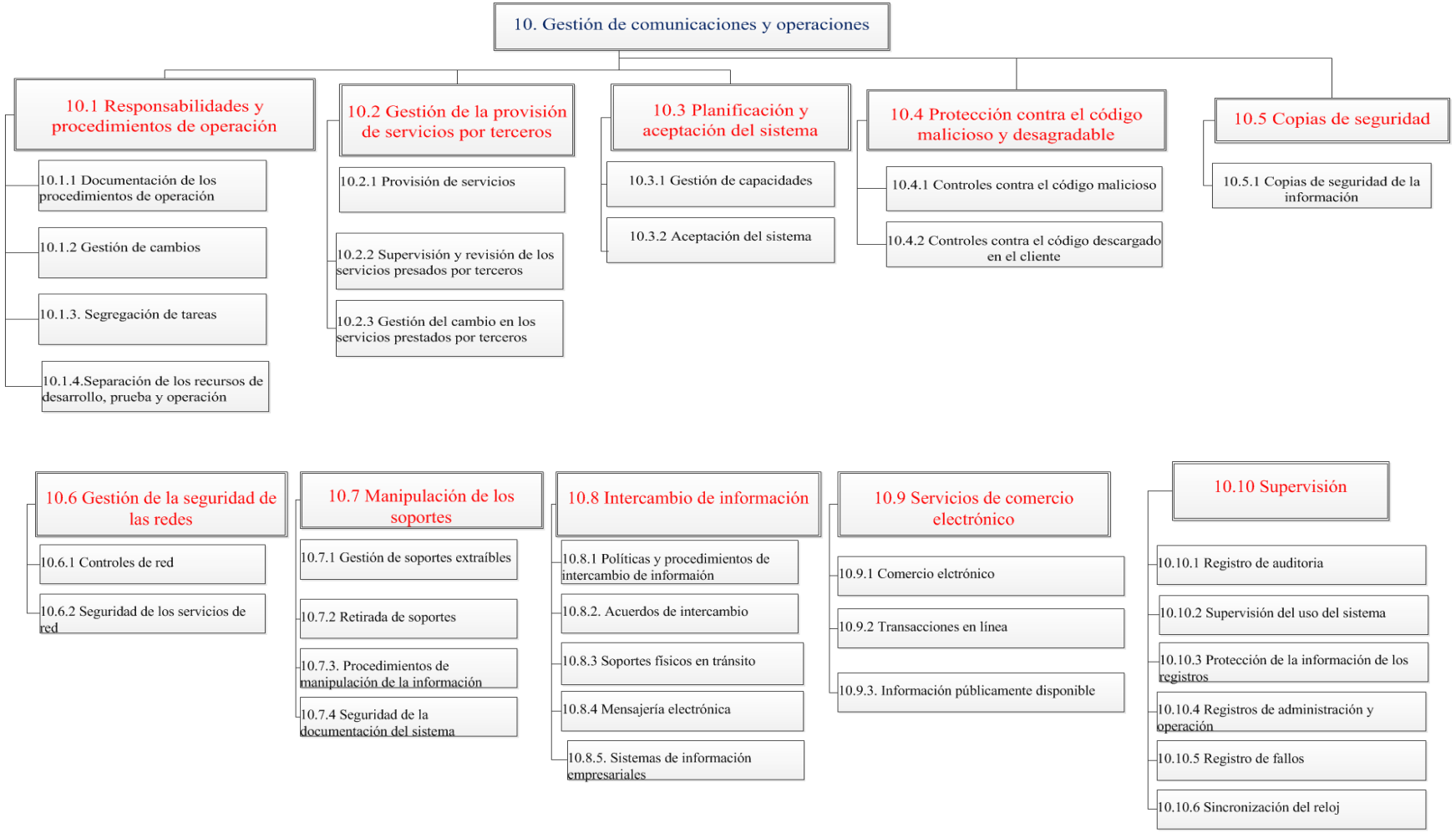


FIGURA 1.11: Esquema del 6to dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

g. Control de accesos.

Su objetivo es controlar los accesos a la información evitando accesos no autorizados a los activos de la organización y protegiendo los servicios de red

Éste posee siete objetivos de control y 25 controles, los que se muestran a continuación en la Figura 1-12 y Figura 1-13 :

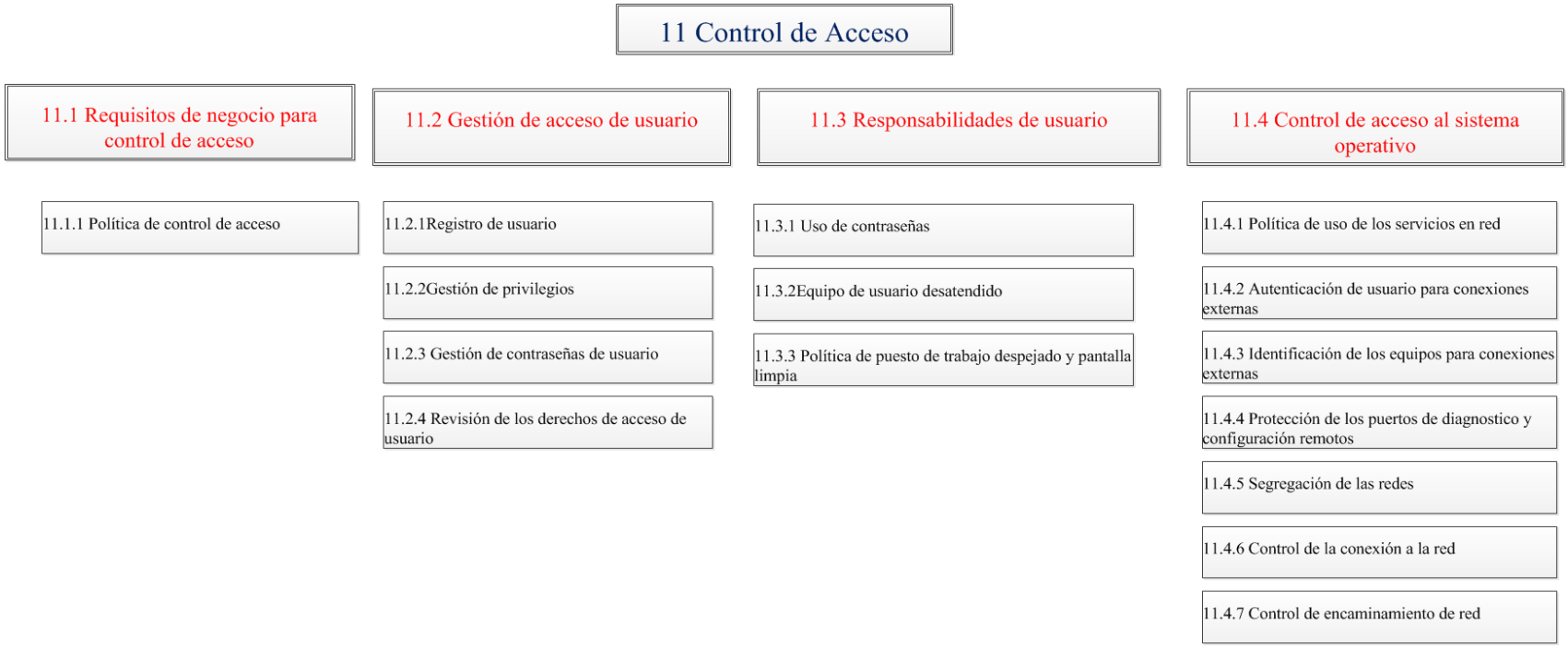


FIGURA 1.12: Esquema de la primera parte del 7mo dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

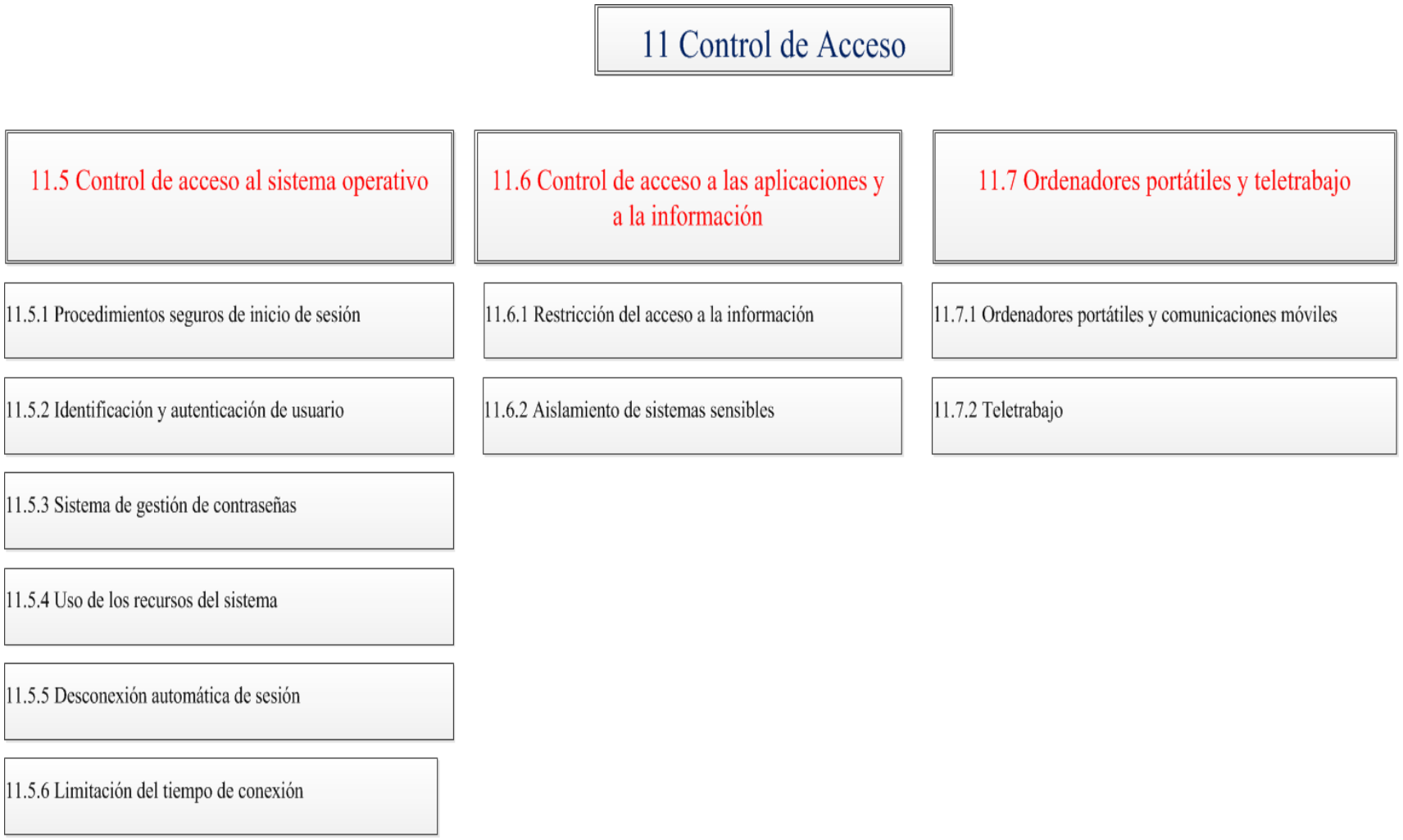


FIGURA 1.13: Esquema de la segunda parte del 7mo dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

h. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Su principal objetivo es la administración de la seguridad en el desarrollo, mantenimiento y operación exitosa del sistema de información, evitando pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

Éste posee seis objetivos de control y 16 controles, los que se muestran a continuación en la Figura 1-14:

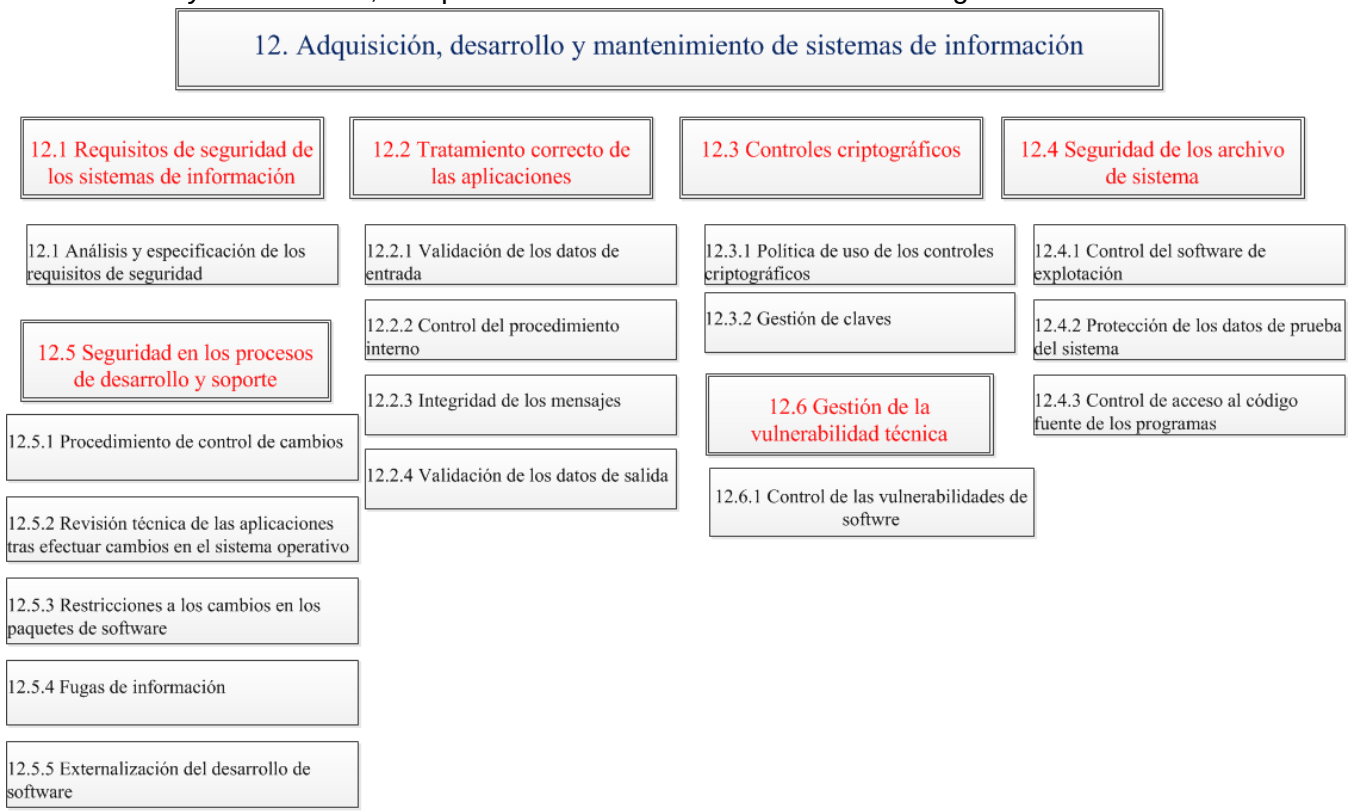


FIGURA 1.14: Esquema del 8vo dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

i. Gestión de incidentes en la seguridad de la información.

Tiene como objetivo comunicar los eventos en la seguridad de información, de manera oportuna, efectiva y ordenada, estableciendo responsabilidades y procedimientos de gestión. En caso de haberse encontrado una acción inapropiada de una persona o grupo dentro de la organización, se debe recolectar la evidencia, la misma que será retenida y presentada para tomar acciones legales.

Éste posee dos objetivos de control y 5 controles, los que se muestran a continuación en la Figura 1-15:

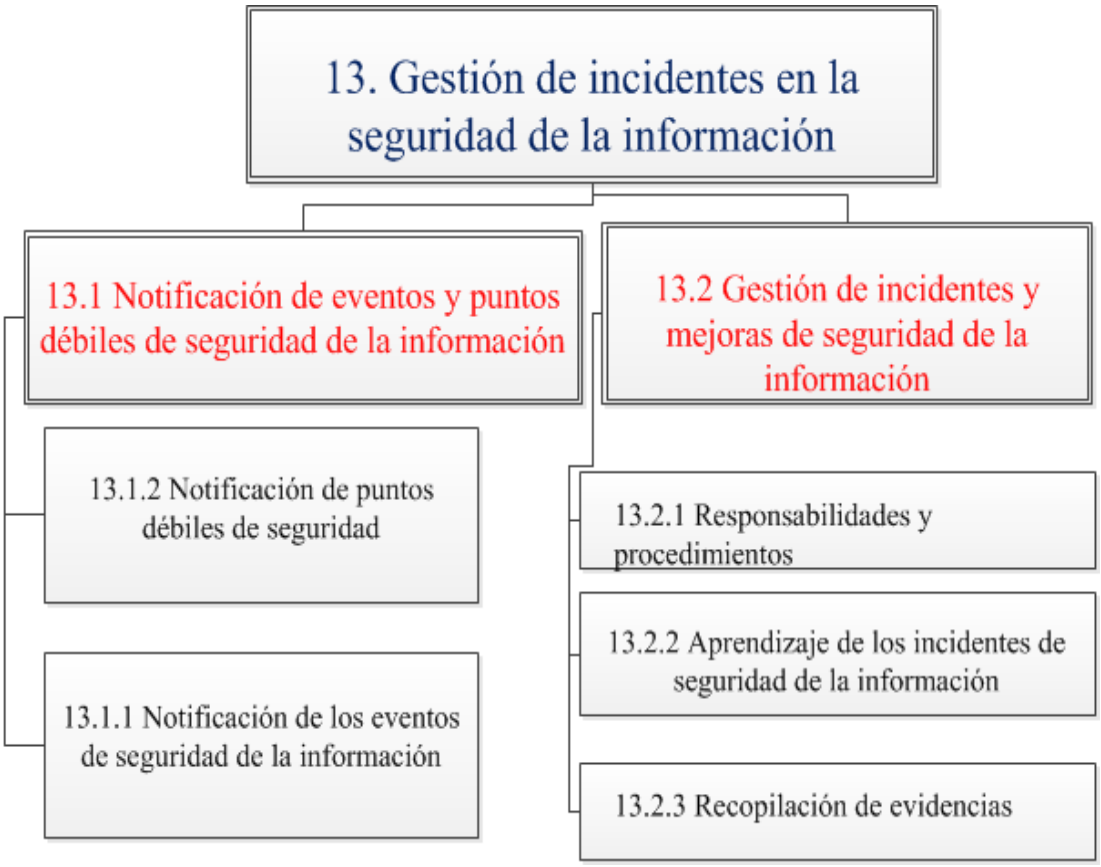


FIGURA 1.15: Esquema del 9no dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

j. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Su principal finalidad es reaccionar frente a las interrupciones operacionales de actividades del negocio, protegiendo sus procesos críticos frente a grandes fallas y desastres naturales.

Éste posee un objetivo de control y 5 controles, los que se muestran a continuación en la Figura 1-16:

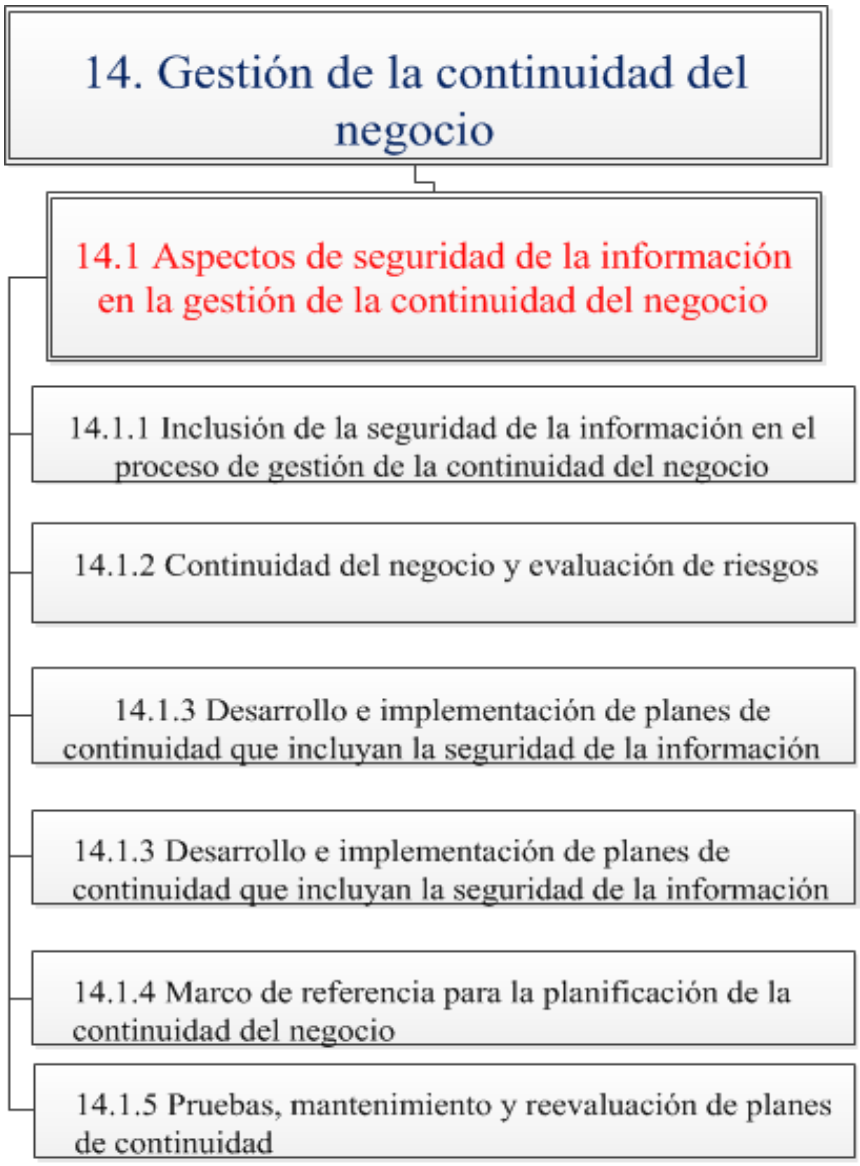


FIGURA 1.16: Esquema del 10mo dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

k. Cumplimiento.

Su finalidad es evitar el incumplimiento de cualquier ley, estatuto, regulación y de cualquier requisito de seguridad, mediante el uso de asesores legales, los mismos que aseguraran la conformidad legal de la organización, y garantizarán la alineación de los sistemas con política de seguridad de la organización.

Éste posee tres objetivos de control y 10 controles, los que se muestran a continuación en la Figura 1-17:

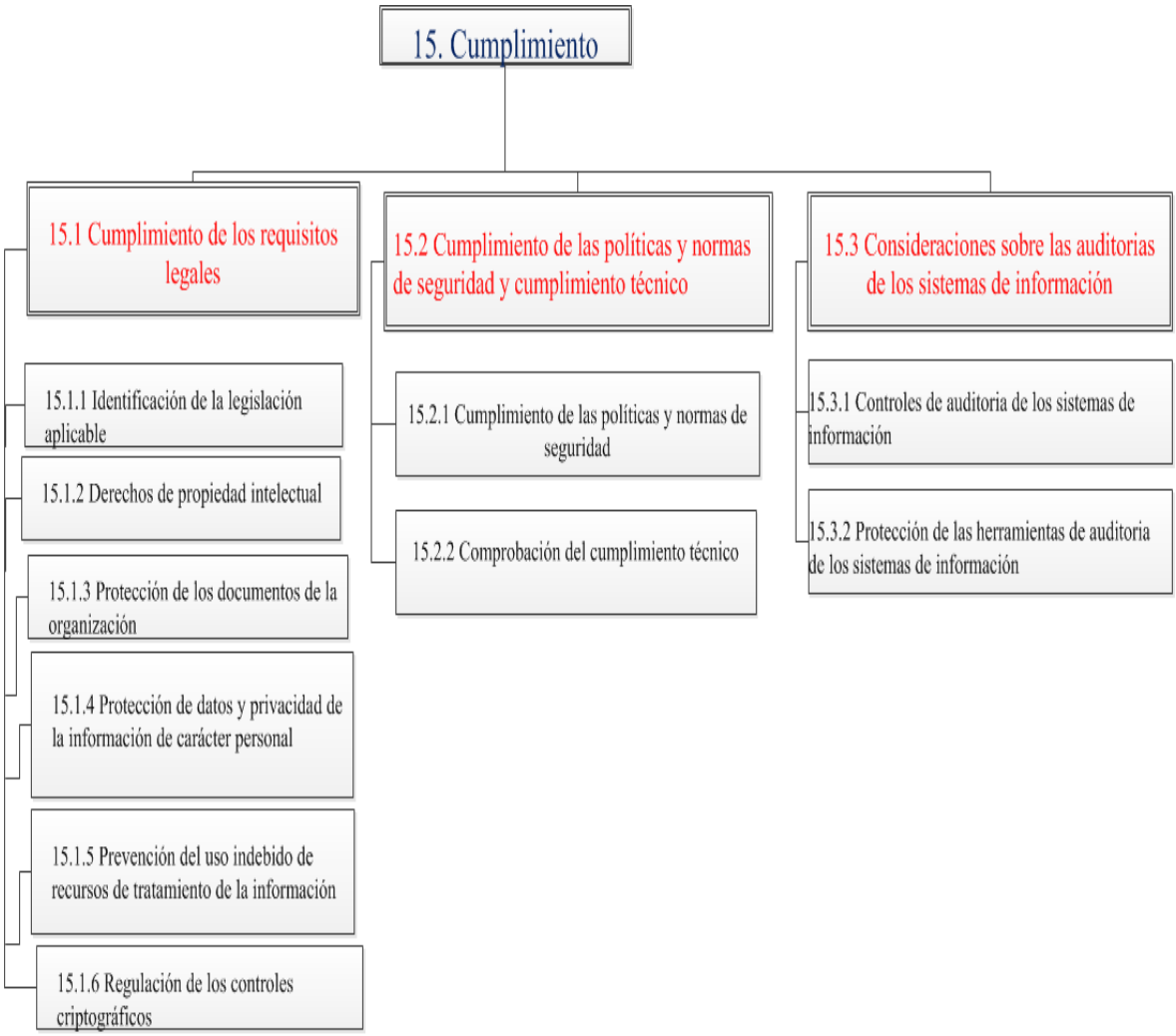


FIGURA 1.17: Esquema del 11avo dominio de la Norma ISO/IEC 27002:2009

Fuente: Adaptada de NTE INEN ISO/IEC 27002

1.3 SEGURIDAD FÍSICA

Esta capa prácticamente incorpora a las capas superiores del modelo defensa en profundidad, ya que de nada sirve contar con las mejores defensas en el área de red interna y perimetral, o los mejores antivirus para los host de la organización, si el cuarto de equipos tiene las puertas abiertas para todos aquellos que deseen entrar, sean estas personas autorizadas o no.

1.3.1 PRINCIPIOS DE PROTECCIÓN EN LA SEGURIDAD FÍSICA

Según el artículo *Minute Security Advisor - Basic Physical Security*, publicado en mayo de 2002, hay tres principios simples a seguir: Control de acceso, restricción del acceso físico y proteger el cableado estructurado.

1.3.1.1 CONTROL DE ACCESO

La mejor protección que puede tener una entidad es llevar un control estricto en cuanto a la autenticación del personal que ingresa a los cuartos de equipos, ya sea usando biométricos, libros de seguridad, entre otros; evitando de esta manera que se produzcan ataques de denegación de servicios, de modificación de información.

1.3.1.2 RESTRINGIR EL ACCESO FÍSICO

Proteger los host, no solo del acceso hacia el lugar en donde se encuentran, sino también protegerlos en caso de que accedan a ellos, de manera tal que hay que mantenerlos seguros, ya sea bloqueándolos, o con un candado de seguridad para las portátiles, utilizando algún sistema de cifrado de archivos para evitar el robo de contraseñas e información.

1.3.1.3 PROTEGER EL CABLEADO ESTRUCTURADO

El cableado estructurado de red resulta uno de los puntos más vulnerables, ya que si se encuentra visible, cualquier persona puede cortarlo, causando así la detención del tránsito de los datos, si no cumple con todas las normas, con el tiempo puede causar serios problemas en la transmisión de información.

1.4 RED PERIMETRAL

La seguridad perimetral en una red es la seguridad más importante para detectar y detener accesos no autorizados, salida de datos desde el interior y ataques desde el exterior. El perímetro está formado por dispositivos que se encuentran en la frontera de nuestra red, los mismos que interactúan con el exterior y con otras redes.

En la Tabla 1- 1 se puede observar las claras diferencias entre una red perimetral insegura y una segura.

TABLA 1.1: Comparación entre una red perimetral segura vs una red perimetral insegura

TIPO DE RED	
Red Insegura	**Red Segura**
Tiene una red plana, sin tomar las medidas necesarias de segmentación.	Permite solo ciertos tipos de tráfico a su red, y rechaza conexiones a servicios comprometidos
Utilizan una base de datos para realizar las publicaciones de sus servicios internos.	Proporcionar un único punto de interconexión con el exterior.
No cuenta con dispositivos de monitorización.	Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet
No realiza filtrado de tráfico entrante y saliente.	Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
No verifica malware o spam en el correo electrónico.	Auditar el tráfico entre el exterior y el interior
Los clientes acceden de forma remota directamente a los servicios sin ningún tipo de autenticación.	Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos.

Fuente: Elaborada por Andrea Zura

Nota. Se pueden clasificar a las redes como seguras o inseguras, de acuerdo a la administración que éstas posean.

En una red perimetral se deben considerar los siguientes dispositivos:

1.4.1 FIREWALL

Según Estrada (2011), un firewall “es un dispositivo que, como la palabra lo indica hace las veces de “barrera”, su misión es, de alguna forma bloquear el paso a cierto tipo de información.”(Pág. 187).

1.4.1.1 CARACTERÍSTICAS DE UN FIREWALL

Además Estrada, en su libro Seguridad por niveles, menciona ciertas características de los firewalls, las mismas que se mencionan a continuación:

- Tiene la capacidad de “escuchar” la totalidad del tráfico que deseamos analizar.
- Está en la capacidad de “desarmar” los encabezados de cada protocolo.
- Tiene patrones estandarizados para comprender cada protocolo.
- Cuenta con “elementos de juicio”, que permiten decidir que tráfico pasa y qué no.
- Posee una capacidad de enrutamiento, es decir puede trabajar como un Router. (Pág. 188-189)

1.4.1.2 FUNCIONAMIENTO DE UN FIREWALL

Los firewalls basan su funcionamiento en reglas, que verifican si cumplen o no con ellas para luego tomar una decisión; es así que dichas reglas toman el nombre de políticas y pueden ser: (Estrada, 2011)

- Política restrictiva: Se deniega todo, excepto lo que se acepta explícitamente.
- Política permisiva: Se acepta todo, excepto lo que se deniega explícitamente

1.4.2 SISTEMAS DE DETECCIÓN (IDS)

Un sistema de Detección de Intrusos es un programa utilizado para detectar acceso no autorizado a una red, técnica relativamente nueva que se agrega a los métodos ya conocidos de defensa, básicamente para recolectar información utilizando plugins como sensores que buscan patrones o firmas de ataques conocidos analizando el tráfico de una red. (Sarubbi, 2008).

1.4.2.1 CLASIFICACIÓN DE LOS IDS

En la Tabla 1-2, se hace un breve resumen de la clasificación de los IDS/IPS.

TABLA 1.2: Clasificación de los IDS

Clasificación de los IDS		
Según el modo de análisis	Detectores de usos indebidos	
	Detectores de anomalías	
Según el tipo de sensores	De red	
	De máquina	Sistema Operativo
		De aplicación
		Hardware
Según el tiempo de ejecución	Periódicos	
	De tiempo real	
Según el tipo de respuesta	Activos	
	Pasivos	
Según la arquitectura	Centralizados	
	Distribuidos	

Fuente: Elaborada por Andrea Zura

Nota. Fuente: Salinas R. Revista del Instituto Tecnológico de Informática. "*Sistemas de Detección de Intrusos*".

1.4.3 ZONA DESMILITARIZADA (DMZ)

Dentro de una organización se cuenta con uno o varios servidores, dependiendo de las funciones y las necesidades que tenga la misma, dichos servidores pueden contener información muy confidencial, la cual debe ser protegida de usuarios externos a la entidad. Para ello es necesario tener una zona DMZ o zona desmilitarizada que según (Mathon, 2002)

Es una subred en la que están disponibles servidores accesibles desde Internet, típicamente un relevo SMTP, un servidor WEB etc. Esta zona no debe incluir servidores con datos de la red privada (controlador de dominio, servidor de archivos…). Está protegida al menos por un cortafuego que define las reglas de acceso a los servidores de la DMZ para los usuarios de Internet.

En la figura 1-18, se puede observar una representación gráfica de una Zona Desmilitarizada.

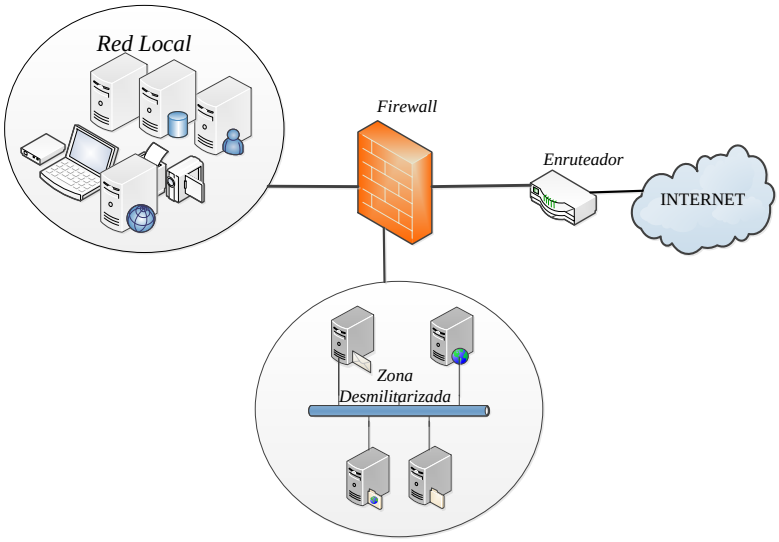


FIGURA 1.18: Zona Desmilitarizada

Fuente: Adaptado de http://www.losdel4a.com/2013/02/la-frikada-de-losdel4a/ (2013)

1.4.3.1 CARACTERÍSTICAS DE UNA DMZ

Una DMZ, puede brindar ciertas características que ayudarán a mejorar la seguridad en una red; las mismas que (Jorge A. Zárate Pérez & Mario Farias Elinostales, 2006) las describen así:

- Filtrado de paquetes a cualquier zona
- NAT, Mapeo Bidireccional
- Colas de tráfico y Prioridad
- Salidas redundantes / balanceo de carga
- Balanceo de carga a servicios
- Filtrado de contenido (web-cache)
- Monitoreo de tráfico en interfaces vía netflow

1.5 RED INTERNA

Existen varios riesgos dentro de la red local en una organización, especialmente con la información que cruza a través de ella.

1.5.1 RECOMENDACIONES PARA MANTENER SEGURA NUESTRA RED LOCAL

- En caso de existir varias redes en la organización, es recomendable realizar evaluaciones individuales y minuciosas, en cada uno de los equipos de capa 2, y capa 3.

- Realizar una copia de seguridad de la información importante para la institución, en un servidor de datos; el mismo que debería tener un dominio para su adecuada administración, contando con los permisos de usuarios que se admiten ha dicho servidor.

- Tener un firewall, ya sea físico o lógico, el mismo que sea una barrera de separación entre la red interna y el internet, teniendo control sobre todos los accesos a internet por parte de los usuarios de la red local, y el acceso hacia los datos más sensibles de la entidad.

- Proteger todos los hosts de la red local, mediante un software antivirus actualizado.

- Fomentar el uso adecuado de contraseñas en los equipos de todos los usuarios de la red interna.

- Realizar el mantenimiento continuo y adecuado de los computadores, manteniéndolas actualizadas con el software del momento.

Adicionalmente a estas recomendaciones se debe tener una adecuada configuración en la red, para lo cual es necesario tener claro ciertos conceptos:

1.5.1.1 RED DE ACCESO LOCAL VIRTUAL (VLAN)

Reciben el nombre de LANs virtuales en el sentido de que la segmentación de la red en dominios de difusión se va a hacer independientemente de la topología física que exista por debajo. Con conmutadores VLAN podemos hacer que equipos que sin VLAN estarían en el mismo dominio de difusión, pertenezcan a dominios de difusión separados. (Romero Ternero, y otros, 2010)

En la Figura 1-19 se puede observar una red segmentada con diferentes LANs virtuales.

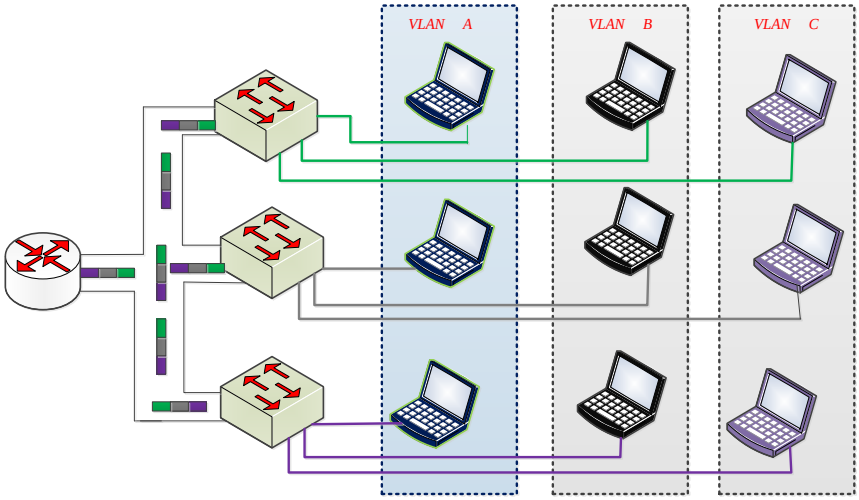


FIGURA 1.19: Red de Área Local Virtual

Fuente: Adaptada de (Romero Ternero, y otros, 2010), Pág. 212.

- Características de VLANs

De acuerdo a los autores del libro Redes Locales (Romero Ternero, y otros, 2010), éstas son las características de las VLANs.

- Todos los dispositivos que conforman la red, comparten el ancho de banda proporcionado por el medio físico.
- Se crea una topología virtual independiente de la topología física.
- Permiten agrupar a los usuarios en grupos de trabajo flexibles, sin importar su ubicación.
- Funcionan en la capa de enlace de datos y capa de red del modelo OSI.
- Para que se puedan comunicar entre las diferentes VLANs es necesario un equipo de capa 3 para su enrutamiento. (Pág. 212-213).
- Protocolos aplicados a las VLANs

Las VLANs al igual que cualquier otra tecnología, debe seguir ciertas reglas que permiten la transferencia de información de forma adecuada. Para su implementación la IEEE ha desarrollado el estándar 802.1Q en conjunto con el estándar 802.1P; adicionalmente existen otros protocolos que son variantes del 802.1Q como el ISL (Inter Switch Link) y el VTP (VLAN Trunk Protocol) de CISCO. (Guanoluisa, Semanate & Tello)

A continuación se detallarán cada uno de esos protocolos:

a. IEEE 802.1Q

Este protocolo fue desarrollado por el grupo de trabajo 802 de IEEE, con la finalidad de interconectar múltiples redes con enrutadores, compartiendo virtualmente el mismo medio físico. Adicionalmente este estándar permite la comunicación de VLANs de diferentes fabricantes.

El estándar 802.1 Q establece un etiquetado de trama, el cual asigna de forma exclusiva un identificador de VLAN en cada trama Ethernet entre la dirección origen y el campo de longitud, el cual tiene 4 octetos, es decir, 32 bits. Dicho identificador es examinado por cada switch antes de iniciar cualquier transmisión hacia otros equipos de red; una vez iniciada la transmisión el switch elimina dicho identificador antes de que la trama se transmita al host final. El formato de la trama fue publicado en el estándar IEEE 802.1Q en el año 1998. (Tanenbaum, 2003)

b. ISL (Inter- Switch Link Protocol)

Es un protocolo propietario de Cisco, trabaja en topologías punto a punto, e interconecta varios switches. Actualmente se encuentra en desuso.

ISL puede transportar cualquier protocolo de enlace, como por ejemplo PPP, Token Ring, FDDI, ATM, Ethernet, entre otros, además soporta PVST (Per VLAN Spanning Tree). Cabe recalcar que una de las características de este protocolo es que no usa una VLAN nativa.

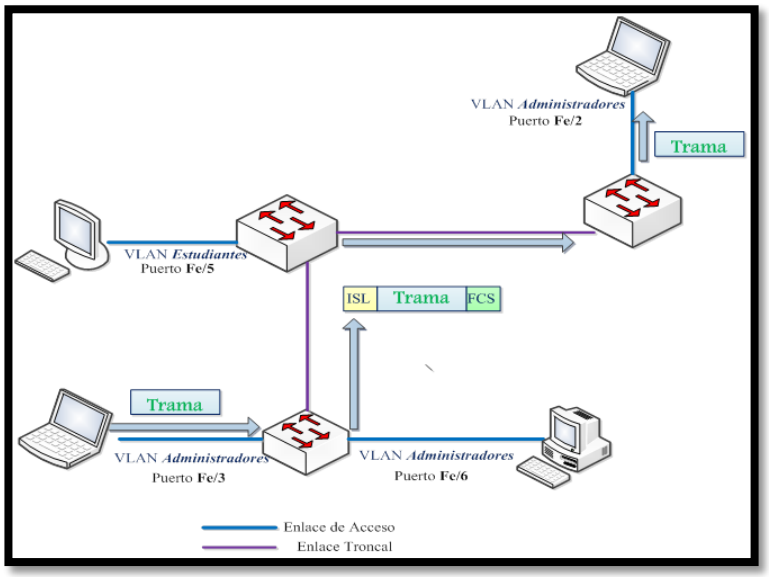


FIGURA 1.21: Encapsulación ISL

Fuente: Adaptada de http://tinyurl.com/paynrnd (Huertas, 2012)

c. VTP (Vlan Trunk Protocol)

Es un protocolo de enlace troncal de VLAN, propietario de CISCO, el cual fue creado para resolver problemas operativos en la administración de una red grande conmutada con VLAN, ya que a medida que aumenta el número de switch la administración en general se vuelve un desafío.

La función principal de VTP es mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común, mediante la utilización de ramas de enlace troncal para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. (CCNA Exploration 4.0 Conmutación y conexión inalámbrica)

- Modos de operación de VTP

El protocolo VTP opera en uno de tres modos posibles, los cuales se pueden observar en la Figura 1-21. Por defecto el switch viene configurado en modo servidor.

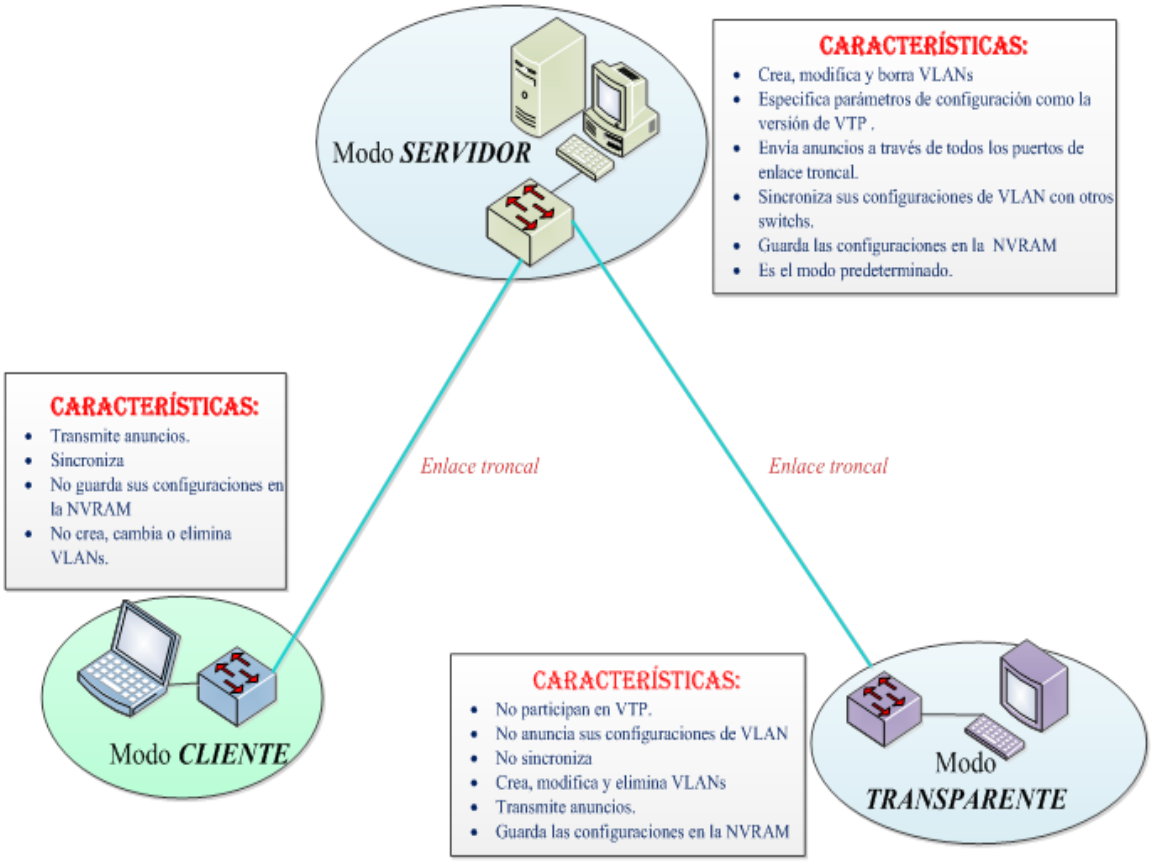


FIGURA 1.21: Modos de trabajo VTP

Fuente: Adaptada de http://www.datuopinion.com/vtp (2011)

1.5.1.2 LISTAS DE ACCESO (ACL)

En el nivel de red es importante tener en cuenta las políticas de seguridad que se pueden aplicar al tráfico de red, utilizando listas de acceso para controlar el tráfico que fluye a través de la red.

Una lista de acceso permite al conmutador impedir o autorizar cierto tipo de tráfico, además permiten controlar que dispositivos de red pueden comunicarse en la red.

Una lista de acceso es una serie de sentencias de permiso o denegación que se aplican a direcciones o protocolos, que para ser aplicadas el switch necesita inspeccionar cada uno de sus elementos y comprobar si coincide o no con cada una de las reglas definidas en la ACL. (Ternero, 2004)

- Tipos de ACL

Cisco define dos tipos de ACL:

a. Estándar

Son las listas de acceso más simples, y permiten o deniegan el tráfico desde las direcciones IP origen. Especifican un par de direcciones dirección/wildcard[1].

Se crean en el modo de configuración global con el comando access-list seguido de un número de 1 a 99. Además se debe ubicar lo más cerca posible del destino, debido a que en sus especificaciones las direcciones de destino no se toman en cuenta.

Su configuración se la resume en 3 simples pasos:

1. En modo de configuración global se crea la ACL.

2. Se aplica la ACL en una interfaz, indicando la dirección del tráfico al ser aplicado.

3. Verificar su funcionamiento.

- Formato de una ACL estándar

Una lista de acceso estándar filtra los paquetes IP únicamente basándose en la dirección de origen. Así se muestra en la Figura 1-22.

[1] Es una secuencia de 32 dígitos binarios que indican a un router que parte de una dirección de red debe coincidir para llevar a cabo determinada acción, se utiliza al configurar sentencias de listas de control de acceso (ACLs), al configurar el protocolo de enrutamiento OSPF. (Guiovanni, s.f.)

ACL ESTÁNDAR

Formato	Access-list	N° (0-99)	Condición (permit/denny)	Dirección / Wildcard
Ejemplo	access-list	15	permit	192.168.1.0 0.0.0.255

FIGURA 1.22: Formato de una ACL estándar.

Fuente: Adaptada de http://tinyurl.com/pjz5gzl (Ternero 2004)

b. Extendida

Una lista de acceso extendida filtra los paquetes IP basándose en varias condiciones, sean estas por ejemplo el tipo de protocolo, las direcciones IP tanto de origen como de destino, los puertos UDP y TCP origen y destino; entre otros.

Se crean en el modo de configuración global con el comando access-list seguido de un número de 100 a 199. Además se debe ubicar lo más cerca posible del origen del tráfico que se va a denegar; logrando así que el tráfico no deseado se filtre sin necesidad de atravesar la red.

- Formato de una ACL extendida.

Una lista de acceso extendida filtra los paquetes considerando algunas condiciones. Así se muestra en la Figura 1-23.

ACL EXTENDIDA

Formato	access-list	N° (100-199)	Condición (permit/denny)	Puerto (TCP/UDP)	Dirección IP Origen / Wildcard	Dirección IP Destino / Wildcard	Operador (eq-gt-eq-neq)	Operadorando Número de puerto
Ejemplo	access-list	110	deny	tcp	192.168.10.0 0.0.0.255	192.168.20.0 0.0.0.255	eq	80

FIGURA 1.23: Formato de una ACL extendida.

Fuente: Adaptada de http://tinyurl.com/pjz5gzl (Ternero 2004)

1.5.1.3 SECURE SHELL (SSH)

El acceso a los routers o swtiches de forma remota, es uno de los métodos más utilizados por los administradores de red, debido a su seguridad y facilidad; pero si no es configurado de manera adecuada este podría ser el medio para que un agresor ingrese a la red y viole la confidencialidad de la misma.

Existen algunos protocolos que le permiten al administrador ingresar de manera remota a los equipos, por ejemplo Telnet, pero dicho protocolo es inseguro ya que envía el tráfico de la red sin ningún tipo de cifrado, por lo que cualquier individuo podría obtener la contraseña de administración e ingresar a las configuraciones de los equipos. Es por estas razones que la recomendación para el acceso remoto a los equipos es la de proteger las líneas de administración y después configurar los dispositivos con un protocolo seguro como SSH. (Smaldone, 2004).

- Características de SSH

SSH es un protocolo diseñado para reemplazar algunas herramientas de acceso remoto inseguras, que proporciona ciertas características que se detalla en la Tabla 1-3:

TABLA 1.3: Características de SSH

SSH	
Característica	**Descripción**
Confidencialidad	• Se garantiza mediante el cifrado. • Se aplica un cifrado simétrico a los datos. • Se realiza un intercambio seguro de claves entre cliente y servidor. • Oculta ciertas características del tráfico tal como la longitud real de los paquetes
Autenticación	• Se realiza conjuntamente con el intercambio de claves mediante el algoritmo de Diffie-Hellman[a]. • La autenticidad de los datos se garantiza añadiendo a cada paquete un código MAC calculado con una clave secreta.
Eficiencia	• Comprime los datos intercambiados para reducir la longitud de los paquetes. • Negocia el algoritmo que se utilizará en cada sentido de la comunicación. • Define mecanismos para intentar acortar el proceso de negociación

Fuente: Elaborada por Andrea Zura

Nota. SSH como protocolo seguro tienen 3 características principales, de las cuales dos forman parte de los pilares fundamentales de la seguridad de información.

[a] Diffie-Hellman: Algoritmo de cifrado de claves.

HOST

En esta capa, las amenazas se dan por software mal intencionado, vulnerabilidades que son aprovechadas por los atacantes en contra del sistema, es por ello que se debe evaluar cada host de la red, realizando escaneos constantes, actualizaciones de antivirus, así como también un control y cambio permanente de contraseñas; creando de esta manera una barrera de seguridad para el atacante.

Se deben tomar ciertas consideraciones según (Microsoft, 2004) para lograr un claro objetivo de impedir el acceso al atacante hacia los host de la red, las mismas que se detallan a continuación:

- La configuración predeterminada de instalación de los sistemas operativos, tales como nombres de usuario y contraseñas deben cambiarse de forma inmediata.
- Conservar la confidencialidad de la información, es importante, por lo que se debe cuidar el acceso y la autenticación hacia los recursos de la red.
- Desinstalar las aplicaciones innecesarias, optimizaran el recurso en cuanto a espacio de disco, y permitirá mayor rapidez de procesamiento.
- La instalación de softwares antivirus, firewall, IDS/IPS permitirá asegurar los host.

APLICACIÓN

La inseguridad a nivel de aplicación es realmente alta, debido a que en esta capa se dan la mayoría de los ciberataques, debido a que maneja múltiples protocolos como HTTP, VoIP, SMTP, FTP, DNS, entre otros; protocolos que un atacante podría aprovechar para obtener acceso a las aplicaciones que se estén ejecutando.

Existen algunas recomendaciones a considerar en esta capa, tales como la validación del cumplimiento de estándares, así como también el uso adecuado de los puertos utilizados por los protocolos antes mencionados, el bloque de datos maliciosos, y de manera especial el control de las operaciones de aplicaciones por parte del programador, que es

la persona encargada de proporcionar una protección adicional a sus aplicaciones. (Microsoft, 2004)

DATOS

La información es el activo más importante dentro de un organización, y a la vez es el activo más requerido por personas mal intencionadas, es por ello que el riesgo a este nivel es alto. Por esta razón es indispensable tomar en cuenta ciertas medidas de seguridad para cuidar este activo, tales como el cifrado de los datos, o la utilización de firmas digitales, entre otras. Métodos que se deben estudiar detalladamente, considerando las ventajas y desventajas que uno proporciona, para de ésta manera saber cuál de ellos utilizar. (Microsoft, 2004)

En la Tabla 1-4, se detallará algunos de los métodos más utilizados. Cabe señalar que este documento no se entrará en detalle de las características, prestaciones y funcionamiento de los mismos.

TABLA 1.4: Métodos utilizados en la seguridad de los Datos

Métodos de seguridad en los Datos				
Algoritmos de encriptación			**Seguridad en el comercio electrónico**	**Seguridad en la WEB**
Algoritmos Simétricos		**Algoritmos Asimétricos**		
Algoritmo DES		EL GAMAL	Cyber cash	MD2
Algoritmo IDEA		DSA	PGP	MD4
Algoritmo RIJNDAEL		Pohlig-Hellman	SET	MD5
Modo ECB	RSA		SHA	
Modo CBC	Diffie-Hellman		SHA1	
Modo CFB			SSL	
Modo OFB			S-HTTP	
			HMAC	

Fuente: Elaborada por Andrea Zura

Nota. Los algoritmos de encriptación se clasifican en simétricos y asimétricos, los mismos que presentan ventajas y desventajas el uno del otro; entre las que se destaca que la gran velocidad de cifrado y descifrado que presenta los simétricos frente a los asimétricos**.**

CAPÍTULO II

2 LEVANTAMIENTO DE INFORMACIÓN EN LA RED DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE OTAVALO

En este capítulo se describirá la situación actual de la red de datos del GAD Municipal de Otavalo tanto de la red física como lógica y se determinará las vulnerabilidades y amenazas a las que está expuesta; con la ayuda del Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM 3.0).

2.1 DESARROLLO DE LA METODOLOGÍA DE LA INVESTIGACIÓN

Según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, México) desarrollar una metodología de investigación "es afinar y estructurar más formalmente la idea de investigación, desarrollando tres elementos: objetivos de investigación, preguntas de investigación y justificación de ésta." Es así que en la Figura 2-1, se muestra el diagrama del desarrollo de la metodología de investigación.

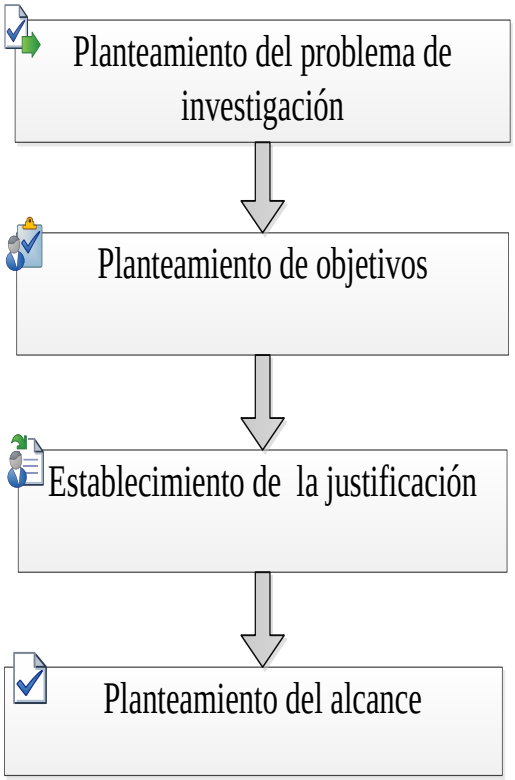


FIGURA 2.1: Pasos de la metodología de investigación

Fuente: Adaptada de http://slideplayer.es/slide/1540817/

2.1.1 PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

Una vez realizado el planteamiento de la idea principal de la investigación, el siguiente paso será plantear el problema de investigación, el cual es una estructuración de esta idea. Hay que tomar en cuenta que la base del desarrollo de dicho proyecto tiene su base en este planteamiento. Es recomendable que la formulación del planteamiento del problema se la debe realizar en forma de pregunta, así:

¿Está la red de datos del GAD Municipal de Otavalo expuesta a ataques internos y externos, debido a las vulnerabilidades de diseño, implementación, configuración y administración?

Una vez formulada la pregunta para el planteamiento del problema, es recomendable realizar un árbol de causas y efectos, herramienta que permite identificar y representar de manera gráfica las repercusiones del problema:

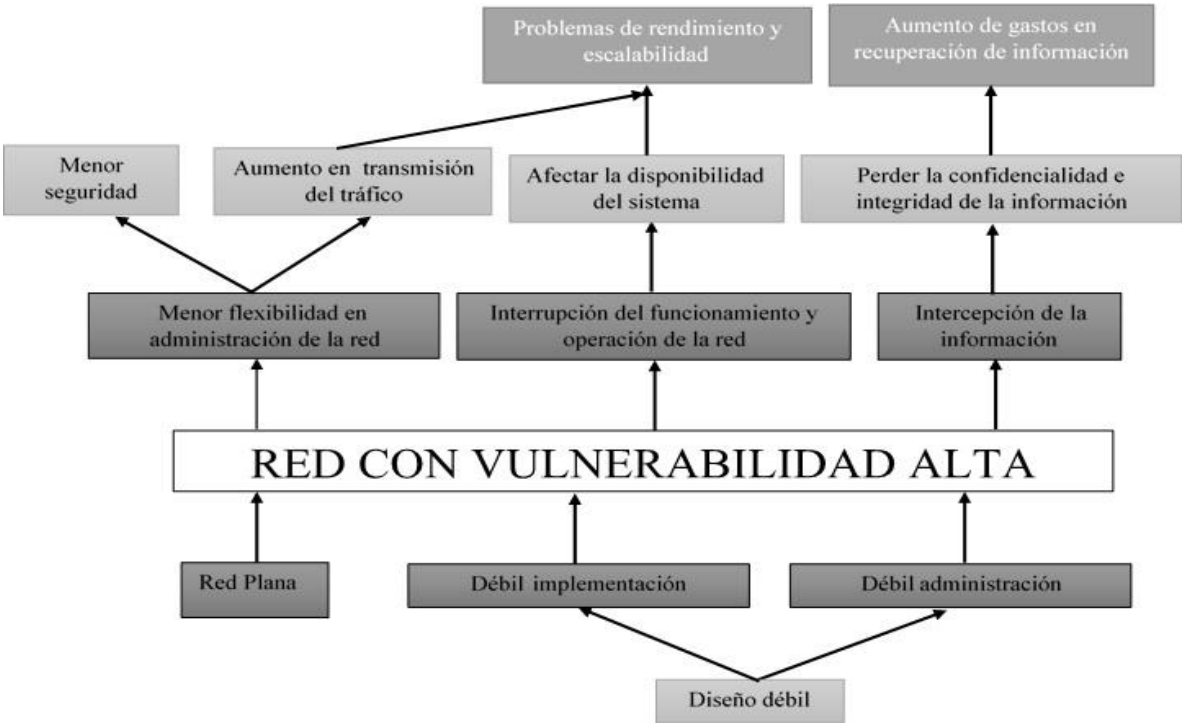


FIGURA 2.2: Árbol de causas y efectos
Fuente: Elaborada por Andrea Zura

En la figura 2-2 se muestra gráficamente el problema, que se lo ha denominado ***"***RED CON VULNERABILIDAD ALTA"; ubicando sobre el los efectos directos; después se colocarán un segundo y/o más niveles de efectos derivados del primer nivel, todos unidos por flechas.

En base a la pregunta planteada y al árbol de causas y efectos se procede a plantear el problema:

En la actualidad las instituciones públicas tienden a proporcionar distintos servicios de telecomunicaciones en beneficio de la población. El GAD Municipal de Otavalo no es la excepción, ya que posee una red de datos distribuida en red interna, enlaces inalámbricos y acceso a las TIC's tanto en el sector urbano como en el rural. Para lograr dicho objetivo, en los últimos años han mejorado su infraestructura.

Año tras año se tiene un incremento en los usuarios de la red del GAD Municipal de Otavalo, lo que trae como consecuencia dificultad en la administración de la red ya que no se ha tomado las consideraciones de segmentación en la misma, causando caída en la enlaces. Pero el aumento de los usuarios no solo ocasiona problemas de administración, sino también problemas en la seguridad de la información, a pesar de que este tema ha sido tomado en cuenta y que no se ha presentado ningún tipo de amenaza o ataque activo, se ha tomado como un mecanismo de seguridad, la adquisición de un Firewalls Sophos UTM, el cual se ha configurado con mínimas políticas de seguridad basadas en la restricción de páginas web para la intranet, políticas que no son suficientes, para prevenir ataques de acceso, de modificación, así como también ataques de denegación de servicios, entre otros; haciendo que la red sea aun vulnerable tanto externa como internamente.

Debido a estos inconvenientes, será necesario implementar mecanismos que permitan contrarrestar estas vulnerabilidades, tomando en cuenta que el nivel de seguridad no solo se debe considerar de forma interna sino fuera de ella, por lo que se debe segmentar la red aplicando controles de listas de acceso hacia las VLANs, implementar el modelo de seguridad basado en la "Defensa en Profundidad" en los niveles de usuario, red interna y red perimetral; y considerar nuevas políticas de seguridad que ayudará a prevenir ataques, detectándolos a tiempo y dando una respuesta oportuna para evitar daños posteriores.

2.1.2 PLANTEAMIENTO DE OBJETIVOS.

Una vez planteado el problema, hay que considerar el planteamiento de los objetivos, que son parte esencial de la investigación. Para ello se procederá a realizar un árbol de objetivos, el mismo que se realiza consecuentemente del árbol de causas y efectos, ya que si los efectos son importantes, éstos merecen una solución.

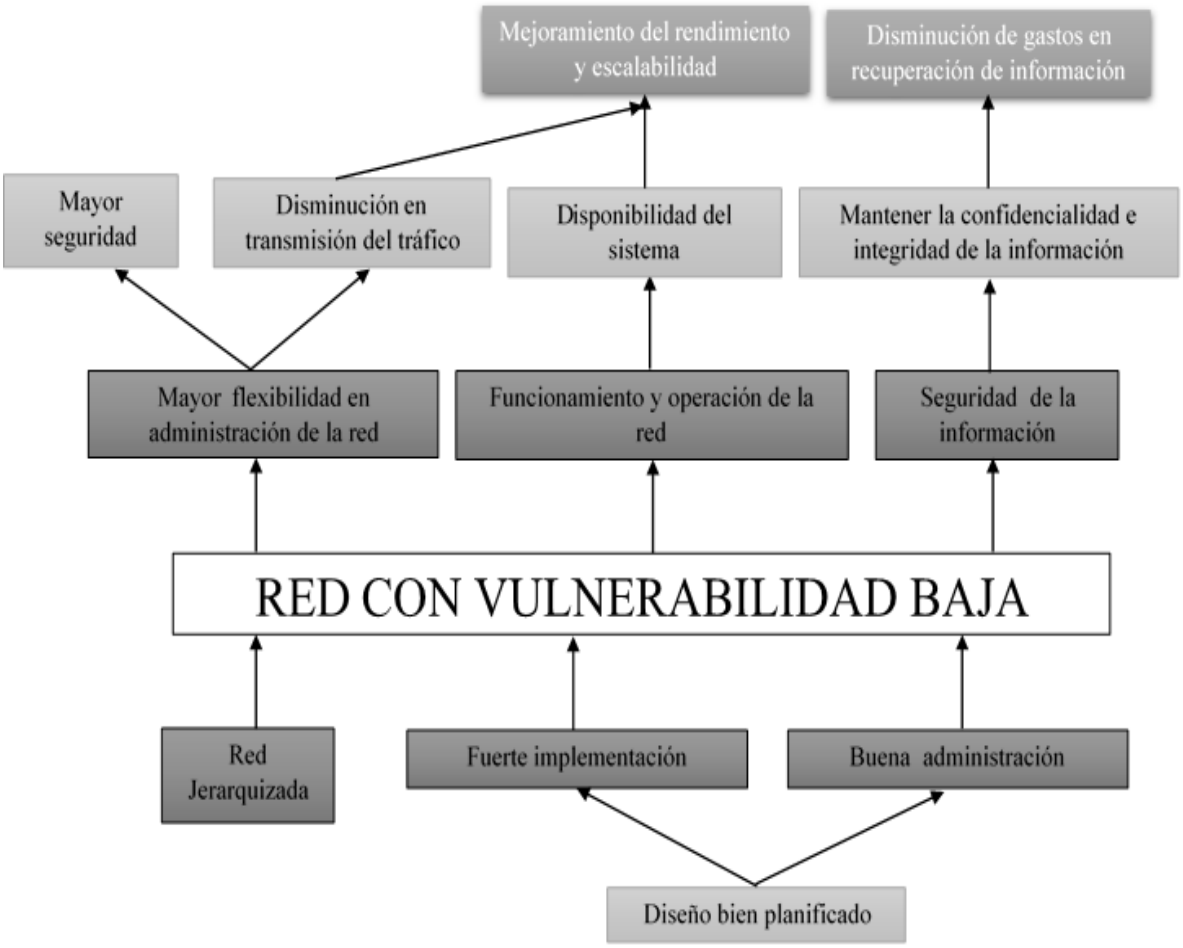


FIGURA 2.3: Árbol de Objetivos
Fuente: Elaborada por Andrea Zura

En la figura 2-3 se muestra gráficamente la solución esperada al nuestro problema, la mismas que se ha denominado “RED CON VULNERABILIDAD BAJA”; se expresa de manera contraria al árbol de causas y efectos.

Con el planteamiento del problema y con la ayuda del árbol de objetivos se pueden redactar los objetivos de la investigación de éste proyecto, así:

2.1.2.1 OBJETIVO GENERAL

Realizar el diseño e implementación del modelo de seguridad “Defensa en Profundidad” en la red de datos del GAD Municipal de Otavalo, aplicando nuevas políticas de seguridad en base a la norma ISO/IEC 27002, de manera que ataques externos e internos puedan ser detectados y evitados oportunamente.

2.1.2.2 OBJETIVOS ESPECÍFICOS

- Revisar la norma internacional ISO/IEC 27002, la misma que servirá de base para el diseño e implementación de este proyecto.

- Realizar el levantamiento de información de la situación actual de la red lógica y física del GAD Municipal de Otavalo.

- Diseñar el modelo de seguridad "Defensa en Profundidad" en los niveles de acceso de usuarios, red interna y red perimetral, mediante la protección multicapa que éste propone, con la finalidad de que los ataques informáticos sean bloqueados.

- Implementar el modelo de seguridad "Defensa de Profundidad", en el nivel perimetral con el diseño de un sistema de prevención de intrusos "SURICATA" bajo plataforma Linux, la reubicación de los servidores en una DMZ y la configuración de políticas en el firewall; en el nivel de red con el adecuado diseño de segmentación con políticas de acceso a las VLANs, y el nivel de acceso de usuarios con propuestas de políticas de seguridad, mediante la norma internacional ISO/IEC 27002 con el fin de que la confidencialidad, integridad y disponibilidad de la información sean preservadas.

- Efectuar pruebas de simulación de ataques en base a los objetivos de hacking ético, evaluando y verificando la seguridad física y lógica de la red.

- Realizar un presupuesto referencial de la implementación del sistema de seguridad defensa en profundidad para la red de datos del GAD Municipal de Otavalo.

2.1.3 ESTABLECIMIENTO DE LA JUSTIFICACIÓN

Para justificar la elaboración de este proyecto, se debe señalar las razones prácticas y los elementos específicos que se van a llevar a cabo durante el desarrollo del proyecto; en base a esto se detalla a continuación dicha justificación:

Actualmente en nuestro país existe un creciente avance tecnológico, y con ello crecientes formas de atacar las redes de datos, valiéndose de las debilidades y vulnerabilidades que se encuentran en ellas, aprovechándose así de un activo importante como lo es la información.

El GAD Municipal de Otavalo cuenta con una red de datos muy extensa, por la que cruza la información utilizada en diferentes softwares aplicativos, los mismos que son usados

para brindar servicios a la comunidad; si esta información sufriera algún tipo de falla o daño se tendría una perdida, no solo de información sino también una pérdida económica.

La implementación de un sistema de seguridad basada en multicapas representa una defensa para el atacante en su objetivo de acceder a los datos, de tal forma que si falla alguno de los controles en una capa haya defensas adicionales que reduzcan la amenaza. Es por ello que en este proyecto se profundizará en ciertas capas como lo son la red perimetral, la red interna y finalmente el nivel de usuario.

La protección de la red perimetral es el aspecto más importante para detener los ataques externos. El GAD Municipal de Otavalo cuenta con un Firewall Sophos UTM, el cual está destinado a proteger cada punto de acceso a la red, pero es necesario clasificar el tipo de tráfico que se permitirá, y que tipo de tráfico será bloqueado; además una Zona Desmilitarizada será importante ya que mantendrá aisladas las redes LAN de las WAN, de esta forma si los servicios son atacados no pasarán hacia la red interna protegiendo así la confidencialidad de la información; considerar la instalación de un IDS/IPS permitirá detectar los ataques en caso de que se produzcan.

Los riesgos en las redes internas en una entidad están relacionados con los datos confidenciales que se transmiten a través ellas, es así que el tener una adecuada segmentación y con ello la examinación del tráfico admisible a su red y el bloquear lo que no sea necesario; así como el considerar el uso de SSH para las comunicaciones remotas, y la aplicación de listas de acceso debido a que no todos los usuarios tienen los mismos privilegios de acceso a las redes reducirá las vulnerabilidades en este nivel.

El aprendizaje de los usuarios es una parte importante en éste modelo de seguridad ya que por lo general el desconocimiento de la importancia de llevar la información con responsabilidad puede llevar consigo varios riesgos, es por eso que la creación de un Manual de políticas y procedimientos en base a la norma ISO/IEC 27002, garantizará la integridad, disponibilidad y confidencialidad de la información que cursa por la red, protegiéndola de posibles ataques externos e internos.

2.1.4 PLANTEAMIENTO DEL ALCANCE

Para determinar el alcance del proyecto se debe delimitar de manera adecuada el campo de acción de la investigación, considerando la información obtenida en el estudio de la situación actual. En base a ello tenemos:

El presente proyecto de titulación consiste en la propuesta de políticas de seguridad en base a los tres pilares fundamentales como son la integridad, disponibilidad y confidencialidad de la información frente a las amenazas externas e internas a las que la red puede estar expuesta continuamente.

El proyecto inicia con la revisión de los fundamentos teóricos en el que se hará una investigación de la norma ISO/IEC 27002, la funcionalidad y aplicabilidad del Modelo de seguridad “Defensa en Profundidad”, se resaltará la importancia de instalar un IDS/IPS, así como la reorganización de los servidores en una DMZ, sin dejar de analizar los fundamentos necesarios que nos permitirán realizar la segmentación de la red mediante VLANs con políticas de acceso a las mismas.

Se realizará después el levantamiento de información de la situación actual de la red de datos del GAD Municipal de Otavalo, tanto de la red física como lógica y se determinará las vulnerabilidades y amenazas a las que está expuesta. En base a estos aspectos se establecerá los requerimientos de seguridad, lo que permitirá diseñar un esquema que se adapte a las necesidades de dicha entidad.

Con la información obtenida en el levantamiento de información, a nivel de red interna se realizará el diseño de segmentación previamente establecido, las configuraciones de VLANs y listas de acceso a las mismas; en el nivel de Red Perimetral se aplicarán en el Firewall diferentes políticas de seguridad tanto para la red interna como externa; así también se considerará una Zona Desmilitarizada para los servidores, manteniendo así aisladas las redes LAN de las WAN, de esta forma si los servicios son atacados no pasarán hacia la red interna protegiendo de esta forma la información, de manera tal que la entidad no corra el riesgo de comprometer la seguridad de su información; además se instalará un sistema de prevención y detección de intrusos “SURICATA” bajo software libre; el mismo que puede alcanzar grandes velocidades debido a que soporta procesamiento Multi-Hilos; además debido a que se puede reconocer automáticamente los protocolos, con un solo comando este IDS/IPS puede eliminar el MalWare lo que permitirá el bloqueo de ataques externos e internos; en el nivel de acceso de usuarios se realizará un Manual de políticas y procedimientos de seguridad, el mismo que será socializado conjuntamente con el administrador de la red hacia los usuarios de las políticas que se establecieron durante el desarrollo de este proyecto.

Una vez terminado el diseño y la implementación del sistema se realizarán pruebas de simulación de ataques siguiendo los objetivos de un hacking ético, los mismos que permiten evaluar las vulnerabilidades mediante la identificación de debilidades provocadas por una mala configuración de las aplicaciones, analizar y categorizar dichas debilidades explotables, proveer recomendaciones en base a las propiedades de la organización, eliminar las vulnerabilidades y poder reducir el riesgo.

Se realizará un presupuesto referencial tomando en cuenta una comparación de tener una solución licenciada y una solución en software libre, así como también en el beneficio en cuanto a prestaciones que tienen los equipos para soportar las configuraciones frente a aquellos equipos que no.

Se efectuará las recomendaciones necesarias en los niveles de Seguridad Física, Host, Aplicación y Datos, además se mencionará las conclusiones y recomendaciones que se obtendrán a lo largo de la realización de este proyecto.

2.2 ESTUDIO DE LA METODOLOGÍA DE ANÁLISIS DE SEGURIDAD

Existen un sinnúmero de metodologías para realizar el análisis del nivel de seguridad de información dentro de una organización. En este caso de estudio se eligió la metodología de OSSTMM, a lo largo de este capítulo se detallará su funcionalidad, características y ventajas.

2.2.1 OSSTMM

Según (Alvarado) OSSTMM “representa uno de los estándares profesionales más completos y utilizados en Auditorías de Seguridad para analizar la Seguridad de los Sistemas. Describe minuciosamente, las fases que habría que realizar para la ejecución de la auditoria.”

Existen varias metodologías para analizar los riesgos dentro de una organización, a continuación se detallan las razones por las que se eligió a OSSTMM para este trabajo:

- Este manual contempla el cumplimiento de normas y mejores prácticas como la ISO/IEC 27002; siendo así el complemento para la realización de este trabajo.
- Expresa con un valor numérico el nivel de seguridad de una organización.
- Provee guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM.

- Permite realizar un test que es válido en un futuro.
- Permite obtener un test certificado de OSSTMM; el mismo que sirve como prueba de un testeo de OSSTMM minucioso, además brinda una apropiada visión general, dándole al cliente una declaración precisa sobre el testeo.

2.2.1.1 PROPÓSITO

Su principal propósito es proveer de una metodología científica para examinar la organización, realizando pruebas sobre la seguridad de adentro hacia afuera.

Un segundo propósito es proveer guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM.

El Documento provee una serie de descripciones específicas para el desarrollo de un test de seguridad operacional sobre todos los canales incluyendo aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción de una métrica real. (Alvarado).

2.2.1.2 ÁMBITO

El ámbito debe abarcar toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en la Tabla 2-1:

TABLA 2.1: Ámbito de OSSTMM

Seguridad Física[a]		**Seguridad de Espectro[a]**	**Seguridad de Comunicaciones[a]**	
Humano[b]	Físico[b]	Comunicaciones Inalámbricas[b]	Telecomunicaciones[b]	Redes de Datos[b]
Comprende el elemento humano de la comunicación.	Comprende el elemento tangible de la seguridad	Comprende todas las comunicaciones electrónicas, señales, y las emanaciones que se producen en el (EM).	Comprende todas las redes de telecomunicación, digitales o analógicas.	Comprende todos los sistemas electrónicos y redes de datos.

Fuente: Elaborada por Andrea Zura

Nota: La tabla fue adaptada de (Herzog, OSSTMM 3.0)

[a] Clases: Son definidas como áreas de estudio, de investigación o de operación.

[b] Canales: son los medios específicos de la interacción con los activos.

2.2.1.3 FASES

OSSTMM está conformada por cuatro fases:

2.2.1.3.1 FASE DE REGLAMENTACIÓN

Cada viaje comienza con una dirección. En la fase de regulación, el auditor comienza la auditoría con una comprensión de los requisitos de auditoría, el alcance y las limitaciones a la auditoría de este alcance. A menudo, el tipo de prueba se determina mejor después de esta fase. (Herzog, OSSTMM 3.0)

2.2.1.3.2 FASE DE DEFINICIÓN

“El centro del test seguridad básica requiere conocer el alcance en relación a las interacciones con los objetivos transmitidos a las interacciones con los activos. En esta fase se definirán los aspectos.” (Herzog, OSSTMM 3.0)

2.2.1.3.3 FASE DE INFORMACIÓN

El auditor va descubriendo información, donde la intención es descubrir la mala gestión de la información. En esta fase se considera la verificación de procesos, de configuración, la validación de propiedad, una revisión de segregación y de exposición, una exploración de la Inteligencia Competitiva. (Alvarado)

2.2.1.3.4 FASE INTERACTIVA DE PRUEBAS DE CONTROLES

Estas se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de seguridad, y esta no puede realizarse mientras las otras no se hayan realizado. En esta fase se considera la verificación de la cuarentena, la auditoria de privilegios, la validación de sobrevivencia, revisión de alertas y registros. (Alvarado)

2.2.2 ANÁLISIS DE RIESGOS EN LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO SIGUIENDO LA METODOLOGÍA DE OSSTMM

OSSTMM 3.0 especifica una metodología de análisis de riesgos utilizando métricas operacionales de seguridad; las mismas que permiten la realización de una prueba de seguridad con mediciones exactas sobre el estado de la seguridad. Es así que con la

ayuda de dichas métricas se cran los RAV[2], que no son más que una descripción imparcial y objetiva de una superficie de ataque.

2.2.2.1 PROCESO

El proceso de un análisis de seguridad, se concentra en evaluar los ítems de la estructura presentada en OSSTMM 3.0, basados en el cálculo del RAV.

2.2.2.1.1 SEGURIDAD OPERACIONAL

El primer paso será calcular el RAV en la seguridad operacional, la misma que se define como "la medida de la visibilidad, accesos y confianza dentro del alcance." (Toth & Sznek, 2014)

- Visibilidad

"Componentes de la presencia de seguridad que pueden ser remotamente identificados." (Herzog, OSSTMM 2.1)

Por ejemplo para realizar una auditoría, en la sección "Humana" se emplea a 50 personas; sin embargo, sólo 38 de ellos son interactivos a partir del vector de prueba y canal. Esto haría una visibilidad de 38. (Herzog, OSSTMM 3.0)

- Accesos

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o donde un computador interactúa con otro por medio de una red. (Herzog, OSSTMM 2.1)

Por ejemplo en una auditoría física, si se tiene un edificio con 2 puertas y 5 ventanas abiertas se trata de un Acceso de 7. Si se sierran todas las puertas y ventanas, a continuación, se trata de una Acceso de 0 ya que estos no son los puntos donde se puede obtener la entrada. (Herzog, OSSTMM 3.0)

[2] El RAV es una medición de la escala de la superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula por el equilibrio cuantitativo entre las operaciones, limitaciones y controles. (Herzog, OSSTMM 3.0)

- Confianza

“La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.” (Herzog, OSSTMM 2.1)

“Por ejemplo, un proxy que redirige todo el tráfico de entrada a un equipo que procesa la petición sin verificar el origen, representaría una confianza.” (Toth & Sznek, 2014).

2.2.2.1.2 CONTROLES

Para continuar en el cálculo del RAV, es importante definir los controles; los mismos que son mecanismos de seguridad establecidos para proporcionar una seguridad y protección durante las interacciones.

- Autenticación

“La autenticación es la medida por la cual cada interacción en el proceso está privilegiada.” (Toth & Sznek, 2014)

Por ejemplo en una auditoría en la Sección Física, si se requiere tanto una tarjeta de identificación especial y un Biométrico para acceder, a continuación, se puede añadir 2 para la Autenticación. Sin embargo, si el acceso sólo requiere uno o el otro, entonces sólo se cuenta 1 a la Autenticación. (Herzog, OSSTMM 3.0)

- Indemnización

Es un compromiso entre el propietario del activo y la parte que interactúa. Puede ser un aviso legal para el caso en que una de las partes no cumpla con las reglas prefijadas; o puede ser un seguro contratado a terceros para el caso que se produzcan fallas o pérdidas de algún tipo. (Toth & Sznek, 2014)

Por ejemplo en un seguro de bienes, que tiene como alcance 200 computadoras, una póliza de seguro contra él se aplica a todas los 200 y por lo tanto se una cuenta de 200. (Herzog, OSSTMM 3.0)

- Subyugación

“Define las condiciones en las cuales ocurrirán las interacciones. Esto quita libertad en la forma de interacción pero disminuye los riesgos.” (Toth & Sznek, 2014)

Por ejemplo en una auditoria de sección Humana, Toth & Sznek recalcan en un proceso de no repudio donde la persona debe firmar un registro y proporcionar un número de identificación para recibir un documento se encuentra bajo controles de subyugación cuando el proveedor del documento registra el número de identificación, en lugar de que lo haga el receptor para eliminar el registro de un número falso con un nombre falso.

- Continuidad

“Permite mantener la interacción con los activos aun en caso de fallas.” (Toth & Sznek, 2014)

Por ejemplo en una auditoría física, si se descubre que una puerta de entrada a una tienda se bloquea de forma que no hay alternativa de entrada y los clientes no pueden entrar, entonces este acceso no tiene continuidad. (Herzog, OSSTMM 3.0)

- Resistencia

“Es el mecanismo que brinda protección a los activos en caso que las interacciones sufran alguna falla.” (Toth & Sznek, 2014)

Por ejemplo en una auditoría de Sección Física el control de 2 guardias de acceso a una puerta, si uno se retira y la puerta no se puede abrir por el guardia restante, entonces tiene la capacidad de resistencia.

- No repudio

Herzog en el Manual de OSSTMM 2.1 define el no repudio como aquel que “provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.”

- Confidencialidad

(Herzog, OSSTMM 2.1) Señala que la confidencialidad “es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.”

Un ejemplo claro de confidencialidad es la encriptación. (Herzog, OSSTMM 3.0)

- Privacidad

(Herzog, OSSTMM 2.1) Señala que la privacidad “implica que el proceso es conocido únicamente por los sistemas o partes involucradas.”

Un ejemplo claro puede ser “simplemente tomando la interacción en un cuarto cerrado lejos de otras personas.” (Herzog, OSSTMM 3.0)

- Integridad

“Permite identificar cuando un activo ha sido modificado por alguien ajeno a la interacción en curso.” (Toth & Sznek, 2014)

En una auditoria en las redes de datos, el cifrado puede proporcionar el control de la integridad sobre el cambio del archivo en la transmisión. (Herzog, OSSTMM 3.0)

- Alarma

“Es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción.” (Herzog, OSSTMM 2.1)

En una auditoria en las redes de datos, se cuenta cada servidor y el servicio que brinda: cuenta como una alarma al ser monitoreado por el sistema de detección de intrusos. (Herzog, OSSTMM 3.0)

- Limitaciones

Las limitaciones son aquellos inconvenientes que se presentan en los controles, con el objetivo de separar los activos y las amenazas. (Toth & Sznek, 2014)

- Vulnerabilidad

“Es una falla que puede permitir el acceso no autorizado a un activo o puede denegar dicho acceso a alguien que si este autorizado.”

- Debilidad

“Es una falla que reduce o anula los efectos de los controles de interacción”.

- Preocupación

“Es una falla que reduce los efectos de los controles de proceso.”

- Exposición

“Es una acción injustificada que permite dejar visible, ya sea de forma directa o indirecta, a un activo.”

- Anomalía

“Es un elemento desconocido y no se encuentra dentro de las operaciones normales. Por lo general es síntoma de algún fallo pero que todavía no se comprende.”

2.3.2 PROCESO DE CUATRO PUNTOS

El proceso de los cuatro puntos son las instrucciones específicas y los medios utilizados para llegar a los informes; asegurando de esta manera una revisión integral. Los cuatro puntos que intervienen en dicho proceso se muestran y explican en la Tabla 2-2.

TABLA 2.2: Proceso de 4 puntos

PROCESO DE 4 PUNTOS			
Fases	**Descripción**	**Etapas**	**Descripción**
Inducción	Estudiar el entorno donde reside el objetivo.	Revisión del entorno	Conocer las normas, leyes, políticas y cultura organizacional que influyen en los requerimientos de seguridad
		Logística	Obtener detalles del canal de análisis para evitar falsos positivos o falsos negativos
		Verificación de detección activa	Averiguar si existen controles que detecten intrusiones que puedan filtrar o bloquear intentos de análisis.
Interacción	Interactuar directamente con el objetivo y observar las	Auditoría de visibilidad	Enumerar los objetivos visibles dentro del alcance.
		Verificación de accesos	Determinar los puntos de acceso, la forma de interacción y el propósito de su existencia.

	respuestas obtenidas	Verificación de confianza	Verificar las relaciones de confianza entre los objetivos, donde exista acceso a la información sin necesidad de autenticación.
		Verificación de controles	Verificar la efectividad de controles de proceso
Investigación	Analizar los indicadores que provengan del objetivo.	Verificación de procesos	Comprobar el mantenimiento y efectividad de los niveles de seguridad en los procesos establecidos
		Verificación de la configuración	Revisar el funcionamiento de los procesos en condiciones normales
		Validación de propiedad	Revisar la procedencia de los datos, información, sistemas, etc.
		Revisión de segregación	Revisar los controles que aseguran separación entre la información personal y organizacional
		Verificación de exposición	Buscar información, disponible de manera abierta, que permita conocer detalles del objetivo.
		Exploración de inteligencia de negocios	Verificar la existencia de fuentes de información que contengan datos de negocio que debieran ser confidenciales
Intervención	Modificar los recursos del entorno que necesita el objetivo y observar cómo responde.	Verificación de cuarentena	Verificar la efectiva separación de elementos hostiles
		Auditoría de privilegios	Analizar el correcto uso de los sistemas de autenticación y autorización.
		Continuidad de negocio	Analizar la efectividad de los controles de resistencia y continuidad.
		Alerta y revisión de logs	Verificar si la relación entre las actividades realizadas y los registros almacenados es correcta.

Fuente: adaptada de (Herzog, OSSTMM 3.0)

2.3.2.1 DIAGRAMA DE FLUJO

“Define una metodología aplicable a cualquier tipo de test y sobre cualquier canal”. (Toth & Sznek, 2014). Dicho diagrama se muestra en la Figura 2-4.

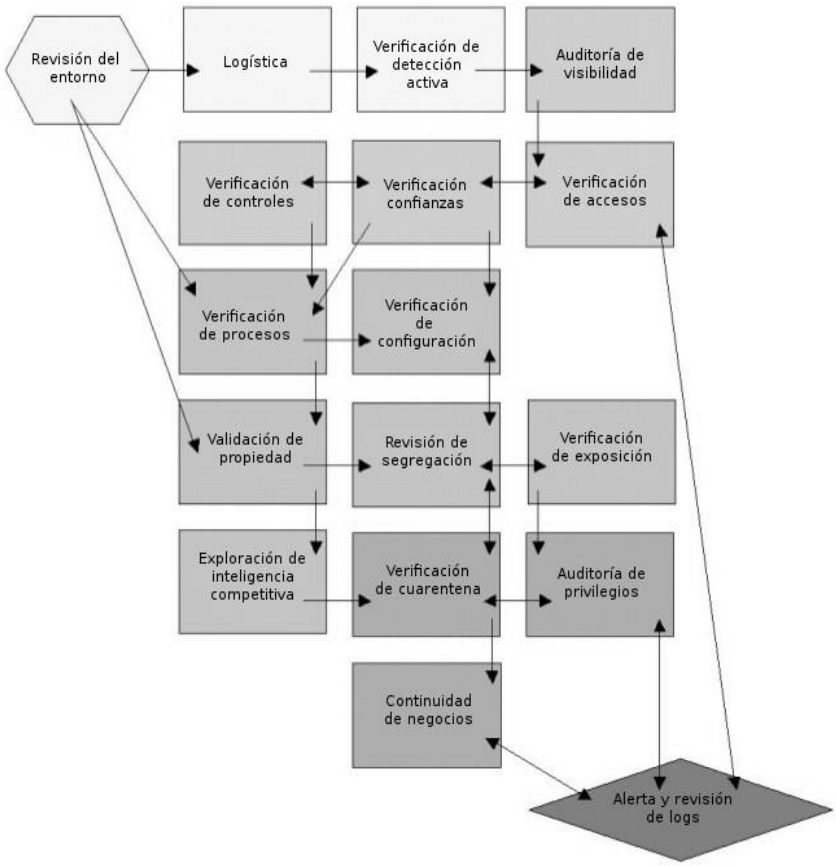


FIGURA 2.4: Diagrama de Flujo OSSTMM

Fuente: Obtenida de (Toth & Sznek, 2014)

Siguiendo este diagrama es posible obtener los datos que se requieren como entrada para determinar el estado de la seguridad en un momento determinado. Previamente es necesario clasificar la información obtenida según las indicaciones de las secciones siguientes.

2.3.3 DETERMINACIÓN DEL RIESGO

En esta etapa se determinará el riesgo de la organización siguiendo las diferentes áreas y medios especificados en el alcance de la metodología de OSSTMM 3.0.

2.3.3.1 SEGURIDAD FÍSICA

En el área de la seguridad física interviene el medio humano y físico, en los cuales se tendrán que evaluar los diferentes módulos de los 4 puntos de interacción que involucran al proceso de OSSTMM.

- Humano

El objetivo de realizar las pruebas de seguridad en este canal es verificar la concienciación sobre la seguridad personal y la medición de la responsabilidad con el estándar de seguridad requerido, esto incluye las políticas de la empresa, regulaciones de la industria, o la legislación regional. (Herzog, OSSTMM 3.0). Los resultados se pueden observar en el Anexo A.

- Físico

El objetivo de realizar las pruebas de seguridad en este canal es intentar penetrar las barreas físicas y lógicas de la organización. Los resultados se pueden observar en el Anexo B.

2.3.3.2 SEGURIDAD DE COMUNICACIONES

En el área de la seguridad de comunicaciones interviene la sección de telecomunicaciones y la de redes de datos, en los cuales se tendrán que evaluar los diferentes módulos de los 4 puntos de interacción que involucran al proceso de OSSTMM.

- Telecomunicaciones

Comprende todas las redes de telecomunicación, digital o analógico, donde la interacción se lleva a cabo a través de los teléfonos y las líneas telefónicas. (Herzog, OSSTMM 3.0).

Tiene como objetivo monitorear las telecomunicaciones; mediante pruebas de controles a nivel de red para bloquear actividades no autorizadas y las respuestas de registro y tiempo de respuesta, como los filtros de acceso basados en llamadas de teléfono (CLID), de direcciones de red de usuario (NUA), o grupo cerrado de usuarios (CUG) y mediante pruebas de controles a nivel de aplicación; verificando que están en su lugar para bloquear actividades no autorizadas y las respuestas de registro y tiempo de respuesta. Los resultados de dicha evolución se muestran en el Anexo C.

- Redes de Datos

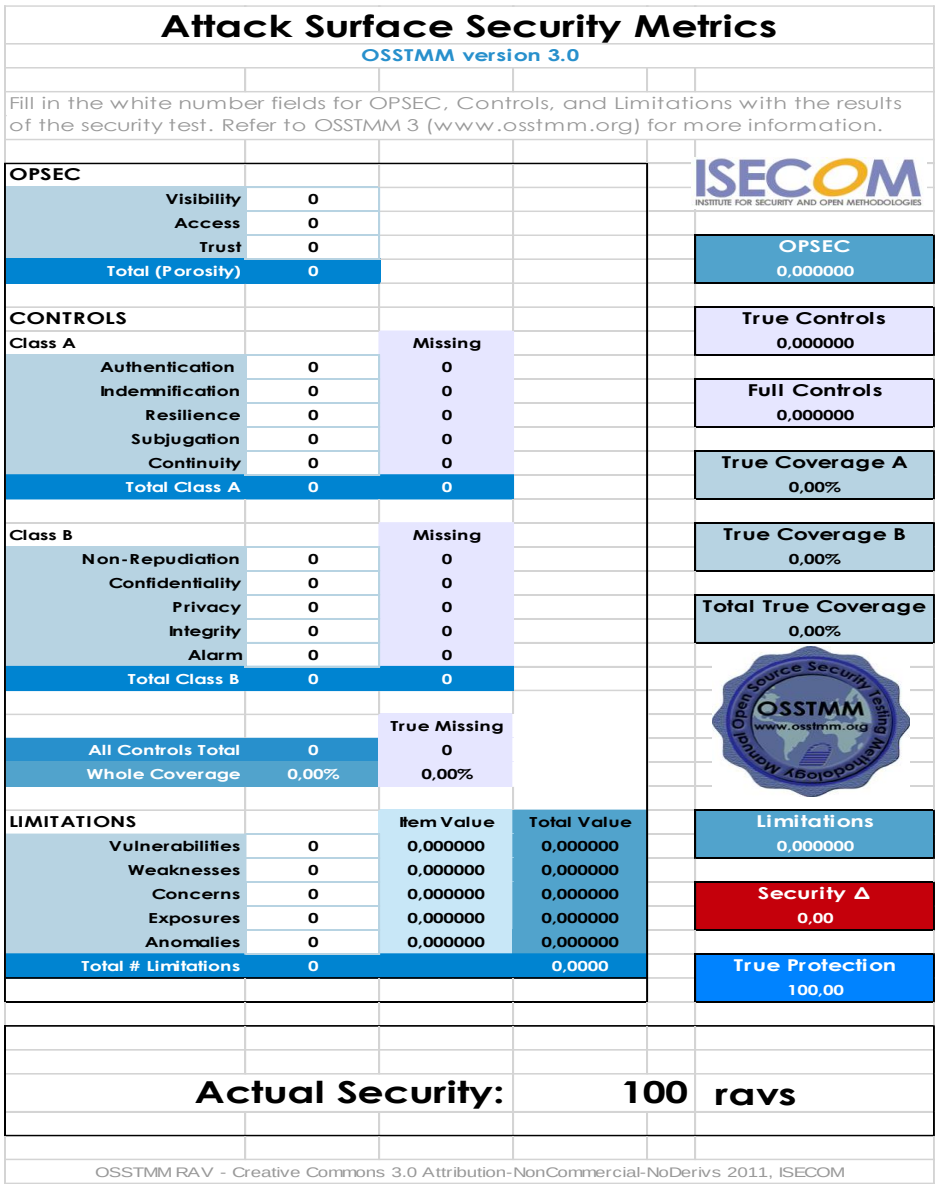
Comprende todos los sistemas y redes de datos electrónicos donde la interacción se lleva a cabo a través de redes de datos cableados. (Herzog, OSSTMM 3.0).

Tiene como objetivo monitorear los datos de entrada y salida de la red de comunicaciones a través de web, mensajería instantánea, chat, foros de discusión basados en la Web, o por e-mail, con la finalidad de verificar si consigo traen códigos maliciosos, conductas inapropiadas. Los resultados de la evolución se muestran en el Anexo D.

2.3.4 RESULTADO

Una vez calculados los valores de Seguridad Operacional, controles y limitaciones se puede realizar un cálculo de los RAVs, para medir el nivel de seguridad cuantitativamente, es así que en la página oficial de OSSTMM se encuentra una calculadora de RAVs, en la misma que se ingresan los datos obtenidos en las pruebas de penetración realizadas, y ésta automáticamente nos devolverá los valores mediante algunas fórmulas.

En la figura 2-5 se puede observar la imagen de la calculadora de RAVs oficial de la OSSTMM.



Attack Surface Security Metrics

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC			
Visibility	0		
Access	0		
Trust	0		
Total (Porosity)	0		

OPSEC
0,000000

CONTROLS			
Class A		Missing	
Authentication	0	0	
Indemnification	0	0	
Resilience	0	0	
Subjugation	0	0	
Continuity	0	0	
Total Class A	0	0	
Class B		Missing	
Non-Repudiation	0	0	
Confidentiality	0	0	
Privacy	0	0	
Integrity	0	0	
Alarm	0	0	
Total Class B	0	0	
		True Missing	
All Controls Total	0	0	
Whole Coverage	0,00%	0,00%	

True Controls
0,000000

Full Controls
0,000000

True Coverage A
0,00%

True Coverage B
0,00%

Total True Coverage
0,00%

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	0,000000	0,000000
Weaknesses	0	0,000000	0,000000
Concerns	0	0,000000	0,000000
Exposures	0	0,000000	0,000000
Anomalies	0	0,000000	0,000000
Total # Limitations	0		0,0000

Limitations
0,000000

Security Δ
0,00

True Protection
100,00

Actual Security: 100 ravs

FIGURA 2.5: Calculadora de RAVs oficial de OSSTMM

Fuente: Obtenida de http://www.isecom.org/research/ravs.h

CAPÍTULO III

3 DISEÑO E IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD "DEFENSA EN PROFUNDIDAD"

Este capítulo constará con el planteamiento de las normas y políticas de seguridad establecidas en la norma ISO/IEC 27002, el diseño de la segmentación de la red, de igual manera los diseños del IDS/IPS, firewalls de acuerdo a los resultados obtenidos en el levantamiento de información previa, adicionalmente se realizaran pruebas de simulación siguiendo los objetivos de un hacking ético, los mismos que permiten evaluar las vulnerabilidades mediante la identificación de debilidades provocadas por una mala configuración de las aplicaciones, analizar y categorizar dichas debilidades explotables y proveer recomendaciones en base a las propiedades de la organización, eliminar las vulnerabilidades y poder reducir el riesgo.

3.1 DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL DE USUARIO

La educación al usuario mediante normas y procedimientos es la base de seguridad en el primer nivel del modelo Defensa en Profundidad; es por ello que, en esta sección se desarrollará una guía práctica para el desarrollo de normas de seguridad en el GADMO, para crear confianza en las actividades de dicha entidad. (NTE INEN-ISO/IEC 27002, 2009)

3.1.1 ELABORACIÓN DEL MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27002

Gracias a los resultados obtenidos en el Análisis de Riesgos realizados en el capítulo anterior con la Metodología OSTMM, se podrá "determinar la acción de gestión adecuada y las prioridades para la gestión de los riesgos de la seguridad de la información, así como para implementar los controles seleccionados para la protección contra estos riesgos". (NTE INEN-ISO/IEC 27002, 2009)

En base a dichos resultados se ha propuesto crear esta guía de seguridad; la misma que tiene por objetivo mantener y mejorar la gestión de la seguridad de la información en la organización, así como también tener una concientización en los funcionarios del GADMO del buen uso de la información, y "el cumplimiento de requisitos legales, estatutos,

reglamentos y contractuales que debe cumplir la institución, sus socios comerciales, los contratistas y los proveedores de servicio, así como su entorno socio-cultural.” (NTE INEN-ISO/IEC 27002, 2009).

Una vez que se han identificado los requisitos y los riesgos de la seguridad y se han tomado las decisiones para el tratamiento de los riesgos, es conveniente seleccionar e implementar los controles para garantizar la reducción de los riesgos hasta un nivel aceptable. (NTE INEN-ISO/IEC 27002, 2009)

Se debe recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de la seguridad para apoyar las metas de la organización. (NTE INEN-ISO/IEC 27002, 2009)

Gobierno Autónomo Descentralizado Municipal del Cantón Otavalo		
GAD MUNICIPAL DEL CANTÓN OTAVALO	**Manual de Normas y Procedimientos de Seguridad de la Información**	Nuevo OTAVALO ADMINISTRACIÓN 2014 - 2019
Versión:	1.0	
Revisado por:	Ing. Luis López Ing. Marcelo Guerra	
Aprobado por:	Wilman Garcés. Director TIC´s	
Fecha de aprobación:		

I. Introducción

İ. Seguridad de la información

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversión y oportunidades del negocio.

a. Alcance

Implementar un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

b. Importancia

La seguridad de la información es importante para mantener la competitividad, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial de los procesos, los sistemas y redes que son activos importantes del negocio.

ii. Marco Referencial

a. Evaluación de riesgos

Los resultados de una evaluación de riesgos ayudarán a guiar y a determinar la acción de gestión adecuada y las prioridades para la gestión de los riesgos de la seguridad de la información, así como para implementar los controles seleccionados para la protección contra estos riesgos.

b. Gestión del riesgo

Decidir los criterios para determinar si se pueden aceptar o no los riesgos; en caso de aceptarlos la elección adecuada de controles, los mismos que se deberían seleccionar e implementar de modo que satisfaga los requisitos identificados por una evaluación de riegos.

iii. Políticas de seguridad

Es una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Esta a su vez establece las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

II. OBJETIVO

Establecer un proceso eficaz para la gestión de los incidentes de la seguridad de la información, mediante políticas, objetivos y actividades plasmado en un Manual de Normas y Procedimientos, mismo que permitirá una formación, educación y concienciación adecuada de todos los usuarios de los activos informáticos del Gobierno Autónomo Descentralizado del Cantón Otavalo.

III. RESPONSABILIDADES

Es responsabilidad del coordinador del departamento de TIC´s desarrollar, mantener y mejorar la gestión de la seguridad de la información en la institución; así como también divulgar mediante medios de difusión las políticas y procedimientos a todos los funcionarios, consiguiendo así una educación y concienciación de la responsabilidad de mantener la integridad, disponibilidad y confidencialidad de la información.

IV. VIGENCIA

El presente documento como manual de normas y procedimientos entrará en vigencia una vez aprobado por las autoridades pertinentes del GADMO. Dicho manual debe ser monitoreado, revisado y mejorado, donde sea necesario, para asegurar que se cumplan los objetivos de la seguridad y del negocio de la organización.

V. MARCO NORMATIVO

El presente documento se realizó en base a la Norma NTE INEN-ISO/IEC 27002; la misma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Cabe recalcar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de la seguridad para apoyar las metas de la organización.

VI. ESTRUCTURA

Este documento se encuentra estructurado en base a los siguientes dominios y controles que se tomaron de referencia de la Norma NTE INEN-ISO/IEC 27002:2009.

1. Política de la seguridad

1.1. Política de la seguridad de la información.

1.1.1. Documento de la política de la seguridad de la información.

1.1.2. Revisión de la política de la seguridad de la información.

2. Organización de la seguridad de la información.

2.1. Organización interna

2.1.1. Asignación de responsabilidades para la seguridad de la información.

2.2. Partes Externas

2.2.1. Identificación de los riesgos relacionados con las partes externas

VII. TÉRMINOS Y DEFINICIONES

Para el propósito de este documento se aplican los siguientes términos y definiciones:

Activo	Es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección.
Amenaza	Es un peligro posible que podría explotar una vulnerabilidad.
Ataque	Es un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado para eludir los servicios de seguridad y violar la política de seguridad de un sistema
Autenticidad	Es algo válido y utilizable.
Base de Datos	Es el conjunto de datos referentes a diversos temas y categorizados de diferente manera, pero que de una u otra forma están entrelazados entre si y se encuentran almacenados en un mismo contenido.
Confiabilidad	Es el grado de garantías en que las prácticas se han realizado tal y como se tenía planeados.
Confidencialidad	Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados.
Control	Medios para gestionar el riesgo, incluyendo políticas, procedimientos, prácticas o estructuras.
Controles criptográficos	Transforma el texto plano a datos ilegibles, para quienes no poseen los métodos ni permisos para restaurarlos.
Data Center	Es un espacio físico cuya función principal es alojar equipos informáticos con adecuados sistemas de energía, aire acondicionado y seguridad e informática y sus áreas de soporte.

Disponibilidad	Es un requisito necesario para garantizar que el sistema trabaje puntualmente, con prontitud y que se deniegue el servicio a ningún usuario no autorizado.
Gusanos	Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del computador.
Hardware	Son todos los componentes físicos, es decir, todo lo que se puede ver y tocar.
IEC	Es la Comisión Electrotécnica Internacional; la misma que participa en el desarrollo de las Normas Internacionales por medio de comités técnicos establecidos por la organización respectiva, para atender campos particulares de la actividad técnica.
Integridad	Garantiza que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la pérdida de consistencia.
Interceptación	Se refiere a detener algo en su camino; interrumpir una vía de comunicación; o apoderarse de algo antes de que llegue a su destino.
ISO	Es la Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales.
Medios ópticos	Son dispositivos de almacenamiento para grandes sistemas electrónicos de archivo.
No repudio	Proporciona protección contra la interrupción por parte de una de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación
Programas dañinos	Programas diseñados para entrar en el sistema operativo del computador, causando daños significativos sin su conocimiento.
Responsabilidad	Es el requisito que permite que pueda trazarse las acciones de una entidad de forma única.

Seguridad de la información	Prevención de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
Software	Son todos los programas y/o aplicaciones que permiten realizar tareas específicas; no existen físicamente, es decir, no se pueden ver ni tocar.
Software Antivirus	Es un programa que detecta, previene y toma medidas para eliminar programas de software malintencionados, como virus y gusanos.
UPS	Es un dispositivo que proporciona energía de respaldo cuando se dé un corte de energía en el suministro de la red eléctrica, por un cierto periodo de tiempo, evitando pérdida de información.
Usuario	Es aquella persona que utiliza los recursos del sistema de información y/o comunicación,
Virus	Son pequeños programas diseñados para propagarse de una computadora a otra e interferir con el funcionamiento de las mismas. Estos pueden propagarse a menudo a través de documentos adjuntos en mensajes de correo electrónico y en las descargas de internet.

VIII. DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD

Dominio	Política de la seguridad	**Destinatarios**
Objetivos de Control:	Política de la seguridad de la información	Equipo de trabajo de la Coordinación de TIC's
Control:	Documento de la política de la seguridad de la información	

Art. 1. La Coordinación de TIC's elaborará un Manual de Políticas de Seguridad de la Información, en el que se explique el cumplimiento de los requisitos legales y reglamentos, así como también, los requisitos de educación, formación y concienciación sobre seguridad y las consecuencias de las violaciones de dichas políticas.

Art. 2. El Manual de Políticas de Seguridad de la Información se deberá comunicar de manera pertinente, accesible y compresible para a todos los usuarios de los activos del GADMO.

Dominio	Política de la seguridad	**Destinatarios**
Objetivos de Control:	Política de la seguridad de la información	Equipo de trabajo de la Coordinación de TIC's
Control:	Revisión de la política de la seguridad de la información	

Art.3. La Coordinación de TIC's deberá asumir la responsabilidad de la revisión periódica de los lineamientos y del Manual de Políticas de Seguridad de la Información, para garantizar que éste siga siendo adecuado, suficiente y eficaz.

Art.4. Se definirán procedimientos programados para la revisión del Manual de Políticas de Seguridad de la Información, además se tomará en cuenta cambios significativos que pudieran afectar el entorno de la organización, incidentes reportados por los usuarios, recomendaciones de las autoridades y tendencias relacionadas con amenazas y vulnerabilidades

Dominio	Organización de la seguridad de la información.	**Destinatarios**
Objetivos de Control:	Organización interna	Equipo de trabajo de la Coordinación de TIC's
Control:	Asignación de responsabilidades para la seguridad de la información.	

Art. 5. La Coordinación de TIC's deberá definir claramente las responsabilidades de protección de activos individuales y para ejecutar procesos específicos de seguridad.

Art. 6. De ser necesario aquellos individuos responsables de la seguridad, pueden delegar las labores a otros. Sin embargo siguen siendo responsables y deben asegurarse de la correcta ejecución de las labores delegadas.

Dominio	Organización de la seguridad de la información.	**Destinatarios**
Objetivos de Control:	Partes Externas	Todos los usuarios
Control:	Identificación de los riesgos relacionados con las partes externas	

Art. 7. En caso de existir la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información, o a la información de la organización, se deberá definir el tipo de acceso físico y lógico que tendrá a oficinas, gabinetes de archivos, bases de datos y sistemas del GADMO.

Art. 8. Se determinarán diferentes medios de control utilizados para identificar, verificar y confirmar la autenticidad de la persona u organización externa que se vaya involucrar de manera directa con los activos del GADMO.

Art. 9. El acceso de las partes externas a la información del GADMO no se deberá brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y condiciones, requisitos legales y reglamentarios, y obligaciones para la continuación del acceso.

Dominio	Gestión de Activos	**Destinatarios**
Objetivos de Control:	Responsabilidad por los activos	Todos los usuarios
Control:	Inventario de activos	

Art. 10. Se deberá tener claramente identificados todos los activos de la dirección ya sean estos información, activos físicos, activos de software, servicios y personas; documentando toda la información necesaria de los mismo, tal como, el tipo de archivo, el formato, la ubicación, la información de soporte, la información sobre las licencias y el valor para el negocio.

Dominio	Seguridad de los recursos humanos	**Destinatarios**
Objetivos de Control:	Durante la vigencia del contrato laboral	Todos los usuarios
Control:	Educación, formación y concienciación sobre la seguridad de la información.	

Art. 11. Se emitirá información adecuado en concienciación y actualizaciones regulares sobre las políticas y los procedimientos del GADMO, considerando las funciones laborales en las que se desempeñan.

Art. 12. En caso de necesitarlo, será responsabilidad de cada usuario solicitar capacitación al personal de la Coordinación de TIC's capacitaciones en el manejo de paquetes informáticos utilizados en los equipos, con el propósito de evitar fallas que pongan en riesgo la seguridad de la información.

Art. 13. No será permitido en ningún momento la instalación, desinstalación de software en los equipos informáticos sin previa consulta al personal autorizado en Mantenimiento.

Art. 14. Será responsabilidad de cada usuario, realizar respaldos de sus datos, acorde a la importancia de los mismos.

Art. 15. Se presentará notificaciones inmediatas a la coordinación de TIC's en caso de cualquier falla en los sistemas, o por la mala manipulación de software o hardware de los equipos.

Dominio	Seguridad de los recursos humanos	**Destinatarios**
Objetivos de Control:	Terminación o cambio de la contratación laboral	Todos los usuarios
Control:	Devolución de activos	

Art. 16. Una vez culminado el contrato de trabajo, o cuando existe cambios de responsabilidades se deberá continuar durante un tiempo determinado con los términos y condiciones laborales, así como también con las responsabilidades contenidas en cualquier acuerdo de confidencialidad.

Art. 17. Todos los empleados, contratistas o usuarios de terceras partes deberán devolver todos los activos pertenecientes al GADMO que se encuentren en su poder al finalizar su contratación laboral, contrato o acuerdo.

Art. 18. Se deberá formalizar el proceso de terminación para iniciar la devolución de los documentos corporativos, equipos, dispositivos móviles, tarjetas de crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

Art. 19. Si un empleado, contratista o usuario de terceras partes utiliza un equipo del GADMO o utiliza su propio equipo, se deberá seguir los procedimientos necesarios para garantizar que toda la información se transfiera al GADMO y se elimine con seguridad de tal equipo.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Áreas seguras	Equipo de trabajo de la Coordinación de TIC's
Control:	Perímetro de la seguridad física	

Art. 20. Se deberá definir claramente los perímetros de la seguridad y la ubicación de cada lugar que contenga servicios de procesamiento de información y protegerlos con paredes externas, puertas con protección adecuada contra el acceso no autorizado con medidas de control tales como barras, alarmas, relojes, biométricos, etc.

Art. 21. Se deberá establecer un área de recepción con personal u otro medio para controlar el acceso físico a los sitios con acceso restringido.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Áreas seguras	Equipo de trabajo de la Coordinación de TIC's
Control:	Controles de acceso físico	

Art. 22. El ingreso al Data Center del GADMO será, única y exclusivamente al personal de la Coordinación de TIC´s. Éste será registrado con fecha y hora de entrada y salida.

Art. 23. Al personal de servicio de mantenimiento y/o soporte de terceras partes se le deberá dar acceso restringido al Data Center; es decir éste será autorizado previamente por el Coordinador de TIC´s, y será monitoreado por el mismo.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Áreas seguras	Directores GADMO
Control:	Seguridad de oficinas, recintos e instalaciones	

Art. 24. No se deberá tener indicaciones, o señales visibles que identifiquen la presencia de actividades de procesamiento de información.

Art. 25. Las listas telefónicas internas que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían estar a la vista y acceso al público.

Art. 26. Se deberá rediseñar y/o reubicar las oficinas y recintos de procesamiento de información, evitando el acceso al público a los mismos y considerando para ello los reglamentos y las normas pertinentes de seguridad y salud.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Áreas seguras	Equipo de trabajo Coordinación TIC´s
Control:	Protección contra amenazas externas y ambientales.	

Art. 27. El Data Center deberá contar con protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Seguridad de los equipos	Equipo de trabajo Coordinación TIC´s
Control:	Ubicación y protección de los equipos	

Art. 28. Se deberá aplicar protección contra rayos a todas las edificaciones del GAMO y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Servicios de suministro	Todos los usuarios
Control:	Ubicación y protección de los equipos	

Art. 29. Se deberá inspeccionar y someter a diferentes pruebas regularmente todos los servicios de suministro, sean estos, electricidad, calefacción/ ventilación y aire acondicionado; para garantizar su funcionamiento reduciendo cualquier riesgo debido a su mal funcionamiento o falla.

Art 30. Se deberá revisar con regularidad la disponibilidad del Sistema de alimentación ininterrumpida (SAI) y generadores eléctricos para dar soporte al funcionamiento continuo de equipos que soportan operaciones críticas para el negocio.

Art. 31. Se deberá evitar consumir alimentos y/o ingerir líquidos mientras se manipula equipos de cómputo, debido a que esto puede ocasionar daño en el equipo.

Art. 32. El usuario deberá tener cuidado de no pisar o maltratar los cables de conexiones tanto eléctricos como de red.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Servicios de suministro	Equipo de trabajo Coordinación TIC´s
Control:	Seguridad del cableado	

Art. 33. El cableado de red deberá estar protegido contra interceptación no autorizada o daño, utilizando conductos o evitando rutas a través de áreas públicas.

Art. 34. Con el fin de evitar interferencia se deberá mantener separados los cables de energía de los cables de comunicaciones.

Art. 35. Se deberá etiquetar claramente los equipos y cables, adicionalmente la elaboración de un plano de cableado ayudará a minimizar los errores en el manejo.

Dominio	Seguridad física y del entorno	**Destinatarios**
Objetivos de Control:	Servicios de suministro	Todos los Usuarios
Control:	Mantenimiento de los equipos	

Art. 36. Todas las estaciones de trabajo que requieran mantenimiento por problemas en el hardware y/o software deberán ser reparados únicamente por los miembros del Área de mantenimiento; los equipos que presenten fallas no deben ser manipulados por el usuario; de ser así serán retirados del mismo.

Art 37. El personal del área de mantenimiento deberá llevar un registro de todas las fallas reales o sospechosas y de todo el mantenimiento preventivo y correctivo.

Art. 38. Se deberá implementar un calendario de mantenimiento preventivo, considerando la información de garantías, licencias y fechas de adquisición.

Dominio	Gestión de comunicaciones y operaciones	**Destinatarios**
Objetivos de Control:	Procedimientos operacionales y responsabilidades	Todos los Usuarios
Control:	Documentación de los procedimientos de operación	

Art. 39. Se deberán elaborar manuales de procesamiento, los mismos que deben estar documentados y disponibles para todos los usuarios que los necesiten.

Art. 40. Los procedimientos de operación deberán especificar instrucciones para la ejecución detallada de trabajo, incluyendo:

- Procesamiento y manejo de información
- Copias de respaldo
- Requisitos de programación
- Instrucciones para el manejo de errores.
- Contactos de soporte en caso de dificultades técnicas
- Procedimiento para el reinicio y recuperación del sistema.

Dominio	Gestión de comunicaciones y operaciones	**Destinatarios**
Objetivos de Control:	Protección contra código malicioso y móviles	Todos los Usuarios
Control:	Controles contra códigos maliciosos	

Art. 41. Se recomienda no descargar, adquirir o utilizar software de dudosa procedencia, o de fuentes no confiables.

Art. 45. Todas las estaciones de trabajo, y servidores deberán tener instalado software antivirus activo y con sus respectivas actualizaciones.

Art. 43. Antes de usar archivos provenientes de medios ópticos o electrónicos, y descargas de correos electrónicos todos los usuarios deberán realizar detección y reparación de códigos maliciosos.

Dominio	Gestión de comunicaciones y operaciones	**Destinatarios**
Objetivos de Control:	Respaldo	Equipo de trabajo Coordinación TIC´s
Control:	Respaldo de la información	

Art. 44. El responsable de software dentro de la Coordinación de TIC´s, realizará copias de seguridad, considerando el tipo de información y la frecuencia con la que se debe realizar los respaldos acorde al tipo. Se ha clasificado de la siguiente manera:

Tipo de información	Frecuencia
BDD SQL Server	Diario
Código Fuente	En cada cambio de versión
Proyectos	Mensual, o al realizarse cambios importantes.
Informes e Investigaciones	Mensual
Actas, Memorándums, Oficios	Trimestral

Art. 45. Los respaldos se deberán almacenar únicamente en medios como: servidores, y discos duros externos.

Art. 46. Las copias de seguridad se realizarán al terminar la jornada de trabajo. En caso de ser automáticas de igual manera al final de la jornada laboral se revisará que se hayan completado con éxito.

Art. 47. Trimestralmente, se deberán realizar copias por duplicado, dichos respaldos serán entregados la Dirección Administrativa para mayor seguridad.

Dominio	Control del acceso	**Destinatarios**
Objetivos de Control:	Gestión del acceso de usuario	Todos los Usuarios
Control:	Registro de usuarios	

Art. 48. Todos los usuarios de la red del GADMO deberán contar con una identificación de usuario (ID), con la que se vinculará y se responsabilizará de sus acciones con el uso de sistemas o servicios de información

Art. 49. Los derechos de acceso a los usuario se delimitarán acorde a las funciones que desempeñen,

Art. 50. La coordinación de TIC's deberá emitir a todos los usuarios una declaración escrita de sus derechos de acceso.

Art. 51. Todos los usuarios deberán firmar ésta declaración, con lo que indicarán que entienden las condiciones a dichos accesos emitidos.

Dominio	Control del acceso	**Destinatarios**
Objetivos de Control:	Gestión del acceso de usuario	Todos los Usuarios
Control:	Gestión de contraseñas para usuarios.	

Art. 52. Se establecerá una contraseña temporal a todos los usuarios para ingreso a sistemas, previo a la verificación del ID; la misma que será única para cada individuo y no será descifrable.

Art. 53. Se exigirá a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales emitidas por la Coordinación de TIC´s.

Art 54. Las contraseñas emitidas por la Coordinación son temporales, el usuario deberá cambiarlas inmediatamente.

Art. 55. La longitud mínima en una contraseña se establece en 6 caracteres; sean estos alfanuméricos y especiales.

Art. 56. El formato de la contraseña establece que tenga una letra mayúscula, un alfanumérico, un especial y que no sobrepase los 15 caracteres.

Art. 57. Al tener contraseñas predeterminadas por el proveedor, estas deberán ser cambiadas de inmediato después de la instalación del sistema o software.

Dominio	Control del acceso	**Destinatarios**
Objetivos de Control:	Responsabilidades de los usuarios	Todos los Usuarios
Control:	Uso de contraseñas	

Art. 58. El personal de trabajo de la Coordinación de TIC´s emitirá una charla de las buenas prácticas de la seguridad en la selección y el uso adecuado de las contraseñas.

Art 59. Evitar conservar registros de las contraseñas en papeles o archivos que estén a la vista de cualquier usuario

Art.60. Es responsabilidad del usuario el cambio periódico de contraseña, evitando la reutilización de contraseñas antiguas. En caso de no saber hacerlo pedir asesoría en Coordinación de TIC's.

Sobre el uso del servicio de Internet del GADMO

Art. 61. Tienen derecho a solicitar acceso al uso de los Servicios de Internet en el GADMO:

a) El Alcalde/sa, las Concejalas y Concejales.
b) Los Directores/as
c) Los Jefes/as Departamentales.
d) Los empleados de las diferentes dependencias de la Municipalidad.
e) Las personas particulares y miembros de Instituciones que trabajen como resultado de acuerdos y convenios con la Municipalidad, siempre que lo soliciten con el respaldo escrito de la autoridad pertinente.

Art. 62. Las personas facultadas para el uso del internet velarán por su efectiva, eficiente y correcta utilización, caso contrario será sancionado y se les quitará el derecho a ser usuarios del mismo.

Art. 63. El uso del servicio de internet debe ser exclusivamente para actividades del GADMO.

Art. 64. El GADMO podrá suspender el servicio de internet o cancelar la cuenta de correo electrónico por mal manejo, sin perjuicios de imponer las sanciones correspondientes según la gravedad de la falta.

De la asignación de cuentas de correo electrónico institucional.

Art. 65. La utilización de las cuentas de correo se hace a través de una cuenta electrónica personal e intransferible para cada usuario creado para tal fin en el servidor de comunicaciones de la Municipalidad.

Art. 66. Es responsabilidad grave de cada usuario proteger su clave de acceso personal a la cuenta de correo, manteniéndola en estricto secreto, con la finalidad de evitar que cualquier otra persona la utilice para fines contrarios a lo establecido por este Manual de Normas y Procedimientos.

Art. 66. Todo menaje enviado desde la dirección de correo electrónico del usuario es de total responsabilidad del mismo, aunque no haya sido enviado personalmente por él.

Art. 67. El GADMO no se hace responsable por lo que se haga o diga en nombre de una cuenta particular; por lo cual está prohibido el uso de cuentas por personas ajenas a su titular. Por lo tanto, cada usuario debe:

a) No dar a conocer su clave secreta a ninguna personas, por ningún motivo, ni compartir su acceso con otros usuarios.
b) No abandonar, ni alejarse físicamente de su estación de trabajo, sin antes cerrar sesión de la cuenta de correo electrónico.
c) Procurar que nadie pueda fijarse en la secuencia de teclas que se pulsan al escribir la clave de acceso
d) No escribir la contraseña en un papel, ni tenerla en lugares visibles o evidentes.
e) Deberá notificar de manera fehaciente e inmediata a la Coordinación de TIC's, cualquier uso no autorizado de su cuenta o cualquier otra vulneración de su seguridad

Art. 68. Es responsabilidad grave de cada usuario utilizar el Internet de acuerdo a la ética y a las leyes y reglamentos pertinentes, por tanto:

a) El usuario es el único responsable de todas las acciones y mensajes que se lleven a cabo en su nombre. Todo mensaje enviado por su usuario debe incluir su identificación.
b) El uso de leguaje inapropiado u ofensivo, en mensajes privados o públicos.
c) El uso de los servicios para asuntos particulares, actividades no relacionadas al GADMO, para el beneficio particular de terceras personas o de instituciones que no tengan autorización o cuerdos con el GADMO, o para cualquier finalidad que no concuerde con el espíritu de esos acuerdos.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Procesamiento correcto en las aplicaciones	Área de Desarrollo de proyectos
Control:	Validación de los datos de entrada	

Art. 69. Los desarrolladores de proyectos y software, diseñarán controles apropiados en las aplicaciones, para garantizar el procesamiento correcto de las mismas, considerando:

a) La verificación de los datos de entrada, con el fin de detectar los siguientes errores:
   i. Valores fuera de rango.
   ii. Caracteres no válidos en los campos de datos
   iii. Datos incompletos o ausentes
   iv. Exceso en los límites superiores e inferiores del volumen de datos
   v. Datos de controles inconsistentes o no autorizados.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Procesamiento correcto en las aplicaciones	Área de Desarrollo de proyectos
Control:	Control de procesamiento interno	

Art. 70. Los desarrolladores de proyectos y software, deberán incorporar verificaciones en las aplicaciones para detectar cualquier daño o pérdida de la información por errores de procesamiento o actos deliberados. Las áreas específicas que se han de considerar incluyen:

a) Utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos.
b) Procesamientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de una falla previa del procesamiento
c) Utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos.
d) Protección contra ataques empleando desbordamiento / exceso en el búfer.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Controles criptográficos	Equipo de trabajo de Coordinación de TIC's
Control:	Política sobre el uso de controles criptográficos	

Art. 71. La coordinación de TIC's deberá enfocarse hacia el uso de controles criptográficos en todo el GADMO, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio.

Art. 72. La coordinación de TIC's será el área responsable de implementar una política de controles criptográficos, y de la generación y gestión de claves.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Controles criptográficos	Equipo de trabajo de Coordinación de TIC's
Control:	Gestión de claves	

Art. 73. Se deberán establecer métodos criptográficos que generen claves que tengan protección contra modificac ión, pérdida, destrucción y divulgación no autorizado

Art.74. Se deberá contar con un sistema de gestión de claves basado en un conjunto de normas, procedimientos y métodos seguros para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;
b) Generar y obtener certificados de claves públicas
c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves;
d) Cambiar o actualizar las claves incluyendo reglas de cuando cambiarlas y cómo hacerlo;
e) Recuperar claves pérdidas o corruptas como parte de la gestión de continuidad del negocio.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Seguridad de los archivos del sistema	Equipo de trabajo de Coordinación de TIC's
Control:	Control del software operativo	

Art. 75. Únicamente el personal autorizado por la Coordinación de TIC's puede realizar la actualización del software operativo, las aplicaciones y las bibliotecas de los programas.

Art. 76. Los sistemas operativos únicamente se deberán mejorar cuando existe una necesidad para hacerlo, por ejemplo cunado la versión actual del sistema operativo ya no da soporte a los requerimientos del negocio.

Art. 77. Si es necesario la actualización de software suministrado externamente, dicha actualización deberá ser monitoreada y controlada para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

Art. 78. Como medida de contingencia será necesario la activación de versiones antiguas de software de aplicación.

Art. 79. Antes de la actualización de sistema operativo, se deberá restaurar el sistema al estado anterior por motivos de seguridad.

Dominio	Adquisición, desarrollo y mantenimiento de sistemas de información	**Destinatarios**
Objetivos de Control:	Gestión de la vulnerabilidad técnica	Equipo de trabajo de Coordinación de TIC's
Control:	Control de las vulnerabilidades técnicas	

Art. 80. Se deberá obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso.

Art. 81. Se deberá evaluar la exposición del GADMO a las vulnerabilidades técnicas de los sistemas de información y tomar las acciones apropiadas para tratar los riesgos asociados

Art. 82. Se deberá definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potencialmente pertinentes.

Art. 83. Se deberá probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables.

Dominio	Gestión de los incidentes de la seguridad de la información	**Destinatarios**
Objetivos de Control:	Gestión de los incidentes y las mejoras en la seguridad de la información	Todos los usuarios
Control:	Reporte sobre los eventos de seguridad de la información	

Art. 84. Todos los empleados, contratistas y usuarios deberán tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos d la organización.

Art. 85. La coordinación de TIC's deberá elaborar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información.

Art. 86. Se considerará un evento o incidente se seguridad que debe ser reportado los siguientes:

a) Pérdida del servicio, del equipo o de las prestaciones;
b) Mal funcionamiento o sobrecarga del sistema;
c) Errores humanos;
d) Incumplimiento de las políticas o de las directrices;
e) Violación de las disposiciones de seguridad física;
f) Cambios no controlados ene le sistema;
g) Mal funcionamiento del software o del hardware;
h) Violaciones del acceso

Art 87. Deberá darse soluciones rápidas, oportunas y eficientes a todos los incidentes de seguridad reportadas en las estaciones de trabajo.

Art. 88. Todas las anomalías deberán ser documentadas con el objetivo de verificar la notificación y generar respuestas eficientes.

Dominio	Gestión de la continuidad del negocio Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.	**Destinatarios**
Objetivos de Control:	Gestión de los incidentes y las mejoras en la seguridad de la información	Todos los usuarios
Control:	Continuidad del negocio y evaluación de riesgos.	

Art. 89. Se deberá identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Art. 90. Se deberán efectuar con plena participación de los responsables de los recursos y los procesos del GADMO, evoluciones de riesgos para la continuidad del negocio.

Dominio	Cumplimiento	**Destinatarios**
Objetivos de Control:	Cumplimiento de los requisitos legales	Equipo de trabajo de la Coordinación de TIC's
Control:	Derechos de propiedad intelectual	

Art. 91. Se adquirirá software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia.

Art. 92. Se deberá mantener pruebas y evidencias sobre la propiedad de licencias, discos maestros, manuales, etc.

Art. 93, Se deberá implementar un registro del uso de las licencias, para no exceder el número de usuarios permitidos que puedan usar las mismas.

Art. 94. Se deberá verificar que únicamente se instalen software autorizado y productos con licencias originales.

Dominio	Cumplimiento	**Destinatarios**
Objetivos de Control:	Cumplimiento de los requisitos legales	Equipo de trabajo de la Coordinación de TIC's
Control:	Protección de los registros de una organización	

Art. 95. Se deberán clasificar los registros según si tipo así:

a) Registros de contabilidad,
b) Registros de bases de datos
c) Registros de transacciones
d) Registros de auditoria

Una vez clasificados éstos deberán ser almacenados en medios como papel, medios magnéticos, ópticos, etc.

Art. 96. Se deberán implementar controles para proteger todos los tipos de registros contra pérdida, destrucción y falsificación.

Dominio	Cumplimiento	**Destinatarios**
Objetivos de Control:	Cumplimiento de las políticas y las normas de la seguridad y cumplimiento técnico	Todos los usuarios
Control:	Cumplimiento con las políticas y normas de seguridad	

Art. 97. La Coordinación de TIC's será la responsable de supervisar el cumplimiento de las política y lineamientos del GADMO.

Art. 98. En caso de infracciones leves de las normas y cualquier otro requisito de seguridad serán juzgados y sancionados por el Alcalde y/o Director Administrativo previo al informa técnico del Coordinador de TIC's.

Art. 99. En caso de infracciones graves de las normas y cualquier otro requisito de seguridad será juzgado y sancionado por el Alcalde previo al informe del Director Administrativo de acuerdo a la ley del GADMO.

Art. 100. Se considerarán como infracciones graves, una vez analizado por el Director Administrativo, personal Jurídico y Administradores TIC's, el incumplimiento al reglamento las siguientes:

a) Enviar mensajes para la difusión de noticias o correo electrónico sin identificar plenamente a su autor o autores, o enviar anónimos;

b) No hacer un uso racional, eficiente y considerado de los recursos disponibles tales como: el espacio en disco, memoria, red informática, entre otros;

c) Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso propio de trabajo;

d) Acceder a cualquier tipo de comunicaciones ente usuarios, como los CHAT, NEWS GROUP, MESSENGER, CORREO PERSONAL, etc.

e) Descargar archivos o correo electrónico sin la debida precaución de revisión de virus informáticos.

f) Intentar apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, y en especial los pertenecientes a la Municipalidad u otras Instituciones.

g) Usar los servicios de internet para propósitos no municipales o usarlos para propósitos fraudulentos, comerciales o publicitarios, o para la propagación de mensajes destructivos u obscenos.

h) Intentar acceder a computadora, servidores o cuentas de usuario con acceso restringido(utilizando cualquier protocolo, telnet, ftp, etc.; aunque no se consiga el acceso)

i) Decodificar el tráfico de red o cualquier intento de obtención de información confidencial que se trasmita a través de la misma

j) Modificar la configuración de los programas de comunicaciones de los computadores o servidores de red.

k) Ejecutar programas obtenidos a través de internet u otro medio en los computadores sin autorización de la Coordinación de TIC's.

l) Cualquier uso malicioso, violento u obsceno de la red.

m) El uso de internet para ver u obtener archivos de video, páginas pornográficas, música, juegos.

n) Escribir mensajes de contenido fascista, racista, machista, insultante o que puedan herir la sensibilidad de las personas.

o) Dispersar virus, gusanos y otros tipos de programas dañinos para sistemas de procesos de la información.

p) Transmitir cualquier tipo de información confidencial o propia de la Municipalidad bajo cualquier medio sin la debida autorización.

q) Leer, revisar, interceptar, modificar o destruir cualquier tipo de comunicación oficial y confidencial del usuario o de cualquier otra persona o entidad, sin el consentimiento respectivo del remitente y del destinatario de la comunicación.

r) Suscribirse a listas de correo electrónico o que participen en grupos de noticias que divulguen información o mensajes ajenos a las funciones y deberes del usuario sin la debida autorización.

s) No cumplir con los avisos de precaución emitidos por la Coordinación de TIC's

IX. DESARROLLO DE PROCEDIMIENTOS DE SEGURIDAD

En esta sección se describen los procedimientos más significativos para conservar la seguridad de la información del GADMO, con la finalidad de organizar todas las actividades ejecutadas por los usuarios de la municipalidad que conlleven consigo un manejo responsable de los activos informáticos, ya sean físicos o lógicos, promoviendo de esta manera las buenas prácticas de seguridad de la información.

Procedimiento:	Soporte técnico para usuarios de Sistemas de Información		
Objetivo	Brindar soluciones eficaces y eficientes a los problemas presentados por los usuarios de sistemas de información, mediante asesoría técnica por parte del personal de trabajo de la Coordinación de TIC´s.		
Frecuencia	Imprevista	**Código**	CTIC-PRO-01

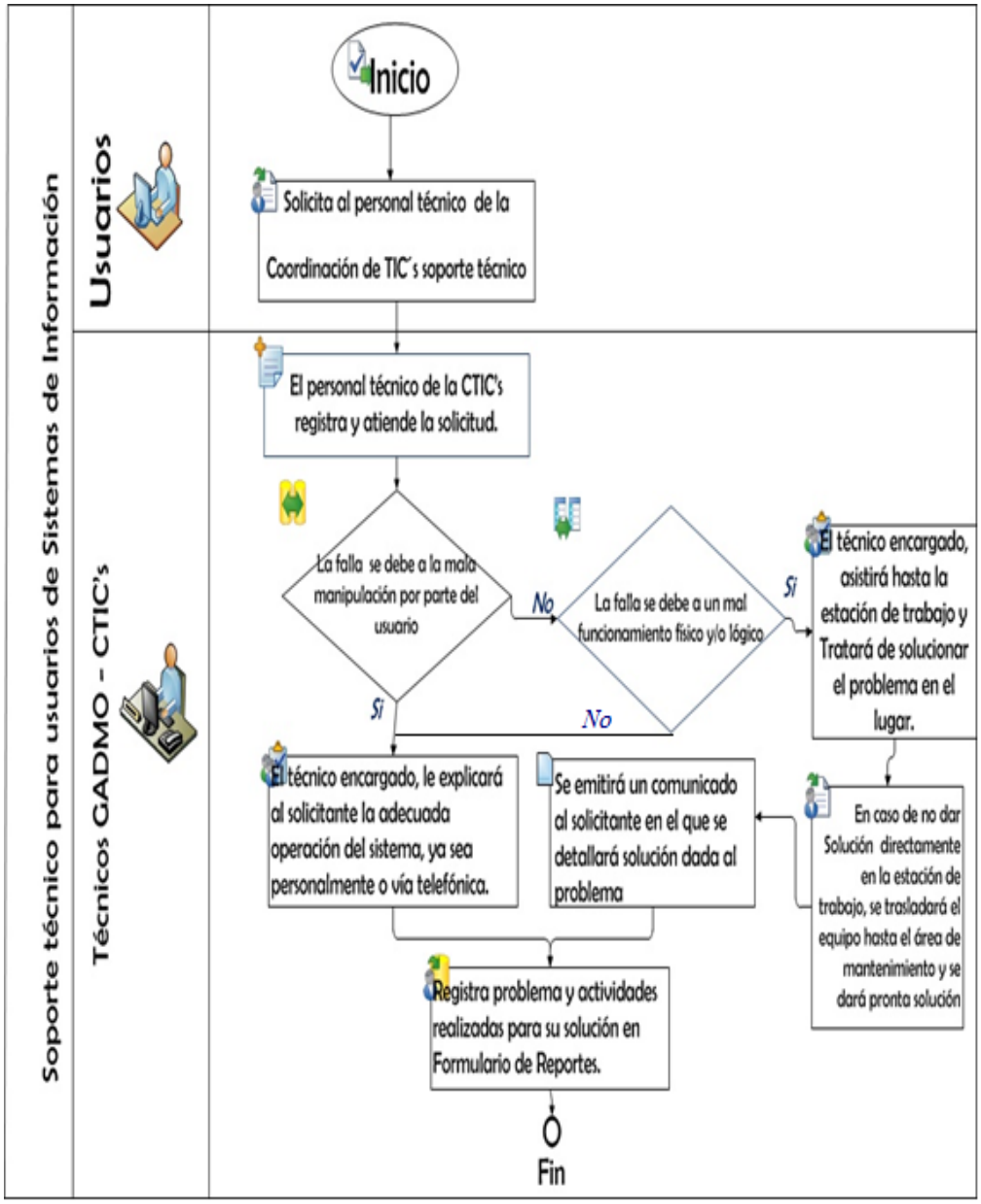
1. Desarrollo de actividades

N° Acción	Descripción
1	En caso de tener inconvenientes en las operaciones de los sistemas de información, el usuario mediante una llamada o de forma personal solicitará al personal técnico de la Coordinación de TIC´s asesoría técnica.
2	El usuario deberá llenar una solicitud de soporte técnico en el formato "**SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS INFORMÁTICOS**"
3	El personal técnico de la TIC's registra y atenderá la solicitud.
4	El tipo de solución dependerá de la causa del soporte técnico solicitado:

Acción	**Reacción**
Si la falla se debe a la mala manipulación por parte del usuario en las operaciones de los sistemas de información	Explicarle al solicitante la adecuada operación del sistema, ya sea personalmente o vía telefónica.
Si la falla se debe a un mal funcionamiento físico y/o lógico.	Se deberá asistir hasta la estación de trabajo y tratar de solucionar el problema en el lugar.
Si no se puede solucionar directamente en la estación de trabajo	Se trasladará el equipo hasta el área de mantenimiento y se dará pronta solución

5	Una vez solucionado el problema se emitirá un comunicado al solicitante en el que se detallará la solución dada al problema
6	Registra problema y actividades realizadas para su solución en Formulario de Reportes.
7	**Fin del procedimiento**

2. **Diagrama de flujo**



3. Anexo

Formato "**SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS INFORMÁTICOS**"

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de TIC's soporte técnico para los inconvenientes que se les presente, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

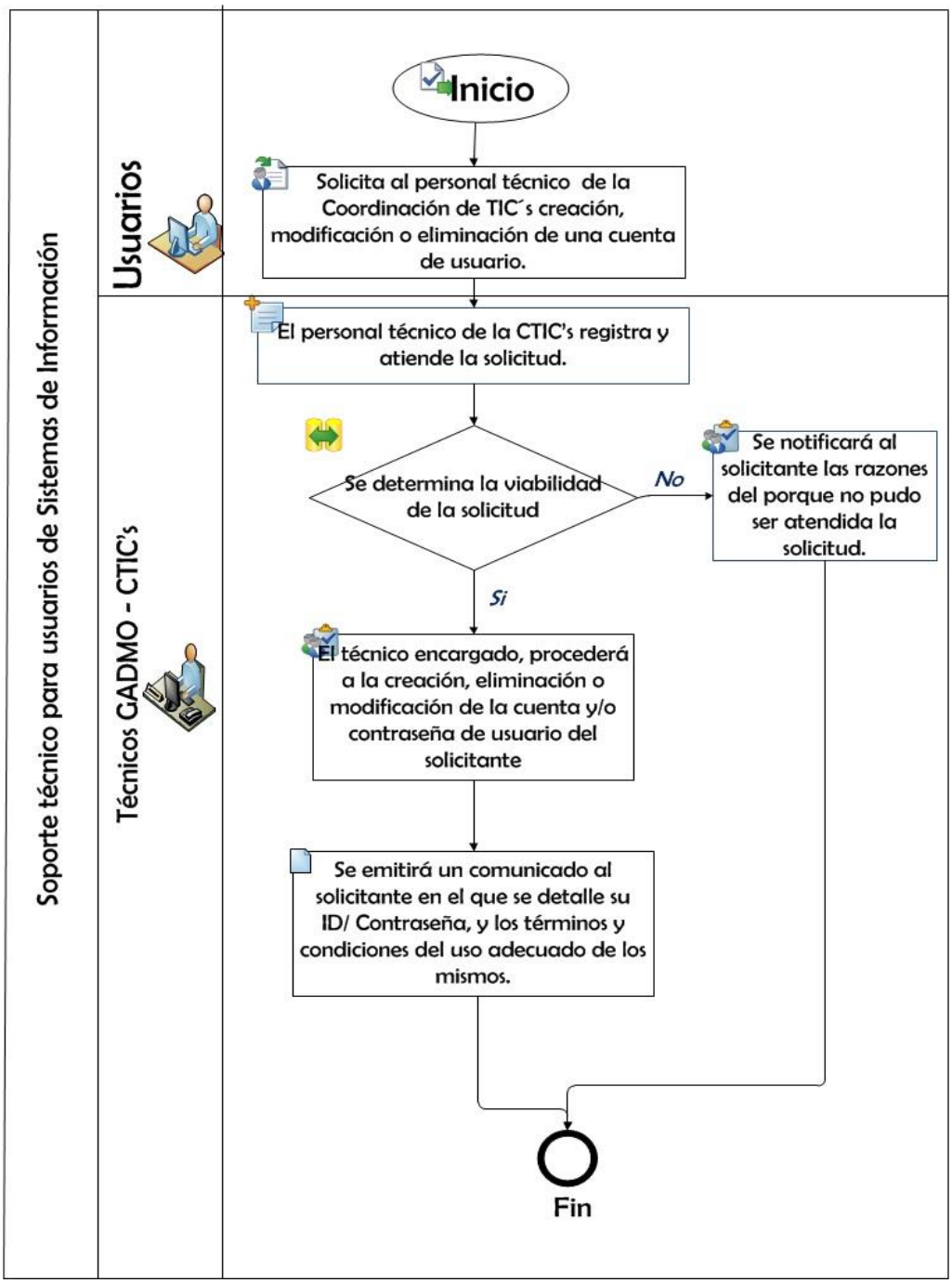
"**SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS INFORMÁTICOS**"								N° 0000
Fecha de solicitud	Día	Mes	Año	*Solicitante:*		***Dependencia:***		
Tipo de solicitud				Adquisición		Tutoría		
				Actualización		Cambio		
				Mantenimiento		Reparación		
Tipo	Equipo			***Características***	Marca			
	Accesorio				N° Serie			
	Software				Responsable			
	Tema tutoría				Tema			
Descripción breve de su solicitud: _____ _____								
Fecha de recibida la solicitud	Día	Mes	Año	***Nombre de quien recibe la solicitud***			***Hora: - -:- -***	
Para uso exclusivo del Coordinador de TIC´s								
Fecha asignación	Día	Mes	Año	***Hora***	_ _ : _ _	***Técnico Responsable***		
Para uso exclusivo del técnico responsable								
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma:***		
Descripción breve del trabajo realizado _____ _____								
Para uso exclusivo del usuario solicitante. Puede entregarlo al Coordinador de TIC´s para su evaluación								
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma de Recibido:***		
El trabajo fue satisfactorio								
Fueron resueltas sus dudas e inconvenientes								
Recomendaciones: _____								

Procedimiento:	Creación de cuentas de usuario		
Objetivo	Integrar a los servicios de comunicaciones del GADMO a los usuarios acorde a las necesidades de las áreas de la Institución.		
Frecuencia	Casual	**Código**	CTIC-PRO-02

1. Desarrollo de actividades

N° Acción	Descripción
1	Al iniciar operaciones como nuevo usuario del GADMO, teniendo ya una estación de trabajo, o al tener obligaciones asignadas para determinada actividad; que requiera la asignación de una cuenta de usuario, ya sea para bases de datos institucionales, correo electrónico y/o acceso a sistema operativo.
2	El usuario deberá llenar y enviar a la coordinación de TIC's la solicitud de **"CREACIÓN, MODIFICACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIO"**
3	El personal técnico de la TIC's registra y atenderá la solicitud.
4	El personal encargado, determinará si es viable la creación de usuario desentendiendo del cargo que ostente el solicitante, y del acceso que según este deba tener a los sistemas de bases de datos.
5	Si es viable, se procederá a la creación de un usuario y/o contraseña para el debido acceso. Si no es viable se notificará al solicitante las razones del porque no pudo ser atendida la solicitud.
6	Una vez creado el usuario y/o contraseña se le notificará el solicitante los mismos, previo a una explicación de los términos y condiciones del uso adecuado de los mismos.
7	**Fin del procedimiento**

2. Diagrama de flujo



3. Anexo

Formato "**SOLICITUD DE CREACIÓN, MODIFICACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIO**"

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de TIC's la creación, modificación y eliminación de cuentas de usuario, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

Solicitud De Creación De Cuentas De Usuario	N° 00000

De: _____ Para: _____

Jefe o Director de departamento Coordinador de TIC's

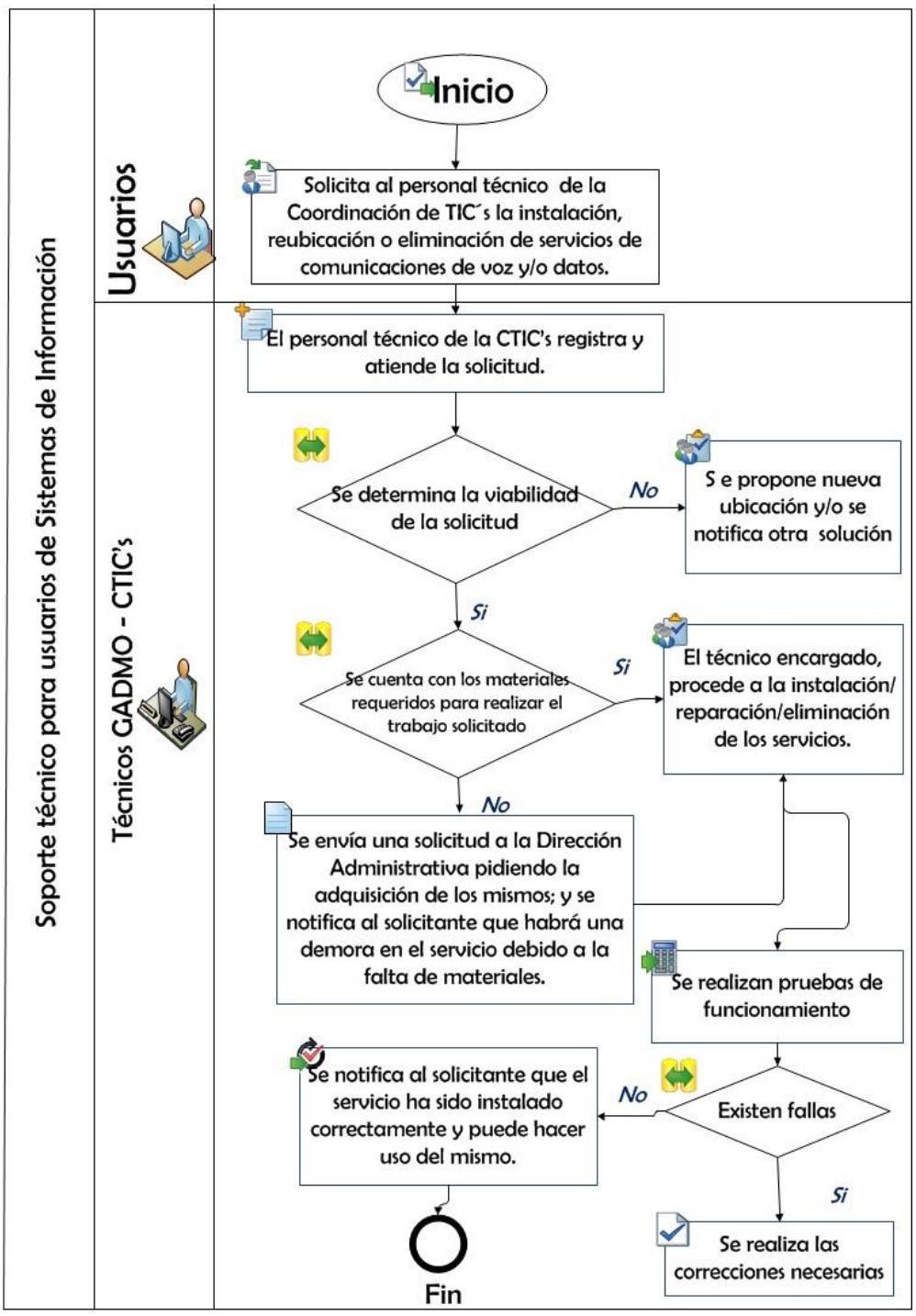
Fecha de solicitud	Día	Mes	Año	*Hora*	_ _ : _ _
Tipo de solicitud	Creación		***Tipo de servicio***	Correo electrónico	
	Modificación			Bases de datos	
	Eliminación			Sistema operativo	
Datos del usuario beneficiario del ID y Contraseña					
Nombres Completos			*C.I.*		
Cargo:					
Para uso exclusivo del Coordinador de TIC´s					
Fecha asignación	Día	Mes	Año	***Hora***	_ _ : _ _
Técnico Responsable					
Para uso exclusivo del técnico responsable					
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _
Firma:					
Nombre del Solicitante					
Cargo:					
Para uso exclusivo del usuario solicitante.					
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _
Firma de Recibido:					
ID de Usuario			***Contraseña***		
Servicio					
ID de Usuario			***Contraseña***		
Servicio					
ID de Usuario			***Contraseña***		
Servicio					

Procedimiento:	Instalación de servicios de voz e internet		
Objetivo	Integrar a la infraestructura de comunicaciones del GADMO a los usuarios, de acuerdo a las necesidades de las áreas de la institución.		
Frecuencia	Casual	**Código**	CTIC-PRO-03

1. Desarrollo de actividades

N° Acción	Descripción
1	Se enviará una solicitud a la coordinación de TIC's de **"SOLICITUD DE SERVICIOS DE COMUNICACIONES"**
2	El personal técnico de la TIC's registra y atenderá la solicitud.
3	Evalúa la solicitud y la viabilidad de la misma. ¿Es viable la ubicación para la instalación?
4	Si no es viable; se propone nueva ubicación y/o se notifica otra solución.
5	Si es viable; en caso de contar con los materiales requeridos se procede a la instalación/reparación/eliminación de los servicios.
6	Si es viable; y no se cuenta con los materiales requeridos; Se envía una solicitud a la Dirección Administrativa pidiendo la adustión de los mismos; y se notifica al solicitante que habrá una demora en el servicio debido a la falta de materiales. Una vez que se tenga los materiales se procede a la instalación/reparación/eliminación de los servicios.
7	Pruebas de instalación
8	Si existen fallas, se realiza las correcciones necesarias. Caso contrario se notifica al solicitante que el servicio ha sido instalado correctamente y puede hacer uso del mismo.
9	**Fin del procedimiento**

2. Diagrama de flujo



3. Anexo

Formato "**SOLICITUD DE SERVICIOS DE COMUNICACIONES"**

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de TIC's la instalación, reubicación o eliminación de servicios de voz y datos, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

Solicitud de Instalación de Servicios de Comunicaciones	N° 00000

De: _____ Para: _____

Jefe o Director de departamento — Coordinador de TIC's

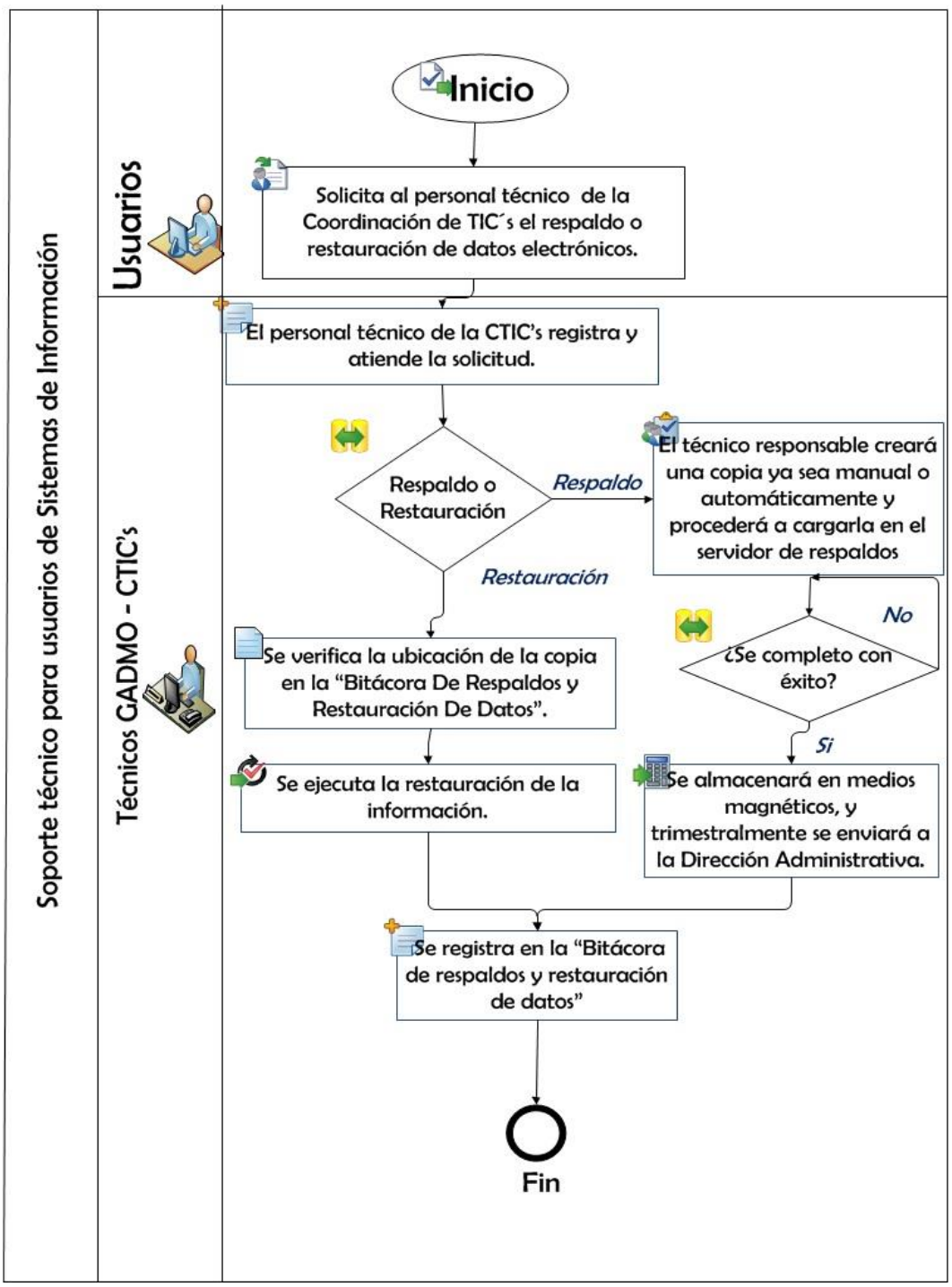
Fecha de solicitud	Día	Mes	Año	*Hora*	_ _ : _ _		
Tipo de solicitud	Creación			***Tipo de servicio***	Datos		
	Re-ubicación						
	Eliminación				Voz		
Datos del usuario beneficiario del Servicio							
Nombres Completos				*C.I.*			
Cargo:							
Para uso exclusivo del Coordinador de TIC´s							
Fecha asignación	Día	Mes	Año	***Hora***	_ _ : _ _	***Técnico Responsable***	
Para uso exclusivo del técnico responsable							
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma:***	
Nombre del Solicitante				***Trabajo realizado***	*Instalación*		
N° Puntos de voz		*N° Puntos de datos*			*Reubicación*		
Para uso exclusivo del usuario solicitante. Puede entregarlo al Coordinador de TIC´s para su evaluación							
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma de Recibido:***	
El trabajo fue satisfactorio							
Fueron resueltas sus dudas e inconvenientes							
Recomendaciones: _____							

Procedimiento:	Respaldo y Restauración de Datos de los usuarios del GADMO		
Objetivo	Avalar la integridad y disponibilidad de los datos electrónicos; mediante el respaldo de los mismos en medios magnéticos y/o virtuales, con la finalidad de evitar pérdida o modificación de éstos.		
Frecuencia	Casual	**Código**	CTIC-PRO-04

1. Desarrollo de actividades

N° Acción	Descripción
1	Si los usuarios requieren el respaldo y/o restauración de sus datos electrónicos, entonces llenarán y enviarán a la Coordinación de TIC's una **"SOLICITUD DE COPIAS DE SEGURIDAD DE INFORMACIÓN"**
2	El personal técnico de la TIC's registra y atenderá la solicitud.
3	Evaluará si es un respaldo o restauración de información.
4	Si es una copia, entonces, el técnico responsable creará una copia ya sea manual o automáticamente y procederá a cargarla en el servidor de respaldos.
5	Se verifica si la copia se realizó completamente y sin errores. De ser así esta se almacenará en medios magnéticos, y trimestralmente se enviará a la Dirección Administrativa y se registra en la "**BITÁCORA DE RESPALDOS Y RESTAURACIÓN DE DATOS.** ". Caso contrario se realizará la copia nuevamente.
6	Si es restauración de la información, se verifica la ubicación de la copia en la "Bitácora De Respaldos Y Restauración De Datos".
7	Se ejecuta la restauración de la información.
8	Se registra el trabajo realizado en le Bitácora de respaldos y restauración de datos.
9	**Fin del procedimiento**

2. Diagrama de Flujo



3. ANEXOS

Formato "**SOLICITUD DE COPIAS DE SEGURIDAD DE INFORMACIÓN"**

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de TIC's, respaldo y restauración de datos, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

Solicitud de Copias de Seguridad de Información	N° 00000

De: _____ Para: _____

Jefe o Director de departamento — Coordinador de TIC's

Fecha de solicitud	Día	Mes	Año	*Hora*	_ _ : _ _		
Nombre del solicitante				***Tipo de solicitud***	Respaldo		
Cargo:					Restauración		
Tipo de información	Confidencial			No confidencial			
	Software	Bases de datos	Sistemas de información	Otros			
Para uso exclusivo del Coordinador de TIC´s							
Fecha asignación	Día	Mes	Año	***Hora***	_ _ : _ _	***Técnico Responsable***	
Para uso exclusivo del técnico responsable							
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma:***	
				Trabajo realizado	*Respaldo*		
Nombre del Solicitante					*Restauración*		
Para uso exclusivo del usuario solicitante. Puede entregarlo al Coordinador de TIC´s para su evaluación							
Fecha entrega	Día	Mes	Año	***Hora***	_ _ : _ _	***Firma de Recibido:***	
El trabajo fue satisfactorio							
Fueron resueltas sus dudas e inconvenientes							
Recomendaciones:							

_____

Formato **"BITÁCORA DE RESPALDO Y RESTAURACIÓN DE DATOS"**

Por medio de esta bitácora se llevará un registro y control de los respaldos y restauraciones de los datos electrónicos.

BITÁCORA DE RESPALDO Y RESTAURACIÓN DE DATOS							N° 00000
Fecha	Día	Mes	Año	Hora Inicio	_ _ : _ _	Hora finalización	_ _ **:** _ _
Responsable:					Firma:		
Tipo de servicio				Respaldo			
				Restauración			
Descripción de Recursos a Respaldar							
Bases de datos			Base Alfanumérica		Base Binaria		Base Especial
Software			Nombre				Versión
Sistemas de información			Nombre			Tipo o extensión	
Otro							
Ubicación del servidor							
Nombre servidor			Dirección IP			Código DVD	
Directorio							

Resultado y/o Observaciones:

_____

_____

_____

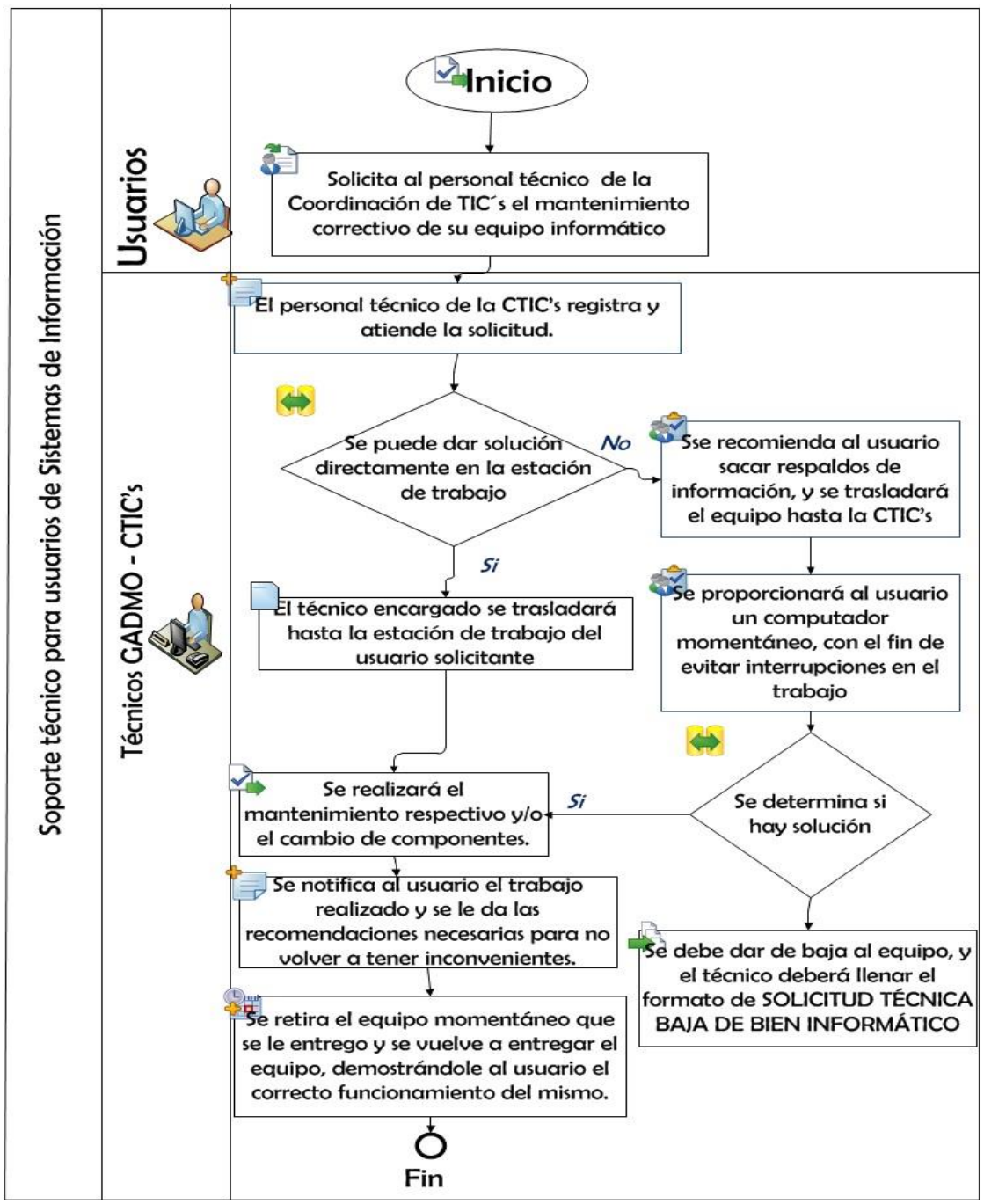
Coordinador TIC's

Procedimiento:	Mantenimiento Correctivo		
Objetivo	Cuidar de la funcionalidad de los equipos de cómputo de todas las dependencias del GADMO, mediante un mantenimiento correctivo y oportuno, con la finalidad de mantener operativos dichos equipos.		
Frecuencia	Casual	**Código**	CTIC-PRO-05

1. Desarrollo de actividades

N° Acción	Descripción
1	El usuario deberá llenar una solicitud de soporte técnico en el formato "**SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS INFORMÁTICOS**"
2	El personal técnico de la TIC's registra y atenderá la solicitud.
3	Se determinará si se puede dar solución directamente en la estación de trabajo. Caso contrario se recomienda al usuario sacar respaldos de información, y se trasladará el equipo hasta la CTIC's.
4	Mientras se da una solución se deberá proporcionar al usuario un computador momentáneo, con el fin de evitar interrupciones en el trabajo.
5	Al llevar el equipo hasta la CTIC's, se determina si se puede solucionar el problema mediante mantenimiento o cambio de componentes. Si no es así se debe dar de baja al equipo, y el técnico deberá llenar el formato de **SOLICITUD TÉCNICA BAJA DE BIEN INFORMÁTICO**
6	En caso de tener solución, se realizará el mantenimiento respectivo y/o el cambio de componentes.
7	Se notifica al usuario el trabajo realizado y se le da las recomendaciones necesarias para no volver a tener inconvenientes. Se retira el equipo momentáneo que se le entrego y se vuelve a entregar el equipo, demostrándole al usuario el correcto funcionamiento del mismo.
8	**Fin del procedimiento**

2. Diagrama de Flujo



3. Anexo

SOLICITUD TÉCNICA BAJA DE BIEN INFORMÁTICO					N° 00000
Fecha :	Día	Mes	Año	*Dependencia :*	
Responsable:			Firma:		

Característica Equipo Informático						
Marca	Modelo	N° Serie	Valor estimado	Motivo de Baja	Dañado	
					Desuso	
					Irreparable	

Observaciones y/o Descripción:

_____

_____

_____

_____

_____

_____

_____

_____ _____

Jefe de Bodega. Coordinador TI´S

_____ _____

Técnico Responsable Solicitante.

3.2 DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL PERIMETRAL

En este subcapítulo se describen las características y funciones del software Suricata, que fue el escogido para el diseño del IDS/IPS sobre software libre, además se describe el proceso para su elaboración, definiendo los parámetros de configuración necesarios para su correcto funcionamiento. Adicionalmente se describe las características del Firewall tanto físico como lógico del GADMO, así como su configuración. Finalmente se describirá las aplicaciones de la granja de servidores y la propuesta de la configuración de una DMZ, que permita minimizar los riesgos de seguridad en la institución.

3.2.1 IDS/ IPS

3.2.1.1 SOFTWARES DE SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS.

Para la elección Suricata como el IDS/IPS, previamente se realizó una comparación con otros softwares, la misma que se presenta en la Tabla 3-1

TABLA 3.1: Comparación de los diferentes softwares libres y comerciales de IDS/IPS.

CARACTERÍSTICAS	SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS			
	BRO	SNORT	SOLUCIONES COMERCIALES	SURICATA
Multi-Hilos	No	No	No	Si
Soporte para IPv6	Si	Si	Cisco, IBM, Stonesoft	Si
IP Reputation	Algo	No	Cisco	Si
Detección automática de protocolos	Si	No	No	Si
Aceleración con GPU	No	No	No	Si
Variables Globales/Flowbits	Si	No	No	Si
Análisis Avanzado de HTTP	Si	No	No	Si
HTTP Access Logging	Si	No	No	Si
SMB Access Logging	Si	No	No	Si
Anomaly Detection	No	No	Si	No
Alta Disponibilidad	No	No	Si	No
GUI de Administración	No	No	Si	No
Gratis	Si	Si	No	Si

Fuente: Elaborada por Andrea Zura

En base a esta comparación realizada, se definió además un análisis FODA del software elegido; el mismo que se presenta en la Figura 3-1.

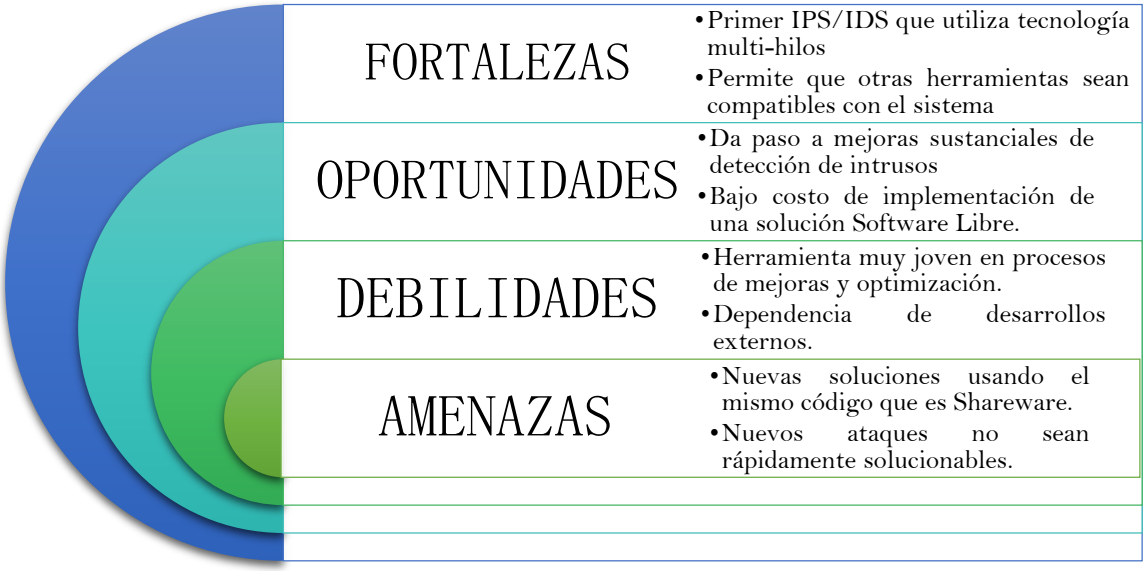


FIGURA 3.1: Análisis FODA de SURICATA

Fuente: Elaborada por Andrea Zura

3.2.1.1.1 SURICATA

Suricata es un motor IPS/IDS de código abierto bajo licencia GPLv2y desarrollado por la comunidad de OISF (Open Infomation Security Foundation), es relativamente nuevo pero con muy buenas características siendo la más importante su arquitectura Multi-hilos, además es totalmente compatible con las reglas Snort y Emerging Threads. (Alfon, 2011).

En la Figura 3-2 se muestra la imagen oficial del software.

FIGURA 3.2: Imagen oficial de IDS-IPS Suricata

Fuente: Extraída de http://suricata-ids.org/

- Características

En la tabla 3-2 se presenta un resumen de las características de SURICATA.

TABLA 3.2: Carca teísticas de SURICATA

SURICATA	
Características	**Descripción**
Procesador Multi-Hilo	Permite la ejecución de varios procesos de forma simultánea, aumentando así el rendimiento. Aprovechando de esta manera el procesamiento Multi-núcleos de los actuales procesadores.
Detección automática de Protocolos	El motor de Suricata tiene palabras claves para algunos protocolos como: IP, TCP, UDP, ICMP, HTTP, TLS, FTP y SMB. Gracias a esto puede detectar una ocurrencia dentro de un stream de datos, sin importar el puerto en donde ocurre. Esta característica es importante para el control y detección de malware.
Independencia de la librería HTP	La librería HTP es un proyecto independiente a Suricata e integrado efectivamente a Suricata. Puede ser utilizado por otras aplicaciones como: proxis, filtros.
Métodos de Entrada Estándar	Soporte para NFQueu, IPFRing y LibPcap standard para la captura de tráfico.
Coincidencia Rápida de Direcciones IP	Puede usar automáticamente un preprocesador especial para validar más rápido las reglas que hagan coincidencia únicamente de IP; por ejemplo, RBN, o las listas de IP de “EmergingThreats”.

Fuente: Elaborada por Andrea Zura en referencia a (Alfon, 2011)

- Definición de la arquitectura del sistema IDS-IPS

En esta sección se llevará a cabo el diseño de la arquitectura que el sistema a desarrollar debe cumplir; para ello se ha considerado que la arquitectura más apropiada de acuerdo a las características que presenta es SELKS.

SELSK, es un sistema abierto basado en Debian con LXDE y administración X-Windows; además de tener una plataforma basada en el motor del IDS-IPS Suricata. En esta arquitectura se distinguen los 5 componentes que indican su nombre:

- **S** – Suricata IDS-IPS
- **E** - Elasticsearch
- **L** - Logstash
- **K** - Kibana
- **S** - Scirius

En la Tabla 3-3 se muestran las principales características de cada uno de estos componentes.

TABLA 3.3: Características de los componentes de SELKS

SELKS	
COMPONENTES	**CARACTERÍSTICAS**
Suricata	IDS-IPS de alto rendimiento, con motor de seguimiento en seguridad de red. Es altamente escalable. Posee protocolos de identificación Además, permite identificar archivos, sumas de verificación MD5, extracción de archivos
Elasticsearch	Permite realizar Análisis de registros Escalable con la búsqueda en tiempo real y enfoque detallado Permite comprender los grandes volúmenes de datos, creando fácilmente barras, líneas y gráficos de dispersión, o gráficos circulares y mapas.
Logstash	Es la solución de registro de código abierto más popular en el mercado hoy en día. Toma registros y otros datos de eventos basado en tiempo, desde cualquier sistema y lo almacena en un solo lugar para la transformación y el procesamiento adicional.
Kibana	Es el motor de visualización de datos de Elasticsearch. Permite interactuar de forma nativa con todos sus datos a través de paneles de control personalizados.
Scirius	Es una interfaz web dedicada a la gestión conjunto de reglas Suricata. Maneja el archivo de reglas y archivos de actualización asociada.

Fuente: Elaborada por Andrea Zura

- Características del Equipo.

Las características del equipo deben satisfacer los requerimientos mínimos del software que a instalarse, el mismo que se describe en la Tabla 3-4, es indispensable indicar que dichos requerimientos permitirán un monitoreo adecuado de la red.

TABLA 3.4: Requerimientos mínimos de instalación de SELKS

Requerimientos mínimos de instalación de SELKS		
Característica	**Descripción**	
Sistema Operativo	SELKS-1.1	
RAM	2048 MB	
Disco Duro	125 GB	
Tarjetas de Red	eth0	Atheros AR8162/8166/8168 PCI-E Fast Ethernet
	eth1	ASIX AX88772 USB2.0 to Fast Ethernet Adapter #2
	eth2 NAT	
Direccionamiento (NIC de Administración)		
Dirección IP	**192.168.2.x**	
Máscara de Subred	**255.255.255.192**	
Gateway	**192.168.2.1**	

Fuente: https://github.com/StamusNetworks/SELKS

- Ubicación Física del IDS-IPS

La localización del IDS/IPS se la pondrá entre el firewall y la red interna, con esta ubicación se pueden obtener ciertas ventajas, tales como:

- Permite monitorear intrusiones que pueden atravesar el firewall.
- Puede detectar ataques dirigidos contra los servidores.
- Permite identificar ataques y escaneos más comunes

Como todo sistema de detección de intrusos, también existen ciertas desventajas, las mismas que se presentan a continuación.

- No permite identificar ataques que utilicen métodos de encriptación
- Dependiendo de la cantidad de tráfico el IDS-IPS, puede o no analizarlo todo. Esto dependerá del diseño del sistema.

En la figura 3-3 se presenta un representación gráfica de la ubicación del sistema de detección y prevención de intrusos.

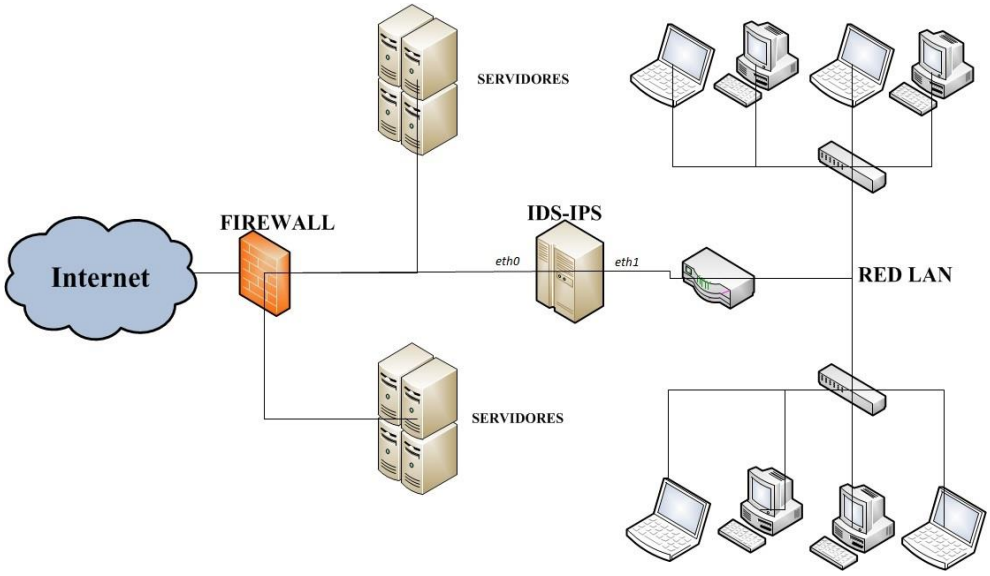


FIGURA 3.3: Ubicación del IDS-IPS en la red.

Fuente: Elaborado por Andrea Zura

3.2.2 FIREWALL

El GADMO cuenta actualmente(Enero 2015) con dos firewall, ASTARO Gateway 320; los mismos que se encuentran configurados de modo que protegen la granja de servidores de los ataques externos. Dicha configuración se muestra en la figura 3-6.

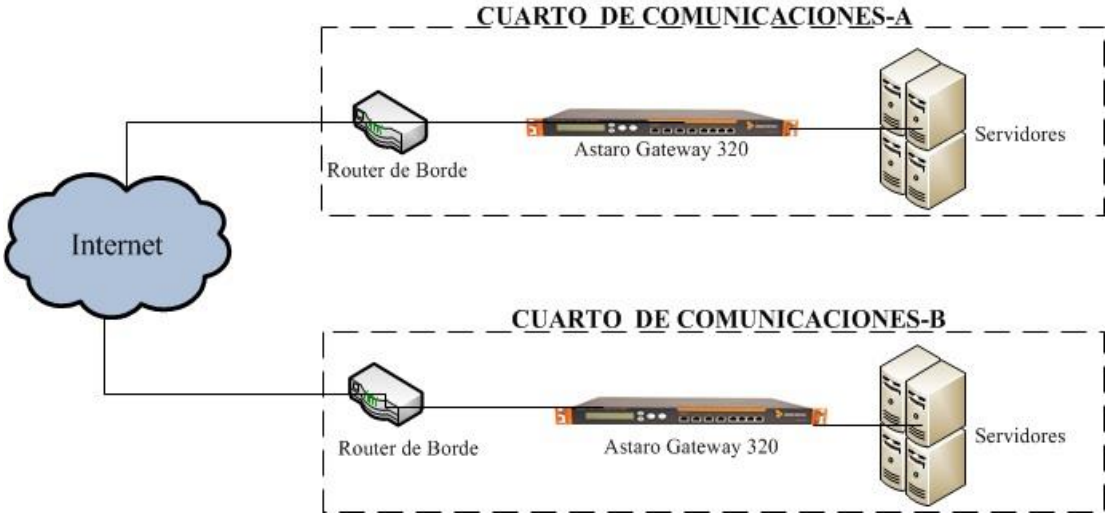


FIGURA 3.4: Topología Actual del Firewall

Fuente: Elaborado por Andrea Zura

3.2.2.1 CARACTERÍSTICAS DEL EQUIPO

Lo primero que se debe analizar son las características técnicas de los equipos Firewall tanto en software como en hardware. El Municipio cuenta con dos Firewall, a nivel de hardware **Astaro Security Gateway 320**, que tienen características que se muestran en la Tabla 3-6.

TABLA 3.5: Información técnica del Firewall Astaro Security Gateway 320

INFRMACIÓN TÉCNICA		
Figura	**Capacidad**	**Especificaciones del hardware:**
Astaro Security Gateway 320 	Rendimiento del cortafuegos: 3.4 Gbit/s Rendimiento de la VPN: 700 Mbit/s Rendimiento del IPS: 1300 Mbit/s Rendimiento del UTM: 165 Mbit/s Correos electrónicos por hora: 600,000 Usuarios: Sin restricción Conexiones simultáneas: 600,000 Almacenamiento en cuarentena: 60 GB Almacenamiento de registros/informes: 80 GB.	Unidad de disco duro: 160 GB Puertos Ethernet: 8 Puertos USB: 4 Puertos COM: 1 (RJ-45) Puertos VGA: 1 (trasero) Pantalla LCD: 1

Fuente: Recuperada de http://www.astaro.com/node/18320

Adicionalmente se muestran en la Tabla 3-7 las aplicaciones que este firewall brinda:

TABLA 3.6: Aplicaciones de Astaro Security Gateway 320

APLICACIONES				
Astaro Network Security 	**Astaro Mail Security** 	**Astaro Web Security** 	**Astaro Web Application Security** 	**Astaro Wireless Security** 
• Cortafuegos configurable. •IPS •DoS • Desvío de tráfico • Herramientas de NAT • Control de Ancho de Banda •VPNs •SSSL •IPSec • Autenticación de Directorios	• Antispam & Phishing •Antivirus Scanning •Email Encryption	• URL Filtering •Spyware Protection •Antivirus Scanning •HTTPS Scanning • User Reporting • Interactive Web Reporting • Control de Aplicaciones	• Web Application Firewall • Cookie Protection • Refuerzo de URL •Antivirus • Reverse Proxy • Form Hardening	• mplementación Plug & Play •Gestión centralizada •Seguridad integrada • Potente cifrado •Lugar de colocación •Acceso a Internet para invitados

Fuente: Recuperada de http://www.astaro.com/node/18320

3.2.2.2 CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD EN FIREWALL SHOPOS UTM

Es recomendable realizar ciertas configuraciones las mismas que se muestran a continuación.

- Cambiar la clave por defecto de admin:

FIGURA 3.5: Cambio de clave y usuario del Firewall

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Activar las notificaciones de alertas:

Esto permitirá definir las acciones de notificación por correo electrónico y trap SNMP para cada tipo de notificación. En este caso se marcarán todas las casillas, ya que todas son importantes y necesarias. Se muestra en la Figura 3-6.

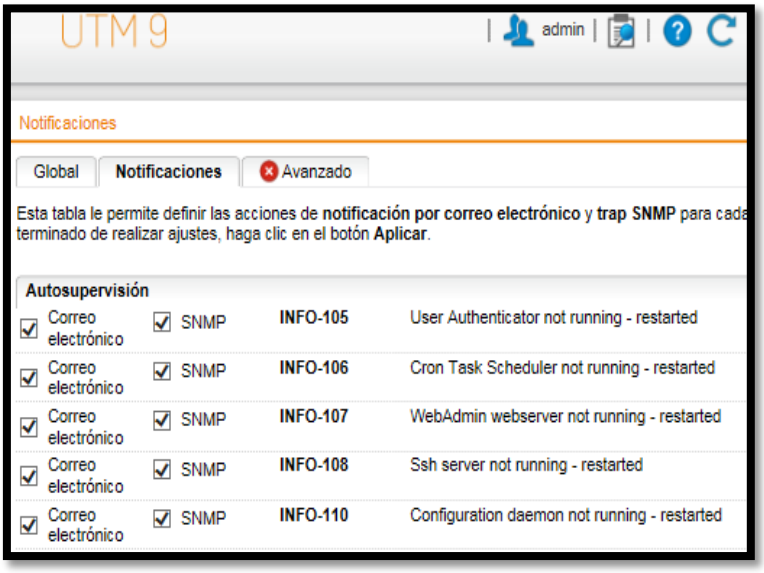


FIGURA 3.6: Activación de notificaciones de alerta

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Activar el acceso SSH:

Al activar SSH se le permite al administrador, acceder de forma remota y segura, en situaciones en las que no se puedan resolver problemas por medio del WebAdmin; además realizar configuraciones de direcciones IP, Logs, DNS; así como también ejecutar comandos tales como ping, tracert; entre otros.

FIGURA 3.7: Activación de SSH

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Activar actualizaciones

Mantener actualizado el firewall con las nuevas versiones permitirá mantener mejoras permanentes en el sistema. Se muestra en la Figura 3-8.

FIGURA 3.8: Activación de actualizaciones

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Activar el envío automático de backups

Esto ayudará a tener los backups siempre a mano, para que el administrador los pueda utilizar cuando los necesite; cabe recalcar que estos ocupan muy poco espacio y se guardan ya sea en el servidor o en nuestro correo electrónico.

Se muestra en la Figura 3-9.

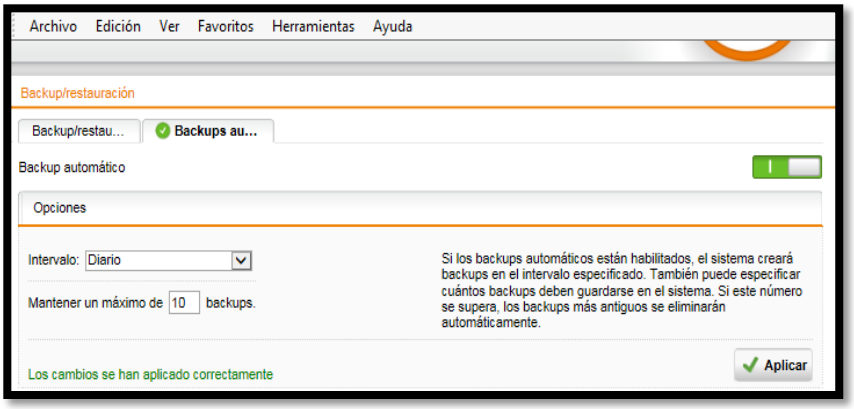


FIGURA 3.9: Activación del envió automático de backup

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Activar el envío periódico de los informes ejecutivos

Resulta una opción útil, debido a que permite revisar información de hechos y sucesos antiguos, que se necesiten en caso de auditorías. Esto se muestra en la Figura 3-10.

FIGURA 3.10: Activación de envió de informes ejecutivos

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Habilitar ICMP

Esto permite ejecutar comandos de ping y tracert hacia y a través del firewall. Esto se muestra en la Figura 3-11.

FIGURA 3.11: Habilitar ICMP

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Creación de Usuarios y grupos

Se crearán grupos de usuarios, los mimos que pertenecerán a VLANs, mostrados en un resumen en la Tabla

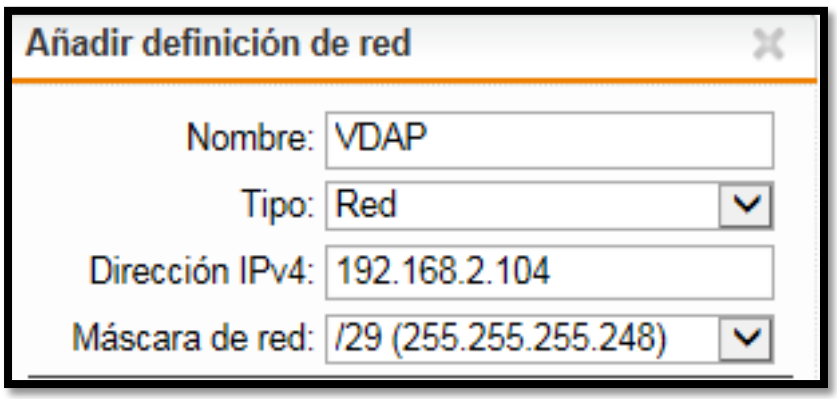


FIGURA 3.12: Creación de grupos de usuarios

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

- Creación de reglas

Las reglas creadas, están acorde a los niveles de acceso de cada VLAN.

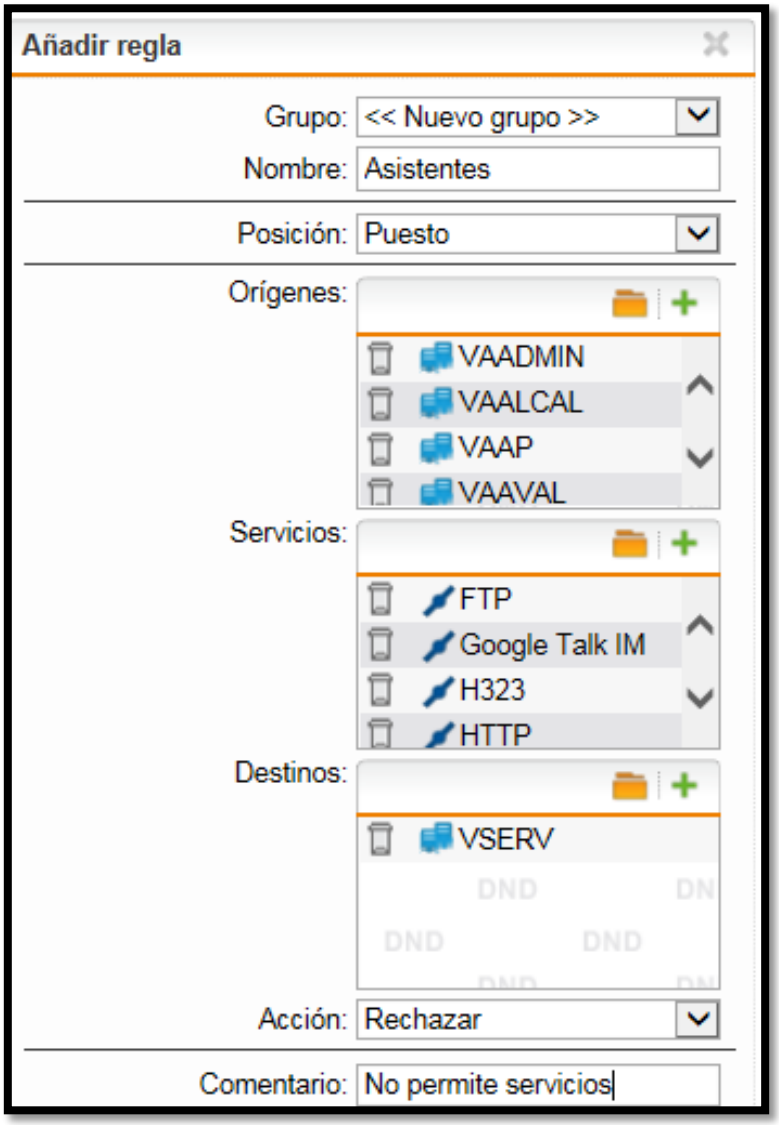


FIGURA 3.13: Configuración de reglas, acorde a los grupos de usuarios.

Fuente: Obtenido del WebAdmin de Firewall Sophos UTM

3.2.3 ZONA DESMILITARIZADA (DMZ)

Para realizar el diseño de la DMZ se debe tener conocimiento de todos los servicios que brinda el GADMO, en que plataformas se encuentran instalados, tanto a nivel de hardware como software; información que se muestra en la Tabla 3-7

TABLA 3.7: Descripción de los servidores del GADMO

Servicios	Descripción	Sistema Operativo
• Active Directory • Sistema SIGMO • BASE DE DATOS SIM2001	COMPAQ PROLIANT Ml370 G3 Procesador: XENON 2.8 RAM: 4GB Disco Duro: 120GB	Win server 2003
• Active Directory Backup • Sistema Comercial • Base de Datos "Comercial fin_otavalo"	COMPAQ PROLIANT Ml370 G3 Procesador: XENON 2.8 RAM: 4GB Disco Duro: 120GB	Win server 2003
• Sistema de tránsito • Base de Datos	CLON PENTIUM Procesador: PIV 3.0 RAM: 2GB Disco Duro: 80GB	Win XP Pro
Servidor Lexis SILECPRO 5.3	CLON PENTIUM Procesador: PD3.4 RAM: 2GB Disco Duro: 160GB	Win XP Pro
Antivirus KASPERSKY	CLON PENTIUM Procesador: PD3.4 RAM: 2GB Disco Duro: 160GB - 1TB	Win XP Pro
Antivirus ESET	CLON PENTIUM Procesador: PD3.2 RAM: 2GB Disco Duro: 120GB	Win server 2003
Servidor comercial	HP PROLIANT ML350 G5 Procesador: XEON QC 2.50 RAM: 14GB Disco Duro: 1200GB	Win Server Standar
SISTEMA VUE	HP PROLIANT DL380G6 Procesador: XEON QC 2.67 RAM: 16GB Disco Duro: 1200GB	Win Server Standar
WEB VUE	HP PROLIANT DL380G6 Procesador: XEON QC 2.66 RAM: 16GB Disco Duro: 1200GB	Win Server Standar
Sistemas: • V7 Olympo • V6 Olympo	HP PROLIANT DL380G7 Procesador: XEON QC 2.66 RAM: 24GB Disco Duro: 1800GB	Server 2008 R2

• V5 Olympo Bases de Datos: • BASEM • BASEMV7 • IMO_ACTV7 • IMO_CONSO11 • IMO_CONSO12 • IMO_CONSOLIDA • IMO_CONTV7 • IMO_INFA • IMO_INV7 • IMO_ROLESV7 • IMOCI • IMOCI03 • IMOV6 • IMOV8		
Sistema de servicios municipales SIGMO	HP PROLIANT DL380G7 Procesador: XEON QC 3.47 RAM: 24GB Disco Duro: 1800GB	Server 2008 R2
Servidor GIS	HP PROLIANT DL380G7 Procesador: XEON QC 2.27 RAM: 12GB Disco Duro: 450GB	Win Server Estándar
Servidor SISTEMAS	HP PROLIANT BL460c GEN8 Procesador: XEON QC 2.50 RAM: 32GB Disco Duro:2TB	Win Server Estándar
Servidor COMERCIAL	HP PROLIANT BL460c GEN8 Procesador: XEON QC 2.00 RAM: 24GB Disco Duro: 600GB	Win Server Estándar

Fuente: Obtenida por la Administración de la Coordinación TIC's.

Actualmente la granja de servidores se encuentra protegida por dos Firewall, pero en una distribución no recomendada debido a que podría haber intentos de intrusión. Dicha distribución se muestra en la Figura 3-12.

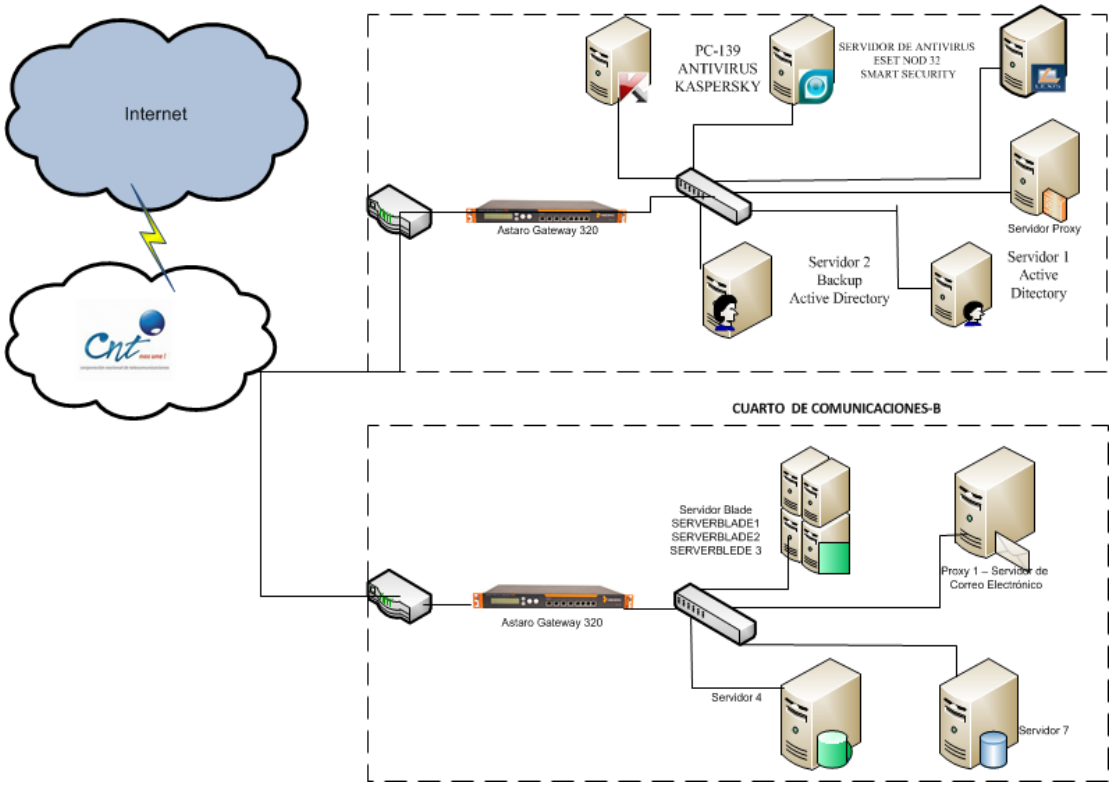


FIGURA 3.14: Topología Actual de la granja de servidores.

Fuente: Elaborada por Andrea Zura

Teniendo claro los tres elementos principales que forman parte de la red perimetral, se muestra en la figura 3-13, el diseño planteado para la red de datos del GADMO, en el que se detalla cada una de estas partes.

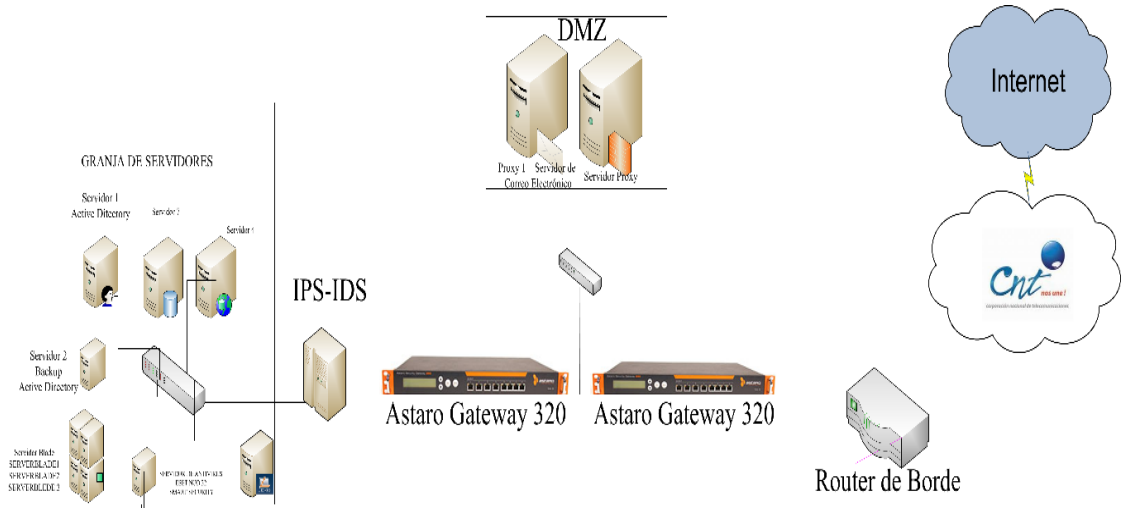


FIGURA 3.15: Diseño red perimetral

Fuente: Elaborada por Andrea Zura

Se observa que en la zona desmilitarizada se encuentran los servicios de Correo electrónico y servidor WEB; los mismo que se encuentran protegidos por el primer firewall, siguiendo continuamente del siguiente firewall, adicionalmente se tiene el IDS-IPS en la ubicación ya antes explicada el mismo que permitirá conservar la seguridad de la LAN.

3.3 DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL DE RED INTERNA

Considerando la infraestructura y requerimientos actuales de la red de datos del GADMO, se propone un modelo jerárquico y la segmentación lógica de la red. Brindando así una solución que mejore las prestaciones y servicios.

3.3.1 DISEÑO DEL MODELO DE RED

El modelo jerárquico de red presenta varias ventajas que permitirán que la red de datos del GADMO sea más segura, escalable, redundante, flexible y eficiente.

Dicho modelo se basa en el diseño y estructuración por capas independientes que cumple funciones específicas. La separación de la diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. (CISCO).

En la figura 0-1 se muestra un ejemplo de una red Jerárquica

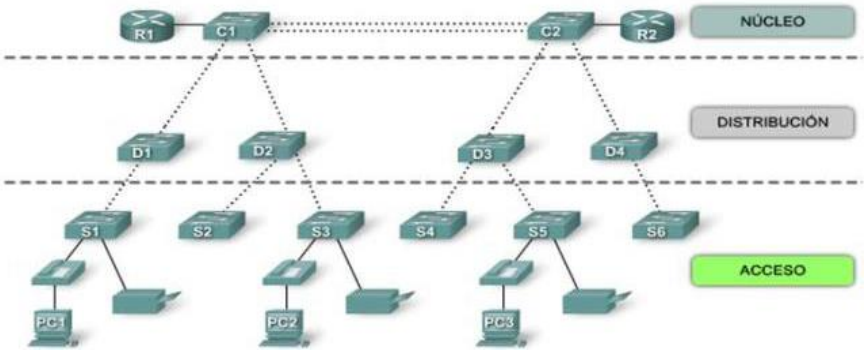


FIGURA 3.16: Modelo Jerárquico de Redes

Fuente: Imagen extraída de (CISCO)

En base a dicho modelo se describirán las características de los switches con los que cuenta el GADMO; en base a sus características serán clasificados en las diferentes capas del modelo jerárquico.

3.3.1.1 SWITCHES DE CAPA DE ACCESO

Los switches de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Por esta razón, necesitan admitir características como seguridad de puerto, VLAN, Fast Ethernet/Gigabit Ethernet, PoE y agregado de enlaces. La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. La seguridad de puerto se aplica en la capa de acceso. En consecuencia, es una importante primera línea de defensa para una red.

La velocidad de puerto es también una característica que se necesita considerar para los switches de la capa de acceso. Según los requerimientos de rendimiento para su red, debe elegir entre los puertos de switch Fast Ethernet y Gigabit Ethernet (100 Mbps y 1000 Mbps respectivamente). Otro requerimiento de la característica de algunos switches de capa de acceso es PoE y el agregado de enlaces.

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla 3-8 un resumen de los elegidos con sus respectivas características:

TABLA 3.8: Características de Switch Capa Acceso

Switch	CARACTERÍSTICAS SWITCHES CAPA DE ACCESO									
	Velocidad (Mbps)	Puertos	Rendimiento	IEEE 802.1Q	IEEE 802.1D	IEEE 802.1W	IEEE 802.1P	ACL	PoE	LACP
3COM 2924 SFP 24P	10/100/1000	GbEthernet	MCS[a] :48Gbps MCT[b]:35,5Mbps	✓	✓	✓	✓	✓	✓	✓
3COM 4400 48P	10/100	Ethernet	MCS: 13,6Gbps MCT: 10,1 Mbps	✓	✓	✓	✓	✓		✓
3COM 2816 16P	10/100/1000	GbEthernet	MCS: 104 Gbps MCT: 74 Mbps	✓			✓	✓	✓	✓
3COM 2226 SFP PLUS 24P	10/100	Ethernet	MCS: 8.8 Gbps	✓	✓	✓	✓	✓		
3COM 2824 SFP PLUS 24P			MCS: 48 Gbps MCT: 35,5 Mbps	✓	✓		✓	✓	✓	
3COM 4500G 48P			MCS: 13,6 Gbps MCT: 10,1 Mbps	✓	✓	✓	✓	✓		

3COM 2928 SFP 24P	10/100/1000	GbEthernet	MCS: 56 Gbps MCT:41.7 Mbps	✓	✓	✓	✓	✓	✓	
3COM 4500G 24P	10/100	Ethernet	MCS: 8.8 Gbps	✓			✓	✓		
3Com 4900 12P	10/100/1000	GbEthernet		✓	✓	✓	✓	✓		✓
3Com 4210 18P	10/100	Ethernet		✓	✓	✓	✓	✓	✓	✓
3COM 2952 48P	10/100/1000	GbEthernet	MCS: 104 Gbps. MCT: 74 Mpps;	✓	✓	✓	✓	✓	✓	✓

Fuente: Elaborada por Andrea Zura

Nota: [a] MCS es la Máxima Capacidad de Conmutación. [b] MCT es la Máxima Capacidad de Transmisión.

- Consideraciones del diseño

La capa de acceso en una red jerárquica es dedicada exclusivamente a la conectividad con el usuario final mediante los equipos de red finales.

En la figura 3-15 se muestran un diagrama físico de los switches de capa de acceso.

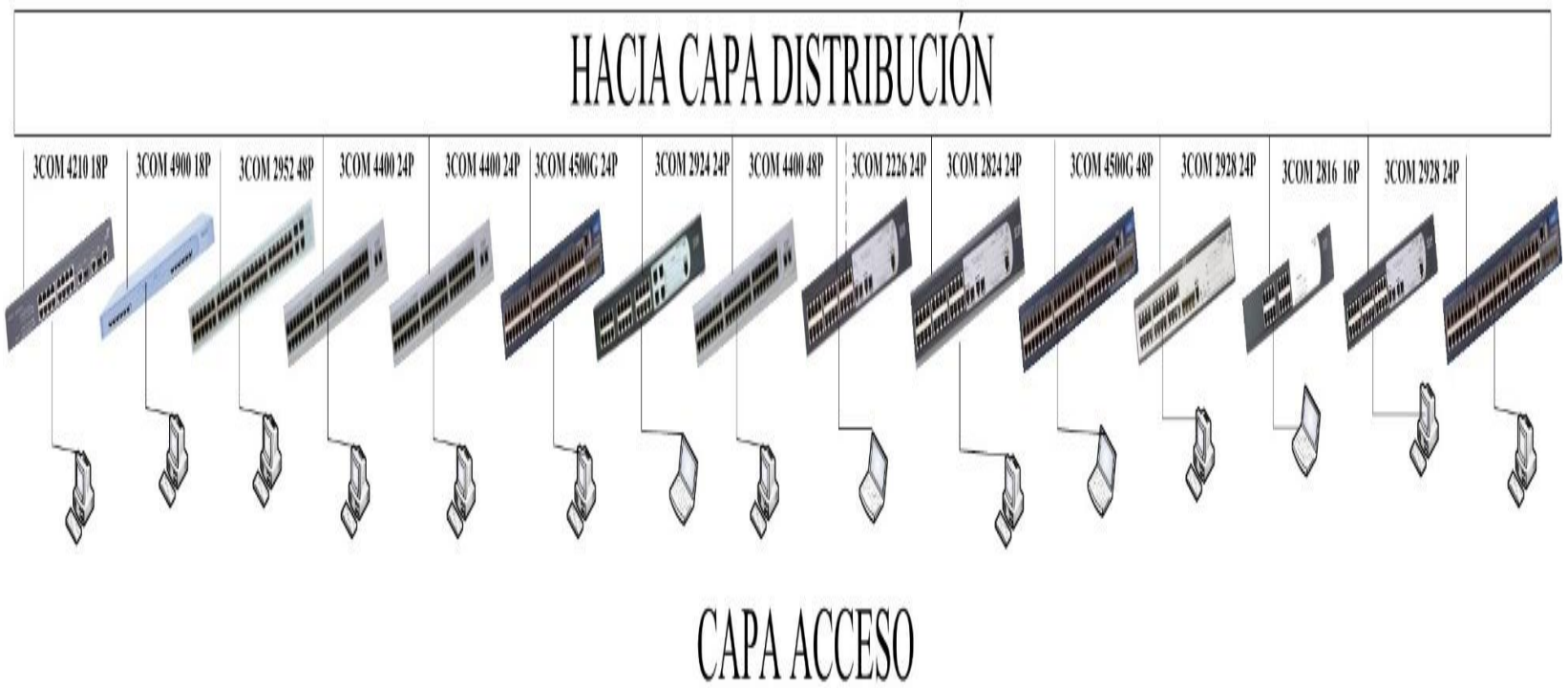


FIGURA 3.17: Diseño de la capa de acceso en la red jerárquica

Fuente: Elaborada por Andrea Zura

Al ser la capa de acceso un enlace directo con el usuario final, esta integra a todos los equipos finales, tales como, computadores, cámaras, teléfonos IP, scanner, impresoras, copiadoras, etc.; lo que permite que el administrador controle todos los equipos que se conecten a la red. Para ello se ha considerado segmentar lógicamente la red.

En el estudio de la situación actual se determinó que los usuarios se encuentran agrupados acorde a la función que éstos desempeñan y acorde a los recursos que utilizan.

Antes de realizar la segmentación hay que tener en cuenta varios aspectos:

- Se debe asignar a cada usuario una dirección IP, la misma que no debe ser modificada sin autorización; para controlar esto; se debe asociar la dirección MAC de cada equipo, con la dirección IP asignada, de tal forma que si las dos no coinciden, el usuario no podrá acceder a la red.

- Se debe tener un registro actualizado de los cambios que se registren la infraestructura de la red.

- Segmentación y Direccionamiento IP

La segmentación de una red permite mejorar significativamente la seguridad, ya que los administradores pueden configurar segmentos de tal forma que transmiten y reciben paquetes únicamente desde su subred, asegurándose que los paquetes no autorizados no se envían dentro o fuera del segmento.

Para realizar la segmentación se ha considerado la agrupación que se mantiene en el GADMO, agrupación por las diferentes direcciones, coordinaciones y/o jefaturas, funciones desempeñadas por cada usuario y los recursos que estos usen y necesiten usar.

En la Tabla 3-11 se resume la asignación de VLAN para cada dirección, coordinación y/o jefatura, junto con el direccionamiento IP aplicado.

TABLA 3.9: Segmentación y Direccionamiento IP Capa de Acceso

Dependencia		#VLAN	Nombre VLAN	#Puntos de red	Direccionamiento	Máscara de subred	Gateway
COORDINACIÓN TIC's	Conmutadores y Enrutadores	VLAN 2	VLAN Native	40	192.168.2.0	255.255.255.192	192.168.2.1
	Servidores	VLAN	VSERV	50	192.168.4.0	255.255.255.192	192.168.4.1
	Unidad de Desarrollo	VLAN 3	VADMIN	30	192.168.2.64	255.255.255.224	192.168.2.65
	Unidad de Redes						
	Unidad de Mantenimiento						
AGUA POTABLE	Director	VLAN 4	VDAP	4	192.168.2.104	255.255.255.248	192.168.2.105
	Técnicos Alcantarillado	VLAN 5	VTAP	12	192.168.1.176	255.255.255.240	192.168.1.177
	Técnicos Comercialización						
	Técnicos Laboratorio						
	Asistentes	VLAN 6	VAAP	4	192.168.3.96	255.255.255.248	192.168.3.97
ALCALDÍA	Alcaldía	VLAN 7	VALCAL	6	192.168.2.96	255.255.255.248	192.168.2.97
	Auditoría Interna	VLAN 8	VTALCAL	28	192.168.1.64	255.255.255.224	192.168.1.65
	Asesoría Jurídica						
	Secretaría General						
	Fiscalización						
	Asistentes	VLAN 9	VAALCAL	4	192.168.3.152	255.255.255.248	192.168.3.153
AVALUOS Y CATASTROS	Director	VLAN 10	VDAVAL	4	192.168.2.112	255.255.255.248	192.168.2.113
	Avalúos Urbanos	VLAN 11	VTAVAL	24	192.168.3.0	255.255.255.224	192.168.3.1
	Avalúos Rurales						
	Asistentes	VLAN 12	VAAVAL	4	192.168.3.80	255.255.255.248	192.168.3.81

DIRECCIÓN ADMINISTRATIVA	Director	VLAN 13	VDADMIN	4	192.168.2.120	255.255.255.248	192.168.2.121
	Coordinadores/as						
	Talento Humano	VLAN 14	VTADMIN	20	192.168.1.96	255.255.255.224	192.168.1.97
	Ventanillas	VLAN 15	VVUE	16	192.168.3.32	255.255.255.224	192.168.3.33
	Asistentes	VLAN 16	VAADMIN	4	192.168.3.90	255.255.255.248	192.168.3.91
COMUNICACIÓN SOCIAL	Director	VLAN 17	VDCXS	4	192.168.2.128	255.255.255.248	192.168.2.129
	Participación Ciudadana	VLAN 18	VTCXS	12	192.168.1.192	255.255.255.240	192.168.1.193
	Asistentes	VLAN 19	VACXS	4	192.168.3.104	255.255.255.248	192.168.3.105
GESTIÓN SOCIAL E INTERCULTURAL	Director	VLAN 20	VDGSI	4	192.168.2.136	255.255.255.248	192.168.2.137
	Técnicos	VLAN 21	VTGSI	10	192.168.1.208	255.255.255.240	192.168.1.209
	Asistentes	VLAN 22	VAGSI	4	192.168.3.114	255.255.255.248	192.168.3.115
DIRECCIÓN FINANCIERA	Director	VLAN 23	VDFIN	4	192.168.2.144	255.255.255.248	192.168.2.145
	Presupuestos	VLAN 24	VTFIN	40	192.168.1.0	255.255.255.192	192.168.1.1
	Contabilidad						
	Rentas						
	Coactivas						
	Recaudación						
	Tesorería						
	Bodega Municipal	VLAN 25	VAFIN	12	192.168.3.64	255.255.255.240	192.168.3.65
	Asistentes						
GESTIÓN AMBIENTAL	Director	VLAN 26	VDGAMB	4	192.168.2.152	255.255.255.248	192.168.2.153
	Residuos Sólidos	VLAN 27	VTGAMB	20	192.168.1.128	255.255.255.224	192.168.1.129
	Gestión Ambiental						
	Junta Cantonal						
	Junta de la Niñez						
	Secretaria de Higiene						

	Asistentes	VLAN 28	VAGAMB	4	192.168.3.120	255.255.255.248	192.168.3.121
PLANIFICACIÓN	Director	VLAN 29	VDPLAN	4	192.168.2.160	255.255.255.248	192.168.2.161
	Proyectos Arquitectónicos	VLAN 30	VTPLAN	14	192.168.1.160	255.255.255.240	192.168.1.161
	Jefatura de Regulación Urbana						
	Comisaria Construcciones						
	Comisaria Municipal						
	Parqueo Tarifado	VLAN 31	VAPLAN	4	192.168.3.128	255.255.255.248	192.168.3.129
	Asistentes						
INFRAESTRUCTURA	Director	VLAN 32	VDINFRA	4	192.168.2.168	255.255.255.248	192.168.2.169
	Topografía	VLAN 33	VTINFRA	8	192.168.1.224	255.255.255.240	192.168.1.225
	Unidad Técnica						
	Ingeniería Vial						
	Asistentes	VLAN 34	VAINFRA	4	192.168.3.138	255.255.255.248	192.168.3.139
PROMOCIÓN SOCIAL Y PATRIMONIO	Director	VLAN 35	VDPSP	4	192.168.2.176	255.255.255.248	192.168.2.177
	Comité de Fiestas Yamor	VLAN 36	VTPSP	8	192.168.1.240	255.255.255.240	192.168.1.241
	Asistentes	VLAN 37	VAPSP	4	192.168.3.144	255.255.255.248	192.168.3.145
ENTES EXTERNOS							
TURISMO	VUE	VLAN 40	VTVUE	14	192.168.5.144	255.255.255.240	192.168.5.145
	Asistentes	VLAN 43	VATURIS	10	192.168.5.160	255.255.255. 240	192.168.5.161
	PYMES	VLAN 42	VPYMES	20	192.168.5.64	255.255.255.224	192.168.5.65
	Director	VLAN 41	VDTURIS	4	192.168.5.200	255.255.255.248	192.168.5.201

UNIDAD DE TRANSPORTES	Técnicos	VLAN 46	VTTRANS	14	192.168.5.128	255.255.255.240	192.168.5.129
	Asistentes	VLAN 45	VATRANS	6	192.168.5.192	255.255.255.248	192.168.5. 193
	Director	VLAN 44	VDTRANS	4	192.168.5.208	255.255.255.248	192.168.5.209
COLIBRI	Técnicos	VLAN 48	VTCOL	10	192.168.5.176	255.255.255.240	192.168.5.177
	Director	VLAN 47	VDCOL	4	192.168.5.216	255.255.255.248	192.168.5.217
	Asistentes	VLAN 49	VACOL	4	192.168.5.224	255.255.255.248	192.168.5.225
CASA DE LA JUVENTUD	General	VLAN 50	VJUVEN	40	192.168.5.0	255.255.255.192	192.168.5.1
MUNICIPIO 2	General	VLAN 51	VMUN	20	192.168.5.96	255.255.255.224	192.168.5.97

Fuente: Elaborado por Andrea Zura

La distribución de VLAN se puede diferenciar las siguientes:

- **VSERV:** VLAN de servidores y equipos; la misma que ha sido destinada para el direccionamiento IP de los servidores y del equipamiento activo de la Coordinación de TIC's.
- **VADMIN:** VLAN de administración; la misma que ha sido destinada para el direccionamiento IP de los administradores de la red, es decir los técnicos e ingenieros de la Coordinación de TIC´s.
- **VTECN:** VLAN de técnicos y colaboradores; la misma que ha sido destinada para el direccionamiento IP del personal de todas las direcciones que requieren el uso páginas web públicas, páginas web informativas y/o comerciales y correo electrónico para su trabajo.
- **VASIST:** VLAN de asistentes; la misma que ha sido destinada para el direccionamiento IP de los asistentes y/o secretarias que únicamente necesitan el correo electrónico para su trabajo.
- **VDIREC:** VLAN directores; la misma que ha sido destinada para el direccionamiento IP de los directores y/o coordinadores, los cuales tendrán acceso prioritario para todos los servicios.

A nivel de acceso se configurará las VLAN en los switch 3com expuestos en la Tabla 3-1, los cuales brindarán la conexión hacia el usuario final, cada uno de los puertos serán configurados según la VLAN asociada al usuario.

Además se muestra en la Figura 3-16 se muestra la propuesta gráfica de la distribución de VLANs para la red de datos del GADMO

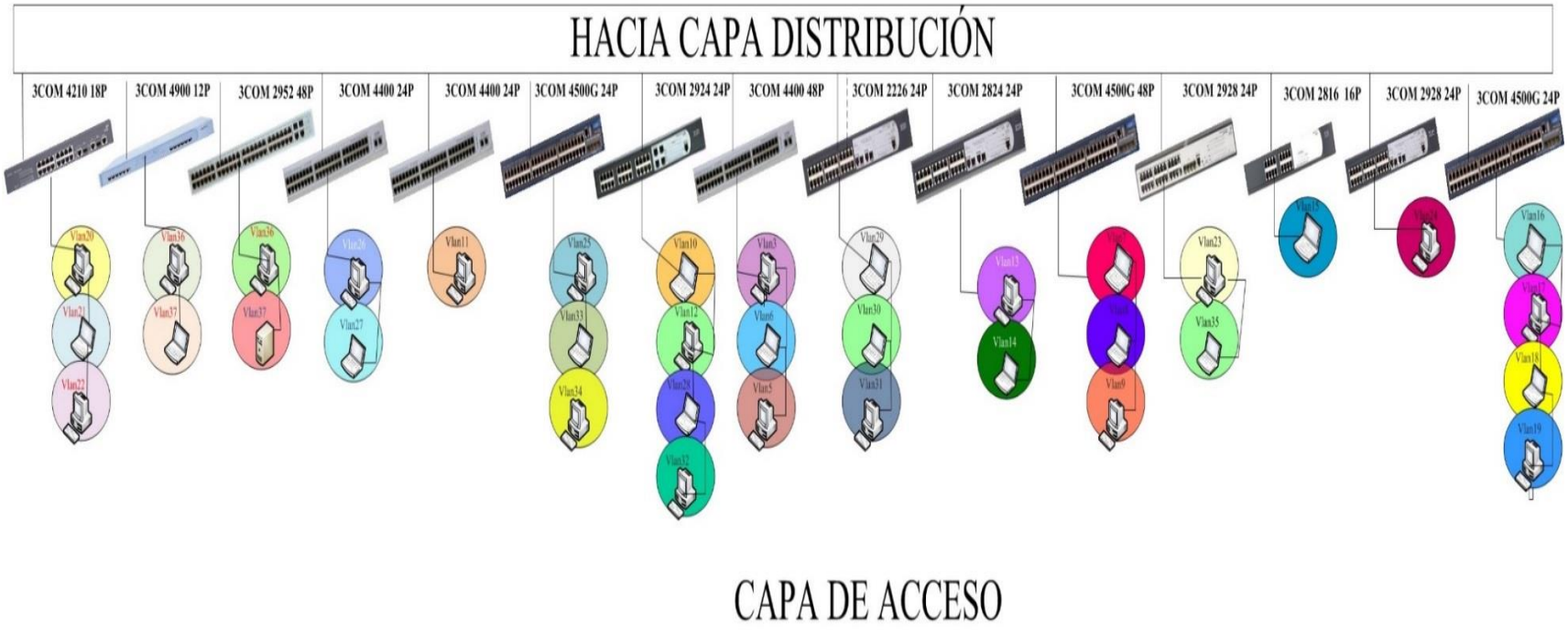


FIGURA 3.18: Propuesta gráfica de distribución de VLANS a nivel de acceso

Fuente: Elaborada por Andrea Zura Configuración de Listas de Acceso a nivel de VLAN

Las listas de control de acceso se asignaron acorde a las políticas de seguridad aplicadas en el Manual de Normas y procedimientos; el cual se realizó en base al estudio de la situación actual.

Se presenta la tabla la asignación de las listas de acceso

TABLA 3.10: Asignación de ACL en función de la VLAN

Nombre del switch	Nombres y números de VLAN	Nombre de Acces-List
Switch GES-SOC	VLAN 20 VDGSI	Ges-total
	VLAN 21 VTGSI	Ges-web
	VLAN 22 VAGSI	Ges-correo
Switch PROM-SOC	VLAN 36 VTPSP	Prom-web
	VLAN 37 VAPSP	Prom-correo
Switch CTIC-AP	VLAN 38 VSERV	CTIC-total
	VLAN 4 VDAP	AP-total
Switch GES-AMB	VLAN 27 VTGAMB	Amb-web
	VLAN 26 VDGAMB	Amb-total
Switch AVALUOS	VLAN 11 VTAVAL	Aval-bdatos
Switch INFRA	VLAN 25 VAFIN	Fin-correo
	VLAN 33 VTINFRA	Infra-web
	VLAN 34 VAINFRA	Infra-correo
Switch Varios1	VLAN 10 VDAVAL	Aval-total
	VLAN 12 VAAVAL	Aval-correo
	VLAN 28 VAGAMB	Amb-correo
	VLAN 32 VDINFRA	Infra-total
Switch CTIC-AP1	VLAN 3 VADMIN	Admin-correo
	VLAN 5 VTAP	AP-web
	VLAN 6 VAAP	Ap-correo
Switch PLANIF	VLAN 30 VTPLAN	Plan-web
	VLAN 29 VDPLAN	Plan-total
	VLAN 31 VAPLAN	Plan-correo
Switch ADMIN	VLAN 13 VDADMIN	Plan-total
	VLAN 14 VTADMIN	Plan-web
Switch COMSOC	VLAN 18 VTCXS	Cxs-web

	VLAN 19 VACXS	Cxs-correo
	VLAN 17 VDCXS	Cxs-total
	VLAN 16 VAADMIN	Admin-correo
Switch ALCALDIA	VLAN 7 VALCAL	Alcal-total
	VLAN 8 VTALCAL	Alcal-web
	VLAN 9 VAALCAL	Alcal-correo
Switch PROMFIN	VLAN 23 VDFIN	Fin-total
	VLAN 35 VDPSP	Psp-total
Switch VUE	VLAN 15 VVUE	Vue-correo
Switch Finanzas	VLAN 24 VTFIN	Fin-web
Switch TURISMO	VLAN 40 VTVUE	Vue-web
	VLAN 43 VATURIS	Turis-correo
Switch TURISMO1	VLAN 42 VPYMES	Pymes-total
	VLAN 41 VDTURIS	Turis-total
Switch TRANSPORTES	VLAN 46 VTTRANS	Trans-web
	VLAN 45 VATRANS	Trans-correo
	VLAN 44 VDTRANS	Trans-total
Switch COLIBRI	VLAN 48 VTCOL	Col-web
	VLAN 47 VDCOL	Col-total
	VLAN 49 VACOL	Col-correo
Switch JUVENTUD	VLAN 50 VJUVEN	Juven-total
Switch MUNICIPIO2	VLAN 51 VMUN	Mun-total

Fuente: Elaborada por Andrea Zura

Las listas de acceso se definieron de la siguiente manera:

Ges-total: Las Vlan de acceso de los directores y/o coordinadores tienen acceso a los servidores web, y correo en todo el horario de la jornada laboral.

Ges-web: Las VLAN de acceso de los técnicos y/o colaboradores tiene acceso a los servidores web, con restricción de horario y páginas web, también tienen acceso al servidor de correo electrónico.

Ges-correo: Las VLAN de acceso de las secretarias y/o asistentes tiene acceso únicamente al servidor de correo.

Aval-bdatos: Las VLAN de acceso a ciertas direcciones que necesitan el acceso a los servidores de bases de datos.

3.1.2 SWITCHES DE CAPA DISTRIBUCIÓN

Los switches de capa de distribución recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo, además proporcionan funciones de enrutamiento entre las VLAN.

Entre las características que deben soportar los switches de capa distribución son la tasa de envió alta, puertos Gigabit Ethernet/ 10Gigabit Ethernet, componentes redundantes, políticas de seguridad/listas de control de acceso, agregado de enlaces y calidad de servicio. (CISCO)

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla 3-11 un resumen de los elegidos con sus respectivas características:

TABLA 3.11: Características Switch Capa Distribución

SWITCH 2952 SFP PLUS 48P	
Funcionalidades	**Descripción**
Rendimiento	48 10BASE-T/100BASE-X/1000BASE-T 4 Gigabit SFP ports Máxima Capacidad de switching: 104 Gbps. Máxima capacidad de transmisión 74 Mpps;
SWITCHING DE CAPA 2	VLANs basadas en protocolo IEEE 802.1Q Protocolo Spanning Tree (STP) IEEE 802.1D Protocolo Rapid Spanning Tree (RSTP) IEEE 802.1w
SWITCHING DE CAPA 3	Rutas estáticas: 32 Virtual VLANs Interface: 8
Priorización de tráfico	Clase de Servicio/Calidad de Servicio (CoS/QoS) IEEE 802.1p en salida
Seguridad	Filtros ACLs basadas en direccionamiento IP y MAC para filtrar el tráfico de red y mejorar el control de la red. ACL basadas en tiempo permiten una mayor flexibilidad con acceso a la red de gestión.

Fuente: Elaborado por Andrea Zura en referencia a http://goo.gl/yIQtdJ

- Consideraciones del diseño

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. (CISCO)

En la figura 3-20, se muestran un diagrama físico de los switches de capa de acceso.

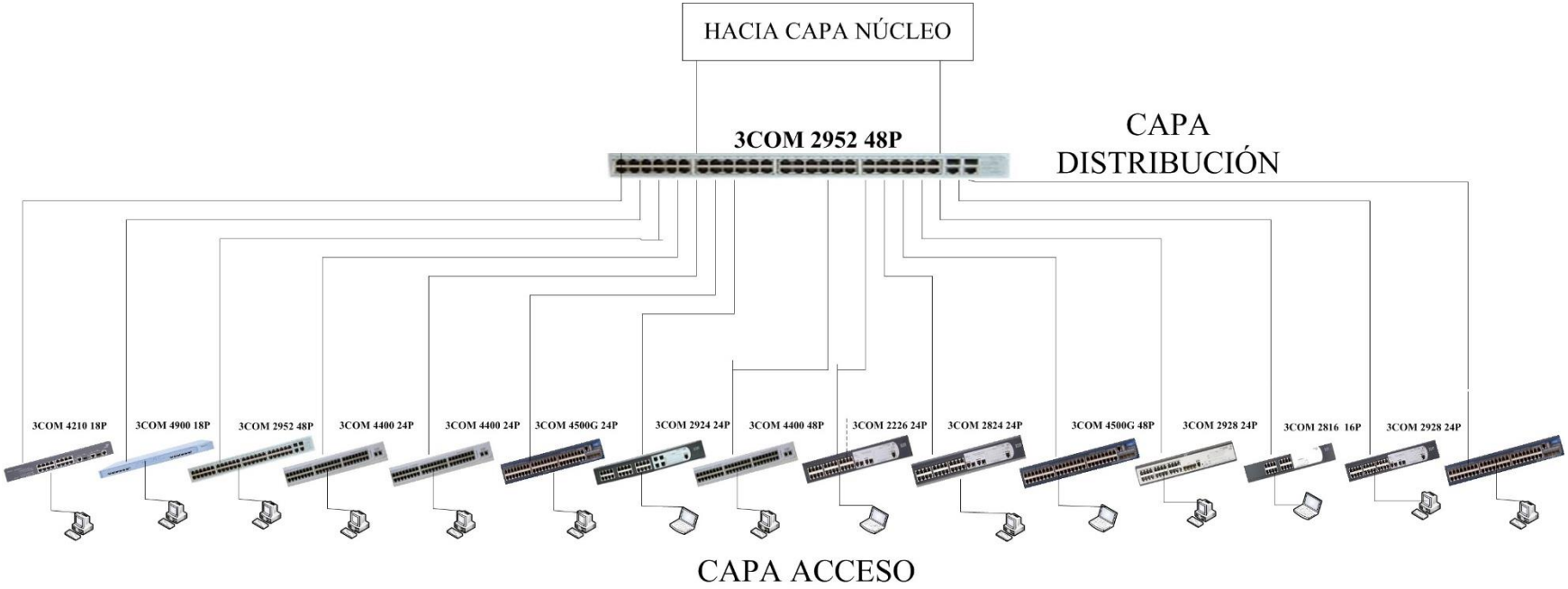


FIGURA 3.20: Diseño de la capa de distribución en la red jerárquica

Fuente: Elaborada por Andrea Zura

Los switches 3COM 2952 SFP PLUS 48P manejarán los enlaces de conexión con todos las conexiones hacia los servidores, conexiones en la red interna así como también el manejo de inter VLANs de la red del GADMO. Adicionalmente estos equipos se configuraran como backup asegurando así la disponibilidad de la red.

3.3.1.3 SWITCHES DE CAPA NÚCLEO

La capa núcleo de una topología jerárquica es una backbone de alta velocidad de la red y requiere switches que pueden manejar tasas muy altas de reenvío. La velocidad de reenvío requerida depende en gran medida del número de dispositivos que participan en la red. Por ello un switch de capa núcleo debe soportar capa 3, sus puertos deberán se Gigabit Ethernet/10 Gigabit Ethernet, tener componentes redundantes, agregado de enlace y soportar calidad de servicio. (CISCO)

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla 3-12 un resumen del switch elegido con sus respectivas características:

TABLA 3.12: Características switch 3com 5500 SFP 24P

SWITCH 3COM 5500 SFP 24P	
Funcionalidades	**Descripción**
Rendimiento	24 puertos 10/100/1000 Mbps 4puertos 1000 Mbps SFP Máxima Capacidad de switching: 184 Gbps. Máxima capacidad de transmisión 136.9 Mbps;
SWITCHING DE CAPA 2	VLANs basadas en protocolo IEEE 802.1Q Protocolo Spanning Tree (STP) IEEE 802.1D Protocolo Rapid Spanning Tree (RSTP) IEEE 802.1w
SWITCHING DE CAPA 3	Routing basado en hardware Rutas estáticas: 100 Interfaces Virtuales IP: 64 RIP (Protocolo de información de ruteo), v1 y v2 Open Shortest Path First (OSPF)
Priorización de tráfico	Clase de Servicio/Calidad de Servicio (CoS/QoS) IEEE 802.1p en salida
Seguridad	Las listas de control de acceso basadas en el tiempo

Fuente: Elaborado por Andrea Zura en referencia a http://goo.gl/QvBQ08

- Considraciones del diseño

La capa de núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. Además puede conectarse a los recursos de Internet. (CISCO)

En la figura 3-21, se muestran un diagrama físico de los switches de capa núcleo.

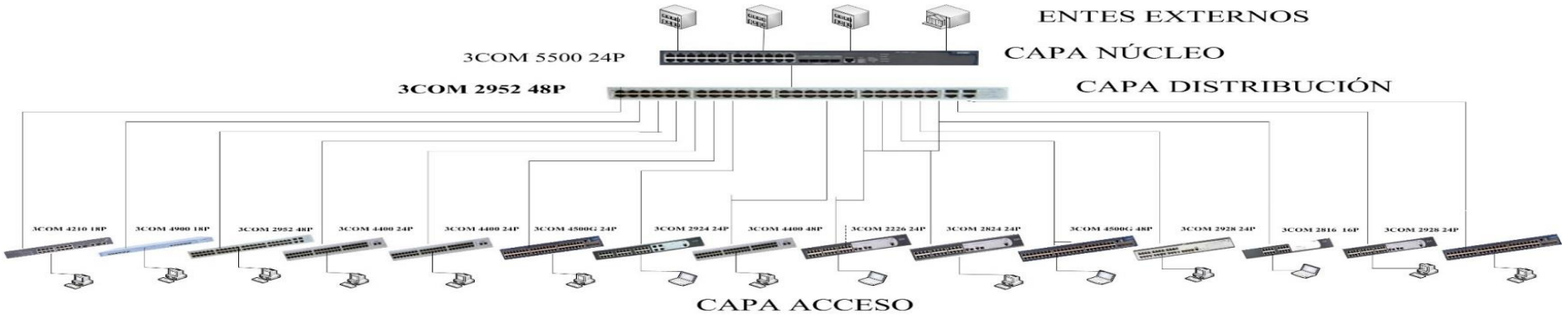


FIGURA 3.21: Diseño de la capa núcleo en la red jerárquica

Fuente: Elaborada por Andrea Zura

Además se pudo evidenciar que la topología actual de la red de datos del GADMO tiene los switches en configuración en cascada por la necesidad de dar servicio a la mayoría de los usuarios, sin embargo esto reduce el rendimiento de la red.

La red de datos del GADMO, cuenta con equipamiento COM, marca propietaria con tecnología XRN, la misma que permite mejorar el funcionamiento de la red, mediante la administración de los diferentes switches como una sola unidad.

3.4 PRUEBAS DE FUNCIONAMIENTO

Las pruebas de funcionamiento se las realizará utilizando métodos de Hacking Ético; el mismo que según (Plata) consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso"

3.4.1 DETECCIÓN DE VULNERABILIDADES

El atacante por lo general, buscara vulnerabilidades en el sistema que pueda aprovechar para transformarlas en ataques o amenazas. Dichas vulnerabilidades pueden ser Consultas a bases de datos, consultas de cabeceras de mails, escaneo de puertos, peticiones http, búsqueda de datos dentro de archivos, entre otros (Tori).

Dado esto, se realizará un escaneo de puertos mediante la herramienta Nmap, cuyo objetivo es la identificación de puertos abiertos, que estén a la espera de nuevas conexiones, permitidas o no.

Cabe aclarar que todas las pruebas realizadas son en base al método White Box Test; que de acuerdo a (Tori): este es un chequeo que es llevado a cabo por un pentester que tiene toda la información acerca del sistema.

3.4.1.1 ATAQUES O INTRUSIONES POR CAPAS

Los objetivos que persigue el Hacking ético de acuerdo a (Plata) son:

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

En base a dichos objetivos se realizaron las pruebas en las diferentes capas del modelo OSI, y tomando como referencia la Figura 3.22

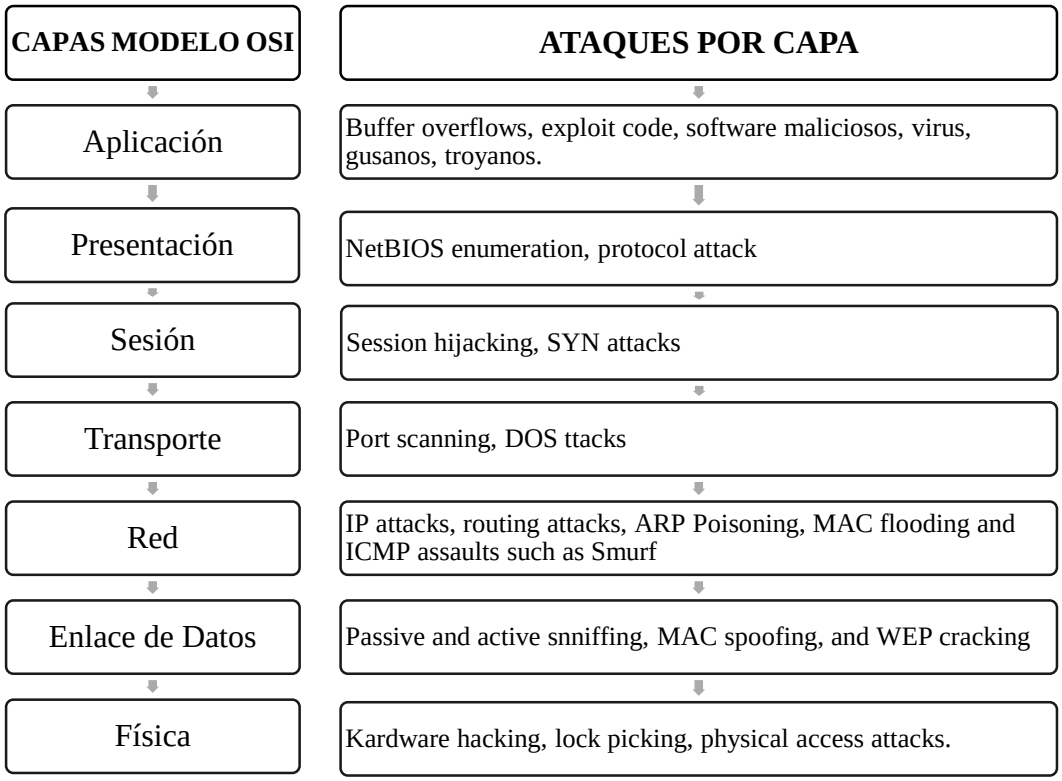


FIGURA 3.22: Ataques para cada capa del Modelo OSI

Fuente: Extraída de (Cabrera, 2012)

a. Capa Enlace de datos.

ARP spoffing fue la técnica elegida para realizar el hacking ético en esta capa; dicha técnica según (Thomas Demuth) es una técnica donde el atacante deliberadamente transmite un paquete ARP falso.

Para realizar el ARP Spoffing se siguieron los pasos siguientes:

Se debe activar el activar IP forwarding para evitar que se corte el tráfico del usuario, la configuración se muestran en la figura

```
root@SELKS:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

FIGURA 3.23: Activación del IP forwarding

Fuente: Extraída del terminal de SELKS

El siguiente paso es envenenar la tabla ARP tanto el **gateway** como el usuario para obtener hacer pasar el tráfico por el sistema del atacante en ambas direcciones:

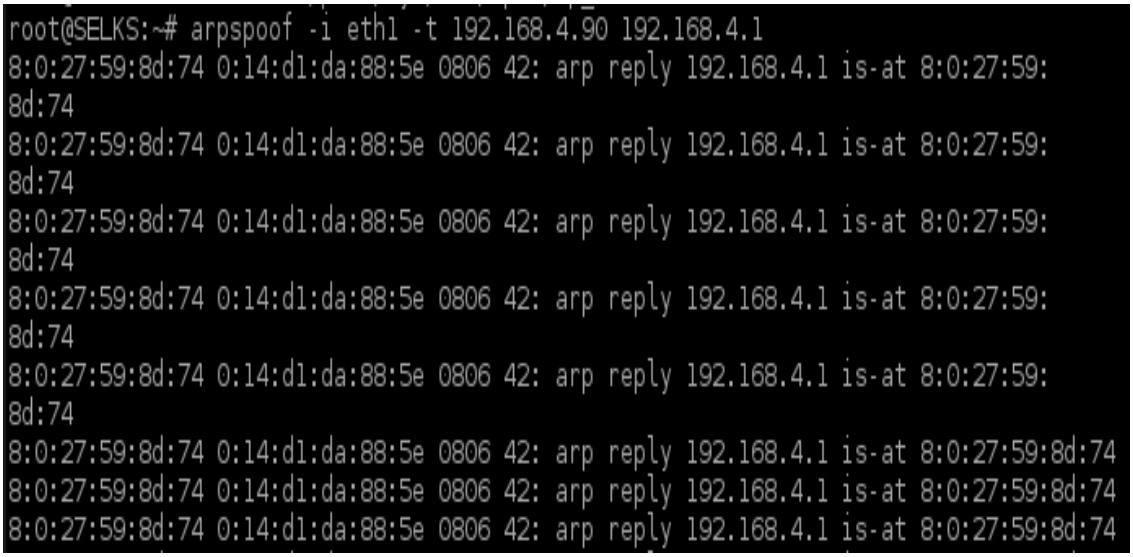


FIGURA 3.24: Envenenamiento IP en usuario

Fuente: Extraída del terminal de SELKS

A continuación hacemos lo mismo pero esta vez con el gateway:

FIGURA 3.25: Envenenamiento IP en Gateway

Fuente: Extraída del terminal de SELKS

Ahora se procede a capturar el tráfico en el host atacante mediante un tcpdump

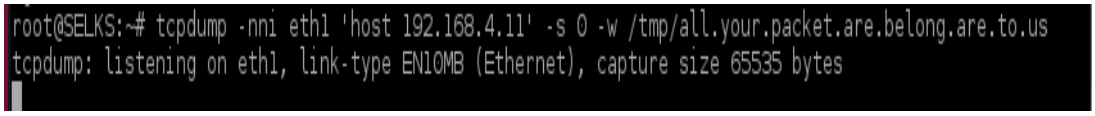
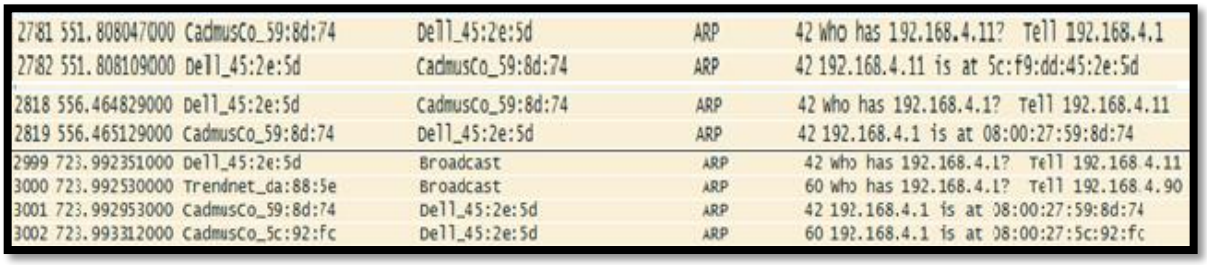


FIGURA 3.26: Captura de tráfico en host atacante.

Fuente: Extraída del terminal de SELKS

Eso es todo el proceso; el mismo se puede evaluar en un snnifer como lo es Wireshark[3], en el cual se podrá observar en la figura 3-27.



2781 551.808047000	CadmusCo_59:8d:74	Dell_45:2e:5d	ARP	42 Who has 192.168.4.11? Tell 192.168.4.1
2782 551.808109000	Dell_45:2e:5d	CadmusCo_59:8d:74	ARP	42 192.168.4.11 is at 5c:f9:dd:45:2e:5d
2818 556.464829000	Dell_45:2e:5d	CadmusCo_59:8d:74	ARP	42 Who has 192.168.4.1? Tell 192.168.4.11
2819 556.465129000	CadmusCo_59:8d:74	Dell_45:2e:5d	ARP	42 192.168.4.1 is at 08:00:27:59:8d:74
2999 723.992351000	Dell_45:2e:5d	Broadcast	ARP	42 Who has 192.168.4.1? Tell 192.168.4.11
3000 723.992530000	Trendnet_da:88:5e	Broadcast	ARP	60 Who has 192.168.4.1? Tell 192.168.4.90
3001 723.992953000	CadmusCo_59:8d:74	Dell_45:2e:5d	ARP	42 192.168.4.1 is at 08:00:27:59:8d:74
3002 723.993312000	CadmusCo_5c:92:fc	Dell_45:2e:5d	ARP	60 192.168.4.1 is at 08:00:27:5c:92:fc

FIGURA 3.27: Análisis de envenenamiento ARP en Wireshark

Fuente: Editado y extraído del software Wireshark

Se observa en la figura 3-27 ocho eventos en los que se describe:

- Eventos **2781-2782** se hace peticiones ARP desde el Gateway hacia el usuario; y se le da a conocer la dirección MAC de la petición.
- Eventos **2818-2819** se hace peticiones ARP desde el usuario hacia el gateway; y se le da a conocer la dirección MAC de la petición.
- Eventos **2999-3000** mediante broadcast se realiza la petición de conocer la dirección MAC tanto del gateway como del usuario.
- Eventos **3001-3002,** se puede observar ya el envenenamiento ARP, ya que en el primer evento se tiene una dirección MAC para la dirección IP del Gateway; pero a evento seguido esta dirección MAC cambia.
- **Mitigación.**

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

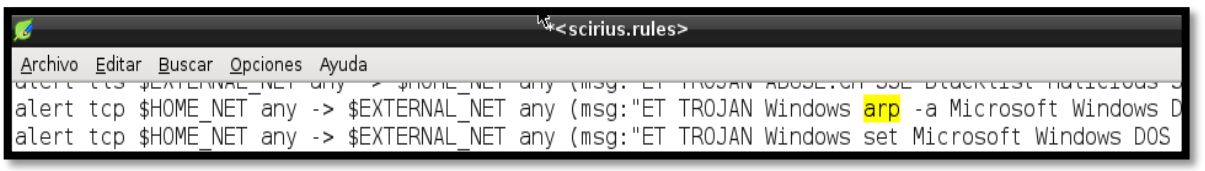


FIGURA 3.28: Mitigación ataque Arp Spoofing

Fuente: Extraído de SELKS

[3] Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. (Febrero, 2011)

El IDS-IPS, mostrará las alertas debido a que este ataque de ARP Spoffing. En la pantalla se muestran todas las direcciones MAC que están haciendo peticiones en la red; y acorde al número de veces que cada dirección MAC haga una petición se realiza un gráfico estadístico.

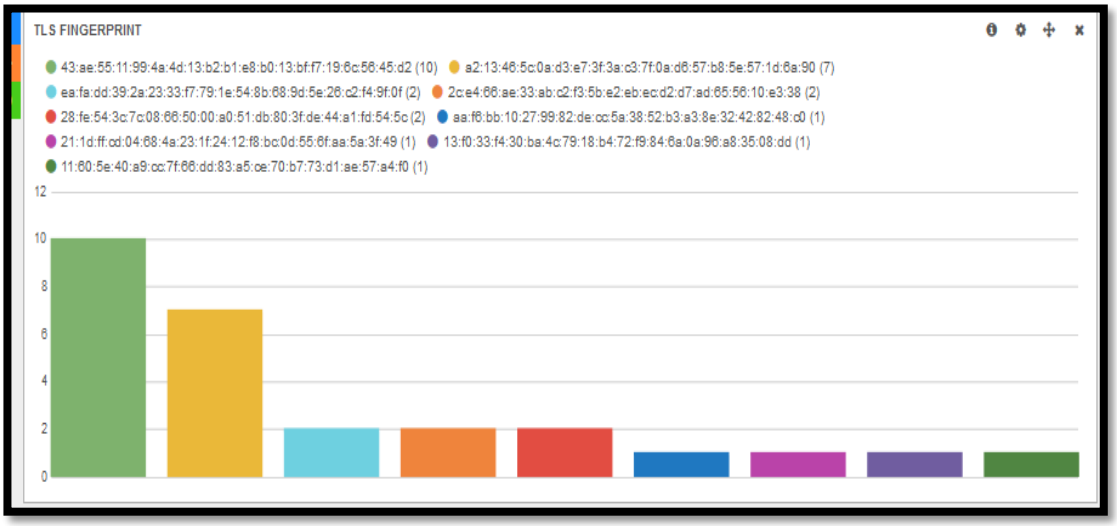


FIGURA 3.29: gráfico estadístico de eventos producidos por ataque ARP Spoffing
Fuente: Extraído del web admin de SELKS

Además se puede observar un resumen de alertas por dicho evento, en el que se indica entre los parámetros más importantes la dirección IP origen y destino.

@timestamp	src_ip	src_port	dest_ip	dest_port	tls.version	tls.subject
2015-02-04T05:48:58.943Z	192.168.4.11	5135	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T05:12:46.472Z	192.168.4.11	4978	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T04:17:03.075Z	192.168.4.11	4535	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T04:08:41.327Z	192.168.4.11	4437	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T04:37:17.230Z	192.168.4.11	4738	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T02:25:54.134Z	192.168.4.11	2662	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
2015-02-04T02:20:22.615Z	192.168.4.11	2636	192.168.4.1	443	TLS 1.2	C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS

FIGURA 3.30: Resumen de alertas producidas
Fuente: Extraído del web admin de SELKS

Se puede además desplegar de manera detallada cada uno de estos eventos; en los que se muestra además de las direcciones IP, las direcciones MAC.

View: Table / JSON / Raw

Field	Action	Value
@timestamp		2015-02-04T05:48:58.943Z
@version		1
_id		BByTFosfTgubmAWY__7ffQ
_index		logstash-2015.02.04
_type		SELKS
dest_ip		192.168.4.1
dest_port		443
event_type		tls
flow_id		35998032
host		SELKS
in_iface		eth1
path		/var/log/suricata/eve.json
proto		TCP
src_ip		192.168.4.11
src_port		5135
timestamp		2015-02-04T00:48:58.943158
tls.fingerprint		a2:13:46:5c:0a:d3:e7:3f:3a:c3:7f:0a:d6:57:b8:5e:57:1d:6a:90
tls.issuerdn		C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.subject		C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.version		TLS 1.2
type		SELKS

FIGURA 3.31: Detalle de alertas producidas

Fuente: Extraído del web admin de SELKS

3.4.1.1.2 CAPA DE RED

En esta capa se puede realizar diferentes tipos de ataques los mismos basan su objetivo en imposibilitar el acceso normal a los servicios y recursos de una organización durante un tiempo indefinido.

- **ICMP Flood**

Satura el un equipo con solicitudes de ICMP Echo Request para que no pueda responder a las peticiones reales.

Para realizar este ataque se utilizó un software denominado ByteDoS[4] v3.2

[4] La herramienta ByteDos utiliza la técnica SYN Flood, que consiste en enviar un flujo de paquetes TCP**/**SYN muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP**/**SYN-ACK y esperando el paquete de respuesta TCP**/**ACK.

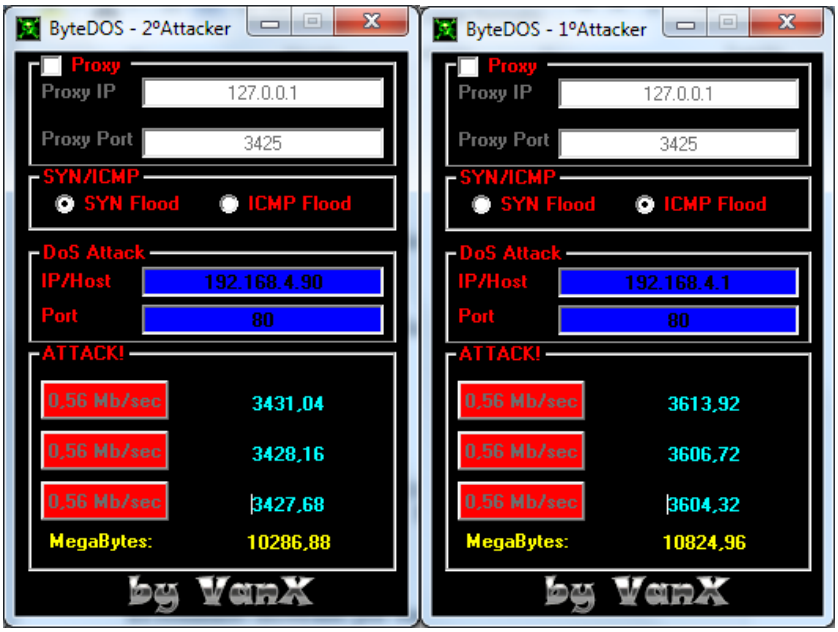


FIGURA 3.32: Saturación de equipo mediante ICMP Flood

Fuente: Extraído de ByteDoS v3.2

Se puede hacer un análisis con Wireshark, en el que se observa que, en un intervalo muy corto de tiempo, existen numerosos intentos de conexión por parte de la IP 192.168.4.11 al puerto 80 de la máquina 192.168.4.1, situación algo inusual.

FIGURA 3.33: Gráfica de flujo en Wireshark

Fuente: Extraída de Wireshark

- **Mitigación**

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

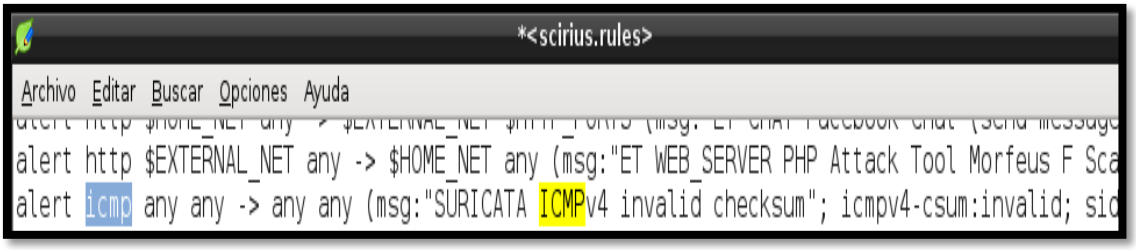


FIGURA 3.34: Mitigación ataque ICMP Flood

Fuente: Extraída de SELKS

El resultado mostrado por Suricata, se lo puede apreciar de diferentes modos; uno de ellos es mediante un gráfico estadístico en donde se muestran todas las alertas suscitadas en la red.

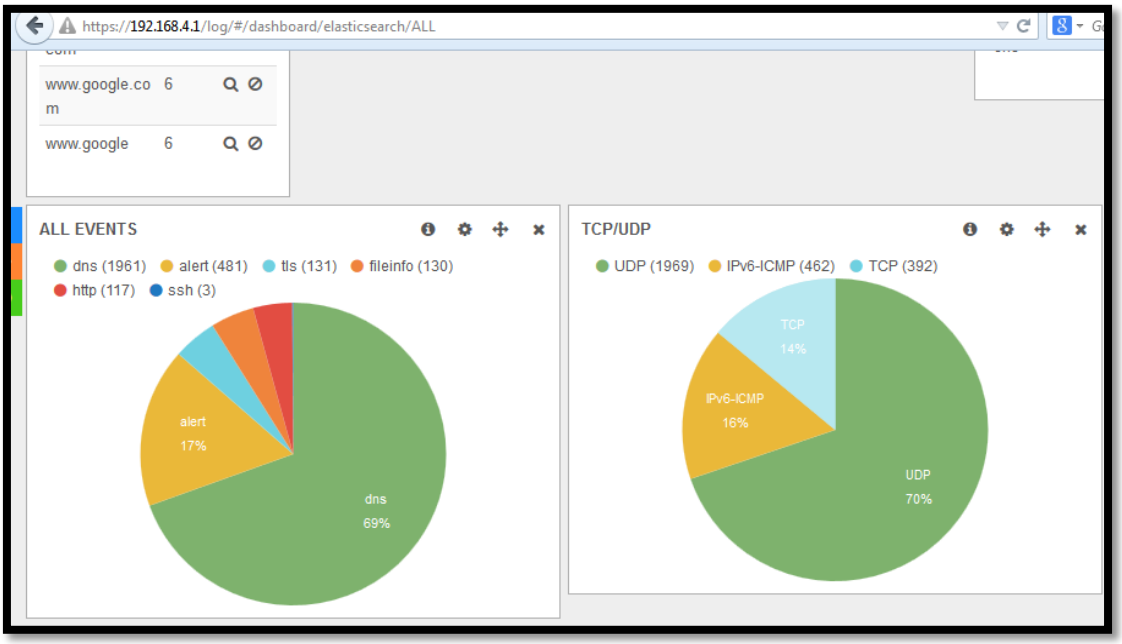


FIGURA 3.35: Resultado estadístico de Suricata

Fuente: Extraído del web admin de SELKS

Además el sistema muestra un gráfica de la ubicación del origen de las intrusiones suscitadas

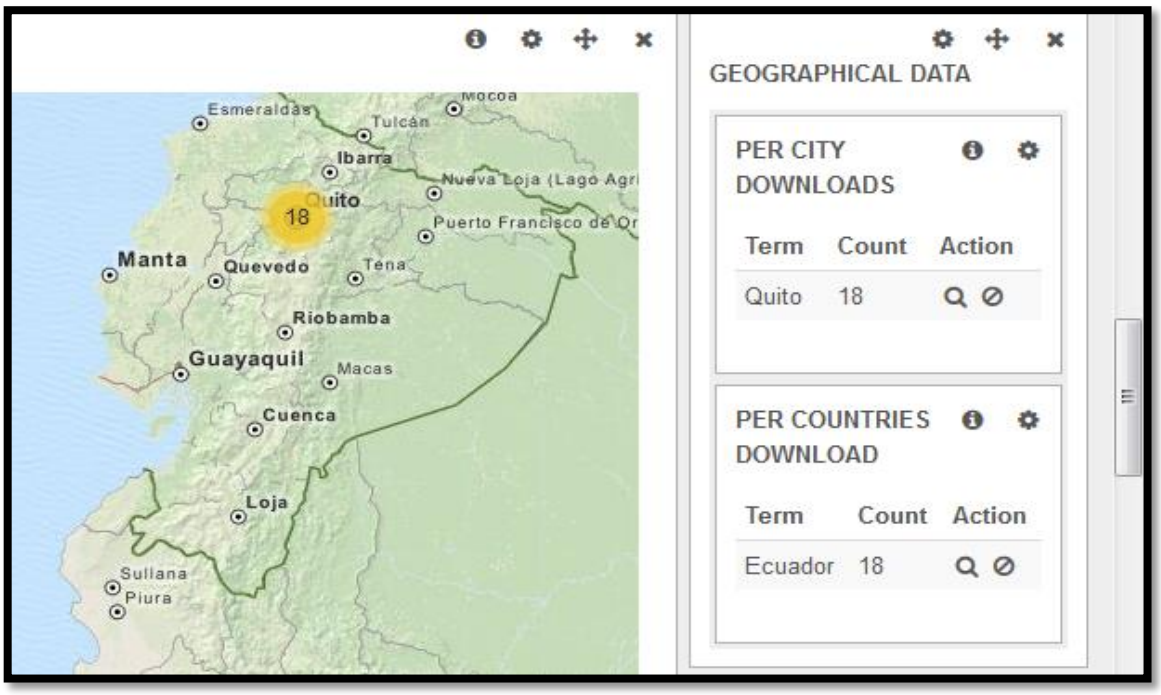


FIGURA 3.36: Gráfica de ubicación de intrusiones

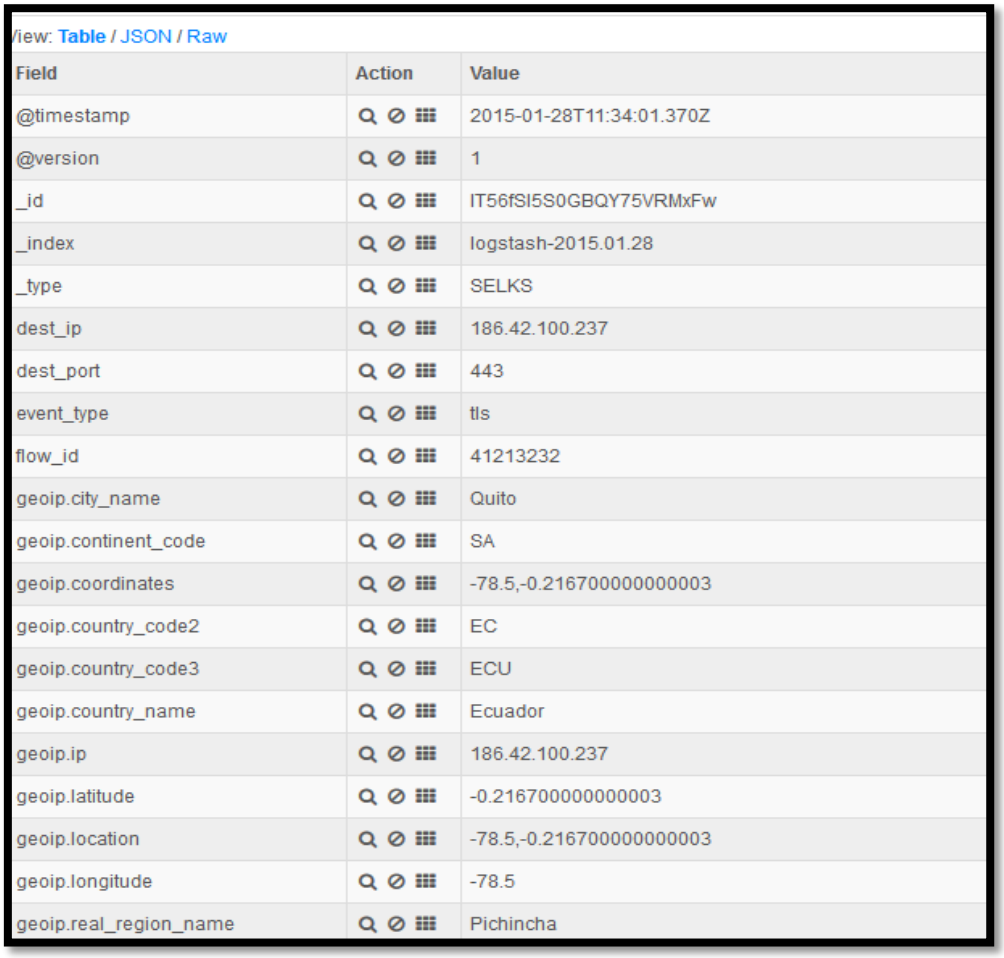
Fuente: Extraído del web admin de SELKS

Puede también mostrar un resumen de todas las alertas emitidas al IDS-IPS Suricata.

FIGURA 3.37: Resumen de alertas de intrución

Fuente: Extraído del web admin de SELKS

De igual manera se puede observar de manera detallada cada una de las alertas, donde se observará la dirección IP de origen, la hora de la penetración entre otros.



View: Table / JSON / Raw

Field	Action	Value
@timestamp		2015-01-28T11:34:01.370Z
@version		1
_id		IT56fSI5S0GBQY75VRMxFw
_index		logstash-2015.01.28
_type		SELKS
dest_ip		186.42.100.237
dest_port		443
event_type		tls
flow_id		41213232
geoip.city_name		Quito
geoip.continent_code		SA
geoip.coordinates		-78.5,-0.216700000000003
geoip.country_code2		EC
geoip.country_code3		ECU
geoip.country_name		Ecuador
geoip.ip		186.42.100.237
geoip.latitude		-0.216700000000003
geoip.location		-78.5,-0.216700000000003
geoip.longitude		-78.5
geoip.real_region_name		Pichincha

FIGURA 3.38: Detalle de alertas de intrución

Fuente: Extraído del web admin de SELKS

3.4.1.1.3 CAPA DE TRANSPORTE

En esta capa existen diferentes tipos de ataques, en los que se encuentra el Escaneo y fingerprinting[5], técnica que permite recopilar información significativa al apuntar un escaneo a los hosts del objetivo o al procesar la información que brinda éste como resultado. (Tori).

- **Escaneo de puertos**

[5] Es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red. Está basada en los tiempos de respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativo. http://urlmin.com/4qp95

Descubrir que puertos están abiertos, filtrados o cerrados, además de averiguar qué tipo y versión de aplicación está corriendo en estos puertos y servicios.

En base a estos conceptos preliminares; se realizó un escaneo de puertos, utilizando la herramienta nmap. Se muestra en la figura

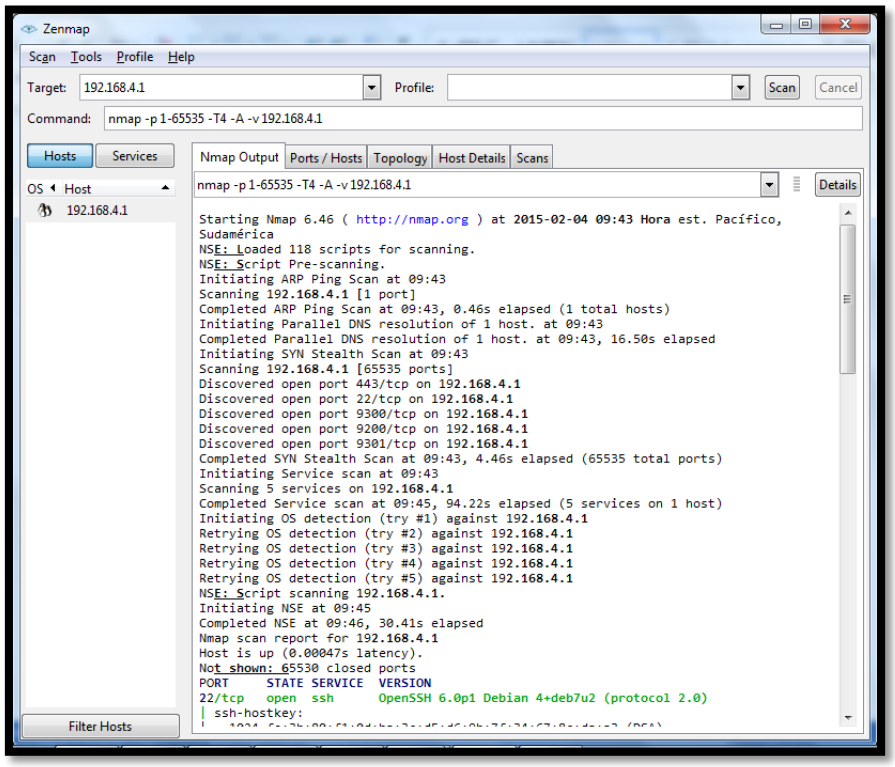


FIGURA 3.39: Escaneo de puertos

Fuente: Extraída del software Zenmap

Se puede observar que se tiene abierto el puerto SSH, por lo tanto se puede aprovechar esta vulnerabilidad y desde un cliente ingresar hasta el servidor; se muestra en la figura

Al igual que en los casos anteriores, es posible realizar un análisis mediante Wireshark, el mismo que se muestra en la figura.

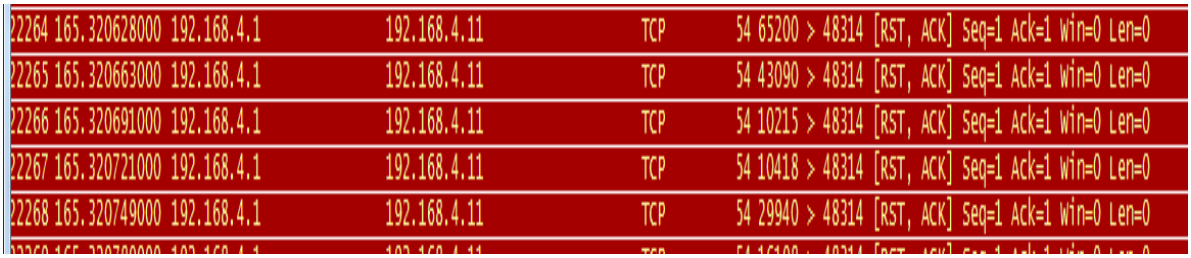


FIGURA 3.40: Análisis de puertos con Wireshark

Fuente: Extraída de Wireshark

- **Mitigación**

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

FIGURA 3.41: Mitigación Ataque de escaneo de puertos

Fuente: Extraído de SELKS

El resultado en Suricata es:

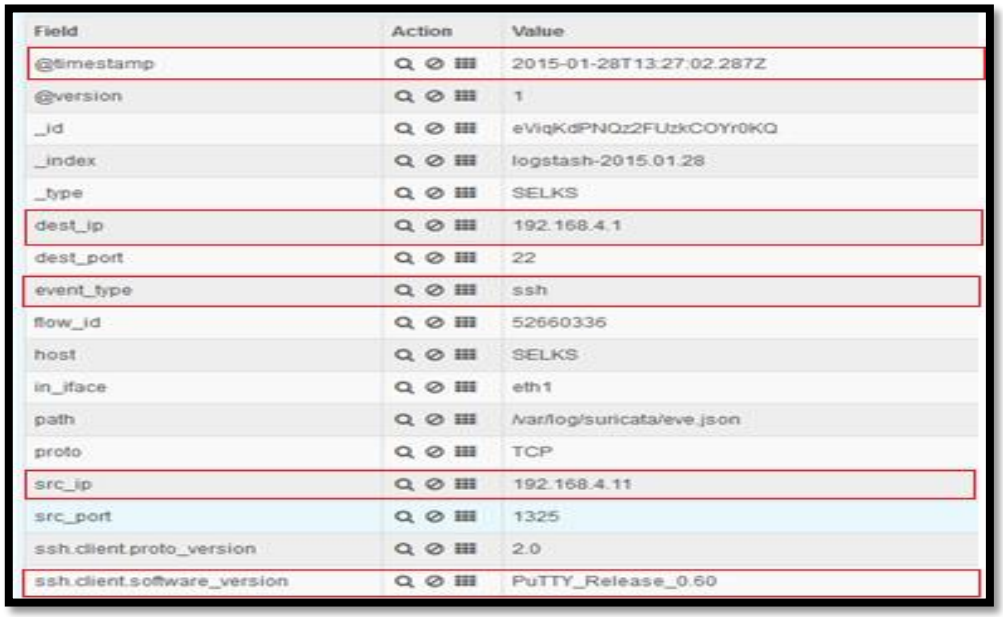


FIGURA 3.42: Resultado de alertas por escaneo de puertos

Fuente: Extraído del web admin de SELKS

En donde destacan información proporcionada por la alerta; tal como la dirección IP desde donde se realizó la petición, el servicio o protocolo; la hora y fecha exacta; así como también el software y la versión utilizada para realizar la intrusión.

3.4.1.1.4 CAPA DE SESIÓN

En esta capa se puede hacer diferentes ataques tales como escaneo TCP SYN, técnica que envía un paquete SYN. Si la respuesta es un paquete SYN/ACK, el puerto está abierto, mientras que si es un RST, se encuentra cerrado.

Es así que mediante la herramienta Znamap se realizá un escaneo TCP SYN; el mismo que nos da como resultado la cantidad de host activos; el sistema operativo que utiliza, la dirección IP y dirección MAC, el estado de los puertos; entre otros detalles.

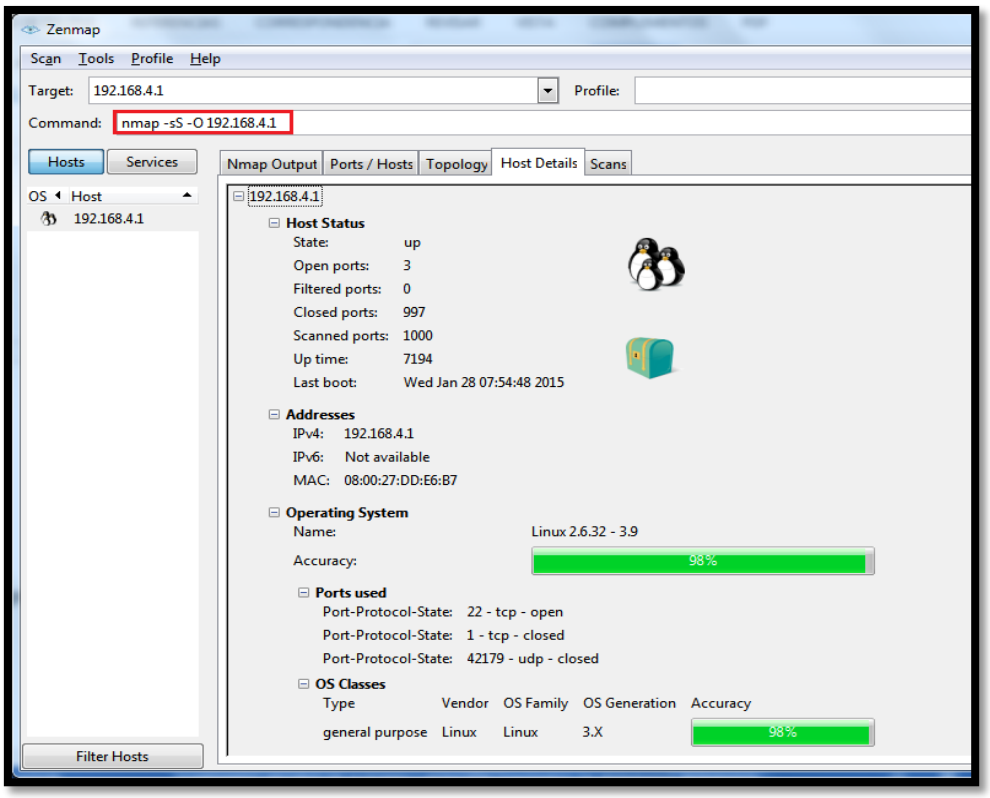


FIGURA 3.43: Escaneo TCP SYN

Fuente: Extraído d la herramienta Zenmap

- **Mitigación**

En el directorio de las reglas de suricata, encontraremos el archivo stream-events.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

FIGURA 3.44: Mitigación ataque escaneo TCP SYN

Fuente: Extraído de SELKS

El resultado de Suricata se presenta en un resumen en el que se indica la dirección IP de origen de la intrusión el tipo de intrusión, la hora en la que sucinto; entre otros.

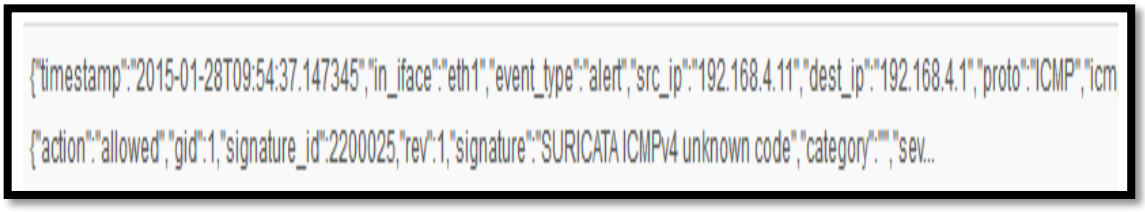


FIGURA 3.45: Resultado de alerta ante intrusión TCP-SYN

Fuente: Extraído del web admin de SELKS

3.4.1.1.5 CAPA DE APLICACIÓN

En esta capa se puede realizar ataques mediante la descarga de aplicaciones de dudosa procedencia.

Para ello desde el cliente realizaremos una descraga de un archivo ejecutable

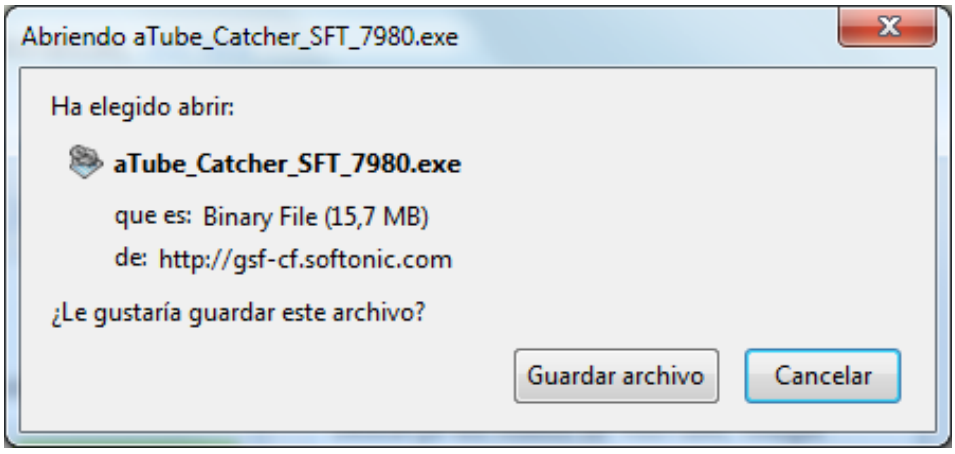


FIGURA 3.46: Descarga desde un cliente de un archivo ejecutable

Fuente: Extraída de entorno web cliente

- **Mitigación**

En el directorio de las reglas de suricata, encontraremos el archivo files.rules; en el cual se pude combatir este ataque; activando la alerta en dicho ataque.

FIGURA 3.47: Mitigación ataques de descargas de archivos dudosos

Fuente: Extraído de SELKS

Es así que el software muestra un gráfico estadístico de las descargas realizadas

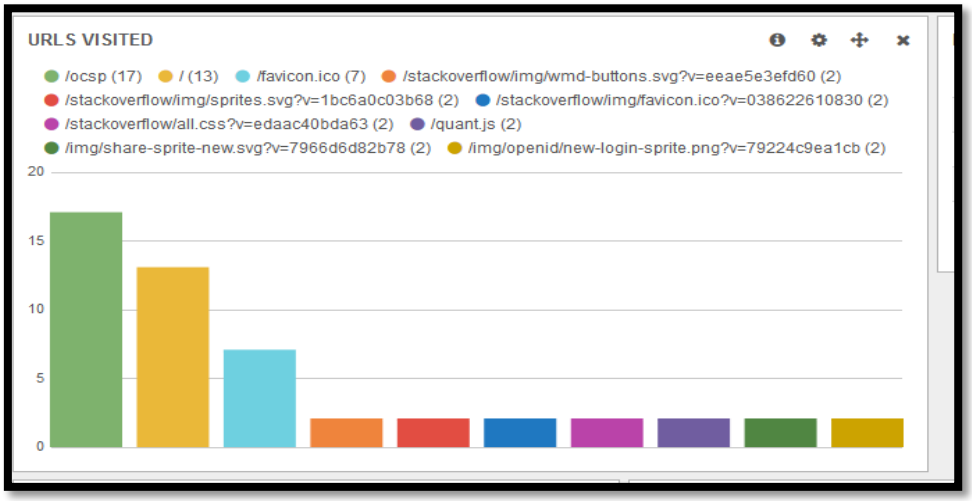


FIGURA 3.48: Gráfico estadístico de descargas realizadas

Fuente: Extraído del web admin de SELKS

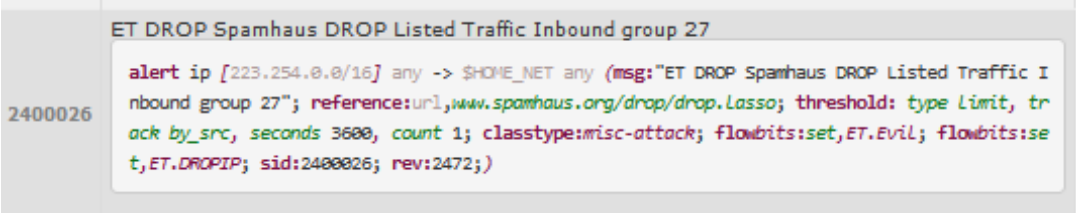


FIGURA 3.49: Gráfico estadístico de descargas realizadas

Fuente: Extraído del web admin de SELKS

CAPÍTULO IV

4 PRESUPUESTO REFERENCIAL

Se realizará un presupuesto referencial tomando en cuenta una comparación de tener una solución licenciada y una solución en software libre, en la instalación de un IDS-IPS.

Cabe recalcar que el análisis del presupuesto referencial tiene como objetivo principal proporcionar una medida del presupuesto invertido en la realización de un proyecto.

4.1 CÁLCULO

Antes de iniciar con el cálculo del presupuesto, es necesario aclarar que para el diseño del modelo presentado en el presente proyecto; en la red interna se realizó con los equipos de conmutación existentes en el GADMO; en la red perimetral de igual manera. En ésta última, se implementó un sistema de detección y prevención de intrusos en software libre, en base a ello se realizará el presupuesto referencial.

Para la migración de un sistema o programa de Software Propietario (no libre) a Software Libre (SL) se utilizará el siguiente método para calcular el Costo Total de la Solución (CTS). Este método deberá aplicarse tanto al Software Propietario como al Software Libre. Si el costo de este último es menor que el del propietario se deberá realizar la migración. (Secretaría Nacional de la Administración Pública, 2014)

Además en el portal web (Secretaría Nacional de la Administración Pública, 2014), se recalca que como requisitos previos de la migración de un sistema comercial a un sistema bajo software libre es necesario tener las siguientes consideraciones:

- Tener las capacidades mínimas funcionales y técnicas requeridas por la organización y los usuarios.
- Mantener o incrementar la productividad de la organización y los usuarios.
- Ser compatible o integrable en las plataformas de hardware y software existentes.

4.1.1 SOPHOS UTM 320 NETWORK PROTECTION

Como se había explicado previamente, el GADMO cuenta con dos equipos de protección de red, a nivel de hardware y software.

4.1.1.1 COSTO TOTAL DE LA SOLUCIÓN (CTS)

Para el cálculo del Costo Total de la Solución (CTS) según (Secretaría Nacional de la Administración Pública, 2014) se considera 3 componentes:

$$CTS = CTI + CTA + CTC$$

ECUACIÓN 4.1: Costo Total de Solución
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

- CTI: Costo Total de Implementación
- CTA: Costo Total Administrativo
- CTC: Costo Total de Capacitación

a. Costo Total de Implementación (CTI)

Es el costo total de rubros y actividades necesarios para poner a funcionar la solución. Se incluye adquisición de equipos, licencias y recurso humano puntual para la implementación. El CTI se calcula de la siguiente forma:

$$CTI = CP + CI + CADH + CADS + CM$$

ECUACIÓN 4.2: Costo Total de Implementación
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

- CP: Costos de las licencias del software considerando la arquitectura
- CI: Costos de instalación, configuración y adaptación (si fuera el caso)
- CADH: Costos adicionales de hardware e infraestructura
- CADS: Costos adicionales de software
- CM: Costos de migración de datos e integración
- Costos de las licencias del software considerando la arquitectura

TABLA 4.1: Gastos de adquisición en licencias de software UTM

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
[a] Sophos UTM 320 Network Protection Subscription	$4,285.00
TOTAL	**$4,285.00**

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

Nota [a]. El valor mostrado es de tres años de licencia.

- Costos de instalación, configuración y adaptación (si fuera el caso)

En este caso, no se incurrió en costos de instalación, configuración y adaptación debido a que la empresa brinda el soporte necesario para estos gastos.

Por lo tanto CI = 0.

- Costos adicionales de hardware e infraestructura

El GADMO cuenta con la infraestructura física del Sophos UTM 320, cuyos costos se muestran en la Tabla 4-2.

TABLA 4.2: Costos de hardware e infraestructura

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
Sophos UTM 320 Base Hardware - 8 GE ports, HDD + Base License for unl. users + power cable	$ 2,875.00
TOTAL	**$ 2,875.00**

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

- Costos adicionales de software

Existen costos adicionales de software, siempre y cuando se requiera instalar servicios adicionales prestados por la solución comercial. Se muestra en la Tabla 4-3.

TABLA 4.3: Costos adicionales de software

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
UTM 320 Full Guard Bundle Subscription	$13,000.00
TOTAL	**$13,000.00**

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

- Costos de migración de datos e integración

No existen rubros, en este caso.

Finalmente, con todos los cálculos realizados para el ***Costo Total de Implementación*** se tiene:

$$CTI = \$4{,}285.00 + \$0 + \$\,2{,}875.00 + \$13{,}000.00 + \$0$$

$$CTI = \$20{,}160.00$$

b. Costo Total Administrativo (CTA)

Es el costo total promedio anual de rubros y actividades necesarios para garantizar la disponibilidad, capacidad y continuidad de la solución implantada. Incluye el costo total promedio anual del recurso humano empleado en estas actividades. El CTA se calcula de la siguiente forma:

$$CTA = CMH + CASS + CRH$$

ECUACIÓN 4.3: Costo Total Administrativo

Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

- CMH: Costos de actualización y mantenimiento del hardware e infraestructura
- CASS: Costos de actualización y soporte del software
- CRH: Costos del Recurso Humano
- Costos de actualización y mantenimiento del hardware e infraestructura

Al comprar el hardware Sophos UTM, es un requisito adquirir también al menos un año de mantenimiento. En la Tabla 4-4 se muestra el presupuesto.

TABLA 4.4: Costos de actualización y mantenimiento del hardware e infraestructura.

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
Sophos UTM Premium Support [a]	$1,750.00
TOTAL	**$1,750.00**

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

Nota: [a] El valor mostrado es el costo de mantenimiento de tres años.

- Costos de actualización y soporte del software

Los CASS representan los costos de actualización de licencias o nuevas versiones y el soporte del software. Este último puede ser un valor fijo anual o estimado por horas/hombre. El valor se muestra en la Tabla 4 -5.

TABLA 4.5: Costos de actualización y soporte del software.

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
Sophos UTM 320 TotalProtect Renewal[a]	$1,465.00
TOTAL	**$1,465.00**

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

Nota: [a] El valor mostrado es el costo de renovación de software anual.

- Costos del Recurso Humano

El cálculo de estos se muestran en la Ecuación 4-4.

$$CRH = CA + CO + CS$$

ECUACIÓN 4.4: Costos del recurso humano

Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

- CA: Costo de personal de la organización para administración de la solución con el fin de garantizar la disponibilidad y correcto funcionamiento.

- CO: Costo de personal de la organización para operación de la solución con el fin de garantizar la continuidad de la misma.

- CS: Costo de personal de la organización para soporte en la solución de incidentes y problemas detectados.

i. Costo de personal de la organización para administración de la solución con el fin de garantizar la disponibilidad y correcto funcionamiento.

Es el costo promedio anual de un ingeniero administrador *número de ingenieros * porcentaje de tiempo dedicado a la administración de la solución * número de años de funcionamiento de la solución.

$$CA = N_{ING} \times \%Tiempo_{ADMIN} \times Años_{FUNCION.}$$

ECUACIÓN 4.5: Costo de administración de la solución
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Entonces

$$CA = 3 \times 10\% \times 3$$

$$CA = 0{,}9$$

ii. Costo de personal de la organización para operación de la solución con el fin de garantizar la continuidad de la misma.

El costo promedio anual de un ingeniero operador * número de ingenieros * porcentaje de tiempo dedicado a la operación de la solución * número de años de funcionamiento de la solución.

$$CO = N_{ING} \times \%Tiempo_{OPERAR} \times Años_{FUNCION.}$$

ECUACIÓN 4.6: Costo de operación de la solución.
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Entonces

$$CO = 1 \times 10\% \times 3$$

$$CO = 0{,}3$$

iii. Costo de personal de la organización para soporte en la solución de incidentes y problemas detectados.

El costo promedio anual de un ingeniero de soporte * número de ingenieros * porcentaje de tiempo dedicado al soporte de la solución * número de años de funcionamiento de la solución

$$CS = N_{ING} \times \%Tiempo_{SOPORTE} \times Años_{FUNCION.}$$

ECUACIÓN 4.7: Costo de soporte de la solución.

Entonces

$$CS = 1 \times 10\% \times 3$$

$$CS = 0{,}3$$

Cabe recalcar que los años de funcionamiento, se hicieron en relación al coste de los años de licencia, que en este caso son tres. En base a ello se tendrá:

$$CRH = 0{,}9 + 0{,}3 + 0{,}3$$

$$CRH = 1{,}5$$

Finalmente, con todos los cálculos realizados para el ***Costo Total Administrativo*** se tiene:

$$CTA = \$1{,}750.00 + \$1{,}465.00 + \$1.50$$

$$CTA = \$\mathbf{3216.50}$$

c. Costo Total de Capacitación (CTC)

Es el costo promedio anual para la capacitación continua del personal (técnico y usuarios) en la operación y explotación de la solución.

$$CTC = CT + CU$$

ECUACIÓN 4.8: Costo Total de Capacitación

Donde:

CT = Costo hora capacitación técnica * número de técnicos * número de horas * número años de funcionamiento de la solución

CU = Costo hora capacitación usuario * número de usuarios * número de horas * número años de funcionamiento de la solución.

En este caso no se ha realizado ningún tipo de capacitación técnica. El costo es $\$0$

Finalmente, con todos los cálculos realizados para **Costo Total de la Solución** del software comercial SOPHOS UTM se tiene:

$$CTS = \$20{,}160.00 + \$3{,}216.50 + \$0$$

$$\boldsymbol{CTS} = \$\mathbf{23{,}376.50}$$

4.1.2 SURICATA IDS-IPS

Ahora se repiten los cálculos para la solución bajo software libre, propuesto en el presente trabajo de titulación.

4.1.2.1 COSTO TOTAL DE LA SOLUCIÓN (CTS)

Para el cálculo del Costo Total de la Solución (CTS) según (Secretaría Nacional de la Administración Pública, 2014) **se** considera 3 componentes:

a. Costo Total de Implementación (CTI)

Es el costo total de rubros y actividades necesarios para poner a funcionar la solución. Se incluye adquisición de equipos, licencias y recurso humano puntual para la implementación. El CTI se calcula de la siguiente forma:

- Costos de las licencias del software considerando la arquitectura

TABLA 4.6: Gastos de adquisición en licencias de software SELKS

SELKS	
DESCRIPCIÓN	**PRECIO**
Sistema Operativo SELKS	$ 0.40[a]
TOTAL	**$ 0.40**

Fuente: Recuperado de: https://www.stamus-networks.com/open-source/#selks

Nota [a]. El sistema operativo SELKS, es un software gratito, descargable desde la web; el tiempo máximo de descarga es menor a 1 hora; $0.40, es el valor/hora del servicio de internet usado.

- Costos de instalación, configuración y adaptación (si fuera el caso)

En este caso, no se incurrió en costos de instalación, configuración y adaptación.

Por lo tanto CI = 0.

- Costos adicionales de hardware e infraestructura

La configuración mínima para el uso de SELKS es un computador con procesador de 2 núcleos y 4 GB en RAM, y mínimo 50 GB en disco duro.

TABLA 4.7: Costos de hardware e infraestructura

SELKS	
DESCRIPCIÓN	**PRECIO**
Inspiron 15 serie 5000 4.ª generación del procesador Intel® Core™ i3 Disco duro de 500 GB Memoria de 4 GB	$459,00
Adaptador Ethernet-USB	$ 20.00[a]
TOTAL	$479,00

Fuente: Recuperado de: http://www.dell.com/ec/p/inspiron-15-5547-laptop/pd?ref=PD_OC

Nota [a] Se considera además el precio de un adaptador de red Ethernet-USB o una tarjeta de red, ya que el IDS necesita de dos tarjetas de red.

- Costos adicionales de software

En este caso no existen gastos adicionales de software. Por lo tanto **CADS = $0.**

- Costos de migración de datos e integración

No existen rubros, en este caso. Por lo tanto **CM= $0.**

Finalmente, con todos los cálculos realizados para el ***Costo Total de Implementación*** se tiene:

$$CTI = \$0.40 + \$0 + \$479{,}00 + \$0 + \$0$$

$$CTI = \$479{,}40$$

b. Costo Total Administrativo (CTA)

Es el costo total promedio anual de rubros y actividades necesarios para garantizar la disponibilidad, capacidad y continuidad de la solución implantada. Incluye el costo total promedio anual del recurso humano empleado en estas actividades.

- Costos de actualización y mantenimiento del hardware e infraestructura

En este caso se puede calcular el costo de mantenimiento preventivo del computador realizado tres veces al año. En la Tabla 4-9 se muestra el presupuesto.

TABLA 4.8: Costos de actualización y mantenimiento del hardware e infraestructura.

SELKS	
DESCRIPCIÓN	**PRECIO**
Mantenimiento preventivo [a]	$180.00
TOTAL	**$180.00**

Fuente: Elaborada por Andrea Zura

Nota: [a] El valor mostrado es el costo de mantenimiento de tres años.

- Costos de actualización y soporte del software

Los CASS representan los costos de actualización de licencias o nuevas versiones y el soporte del software. Este último puede ser un valor fijo anual o estimado por horas/hombre. El valor se muestra en la Tabla 4-10.

TABLA 4.9: Costos de actualización y soporte del software.

Sophos UTM 320	
DESCRIPCIÓN	**PRECIO**
SELKS[a]	$0.40
TOTAL	**$**$0.40

Fuente: Recuperado de: http://www.enterpriseav.com/UTM-320.asp

Nota: [a] No es posible evaluar el tiempo de actualización del software, esto dependerá de las actualizaciones que realice el autor del sistema

- Costos del Recurso Humano

i. Costo de personal de la organización para administración de la solución con el fin de garantizar la disponibilidad y correcto funcionamiento.

Es el costo promedio anual de un ingeniero administrador *número de ingenieros * porcentaje de tiempo dedicado a la administración de la solución * número de años de funcionamiento de la solución.

Entonces

$$CA = 3 \times 10\% \times 3$$

$$CA = 0{,}9$$

ii. Costo de personal de la organización para operación de la solución con el fin de garantizar la continuidad de la misma.

El costo promedio anual de un ingeniero operador * número de ingenieros * porcentaje de tiempo dedicado a la operación de la solución * número de años de funcionamiento de la solución.

Entonces

$$CO = 1 \times 10\% \times 3$$

$$CO = 0{,}3$$

iii. Costo de personal de la organización para soporte en la solución de incidentes y problemas detectados.

El costo promedio anual de un ingeniero de soporte * número de ingenieros * porcentaje de tiempo dedicado al soporte de la solución * número de años de funcionamiento de la solución

Entonces

$$CS = 1 \times 10\% \times 3$$

$$CS = 0{,}3$$

Cabe recalcar que los años de funcionamiento, se hicieron en relación al mismo tiempo efectuado en el software licenciado. En base a ello se tendrá:

$$CRH = 0{,}9 + 0{,}3 + 0{,}3$$

$$CRH = 1{,}5$$

Finalmente, con todos los cálculos realizados para el **Costo Total Administrativo** se tiene:

$$CTA = \$180.00 + \$0\ .40 + \$1.50$$

$$CTA = \$181.90$$

c. Costo Total de Capacitación (CTC)

Es el costo promedio anual para la capacitación continua del personal (técnico y usuarios) en la operación y explotación de la solución.

En este caso, una capacitación del software por tres días es de $1500, además se debe incluir el costo de viáticos. El costo es $\$5000$

Finalmente, con todos los cálculos realizados para **Costo Total de la Solución** del software libre Suricata se tiene:

$$CTS = \ \$479{,}40 + \ \$181.90 + \$5000$$

$$\boldsymbol{CTS} \ = \$\mathbf{5661.30}$$

4.2. RESULTADO

Si el costo del software libre es menor que el del propietario se deberá realizar la migración.

Entonces:

Si $CTS_{Propietario}$ = $23,376.50 y $CTS_{Libre} = \$5661.30$

Se cumple que: $CTS_{Libre} < CTS_{Propietario}$

SE DEBE REALIZAR LA MIGRACIÓN

4.3 CONCLUSIONES Y RECOMENDACIONES

En base al desarrollo del trabajo realizado, en éste capítulo se exponen las principales conclusiones que se obtendrán a lo largo de la realización de este proyecto; y recomendaciones necesarias en los niveles de Seguridad Física, Host, Aplicación y Datos.

4.4 CONCLUSIONES

Se realizó un diseño de seguridad, utilizando un modelo multicapas denominado “Defensa en Profundidad” en la red de datos del GAD Municipal de Otavalo, aplicando nuevas políticas de seguridad en base a la norma ISO/IEC 27002, de manera que ataques externos e internos puedan ser detectados y evitados oportunamente.

La norma ISO/IEC 27002, fue la base principal para la realización del diseño, ya que en ella se establecen ciertas directrices y objetivos que permiten identificar claramente los riesgos a los que puede estar expuesta la organización, y gracias a ello se pudo crear un Manual de Normas y procedimientos de seguridad de la información; además de crear políticas de acceso en la red perimetral y red interna.

El levantamiento de información se ejecutó con OSSTM 3.0; una metodología de pruebas de penetración que permite realizar un análisis de riesgos en los canales, Humano, Físico, Telecomunicaciones y Redes de Datos, obteniendo resultados que permitieron elaborar un Manual de Normas y Procedimientos en Base a la Normo ISO/IEC 27002, la misma que es compatible con la metodología antes mencionada.

El estudio de la situación actual, en cuanto a la infraestructura de red permitió identificar las características y prestaciones de todo el equipamiento; en base a ello se utilizó dicha infraestructura en una nueva topología que ayudará al mejoramiento del servicio y el mejoramiento de la administración.

El beneficio de contar con dos Firewalls, en la infraestructura de Red de datos, ayuda a combatir los focos de inseguridad; siempre y cuando éstos se ubiquen de manera tal, que se aprovechen todas las funciones que dichos equipos ofrecen.

Un modelo de red jerarquizado utilizado para realizar el diseño de red interna, permite optimizar el uso de los recursos de la red; gracias a la aplicación de una topología de red basada en capas se obtienen características de escalabilidad, flexibilidad, y sobre todo seguridad.

Se realizaron pruebas de simulación de ataques en base a los objetivos de hacking ético; en las diferentes capas del modelo OSI, con lo que se pudo verificar el funcionamiento adecuado del IDS-IPS y su sistema de alertas.

Después de realizar el presupuesto referencial, y de establecer las diferencias entre tener una solución licenciada y una solución bajo software libre, se concluyó que el costo total solución bajo software libre es menor a la solución licenciada.

4.5 RECOMENDACIONES

La norma ISO/IEC 27002, establece ciertos objetivos de buenas prácticas para asegurar los sistemas de información de una organización; pero si dicha organización requiere una certificación será recomendable pasar a implementar la norma ISO/IEC 27001 la misma que especifica los requisitos a cumplir para implantar un SGSI certificable.

El levantamiento de información se ejecutó con OSSTM 3.0; dicha metodología de pruebas de penetración que permite realizar un análisis de riesgos en los canales, Humano, Físico, Telecomunicaciones y Redes de Datos; mediante objetivos y parámetros que no todos son obligatorios a cumplir; esto depende de la información que se necesite obtener; pero si se requiere un resultado más minucioso es recomendable cumplir con todos ellos.

La realización del Manual de normas y procedimientos se realizó en base a los resultados obtenidos en el levantamiento de información y a los objetivos de control proporcionados por la Norma ISO/IEC 27002; si se quiere mejorar la seguridad, este documento se debe revisar periódicamente; actualizarlo acorde a las necesidades y socializarlo a todo el personal para el cumplimiento del mismo.

El diseño de la red interna se realizó con los equipos con los que cuenta el GADMO para optimizar recursos; pero dicho diseño pude mejorar si se adquieren equipos nuevos con mejores prestaciones.

Al realizar un presupuesto referencial se comprobó que resulta menos costoso tener un sistema bajo software libre, este puede tener iguales o mejores prestaciones que un sistema licenciado, será recomendable migrar todos los sistemas a software libre para utilizar de mejor manera los recursos.

Para lograr eficiencia operativa en los equipos del Data Center, es necesario contar con adecuado sistema de enfriamiento, a través del uso de aires acondicionados de precisión, los mismos que permitirán mantener la temperatura y humedad dentro de los parámetros ideales. Este sistema debe mantenerse operativos 24/7 al igual que los servidores y equipos.

El cableado estructurado y eléctrico debe mantenerse operativo, es decir, que debe estar instalado siguiendo las normas vigentes, y que cumplan con las debidas pruebas de

certificación, así como también estar claramente identificado mediante etiquetas en las que se indique su origen y destino.

Aplicar políticas de acceso y control al Datacenter, por lo que es necesario la instalación de sistemas de identificación, ya sea éstos biométricos, sistemas de proximidad, identificadores de huella digital, entre otros que ayuden a tener un control y registro de las personas que ingresan al Datacenter.

Para asegurar la disponibilidad de los sistemas, es necesario tener redundancia en todo el Datacenter, o al menos en los sistemas sensibles, tales como la energía eléctrica, la misma que debe provenir de dos fuentes diferentes de alimentación así como también contar un banco de baterías, un generador eléctrico, UPS y TVSS.

Es necesario tener en cuenta las fechas de mantenimiento preventivo que se deben realizar al generador eléctrico para que el voltaje que genera, esté dentro de los parámetros requeridos.

Contar con equipos de monitoreo remoto, con el que se pueda obtener información de alarmas o eventos que requieran acciones inmediatas en el Datacenter; tales como el ingreso de una persona, la lectura de temperatura ambiente y humedad, apagado repentino de equipos.

Realizar un control de parches de softwares instalados para corregir las vulnerabilidades que más aprovechan las amenazas.

En base a las políticas de seguridad planteadas, es necesario tener un control de aplicaciones instaladas y filtrado web en todos los hosts de las estaciones de trabajo.

Tener instalado, actualizado y en constante escaneo al menos un software antivirus y anti-spam para reforzar la seguridad en los hosts e impedir la circulación de correo no deseado, virus y contenido inadecuado por la empresa.

Realizar mantenimientos preventivos periódicos de todos los host de la institución a fin de identificar y limpiar programas maliciosos, o que causen conflictos con el rendimiento de las PCs.

Cifrar los archivos y carpetas empresariales, así como los adjuntos del correo electrónico a fin de asegurar la confidencialidad de los mimos.

En los hosts, en los que se tengan instalado sistemas operativo Windows, resulta indispensable la activación del Firewall instalado por defeco en dichos sistemas.

Verificar que todas las aplicaciones creadas por el personal de la institución, y vayan a prestar servicios a los usuarios estén libres de error, y que no se pueden manipular.

Todas las aplicaciones que ejecutan operaciones relacionadas con información sensibles de la institución deben funcionar adecuadamente, de lo contrario, el éxito legitimidad de la misma se verán comprometidos.

Realizar respaldos automáticos y periódicos de todos los datos que cursen por la red, con mayor precaución y frecuencia de aquellos datos críticos, que comprometan la continuidad de la institución.

Para envíos de información crítica o delicada, es importante considerar herramientas de codificación, que ayudarán a mantener la privacidad, confidencialidad e integridad de los datos.

Es necesario brindar capacitaciones técnicas a todo el personal que trabaja en la Coordinación de TIC’s, con el fin de obtener la certificaciones del caso en todos los sistemas que se manejan en el GADMO, y que éstos a su vez puedan mejorar notablemente en el desempeño de sus actividades y por ende en el mejoramiento de los servicios prestados en la institución.

4.6 BIBLIOGRAFIA

Alfon. (22 de Febrero de 2011). *Seguridad y Redes*. Obtenido de http://seguridadyredes.wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/

Alvarado, M. S. (s.f.). OSSTMM 3. *Análisis y Diseño de Sistemas de Información*, 2.

Bertolín, J. A. (2008). *Seguridad de la Información .* España: Paraninfo.

Cabrera, E. C. (2012). *Metodologías y marcos de trabajo en seguridad de la información. Ataques comunes en capa 3.* Pereira.

CISCO. (s.f.). *CCNA 3.*

CISCO Networking Academic. (s.f.). CCNA Exploration 4.0. En *Conmutación y conexión inalámbrica de LAN.*

Estrada, A. C. (2011). *Seguridad por NIveles.* España: DarFE.

Febrero, B. M. (2011). *ANÁLISIS DE TRÁFICO CON WIRESHARK.* España.

Gómez, D. G. (Julio de 2003). Sistemas de Detección de Intrusiones.

Guiovanni, A. (s.f.). *GUIOOS' Blog*. Obtenido de https://guioos.wordpress.com

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (México). *Metodología de la Ivestigación.* MCGRAW-HILL.

Herzog, P. (s.f.). *OSSTMM 2.1.*

Herzog, P. (s.f.). *OSSTMM 3.0.*

López, P. A. (s.f.). *Seguridad Informática.* Editex.

Martínez, C. G. (2010). Modelo de Defensa en Profundidad.

Mathon, P. (2002). *ISA Server 2000 Proxy y Firewall.* Barcelona: EMI.

Microsoft. (2004). Guía de defensa en profundidad antivirus.

NTE INEN-ISO/IEC 27002. (2009). *Tecnología de la Información- Técnicasde la Seguridad - Códifo de Práctica para la Gestión de la Seguridad de la Información.* Quito.

Plata, A. R. (s.f.). *Ethical Hacking.*

Romero Ternero, M. D., Barbancho Concejero, J., Benjumea Móndejar, J., Rivera Romero, O., Ropero Rodríguez, J., Sánchez Antón, G., & Sivianes Castillo, F. (2010). *Redes Locales.* Madrid: Paraninfo.

Sarubbi, J. P. (2008). *Seguridad Infornática.* Buenos Aires.

Secretaría Nacional de la Administración Pública. (22 de Enero de 2014). *Gobierno Elecctrónico .* Obtenido de http://www1.gobiernoelectronico.gob.ec

Tanenbaum, A. (2003). *Redes de Computadoras.* Mexico: Pearson.

Thomas Demuth, A. L. (s.f.). *ARP Spoofing y Poisoning, TRUCOS DE TRÁFICO.*

Tori, C. (s.f.). *Hacking Ético.* Rosario .

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

INDICE DE ACRÓNIMOS

ACL: Access Control List. (Listas de Control de Acceso)

ATM: Asynchronous Transfer Mode. (Modo de Transferencia Asíncrona)

CCNA: Cisco Certified Network Associate (Asociado en Redes con Certificación Cisco.)

DMZ: Demilitarized Zone (Zona Desmilitarizada)

DNS: Domain Name System (Sistema de Nombres de Dominio)

EMI: ElectroMagnetic Interference (Interferencia Electromagnética)

FDDI: Fiber distributed data interface (Interfaz de Datos Distribuida por Fibra)

FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)

GAD: Gobierno Autónomo Descentralizado

GADMO: Gobierno Autónomo Descentralizado Municipal Otavalo

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

IDS: Intrusion Detection System (Sistema de detección de intrusiones)

IEC: Comisión Electrotécnica Internacional**.**

IEEE: Institute of Electrical and Electronic Engineers (Instituto de Ingeniería Eléctrica y Electrónica)

INEN: Instituto Ecuatoriano de Normalización

IP: Internet Protocol (Protocolo de Internet)

IPS: Intrusion Prevention System (Sistema de Prevención de Intrusiones)

ISECOM: Federal Information Processing Standard (Estándares Federales de Procesamiento de la Información)

ISL: Inter-Switch Link

ISO: International Standard Organization (Organización Internacional para la Estandarización)

MAC: Media Access Control (Control de Acceso al Medio)

NIC: Network Interface Card (Tarjeta de Interfaz de Red)

NTE: Norma Técnica Ecuatoriana

OISF: Open Information Security Foundation (Fundación Abierta de Seguridad de Información)

OSSTMM: Open Source Security Testing Methodology Manual (Manual de la Metodología Abierta de Testeo de Seguridad)

PPP: Point-to-Point Protocol (Protocolo Punto-Punto)

PVST: Protocolo Spanning Tree for VLAN

RAV: Risk Assessment Values (Valores de la Evaluación de Riesgos)

SAI: Sistema de Alimentación Ininterrumpida

SMB: Server Message Block (Servicio de Bloqueo de Mensajes)

SMTP: Simple Mail Transfer Protocol (Protocolo Simple de Transmisión de Correo)

SSH: Secure SHell.

TCP: Transmission Control Protocol (Protocolo de control de transmisión)

TIC: Tecnologías de la información y la comunicación

TLS: Transport Layer Security (Seguridad de la Capa de Transporte)

UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario)

UPS: Uninterrupted Power Supply (Sistema de Alimentación Ininterrumpida)

TVSS: Transient Voltage Surge Suppressors (Supresor de Transitorios de Voltaje)

URL: Uniform Resource Identifier (Identificador uniforme de recurso)

VLAN: Virtual Local Area Network (Red de Área Local Virtual)

VTP: VLAN Trunking Protocol

XRN: eXpandable Resilient Networking.

ANEXO A

A.1 CANAL HUMANO

Para realizar el análisis en este canal se ha considerado interactuar con el elemento humano de una manera física o psicológica.

A.1.1. SEGURIDAD OPERACIONAL

Seguridad Operacional, también conocida como la porosidad del alcance, es el primero de los tres factores de la seguridad real que deberían determinarse. Se mide inicialmente como la suma de la visibilidad del alcance P_V, de acceso P_A, y la confianza P_T. (Herzog, OSSTMM 3.0)

El análisis será sobre la funcionalidad y la interacción que tiene cada funcionario de acuerdo al organigrama funcional del GADMO, con el centro de informática y la seguridad de la información dentro de la entidad.

El resultado obtenido es:

$$_H = P_V + P_A + P_T$$

ECUACIÓN A.1: Seguridad Operacional
Fuente: Obtenida de (Herzog, OSSTMM 3.0)

$$P_H = 1 + 3 + 2$$

$$P_H = 6$$

A continuación se detalla de donde se obtuvieron los resultados de la seguridad operacional en el canal humano.

A.1.1.1 VISIBILIDAD

Enumerar el personal dentro del alcance tanto con acceso autorizado y no autorizado a los procesos dentro del alcance, sin importar la hora o el canal de acceso, y el método para la obtención de esos datos. (Herzog, OSSTMM 3.0)

TABLA A.1: Resultados obtenidos en el segmento Visibilidad

Resultados Obtenidos	**Metodología utilizada**	Observación Directa Encuestas	
	Nombres de la personas de entrada	Wilman G. José H. Rocío P. Marcelo G. Luis L. Marcela E.	Javier P. Curi Y. Efrain A. Soraya R. Roque P.
	Tipo de Acceso	Autorizado	Restringido

Fuente: Elaborada por Andrea Zura

El nivel de visibilidad en el canal "Humano" será de: P_V= 1; debido a que las personas que trabajan directamente en la coordinación de TICs tiene acceso autorizado, y personas que tienen interacción con el alcance tienen acceso restringido, pero pese a ello hay una persona con acceso restringido que puede acceder.

A.1.1.2 ACCESOS

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos. (Herzog, OSSTMM 2.1)

TABLA A.2: Resultados obtenidos en el segmento Accesos

Resultados Obtenidos	Metodología utilizada	Ingeniería Social Observación Directa
	Nombres de la personas de entrada	Wilman G. Roque P.
	Información Obtenida	Aplicaciones de servidores Ubicación del cuarto de equipos # de Extensiones Telefónicas

Fuente: Elaborada por Andrea Zura

El nivel de acceso en el canal "Humano" será de: P_A= 3

A.1.1.3 CONFIANZA

Las pruebas de confianzas entre el personal dentro del ámbito donde la confianza se refiere al acceso a la información o de los activos físicos de otros objetivos dentro del alcance. (Herzog, OSSTMM 3.0)

TABLA A.3: Resultados obtenidos en el segmento Confianza

Resultados Obtenidos	**Metodología utilizada**	Observación Directa
	Nombres de la personas de entrada	Carolina M. Freddy L. Margarita V. Milton F.
	Tipo de Información obtenida	Usuarios y contraseñas a host y correos **CONFIDENCIALES**

Fuente: Elaborada por Andrea Zura

El nivel de acceso en el canal "Humano" será de: P_T= 2.

A.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones. En primer lugar la suma de la pérdida en los controles es LC_{SUM} debe ser determinada por la suma de las 10 categorías de las perdidas en los controles. (Herzog, OSSTMM 3.0).

TABLA A.4: Lista de Controles usados en OSSTMM 3.0

CONTROLES	**Clase A**	Autenticación	LC_{Au}
		Indemnización	LC_{Id}
		Resistencia	LC_{Re}
		Subyugación	LC_{Su}
		Continuidad	LC_{Ct}
	Clase B	No Repudio	LC_{NR}
		Confidencialidad	LC_{Cf}
		Privacidad	LC_{Pr}
		Integridad	LC_{It}
		Alarma	LC_{Al}

Fuente: Editada de (Herzog, OSSTMM 3.0)

Así, la suma de los controles LC_{SUM} se da así:

$$LC_{SUM} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

ECUACIÓN A.2: Suma de pérdida en los controles
Fuente: Obtenida de (Herzog, OSSTMM 3.0)

A.1.2.1 AUTENTICACIÓN

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en el que una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o actividad fraudulenta. (Herzog, OSSTMM 3.0)

TABLA A.5: Resultados obtenidos en el control de Autenticación

Resultados Obtenidos	**Lista de aplicaciones que necesitan autenticación**	Ingreso al sistema de inicio en los host en cada estación. Ingreso a las bases de datos Ingreso a las aplicaciones en todos los servidores
	Bloque del sistema	Después de 3 intentos

Fuente: Elaborada por Andrea Zura

En este caso existen métodos adecuados de autenticación en el canal humano. Por lo tanto:

$$LC_{Au} = 3$$

A.1.2.2 INDEMNIZACIÓN

Documentar y enumerar el abuso o la elusión de la política de los empleados, seguros, confidencialidad, no competencia, contratos de responsabilidad civil, o el uso / renuncias de los usuarios con todo el personal de acceso dentro del alcance sobre todos los canales. (Herzog, OSSTMM 3.0)

TABLA A.6: Resultados obtenidos en el control de Indemnización

Resultados Obtenidos	Lista de contratos, seguros de los empleados, contratos de confidencialidad.	Actas entrega de equipos informáticos Actas de responsabilidad de equipos informáticos Acta de responsabilidad del buen uso de contraseñas de ingreso a sistemas Actas de responsabilidad del buen uso de usuarios y contraseñas del correo institucional. Actas de responsabilidad del buen uso de internet dentro de la entidad. Acuerdo de confidencialidad de información reservada de la entidad
	Lista de abuso o elución de pollita de empleados	

Fuente: Elaborada por Andrea Zura

En este caso no existe abuso o elusión de la indemnización en el canal humano por parte de los empleados, pero si se tiene un control de indemnización. Por lo tanto:

$$LC_{Id} = 6$$

A.1.2.3 RESISTENCIA

Enumerar y probar las insuficiencias en todos los canales del personal en el ámbito el cual la eliminación del personal de puerta de enlace permita el acceso directo a los activos. (Herzog, OSSTMM 3.0)

TABLA A.7: Resultados obtenidos en el control de Resistencia

Resultados Obtenidos	Lista del personal qe interactúan en el ámbito de la seguridad de información.	Luis. L Marcela E. Marcelo G. José H. Rocio P. Wilman G.	
	Canales	***Insuficiencias***	***Aciertos***
	Físico	X	
	Telecomunicaciones	X	
	Redes de datos		X
	Inalámbrico	X	

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control, en todos los canales es de:

$$LC_{Re} = 1$$

A.1.2.4 SUBYUGACIÓN

Es un control que garantiza que las interacciones ocurran solamente de acuerdo con los procesos definidos. El administrador de los activos definen cómo se produce la interacción que elimina la libertad de elección, sino también la responsabilidad de la pérdida del partido interactuar. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de subyugación es nulo; es decir: $LC_{Su} = 0$

A.1.2.5 CONTINUIDAD

Es un control sobre todas las interacciones para mantener la interactividad con los activos en el caso de la corrupción o el fracaso.

Contar cada caso de Access de confianza en el ámbito de aplicación lo que asegura que ninguna interrupción en la interacción a través del canal y el vector pueden ser causados, incluso en situaciones de fracaso total. La continuidad es el paraguas plazo para características como la capacidad de supervivencia, equilibrio de carga, y redundancia. (Herzog, OSSTMM 3.0)

TABLA A.8: Resultados obtenidos en el control de Continuidad

Resultados Obtenidos	**Tipo de Test**	Observación Directa
	Acciones	Si el personal sale de vacaciones o por motivos de salud, o personal necesita de permiso para ausentarse ya sea por horas o días.
	Observaciones	El desarrollo de las actividades cotidianas dentro de la organización puede tener ciertas fallas, ocasionando debilidades en la continuidad.

Fuente: Elaborada por Andrea Zura

Por lo tanto el control de continuidad es: $LC_{Ct} = 0$

A.1.2.6 NO REPUDIO

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma. (Herzog, OSSTMM 2.1)

Enumerar y probar al uso o las deficiencias del personal para identificar y registrar el acceso o la interacción con los activos de pruebas específicas para cuestionar el repudio correctamente. Documentar la profundidad de la interacción que se registra. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de No-Repudio es nulo; es decir: $LC_{NR} = 0$

A.1.2.7 CONFIDENCIALIDAD

La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo. (Herzog, OSSTMM 2.1)

En esta sección, sin embargo, un método de confidencialidad puede incluir murmullo o el uso de señales manuales. (Herzog, OSSTMM 3.0)

TABLA A.9: Resultados obtenidos en el control de Confidencialidad

Resultados Obtenidos	Tipo de Test	Murmullo
	Acciones	En el GADMO se realiza envío de notificaciones o peticiones mediante memorandos, u oficios, en los que se detallan información relevante para la institución.
	Observaciones	Dichos documentos no son leídos únicamente por los interesados, sino por terceras personas; existiendo falta de confidencialidad.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Confidencialidad es:

$$LC_{Cf} = 1$$

A.1.2.8 PRIVACIDAD

Mapa de los guardianes de los activos de información privadas dentro del ámbito de aplicación, la información que se almacena, cómo y dónde se almacena la información, y sobre las que los canales se comunica la información.

TABLA A.10: Resultados obtenidos en el control de Privacidad

Resultados Obtenidos	**Tipo de Test**	Mapa de los guardianes de los activos de información privadas
	Que se almacena, cómo y dónde se almacena la información	Toda información privada se almacena en bases de datos y discos duros.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Privacidad es:

$$LC_{Pr} = 1$$

A.1.2.9 INTEGRIDAD

En HUMSEC, la separación de funciones y otros mecanismos de corrupción de reducción proporcionan un control de integridad. Asegurar la integridad personal en que dos o más personas se necesitan para un único proceso para asegurar la supervisión de ese proceso. Esto incluye que no existe un maestro de acceso a todo el proceso. No puede haber una persona con acceso completo y sin llave maestra para todas las puertas.

TABLA A.11: Resultados obtenidos en el control de Integridad

Resultados Obtenidos	Tipo de Test	Observación directa
	Lista de personas que tienen acceso a todos los lugares	En el GADMO, las personas encargadas de la limpieza, tiene acceso a todas las oficinas; pero no tienen acceso a lugares restringidos como el cuarto de comunicaciones.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Integridad es:

$$LC_{It} = 1$$

A.1.2.10 ALARMA

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en el que una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o actividad fraudulenta. (Herzog, OSSTMM 3.0)

TABLA A.12: Resultados obtenidos en el control de Alarma

Resultados Obtenidos	Tipo de Test	Observación directa
	Observaciones	Cuando existen alarmas emitidas por el antivirus de urls sospechosas al acceder a ciertas páginas de internet, el usuario responde de manera adecuada a este tipo de alarmas cerrando inmediatamente la conexión.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Alarma es: $LC_{Al} = 1$

A.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están ponderadas de forma individual. La ponderación de las vulnerabilidades, debilidades y preocupaciones se basan en una relación entre la suma OpSec, la pérdida de controles.

A.1.3.1 VULNERABILIDAD

Contar por separado cada defecto o error que desafía las protecciones por el que una persona o un proceso pueden acceder, negar el acceso a los demás, u ocultar activos dentro del alcance. (Herzog, OSSTMM 3.0)

TABLA A.13: Resultados obtenidos en Limitación de Vulnerabilidad

Resultados Obtenidos	**Tipo de Test**	Observación directa
	Observaciones	• Debido a tendencias culturales y políticas no se daba información necesaria para ocupar los nuevos puestos. • Falta de capacitación o experiencia para ocupar las vacantes dejadas al ser cambio de autoridades.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, las vulnerabilidades son:

$$L_V = 2$$

A.1.3.2 DEBILIDAD

Es el defecto o error que interrumpa, reduce, abusos, o anula específicamente los efectos de los cinco controles de interactividad: la autenticación, la indemnización, la resiliencia, la subyugación y la continuidad. (Herzog, OSSTMM 3.0)

TABLA A.14: Resultados obtenidos en limitación de Debilidad

Resultados Obtenidos	**Tipo de Test**	Observación directa
	Observaciones	• El no haber un guardia en el acceso al Data Center

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el cálculo de las debilidades es:

$$L_W = 1$$

A.1.3.3 PREOCUPACIÓN

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma. (Herzog, OSSTMM 3.0)

$$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

ECUACIÓN A.3: Cálculo de la Limitación Preocupación
Fuente: (Herzog, OSSTMM 3.0)

$$L_C = 1 + 1 + 1 + 1 + 0$$

$$L_C = 4$$

A.1.3.4 EXPOSICIÓN

Cuente cada injustificable acción, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o bienes dentro del canal ámbito elegido. (Herzog, OSSTMM 3.0).

$$L_K = P_V = 1$$

A.1.3.5 ANOMALÍAS

Cuente cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, por lo general cuando la fuente o el destino del elemento no se pueden entender. Una anomalía puede ser una señal temprana de un problema de seguridad. Dado que las incógnitas son los elementos que no pueden ser controlados, una auditoría adecuada requiere ir observando y anotando todas las anomalías. (Herzog, OSSTMM 3.0)

No se observaron anomalías durante el tiempo que se realizó el test de penetración, por lo tanto:

$$L_A = 0$$

A.2 CALCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática. (Herzog, OSSTMM 3.0).

De acuerdo a los valores obtenidos en la seguridad operacional, controles y limitaciones, se ha realizado el cálculo; el mismo que se muestra en la Figura A-1.

Human Security Testing

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	1		
Access	3		
Trust	2		
Total (Porosity)	6		

CONTROLS			
Class A		Missing	
Authentication	3	3	
Indemnification	6	0	
Resilience	1	5	
Subjugation	0	6	
Continuity	0	6	
Total Class A	10	20	
Class B		Missing	
Non-Repudiation	0	6	
Confidentiality	1	5	
Privacy	1	5	
Integrity	1	5	
Alarm	1	5	
Total Class B	4	26	
		True Missing	
All Controls Total	14	46	
Whole Coverage	23,33%	76,67%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	2	8,666667	17,333333
Weaknesses	1	4,333333	4,333333
Concerns	4	5,333333	21,333333
Exposures	1	1,677778	1,677778
Anomalies	0	1,422222	0,000000
Total # Limitations	8		44,6778

OPSEC	7,722143
True Controls	4,619143
Full Controls	4,619143
True Coverage A	33,33%
True Coverage B	13,33%
Total True Coverage	23,33%
Limitations	13,323878
Security Δ	-16,43
True Protection	83,57

Actual Security: 83,6299 ravs

FIGURA A.1: Cálculo del RAVS en Canal Humano

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

A.2.1 INTERPRETACIÓN DE RESULTADOS

La seguridad operacional es bastante baja, tomando en cuenta que ésta evalúa las diferentes políticas y procedimientos implementados por la administración. Esto refleja la falta de manuales de normas y buenas prácticas del manejo de información.

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que se tiene mucha prioridad en cuanto a la indemnización del personal, más no así en otros controles que son totalmente nulos como la Subyugación y la Continuidad.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a ello se tiene limitaciones nulas como en el no repudio; y casi nulas en cuanto a confidencialidad, privacidad, integridad y alarma.

ANEXO B

B.1 SEGURIDAD FÍSICA

PHYSSEC (seguridad física) es una clasificación para la seguridad material en el reino físico que está dentro de los límites del espacio 3D humano-interactivo. Prueba de este canal requiere la interacción no-comunicativo con las barreras y los seres humanos en posiciones controlador de acceso de los activos. Este canal cubre la interacción del analista dentro de la proximidad de los objetivos. (Herzog, OSSTMM 3.0)

B.1.1 SEGURIDAD OPERACIONAL

A continuación se detalla cómo se obtuvieron los resultados de la seguridad operacional en el canal de seguridad física.

B.1.1.1 VISIBILIDAD

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico.

1. Trazar mapa del perímetro físico

2. Trazar mapa de las medidas de protección físicas (cercas, puertas, luces, etc.)

3. Trazar mapa de las rutas de acceso y/o métodos físicos

4. Trazar mapa de las áreas no monitoreadas (Herzog, OSSTMM 2.1)

TABLA B.1: Resultados obtenidos en Seguridad Operacional: Visibilidad

	Mapa del perímetro físico	**Tipos de medidas de protección física**	**Lista de áreas desprotegidas o insuficientemente protegidas.**
Resultados obtenidos	Por motivos de confidencialidad, el mapa del perímetro físico no será mostrado en este documento.	Personal de guardianía. Alarmas contra incendios.	Por motivos de confidencialidad, las áreas insuficientemente protegidas no serán mostradas en este documento.

Fuente: Elaborada por Andrea Zura

Después del análisis realizado el resultado de visibilidad es: P_V= 8

B.1.1.2 ACCESOS

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos.

TABLA B.2: Resultados obtenidos en seguridad operacional: Accesos

Resultados Obtenidos	**Lista de puntos de acceso físicos**	Ventanas Puertas
	Tipos de autenticación	Biométricos
	Tipos de sistemas de alarmas	Alarmas contra incendios
	Lista de disparadores de alarmas	-

Fuente: Elaborada por Andrea Zura

1. Enumerar áreas de control de acceso

2. Examinar dispositivos y tipos de control de acceso

3. Examinar tipos de alarmas

4. Determinar el nivel de complejidad en un dispositivo de control de acceso

5. Determinar el nivel de privacidad en un dispositivo de control de acceso

6. Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades

7. Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso

El nivel de acceso en el canal "Físico" será de: P_A= 4

B.1.1.3 CONFIANZA

Este es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos. (Herzog, OSSTMM 2.1)

1. Enumerar las áreas de la organización que son visibles.

a. Debido a que es un Municipio, y que está al servicio de la ciudadanía, existen muchos lugares visibles, pro ninguno que comprometa la seguridad de información.

2. Enumerar las áreas dentro de la organización que son audibles.

a. Existen tres lugares audibles que son visibles, pero los 3 están al servicio de la comunidad.

3. Examinar las áreas de la ubicación referentes a las entradas por abastecimiento y búsqueda de puntos débiles y vulnerabilidades.

a. Existen puntos débiles y vulnerables, no se revelará la ubicación por motivos de confidencialidad; pero en este caso se tiene una **confianza de 2.**

4. Listar las empresas y empleados de abastecimiento.

a. Existen varios proveedores de sistemas y correspondencia que representan una vulnerabilidad debido al acceso que tienen al activo más importante dentro de una organización. Para este caso se tiene una **confianza de 4**

5. Listar las empresas y empleados de limpieza.

a. Dentro del edificio hay varias personas encargadas de la limpieza, y pueden significar un punto de vulnerabilidad debido al acceso que tienen. Para este caso se tiene una **confianza de 3.**

TABLA B.3: Resultados obtenidos en Seguridad Operacional: Confianza

Resultados Esperados	Mapa de ubicación física de los bienes Lista de ubicación física de los puntos de acceso Lista de puntos de acceso vulnerables en la ubicación Lista de la ubicación de los accesos de terceras partes	
	Ejemplo:	En una auditoría física, un edificio con una habitación separado por 2 puertas internas abiertas cuenta como confianza de 2. Si se cierran las puertas que separan la habitación, entonces es una confianza de 0 ya que estos no son los puntos donde se puede pasar.

Fuente: Elaborada por Andrea Zura

El nivel de confianza en el canal "Físico" será de: P_T= 9.

B.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

B.1.2.1 AUTENTICACIÓN

La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro de la meta y la autenticación requerida. El punto de acceso es el punto principal de cualquier interacción de activos. La verificación de un punto de acceso que existe es una parte de la determinación de su propósito. (Herzog, OSSTMM 2.1)

TABLA B.4: Resultados obtenidos en Control de Autenticación

Resultados Obtenidos	Ejemplo:	En una auditoría PHYSSEC, si se requiere tanto una tarjeta de identificación especial y una exploración de la huella del pulgar para acceder, a continuación, añadir dos para la autenticación. Sin embargo, si el acceso sólo requiere uno o el otro, entonces sólo una cuenta.
	Cuente cada instancia de autenticación necesaria para acceder. Esto requiere que la autorización e identificación componen el proceso para el correcto uso del mecanismo de autenticación.	

Fuente: Elaborada por Andrea Zura

En este caso existe control de autenticación de huella digital; de acceso más no de registro.

$$LC_{Au} = 1$$

B.1.2.2 INDEMNIZACIÓN

(a) Documentar y enumerar la capacidad de abusar o evadir la política de los empleados, de seguros, de no divulgación, no competencia, contratos de responsabilidad civil, o el uso / renuncias de usuario para el personal dentro del ámbito de aplicación.

(b) Enumerar el uso de señales de advertencia de peligro, vigilancia o alarmas en efecto, problemas de salud, y publicaciones de ninguna entrada.

(c) Verificar el alcance y la finalidad de la acción legal que se utiliza para mantener la indemnización.

TABLA B.5: Resultados obtenidos en Control Indemnización

Resultados Obtenidos	**Lista de de señales de advertencia de peligro, vigilancia o alarmas en efecto, problemas de salud, y publicaciones de ninguna entrada.**	Existen algunas señales de emergencia en el GADMO; mas no las suficientes. Existen también garantías de los activos fijos tales como: • Computadores • Servidores • Equipos de conmutación • Equipos de ruteo. • Impresoras • Ploter • Software; entre otras. Pero cabe recalcar que muchas de ellas ya vencieron.
	Ejemplo	Un ejemplo básico es una señal de peligro que amenaza con enjuiciar intrusos. Otro ejemplo común es el seguro de la propiedad. En un ámbito de 200 computadoras, una póliza de seguro contra el robo de una de ellas, se aplica a todas las 200 y, por tanto, es un recuento de 200.

Fuente: Elaborada por Andrea Zura

En este caso el control de indemnización en el canal físico es de: $LC_{Id} = 8$

B.1.2.3 RESISTENCIA

La determinación y la medición de la capacidad de resistencia de las barreras y guardias en el ámbito de los cambios excesivos u hostiles diseñados para causar insuficiencia de operaciones. (Herzog, OSSTMM 3.0).

TABLA B.6: Resultados obtenidos en Control Resistencia

Resultados Obtenidos	Enumerar y verifique que la distracción, la eliminación o aquietamiento de personal no permitirán el acceso directo a los activos u operaciones.	Existen Policías Municipales que custodian el GADMO.
	Enumerar y verificar que la desactivación o destrucción de las medidas de seguridad o controles operacionales no permitirán el acceso directo a los activos u operaciones.	***Los resultados de este test se mantendrán de manera confidencial, por motivos de seguridad.***
	Compruebe que el aislamiento del alcance de los recursos, como el combustible, la energía, los alimentos, el agua, las comunicaciones, etc. no permite el acceso directo a los activos u operaciones.	***Los resultados de este test se mantendrán de manera confidencial, por motivos de seguridad.***
	Ejemplo:	En una auditoría física cuando el control de 2 guardias de acceso a una puerta, si uno se retira y la puerta no se puede abrir por la guardia restante, entonces tiene resistencia.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de resistencia de:

$$LC_{Re} = 0$$

B.1.2.4 SUBYUGACIÓN

Enumerar y prueba de deficiencias en acceso a los bienes no controlados por la fuente que proporciona el acceso (es decir, números PIN, fotografías de identificación, etc. seleccionados por parte del actor, inicios de sesión con los números de identificación escritas en por parte del actor, etc.) (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de subyugación es nulo; es decir: $LC_{Su} = 0$

B.1.2.5 CONTINUIDAD

TABLA B.7: Resultados obtenidos en Control Continuidad

Resultados Obtenidos	Enumerar y verificar las condiciones en que los retrasos de acceso son abordados adecuadamente a través del personal de copia de seguridad o un medio automatizado para el acceso oportuno a los servicios, procesos y operaciones.	Se tiene un sistema automatizado de copias de seguridad.
	Verificar que el aislamiento del alcance a partir de recursos, tales como combustible, energía eléctrica, alimentos, agua, comunicaciones, etc., no se detendrá o negar el acceso a los servicios, procesos y operaciones.	En este test, mediante observación directa se pudo verificar el control de continuidad a partir de recursos importantes como combustible, transporte y energía. Los resultados no se muestran por motivos de confidencialidad.
	Verificar que la incapacidad para eliminar los residuos, contaminantes u otros contaminantes del ámbito de aplicación no detenga o deniegue el acceso a los servicios, procesos y operaciones.	En este test, mediante aplicación directa se pudo verificar el control de continuidad a partir de la limpieza de cuartos de equipos en el GADMO. Los resultados no se muestran por motivos de confidencialidad.

Fuente: Elaborada por Andrea Zura

Por lo tanto el control de continuidad es:

$$LC_{Ct} = 1$$

B.1.2.6 NO REPUDIO

Enumerar y poner a prueba para su uso o insuficiencias de los monitores y sensores para identificar y registrar el acceso o las interacciones con los activos de pruebas específicas para desafiar repudio correctamente. Documentar la profundidad de la interacción que se registra. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de No-Repudio es nulo; es decir: $LC_{NR} = 0$

B.1.2.7 CONFIDENCIALIDAD

Enumerar y probar el uso o deficiencias de todas las señales, la comunicación física, y los elementos transportados internamente entre ambos y los procesos y el personal que utilicen códigos, lenguaje indescifrable, "tranquilizado" o "cerrado" las interacciones personales para promover la confidencialidad de la comunicación sólo a los que tienen el correcto control de seguridad de esa comunicación clasificada.

De acuerdo al test, el control de Confidencialidad es:

$$LC_{Cf} = 0$$

B.1.2.8 PRIVACIDAD1

Enumerar y probar el uso o insuficiencias de todas las interacciones dentro del alcance utilizando etiquetado no evidente a las interacciones hacia el “cuarto cerrado", y dentro de cuartos elegidos al azar para ocultar o proteger la privacidad de la interacción sólo a los que tienen la habilitación apropiada de seguridad para ese proceso o activo. (Herzog, OSSTMM 3.0)

Se utiliza etiquetado de los activos para proteger la privacidad de los mismos.

De acuerdo al test, el control de Privacidad es:

$$LC_{Pr} = 1$$

B.1.2.9 INTEGRIDAD

TABLA B.8: Resultados obtenidos en Control Integridad

Resultados Obtenidos	Tipo de Test	Observación directa
	Enumerar y probar las deficiencias en de todas las señales y la comunicación entre procesos y personal que utiliza un proceso documentado, sellos, firmas digitales, o marcas cifradas para proteger y asegurar que los activos no pueden ser cambiados, redirigidos, o invierten sin que sean conocidas las partes involucradas en el acceso a todos los lugares	Todos los documentos que se transmiten internamente en el GADMO, tienen sello y firma, por parte de los receptores y emisores; así como de terceras personas que intervengan en el proceso de transporte de los mimos.
	Verificar todos los medios de almacenamiento de información no esté en peligro de la descomposición natural, tales como daños por el calor o la humedad, la decoloración de la luz solar directa, o la degradación magnética.	Algunos medios de almacenamiento de información cumplen con las medidas de seguridad que evitan daños de descomposición natural; mientras que otros no.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Integridad es:

$$LC_{It} = 2$$

B.1.2.10 ALARMA

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, inicie de sesión o mensaje para cada pasarela de acceso cuando una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la actividad fraudulenta, violación o incumplimiento. Asegúrese de que los sensores / sistemas se instalan a las normas nacionales, regionales o internacionales y probados con regularidad para cubrir todos los puntos accesibles. (Herzog, OSSTMM 3.0)

TABLA B.9: Resultados obtenidos en Control Alarma

Resultados Obtenidos	**Tipo de Test**	Observación directa
	Observaciones	Cuando existen alarmas emitidas por el firewall de intentos de intrusión, el administrador de la red actúa de la mejor manera ante dicha alarma.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Alarma es:

$$LC_{Al} = 1$$

B.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están ponderadas de forma individual.

B.1.3.1 VULNERABILIDAD

En la seguridad física, una vulnerabilidad puede ser tan simple como una puerta de cristal, una puerta de metal corroído por el tiempo, una puerta que se puede cerrar por acuñando de monedas en la brecha entre él y su marco, los equipos electrónicos no sellada partir plagas como las hormigas o ratones, una unidad de CD de arranque en un PC, o un proceso que permite a un empleado para tomar un bote de basura lo suficientemente grande como para ocultar o transporte activos fuera del ámbito de aplicación. (Herzog, OSSTMM 3.0)

Debido a razones confidenciales no se van a enumerar las vulnerabilidades de la organización.

De acuerdo al test, las vulnerabilidades son:

$$L_V = 10$$

B.1.3.2 DEBILIDAD

En seguridad física, una debilidad puede ser una cerradura de la puerta que se abre cuando una tarjeta se acuña entre éste y el marco de la puerta, un generador eléctrico de respaldo sin combustible, o un seguro que no cubre los daños por inundaciones en una zona de inundación. (Herzog, OSSTMM 3.0)

TABLA B.10: Resultados obtenidos en Control Alarma

Resultados Obtenidos	**Tipo de Test**	Observación directa
	Observaciones	• Existen licencias de softwares caducadas y sin renovación, • Así como también garantías de activos caducados. • Utilización de sistemas operativos como XP que ya no tienen ningún tipo de garantía por parte del fabricante. Estos son ejemplos de ciertas debilidades, existen más que no se mencionará por seguridad.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el cálculo de las debilidades es: $L_W = 5$

B.1.3.3 PREOCUPACIÓN

En seguridad física, una preocupación puede ser un mecanismo de bloqueo de la puerta cuyos controles y tipos de operación son clave pública, un generador de respaldo sin medidor de potencia o indicador de combustible, un proceso de equipo que no requiere que el empleado firme la salida de materiales cuando se reciben, o una alarma de fuego no lo suficientemente fuerte para ser escuchado por los trabajadores de maquinaria que deban usar tapones para los oídos. (Herzog, OSSTMM 3.0)

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma. (Herzog, OSSTMM 3.0)

$$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

$$L_C = 0 + 1 + 2 + 1 + 0$$

$$L_C = 4$$

B.1.3.4 EXPOSICIÓN

Cuente cada injustificable acción, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o bienes dentro del canal ámbito elegido. (Herzog, OSSTMM 3.0).

$$L_K = P_V = 8$$

B.1.3.5 ANOMALÍAS

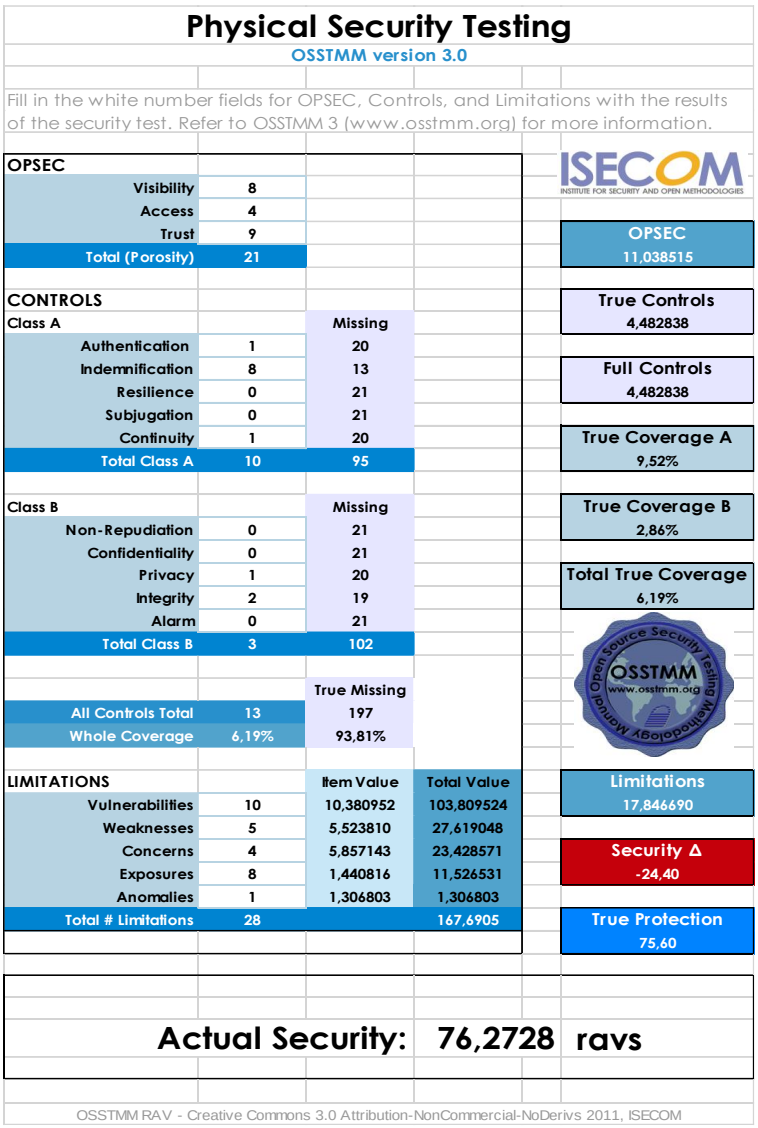
En seguridad física una anomalía puede ser pájaros muertos descubiertos en el techo de un edificio en torno a los equipos de comunicaciones.

$$L_A = 1$$

B.2 CALCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática. (Herzog, OSSTMM 3.0).

De acuerdo a los valores obtenidos en la seguridad operacional, controles y limitaciones, se ha realizado el cálculo; el mismo que se muestra en la Figura B-1.



Physical Security Testing

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	8		
Access	4		
Trust	9		
Total (Porosity)	21		

CONTROLS			
Class A		Missing	
Authentication	1	20	
Indemnification	8	13	
Resilience	0	21	
Subjugation	0	21	
Continuity	1	20	
Total Class A	10	95	
Class B		Missing	
Non-Repudiation	0	21	
Confidentiality	0	21	
Privacy	1	20	
Integrity	2	19	
Alarm	0	21	
Total Class B	3	102	
		True Missing	
All Controls Total	13	197	
Whole Coverage	6,19%	93,81%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	10	10,380952	103,809524
Weaknesses	5	5,523810	27,619048
Concerns	4	5,857143	23,428571
Exposures	8	1,440816	11,526531
Anomalies	1	1,306803	1,306803
Total # Limitations	28		167,6905

OPSEC	11,038515
True Controls	4,482838
Full Controls	4,482838
True Coverage A	9,52%
True Coverage B	2,86%
Total True Coverage	6,19%
Limitations	17,846690
Security Δ	-24,40
True Protection	75,60

Actual Security: 76,2728 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

FIGURA B.1: Cálculo del RAVS en Canal Seguridad Física

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

B.2.1 INTERPRETACIÓN DE RESULTADOS

La seguridad operacional es relativamente alta, tomando en cuenta que ésta evalúa las diferentes políticas y procedimientos implementados por la administración. Esto refleja la prioridad que se le ha dado a la seguridad física.

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que de acuerdo al test realizado, lamentablemente no se tienen implementados controles respectivos a la seguridad física, siendo ésta un blanco para los atacantes informáticos.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a que los valores en seguridad operacional son relativamente altos, estos valores predominan para que el cálculo de las limitaciones sea también relativamente alto. Y resulta así una gran preocupación debido a que se tiene una limitación de vulnerabilidad muy alta en relación a los demás valores.

ANEXO C

C.1 TELECOMUNICACIONES

COMSEC es una clasificación para la seguridad material en el ámbito ELSEC que está dentro de los límites de las telecomunicaciones a través de cables.

Este canal cubre la interacción del analista con los objetivos. Mientras que algunos servicios consideran este simplemente como "phreaking", el objetivo verdadero cumplimiento de las pruebas de seguridad en este canal es la prueba de barrera lógica y medición de la brecha en contra de la norma de seguridad requerida como se indica en la política de empresa, regulaciones de la industria, o la legislación regional. (Herzog, OSSTMM 3.0)

C.1.1 SEGURIDAD OPERACIONAL

A continuación se detalla cómo se obtuvieron los resultados de la seguridad operacional en el canal de seguridad física.

C.1.1.1 VISIBILIDAD

Enumeración e indexación de los objetivos en el ámbito de aplicación a través de la interacción directa e indirecta incluso con entre los sistemas directo.

a) Realizar un mapa de los protocolos de comunicación en uso dentro del ámbito de aplicación.

Utilizando el software NetScan se realizó un escaneo de puertos, y en la figura se puede evidenciar un resumen de algunos de los puertos más conocidos dentro del ámbito de aplicación.

Cabe recalcar algunas características de dicho software.

- Detecta hardware direcciones MAC, incluso a través de routers.
- Detecta las direcciones IP internas y externas.
- Analiza en busca de los puertos de escucha TCP, UDP y algunos servicios de SNMP.
- Puede montar y explorar los recursos de red.
- Se puede iniciar aplicaciones externas de terceros.
- Soporta Wake-On-LAN, apagado remoto y el envío de mensajes de red.

- Recupera información de registro remoto, sistema de archivos y administrador de servicios.

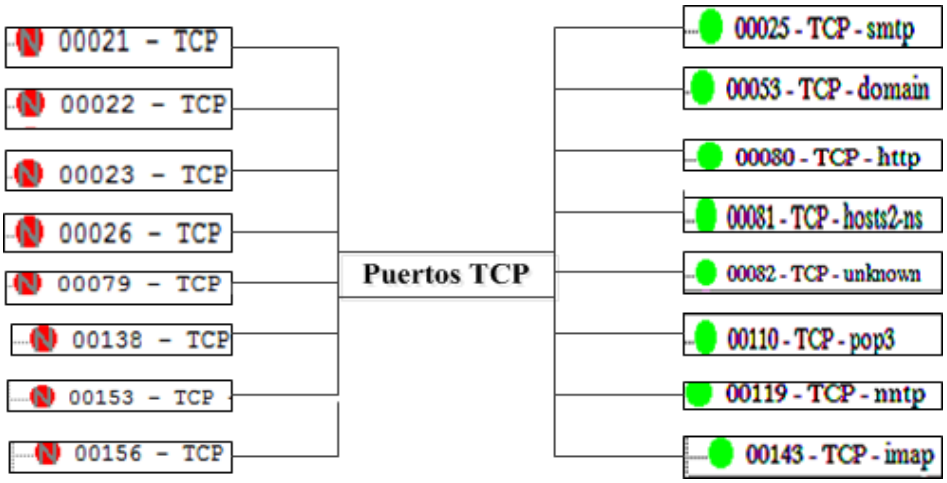


FIGURA C.1: Mapa de los protocolos de comunicación

Fuente: Elaborada por Andrea Zura

b) Esquema de la topología de las redes de telecomunicaciones.

La topología de red del GADMO es una topología plana, es decir no está segmentada o jerarquizada, la misma cuenta con varios dispositivos de red, como conmutadores, enrutadores, servidores y firewalls; enlazados ya sea por fibra óptica o cable UTP Cat 6.

La figura que se presenta, es una representación de la topología de red del GADMO, cabe resaltar que la misma ha sido modificada de a original por motivos de seguridad.

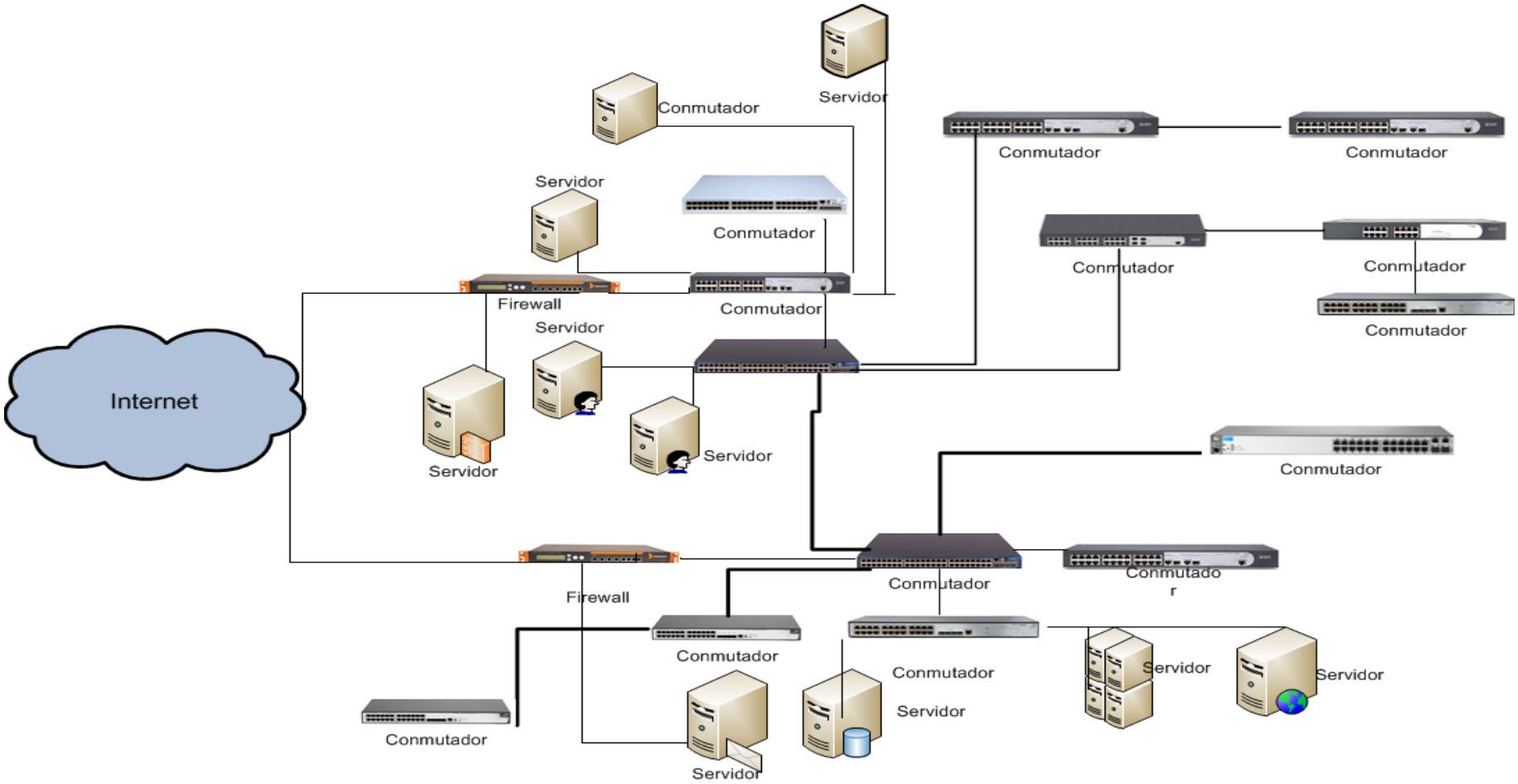


FIGURA C.2: Esquema de la topología de las redes de telecomunicaciones

Fuente: Elaborada por Andrea Zura

c) Identificar los tipos de sistemas operativos y versiones en uso en sistemas dentro del ámbito de aplicación.

Con la utilización del software Znemap, se pudo determinar los sistemas operativos utilizados en host y servidores de la red de datos del GADMO.

En la imagen se puede observar un fragmento de los resultados obtenidos por dicho software, recalcando que la imagen ha sido editada por motivos de seguridad.

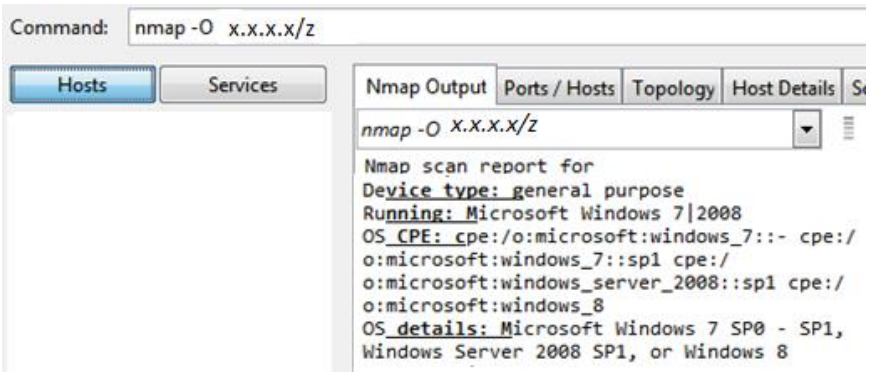


FIGURA C.3: Identificación de sistemas operativos y sus versiones

Fuente: Obtenida del software Znemap

Después del análisis realizado el resultado de visibilidad es: $P_V = 6$

C.1.1.2 ACCESOS

Las pruebas para la medición de la amplitud y profundidad de los puntos de acceso interactivos líderes en el ámbito y la autenticación requerida.

a) Relacionar cada puerto abierto con un servicio y protocolo.

Con el mapa de puertos descrito en el área de Visibilidad, se puede relacionar los servicios con ichos puertos.

b) Verificar la aplicación y su versión en el sistema.

Dicha información fue obtenida mediante observación directa en el GADMO, cuya información no será revelada por motivos de confidencialidad.

c) Identificar los componentes de los servicios en escucha.

Mediante Wireshark que es un software snnifer se pudo identificar los componentes de los servicios.

El nivel de acceso en el canal “Telecomunicaciones” será de: P_A= 4

C.1.1.3 CONFIANZA

Para una auditoría de Telecomunicaciones de redes de datos, el auditor cuenta cada tipo de servicio abierto o puerto abierto como una Confianza. (Herzog, OSSTMM 2.1)

En este caso, se debe realizar un análisis de los puertos que están abiertos y los que están cerrados, y el porqué de su estado. Ya que no es posible que todos los puertos se encuentren cerrados debido a la necesidad de acceder a ciertas aplicaciones; y tampoco que todos estén abiertos debido a las vulnerabilidades que se expone la red.

El nivel de confianza en el canal “Telecomunicaciones” será de: P_T= 21.

C.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

C.1.2.1 AUTENTICACIÓN

a) Enumerar los recursos de telecomunicaciones que requieren autenticación y verificar todas las formas aceptables de privilegios para interactuar o recibir acceso.

Existen controles de autenticación y privilegios de acceso.

b) Asegurarse que las cuentas administrativas no tengan la contraseña por defecto o fáciles de adivinar, para su acceso.

Las contraseñas de las cuentas administrativas no son por defecto y no son fáciles de adivinar.

c) Asegurarse que las cuentas de usuario no tengan la contraseña por defecto o fáciles de adivinar, para su acceso.

Las contraseñas de las cuentas de usuario no son por defecto.

d) Verificar la información de autenticación cuando se realiza un intento de acceso, si es exitoso o fallido. (Herzog, OSSTMM 2.1)

Se tiene un número limitado de intentos de acceso, si se falla el sistema se bloquea automáticamente.

En este caso el control de autenticación es de:

$$LC_{Au} = 5$$

C.1.2.2 INDEMNIZACIÓN

(a) Verificar la legalidad y el lenguaje adecuado en la los limitaciones de responsabilidad.

Se verifico el lenguaje adecuado utilizado en todas las actas de responsabilidad que se entregan en el GADMO, y éste resulta claro y adecuado.

- *Actas entrega de equipos informáticos*
- *Actas de responsabilidad de equipos informáticos*
- *Acta de responsabilidad del buen uso de contraseñas de ingreso a sistemas*
- *Actas de responsabilidad del buen uso de usuarios y contraseñas del correo institucional.*
- *Actas de responsabilidad del buen uso de internet dentro de la entidad.*
- *Acuerdo de confidencialidad de información reservada de la entidad*

(b) Examinar el lenguaje de la póliza de seguro para las limitaciones en los tipos de daños o activos.

Se firman contratos de garantía que cubren daños y robos de los activos de telecomunicaciones que se utilizan en el GADMO.

En este caso el control de indemnización en el canal físico es de:

$$LC_{Id} = 7$$

C.1.2.3 RESISTENCIA

Mapa y documentar el proceso de porteros desconectando canales por incumplimiento o dudas de seguridad como un análisis de las carencias con reglamentación y política de seguridad. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de resistencia de:

$$LC_{Re} = 0$$

C.1.2.4 SUBYUGACIÓN

Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o permitir controles de pérdida no habilitados de forma predeterminada. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de subyugación es nulo; es decir: $LC_{Su} = 0$

C.1.2.5 CONTINUIDAD

TABLA C.1: Resultados obtenidos en Control Continuidad

Resultados Obtenidos	Enumerar y probar las deficiencias de todos los objetivos en materia de retrasos de acceso y los tiempos de respuesta de servicio a través de los sistemas de back-up o el interruptor de canales alternos.	En este test se pudo evidenciar que no se tiene un control de continuidad, debido a que el tiempo de respuesta existente, es demasiado bajo o inexistente en algunos casos.

Fuente: Elaborada por Andrea Zura

Por lo tanto el control de continuidad es:

$$LC_{Ct} = 0$$

C.1.2.6 NO REPUDIO

(a) Enumerar y probar para su uso o insuficiencias de demonios y de los sistemas de identificación y registro de acceso o las interacciones con la propiedad para pruebas específicas para desafiar repudio correctamente.

(b) Documento de la profundidad de la interacción grabada y el proceso de identificación.

(c) Verifique que todos los métodos de interacciones se registran correctamente con la identificación apropiada.

(d) Identificar métodos de identificación que derrota de repudio. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de No-Repudio es nulo; es decir: $LC_{NR} = 0$

C.1.2.7 CONFIDENCIALIDAD

a) Enumerar todas las interacciones con los servicios en el ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, cifrado, interacciones para proteger la confidencialidad de la propiedad de la información entre las partes involucradas.

b) Verificar los métodos aceptables utilizados para la confidencialidad.

c) Prueba de la resistencia y el diseño del método de cifrado o la ofuscación.

d) Verificar los límites exteriores de la comunicación que se pueden proteger a través de los métodos aplicados o confidencialidad. (Herzog, OSSTMM 3.0)

De acuerdo al test, el control de Confidencialidad es nulo debido a que no existen métodos de cifrado en el ámbito de las telecomunicaciones:

$$LC_{Cf} = 0$$

C.1.2.8 PRIVACIDAD

(a) Enumerar los servicios en el ámbito de las comunicaciones o bienes transportados utilizando, firmas individuales específicos, identificación personal, interacciones personales para proteger la privacidad de la interacción y el proceso de suministro de bienes sólo para aquellos dentro de la debida autorización de seguridad para ese proceso, la comunicación, o de activos.

No existen servicios de firmas digitales para proteger la privacidad de las de las comunicaciones

(b) Relacionar información con los puertos que no responden para determinar si la disponibilidad depende de un tipo particular de contacto o protocolo.

En la figura que se muestra a continuación se puede observar un análisis de los puertos que no responden, y que relación se tiene con la privacidad en las telecomunicaciones.

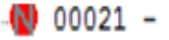
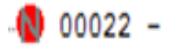
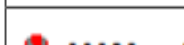
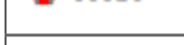
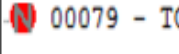
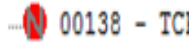
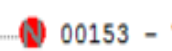
Imagen extraída de NetScan	*Información de puertos bloqueados*	*Función del puerto*	*Análisis*
	FTP (Datos)	Protocolo de transferencia de archivos	Es importante que el bloquea se haya realizado, ya que con ello se evita transferencias no autorizadas de información
	FTP (Control)		
	Telnet	Protocolo de acceso remoto, sin seguridad	Es acertado el bloqueo, ya que telnet es un protocolo no fiable ya que no maneja cifrado de claves.
	SMTP-AUTH	Evita el SPAM, con un mecanismo de autenticación	No debería bloquearse este puerto, ya que éste maneja un mecanismo de autenticación de emisor, eevitando así el SPAM
	Finger	Proporciona información de los usuarios de una máquina	El bloque es acertado ya que los cracker podrían utilizan la información proporcionada para iniciar un ataque de ingeniería social
	NETBIOS Datagram Service	Permite a las aplicaciones 'hablar' con la red.	Es importante que se haya bloqueado ya que por medio de éste puerto un cracker podría tener acceso a los host y a sus aplicaciones
	GSPG	Permite monitorear dispositivos de red	A pesar de ser reemplazado por SNMP, es importante que sea bloqueado para impedir el fisgoneo externo.
	SQL Server	Sistema para la gestión de bases de datos	Es importante el bloqueo de éste puerto para evitar el acceso a las bases de datos

FIGURA C.4: Análisis de Puertos

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Privacidad es:

$$LC_{Pr} = 8$$

C.1.2.9 INTEGRIDAD

TABLA C.2: Resultados obtenidos en Control Integridad

Resultados Obtenidos	Tipo de Test	Observación directa
	Enumerar y probar las deficiencias de integridad donde utilizando un proceso documentado, firmas, cifrado, hachís, o marcas para asegurar que el activo no se puede cambiar, redirigido, o se invierte sin que se conoce a las partes involucradas.	Los documentos, oficios o memorandos transmitidos internamente no se transmiten digitalmente; se lo hace físicamente y cada uno de ellos cuenta con sello y firma, pero no cuenta como n control de integridad.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Integridad es:

$$LC_{It} = 0$$

C.1.2.10 ALARMA

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en una situación sospechosa es observada por el personal en caso de sospecha de intento de evasión, la ingeniería social, o la actividad fraudulenta. (Herzog, OSSTMM 3.0)

TABLA C.3: Resultados obtenidos en Control Alarma

Resultados Obtenidos	Tipo de Test	Observación directa
	Observaciones	Cuando existen alarmas emitidas por el firewall de intentos de intrusión, el administrador de la red actúa de la mejor manera ante dicha alarma.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control de Alarma es:

$$LC_{Al} = 1$$

C.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están ponderadas de forma individual.

C.1.3.1 VULNERABILIDAD

En COMSEC telecomunicaciones, una vulnerabilidad puede ser, una cabina telefónica que permite a cualquier persona acceder a la línea de teléfono de otra persona, un sistema de correo de voz que ofrece mensajes de cualquier teléfono en cualquier lugar, o una máquina de fax que se pueden sondear de forma remota para volver a enviar la última cosa en la memoria para el número del llamante. (Herzog, OSSTMM 3.0)

Debido a razones confidenciales no se van a enumerar las vulnerabilidades de la organización.

De acuerdo al test, las vulnerabilidades son:

$$L_V = 5$$

C.1.3.2 DEBILIDAD

En COMSEC telecomunicaciones, una debilidad puede ser un PBX que todavía tiene las contraseñas administrativas por defecto o un banco de módem para el acceso remoto de acceso telefónico en el que no registra el número de llamadas, hora y duración. (Herzog, OSSTMM 3.0)

TABLA C.4: Resultados obtenidos en Limitación Debilidad

Resultados Obtenidos	Tipo de Test	Observación directa
	Observaciones	• Existe una PBX la misma que no está administrada, por lo tanto representa una debilidad. • Al no estar administrada no se puede llevar un control de número de llamadas, hora y duración. Estos son ejemplos de ciertas debilidades, existen más que no se mencionará por seguridad.

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el cálculo de las debilidades es:

$$L_W = 5$$

C.1.3.3 PREOCUPACIÓN

En COMSEC telecomunicaciones, una preocupación puede ser el uso de una máquina de FAX para el envío de información privada o un sistema de correo de voz que utiliza tonos táctiles para la introducción de un PIN o contraseña. (Herzog, OSSTMM 3.0)

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma. (Herzog, OSSTMM 3.0)

$$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

$$L_C = 0 + 1 + 0 + 0 + 0$$

$$L_C = 1$$

C.1.3.4 EXPOSICIÓN

En COMSEC telecomunicaciones, una exposición puede ser un directorio automatizado empresa ordenada alfabéticamente, lo que permite que cualquiera pueda desplazarse por todas las personas y números, o una máquina de fax que almacena los últimos números marcados.

Cuente cada injustificable acción, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o bienes dentro del canal ámbito elegido. (Herzog, OSSTMM 3.0).

$$L_K = P_V = 6$$

C.1.3.5 ANOMALÍAS

En COMSEC telecomunicaciones, una anomalía puede ser una respuesta del módem desde un número que no tiene módem. (Herzog, OSSTMM 3.0)

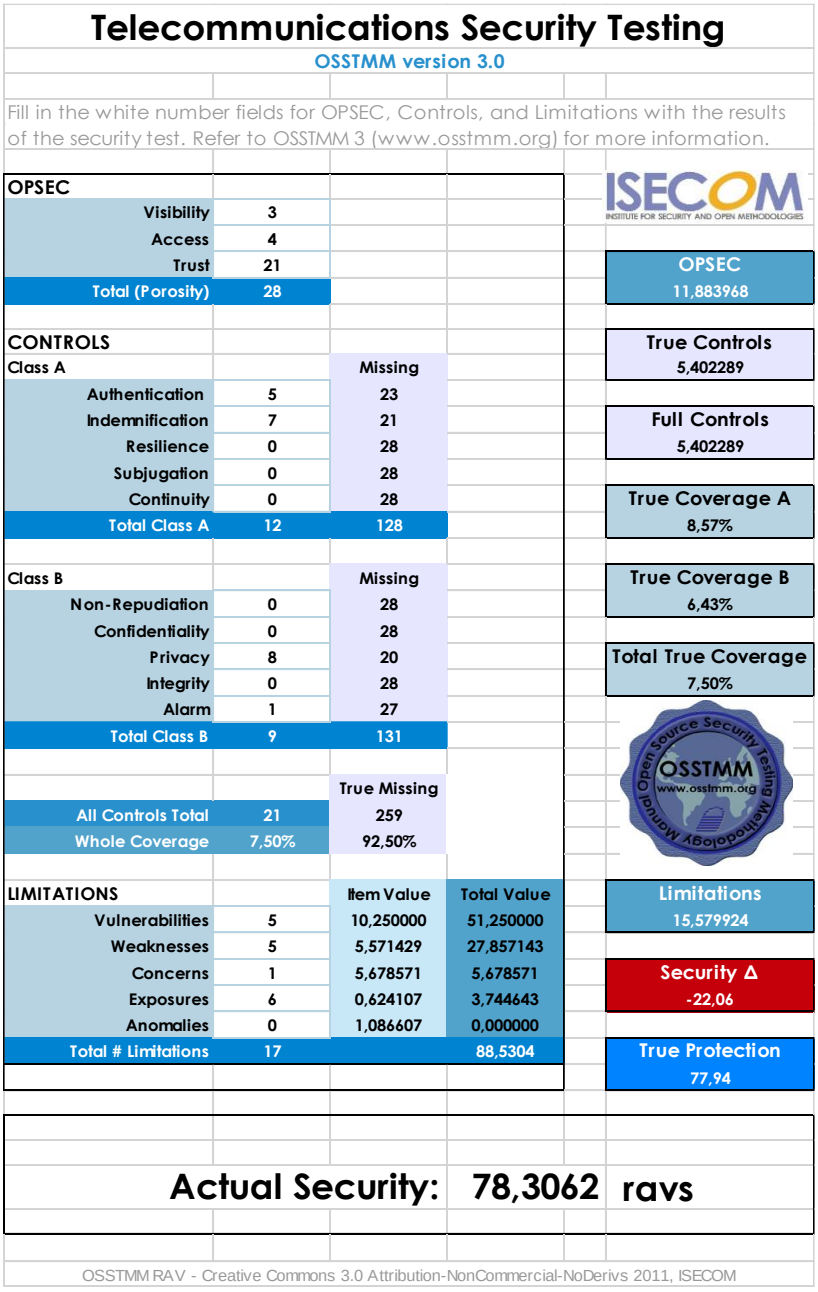
$$L_A = 0$$

C.2 CÁLCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir

de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM.

El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática. (Herzog, OSSTMM 3.0)



Telecommunications Security Testing

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC				
Visibility	3			
Access	4			
Trust	21			
Total (Porosity)	28			
CONTROLS				
Class A		Missing		
Authentication	5	23		
Indemnification	7	21		
Resilience	0	28		
Subjugation	0	28		
Continuity	0	28		
Total Class A	12	128		
Class B		Missing		
Non-Repudiation	0	28		
Confidentiality	0	28		
Privacy	8	20		
Integrity	0	28		
Alarm	1	27		
Total Class B	9	131		
		True Missing		
All Controls Total	21	259		
Whole Coverage	7,50%	92,50%		
LIMITATIONS		Item Value	Total Value	
Vulnerabilities	5	10,250000	51,250000	
Weaknesses	5	5,571429	27,857143	
Concerns	1	5,678571	5,678571	
Exposures	6	0,624107	3,744643	
Anomalies	0	1,086607	0,000000	
Total # Limitations	17		88,5304	

OPSEC 11,883968
True Controls 5,402289
Full Controls 5,402289
True Coverage A 8,57%
True Coverage B 6,43%
Total True Coverage 7,50%
Limitations 15,579924
Security Δ -22,06
True Protection 77,94

Actual Security: 78,3062 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

FIGURA C.5: Cálculo del RAVS en Canal Seguridad Física

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

C.2.1 INTERPRETACIÓN DE RESULTADOS.

La seguridad operacional es alta, principalmente en el aspecto de Confianza, en el que se ha considerado todos los puertos que están abiertos, analizando el porqué de su estado. Esto refleja la importancia que se le ha dado a la seguridad de las telecomunicaciones

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que de acuerdo al test realizado, se tienen únicamente controles de Indemnización, autenticación y privacidad; mientras tanto los demás controles son nulos; dejando así una brecha para la inseguridad de la información.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a que los valores en seguridad operacional son relativamente altos, estos valores predominan para que el cálculo de las limitaciones sea también relativamente alto. Es así que resaltan limitaciones como las Vulnerabilidades, debilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas hacia la seguridad de información.

ANEXO D

D.1 REDES DE DATOS

Redes de datos es una clasificación para la seguridad material en el ámbito ELSEC que está dentro de los límites de las telecomunicaciones a través de cables.

Las pruebas para el canal de redes de datos de seguridad (COMSEC) requieren interacciones con las garantías de funcionamiento de la red de comunicación de datos existentes que se utilizan para controlar el acceso a la propiedad. (Herzog, OSSTMM 3.0)

D.1.1 SEGURIDAD OPERACIONAL

Seguridad Operacional, también conocida como la porosidad del alcance, es el primero de los tres factores de la seguridad real que deberían determinarse. Se mide inicialmente como la suma de la visibilidad del alcance P_V, de acceso P_A, y la confianza P_T. (Herzog, OSSTMM 3.0)

A continuación se detalla de donde se obtuvieron los resultados de la seguridad operacional en el canal humano.

D.1.1.1 VISIBILIDAD

Enumeración e indexación de los objetivos en el ámbito de aplicación a través de la interacción directa e indirecta entre los sistemas directos.

i. El uso de sniffing de red para identificar los protocolos que emanan respuesta de los servicios de red o peticiones en su caso. Por ejemplo, Netbios, ARP, SAP, NFS, BGP, OSPF, MPLS, RIPv2, etc.

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-19 11:03 Hora est.
Pacífico, Sudamérica
Nmap scan report for x.x.x.x/y
Host is up (0.0000060s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server
MAC Address: AA:AA:AA:AA:AA:AA (x-x Company)
Nmap done: 1 IP address (1 host up) scanned in 18.86 seconds
```

Se puede observar un extracto de uno de los escaneos realizados en la Red de Datos del GADMO, se ha editado tanto la dirección IP y MAC utilizada por motivos de seguridad.

ii. Consulta todos los servidores de nombres y los servidores de nombres del ISP o proveedor de alojamiento, en su caso, para la correspondiente A, AAAA, y PTR, así como la capacidad para realizar las transferencias de zona para determinar la existencia de todos los objetivos de la red y cualquier despidos relacionados, balanceo de carga, almacenamiento en caché, proxies, y de hosting virtual.

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-19 12:04 Hora est. Pacífico, Sudamérica
Nmap scan report for mail.otavalo.gob.ec (x.x.x.x)
Host is up (0.031s latency).
All 1000 scanned ports on mail.otavalo.gob.ec ((x.x.x.x) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 49.97 seconds
```

iii. Verificar y examinar el uso de protocolos de enrutamiento de tráfico y para todos los destinos.

No existen protocolos de enrutamiento.

iv. Verificar defecto y probables nombres de comunidad SNMP en uso están de acuerdo con la práctica despliegues de todas las versiones de SNMP.

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-19 11:30 Hora est. Pacífico, Sudamérica
Initiating Parallel DNS resolution of 1 host. at 11:30
Completed Parallel DNS resolution of 1 host. at 11:31, 16.50s elapsed
Skipping SYN Stealth Scan against x.x.x.x because Windows does not support scanning your own
machine (localhost) this way.
Skipping OS Scan against x.x.x.x because it doesn't work against your own machine (localhost)
Nmap scan report for x.x.x.x /y
Host is up.
PORT      STATE   SERVICE
161/tcp   unknown snmp
```

Se puede observar un extracto de uno de los escaneos realizados en la Red de Datos del GADMO, se ha editado tanto la dirección IP y MAC utilizada por motivos de seguridad.

v. Buscar los grupos de noticias, foros, IRC, IM, P2P, VoIP y comunicaciones basadas en la web para la conexión de datos del objetivo para determinar los sistemas de puerta de enlace de salida y direccionamiento interno.

Se realizó la búsqueda de información publicada en la página inicial del GADMO. La dirección Web de la página inicial de la institución es: http://www.otavalo.gob.ec/web/, la información proporcionada está relacionada a información de la ciudad, servicios y proyectos que presta la Municipalidad.

FIGURA D.1: Página Oficial del Municipio de Otavalo

Fuente: Extraído de http://www.otavalo.gob.ec/web

También se realizó la búsqueda de información relevante en los grupos de noticias locales y nacionales; así como también en las bases de datos públicos estos son:

http://www.hoy.com.ec

http://www.aquiotavalo.com/portal/

http://www.elnorte.ec/otavalo.html

http://www.elcomercio.com.ec/tag/otavalo

www.google.com

www.yahoo.com

La información encontrada fue de los años 2013-2014, referente a noticias locales, delincuencia en la ciudad, fiestas locales, turismo entre otras.

Se indagó a la vez de la información proporcionada mediante los dominios de Internet “otavalo.gob.ec” y “visitotavalo.com” en la base de datos Whois.

TABLA D.1: Información de Dominio Otavalo.gob.ec|

INFORMACIÓN DEL DOMINIO	
Dominio:	otavalo.gob.ec
Fecha de Creación:	02 Jul 2010
Fecha de última Modificación:	04 Jul 2014
Fecha de Expiración:	02 Jul 2016
Nombres de Servidores DNS:	pichincha.andinanet.net
	tungurahua.andinanet.net
Registrar:	NIC.EC Registrar
REGISTRANTE:	
Nombre	Mario Cornejo M.
Organización:	GOBIERNO MUNICIPAL DE SAN LUIS DE OTAVALO
Dirección:	García Moreno 505 Parque Central Otavalo, Imbabura 36 EC
Email:	otavalo@andinanet.net
Teléfono:	5936-2920460
Fax:	5936-2920381
CONTACTO ADMINISTRATIVO:	
Nombre:	Wilman Garces
Organización:	GOBIERNO MUNICIPAL DE SAN LUIS DE OTAVALO
Dirección:	García Moreno 505 Parque Central Otavalo, Imbabura EC
Email:	municipio@otavalo.gob.ec
Teléfono:	5936-2924716
Fax:	5936-2924716
CONTACTO TÉCNICO:	
Nombre:	Luis López M.
Organización:	GOBIERNO MUNICIPAL DE SAN LUIS DE OTAVALO
Dirección:	García Moreno 505 Parque Central

	Otavalo, Imbabura EC
Email:	informatica@otavalo.gob.ec
Teléfono:	5936-2924716
Fax:	5936-2920381
CONTACTO DE FACTURACIÓN:	
Nombre	César Pinto Acosta
Organización:	GOBIERNO MUNICIPAL DE SAN LUIS DE OTAVALO
Dirección:	García Moreno 505 Parque Central Otavalo, Imbabura EC
Email:	municipio@otavalo.gob.ec
Teléfono:	5936-2920404
Fax:	5936-2920404

Fuente: Extraído de http://www.nic.ec/whois/resultados.asp

El nivel de visibilidad en el canal "Redes de Datos" será de: P_V= 17;

D.1.1.2 ACCESOS

i. Conocer solicitudes, servicios troyanos comunes que utilizan TCP para conexiones desde todas las direcciones y puertos sin filtrar que han enviado ninguna respuesta a un SYN TCP.

Starting Nmap 6.46 (http://nmap.org) at 2014-08-19 10:42 Hora est. Pacífico, Sudamérica

Nmap scan report for ***x.x.x.x***

Host is up (0.00029s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3128/tcp open squid-http

10000/tcp open snet-sensor-mgmt

MAC Address: ***AA:AA:AA:AA:AA:AA*** (Tenda Technology Co.)

Nmap done: 1 IP address (1 host up) scanned in 17.77 seconds

Se muestra un extracto del escaneo realizado en la red de datos del GADMO, cabe recalcar que por motivos de seguridad y confidencialidad se ha editado las direcciones IP y MAC.

ii. Verificar los servicios de VoIP.

En el GADMO no se cuenta con un sistema de VoIP. Es un proyecto que se encuentra en su fase de desarrollo.

i. Relacionar cada puerto abierto a un demonio (servicio), aplicación (código específico o un producto que utiliza el servicio), y el protocolo (el medio para interactuar con ese servicio o aplicación).

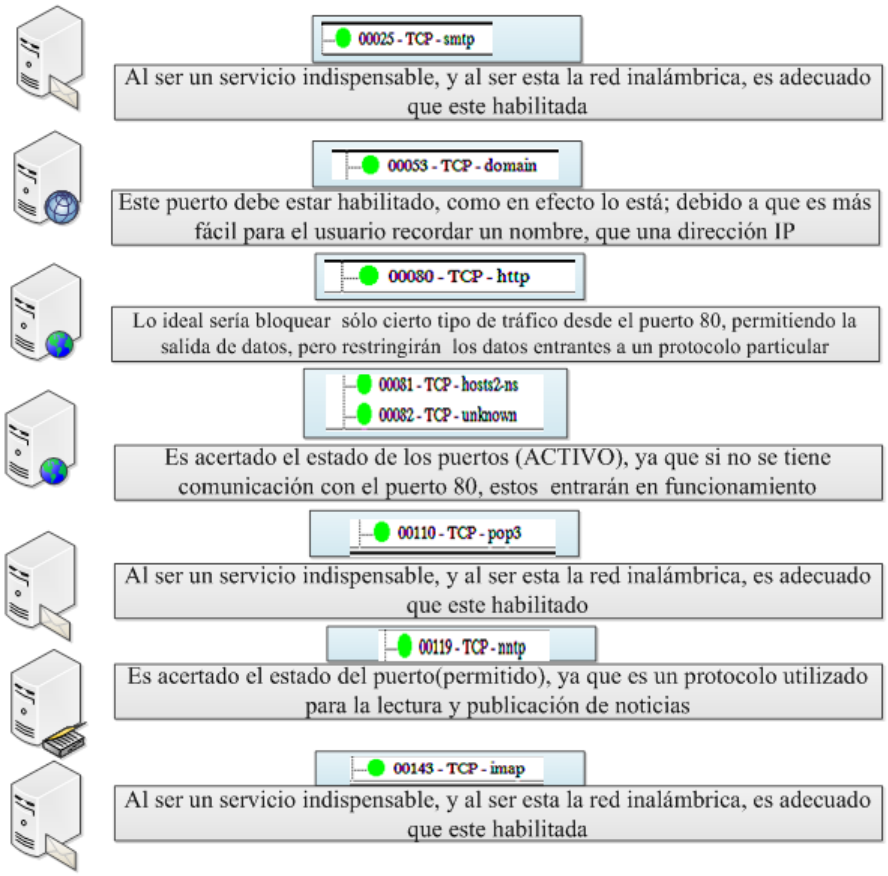


FIGURA D.2: Resumen de puertos abiertos en la red

Fuente: Elaborada por Andrea Zura, en referencia a los resultados obtenidos en software NMAP

En la imagen se puede observar los resultados de los escaneos realizados en la red de datos del GADMO, en donde se hace un análisis de algunos puertos y su relación con las aplicaciones y servicios.

ii. Verificar la disponibilidad del sistema operativo en comparación con las últimas vulnerabilidades y versiones de parches.

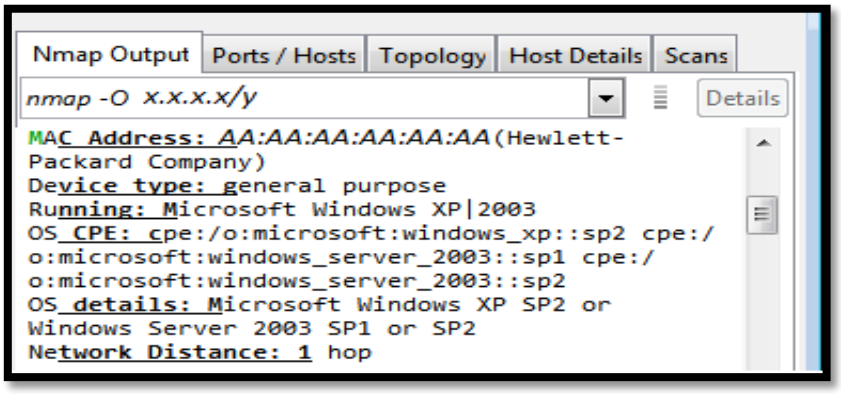


FIGURA D.3: Lista de sistemas operativos activos en la red

Fuente: extraído del software NMAP

Se muestra en la imagen un extracto de uno de los escaneos realizados en la red de datos del GADMO, cabe recalcar que la imagen fue editada en las direcciones tanto IP como MAC.

Se observa que aún se utilizan sistemas operativos como Windows XP, el mismo que actualmente se encuentra totalmente vulnerable debido a que su fabricante dejo de dar garantías y actualizaciones para el mismo.

El nivel de acceso en el canal “Humano” será de: P_A= 14

D.1.1.3 CONFIANZA

Para una auditoría de seguridad de las redes de datos, el auditor cuenta cada tipo de servicio abierto o puerto abierto como una confianza. (Herzog, OSSTMM 3.0)

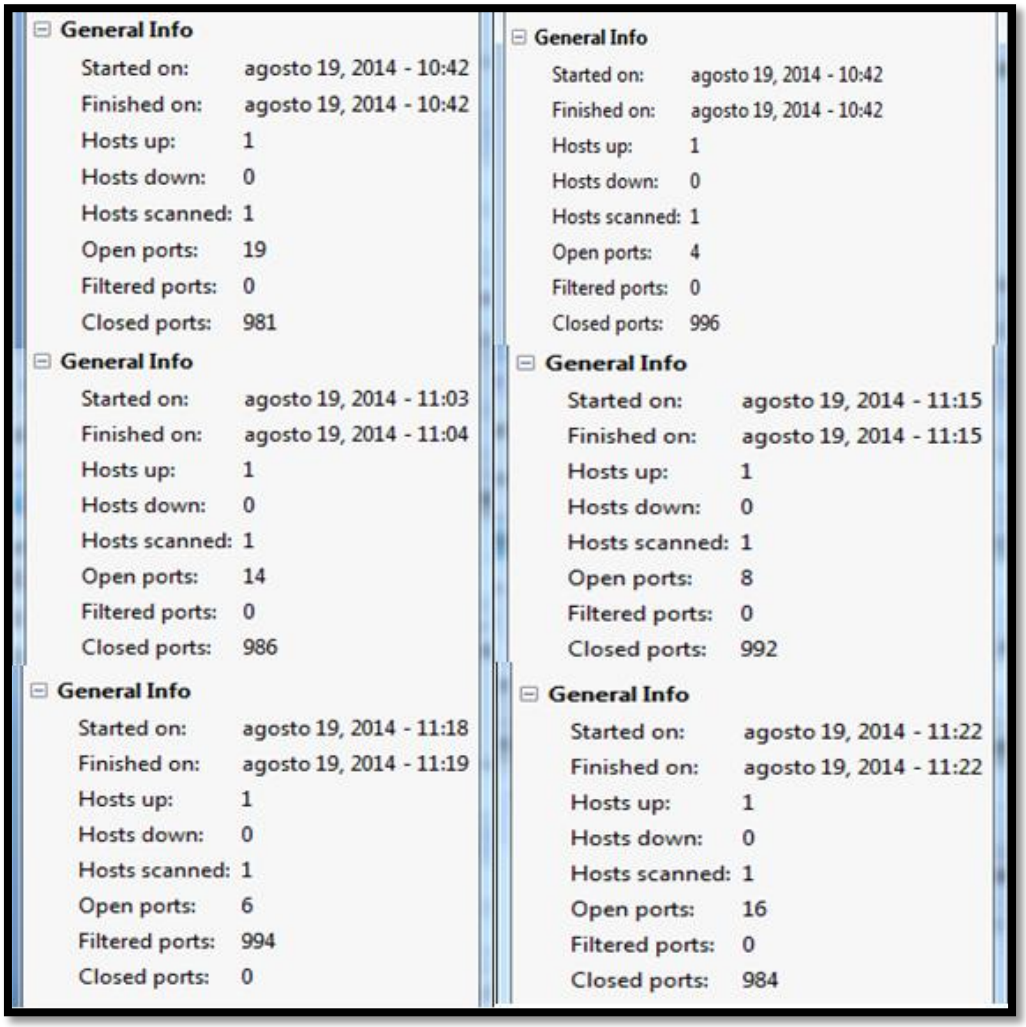


FIGURA D.4: Escaneos realizados en la red

Fuente: Extraído de software NMAP

En la imagen se puede observar los escaneos que se realizaron a diferentes servidores, en donde sumando todos los puertos abiertos se tiene:

El nivel de acceso en el canal “Red de Datos” será de: P_T= 67

D.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

D.1.2.1 AUTENTICACIÓN

i. Enumerar los accesos que requiere autenticación y documentar todos los privilegios descubiertos que se pueden utilizar para proporcionar acceso.

ii. Verificar el método de obtención de la autorización apropiada para la autenticación.

iii. Verificar el método de ser identificados correctamente para contar la autenticación.

iv. Verificar la fortaleza de la autenticación a través de descifrado de contraseñas y volver a aplicar descubrió contraseñas a todos los puntos de acceso que requieren autenticación.

v. Verificar el proceso de recepción de autenticación.

En este caso existen métodos adecuados de autenticación en el canal red de datos. Por lo tanto:

$LC_{Au} = 5$

D.1.2.2 INDEMNIZACIÓN

i. Documentar y enumerar los objetivos y servicios que están protegidos contra el abuso o la elusión de la política de los empleados, están asegurados por robo o daños, o utilizan de responsabilidad y de permisos renuncias.

ii. Verificar la legalidad y la conveniencia de la lengua en los descargos de responsabilidad.

iii. Verificar el efecto de las exenciones de responsabilidad sobre la seguridad o medidas de seguridad.

iv. Examinar el lenguaje de la póliza de seguro para las limitaciones en los tipos de daños o activos.

De acuerdo al test, el control, en todos los canales es de:

$$LC_{Id} = 6$$

D.1.2.3 RESISTENCIA

La determinación y la medición de la resistencia de los objetivos en el ámbito de los cambios excesivos u hostiles diseñados para causar un fallo o degradación del servicio. Denegación de Servicio (DoS) es una situación en la que una circunstancia, ya sea intencional o accidentalmente, impide que el sistema funcione como está previsto. En ciertos casos, el sistema puede estar funcionando exactamente como se diseñó sin embargo, nunca fue pensado para manejar la carga, el alcance, o parámetros que se le

impuso. Supervivencia las pruebas deben ser monitoreados de cerca ya que la intención es causar el fracaso y esto puede ser inaceptable para el dueño del destino.

TABLA D.2: Resultados obtenidos en el Control Resistencia

Resultados Obtenidos	En este test se pudo evidenciar que en ciertas áreas el sistema no está funcionando acorde al diseño realizado, ya que existe una carga mayor de la que puede ser soportada

Fuente: Elaborada por Andrea Zura

De acuerdo al test, el control, en todos los canales es de:

$$LC_{Re} = 3$$

D.1.2.4 CONTINUIDAD

Enumerar y probar las deficiencias de todos los objetivos en materia de retrasos de acceso y los tiempos de respuesta de servicio a través de los sistemas de back-up.

Para dicho control se consideró los sistemas de back-up con los que se cuenta; en base a ello el control de continuidad es:

$$LC_{Ct} = 4$$

D.1.2.5 NO REPUDIO

(a) Enumerar y probar para su uso o insuficiencias los sistemas de identificación y registro de acceso o las interacciones con la propiedad.

(b) Identificar métodos de identificación que la derrota repudio. (Herzog, OSSTMM 3.0).

No se realizaron pruebas de este control; es decir:

$$LC_{NR} = 0$$

D.1.2.6 CONFIDENCIALIDAD

(a) Enumerar todas las interacciones con los servicios en el ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, cifrado, interacciones para proteger la confidencialidad de la propiedad de la información entre las partes involucradas.

(b) Verificar los métodos aceptables utilizados para la confidencialidad.

(c) Prueba de la resistencia y el diseño del método de cifrado o la ofuscación.

(d) Verificar los límites exteriores de la comunicación que se pueden proteger a través de los métodos aplicados de confidencialidad. (Herzog, OSSTMM 3.0)

No se cuentan con métodos de encriptación por lo tanto el control de Confidencialidad es:

$$LC_{Cf} = 0$$

D.1.2.7 PRIVACIDAD

Relacionar información con los puertos TCP y UDP que no respondes, para determinar si la disponibilidad depende de un tipo particular de contacto o protocolo. (Herzog, OSSTMM 3.0)

Se puede observar el resumen de los puertos TCP y el respectivo análisis del estado del puerto

Imagen extraída de NetScan	*Función del puerto*	*Análisis*
00021 00022	Protocolo de transferencia de archivos	Es importante que el bloquea se haya realizado, ya que con ello se evita transferencias no autorizadas de información
00023	Protocolo de acceso remoto, sin seguridad	Es acertado el bloqueo, ya que telnet es un protocolo no fiable ya que no maneja cifrado de claves.
00026	Evita el SPAM, con un mecanismo de autenticación	No debería bloquearse este puerto, ya que éste maneja un mecanismo de autenticación de emisor, eevitando así el SPAM
00079	Proporciona información de los usuarios de una máquina	El bloque es acertado ya que los cracker podrían utilizan la información proporcionada para iniciar un ataque de ingeniería social
00138	Permite a las aplicaciones 'hablar' con la red.	Es importante que se haya bloqueado ya que por medio de éste puerto un cracker podría tener acceso a los host y a sus aplicaciones
00153	Permite monitorear dispositivos de red	A pesar de ser reemplazado por SNMP, es importante que sea bloqueado para impedir el fisgoneo externo.
00156 -	Sistema para la gestión de bases de datos	Es importante el bloqueo de éste puerto para evitar el acceso a las bases de datos

FIGURA D.5: Lista de puertos bloqueados en la red

Fuente: Elaborada por Andrea Zura, en referencia a los resultados obtenidos en software NMAP

Por lo tanto el control de privacidad es:

$$LC_{Pr} = 8$$

D.1.2.8 INTEGRIDAD

En las redes de datos, el cifrado o un hash del archivo pueden proporcionar el control de integridad sobre el cambio del archivo en tránsito.

De acuerdo al test, el control de Integridad es:

$$LC_{It} = 0$$

D.1.2.9 ALARMA

(a) En las redes de datos cuente cada servidor y el servicio en el que esta basad, y si están monitoreados por el sistema de detección de intrusos.

(b) Cuente cada servicio que mantiene un registro monitorizado de interacción.

(c) Cuentan los registros de acceso, incluso si no se utilizan para enviar una notificación de alerta de inmediato

En el GADMO, al contar con un Firewal Sophos UTM, el cual cuenta con un sistema de detección de intrusos, se tienen control de alarmas en tiempo real.

De acuerdo al test, el control de Alarma es:

$$LC_{Al} = 1$$

D.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están ponderadas de forma individual. La ponderación de las vulnerabilidades, debilidades y preocupaciones se basan en una relación entre la suma OpSec, la pérdida de controles.

D.1.3.1 VULNERABILIDAD

En la seguridad de los datos una vulnerabilidad puede ser un defecto en el software que permite a un atacante tener acceso para sobrescribir el espacio de memoria, una falla de cálculo que permite a un atacante bloquear el 100% del uso de la CPU o un sistema operativo que permite que los datos suficientes a se va a copiar en el disco hasta que no puede funcionar más. (Herzog, OSSTMM 3.0)

El tener sistemas operativos obsoletos representa vulnerabilidades, es por ello que de acuerdo al test, las vulnerabilidades es:

$$L_V = 20$$

D.1.3.2 DEBILIDAD

En la seguridad de los datos, una debilidad puede ser que permite intentos ilimitados mediante un log-in a la granja de servidores web. (Herzog, OSSTMM 3.0)

En el GADMO se lleva control del acceso a los servicios, en caso de no autenticarse en un número indeterminado de intentos el servicio se bloqueará.

De acuerdo al test, el cálculo de las debilidades es:

$$L_W = 0$$

D.1.3.3 PREOCUPACIÓN

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma. (Herzog, OSSTMM 3.0)

$$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

$$L_C = 0 + 1 + 0 + 8 + 0$$

$$L_C = 9$$

D.1.3.4 EXPOSICIÓN

En la seguridad de los datos, una exposición puede ser una bandera descriptiva y válida acerca de un servicio o un ICMP echo reply desde un host.. (Herzog, OSSTMM 3.0).

$$L_K = P_V = 17$$

D.1.3.5 ANOMALÍAS

Cuente cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, por lo general cuando la fuente o el destino del elemento no se pueden entender. Una anomalía puede ser una señal temprana de un problema de seguridad. Dado que las incógnitas son los elementos que no pueden ser controlados, una auditoría adecuada requiere ir observando y anotando todas las anomalías. (Herzog, OSSTMM 3.0)

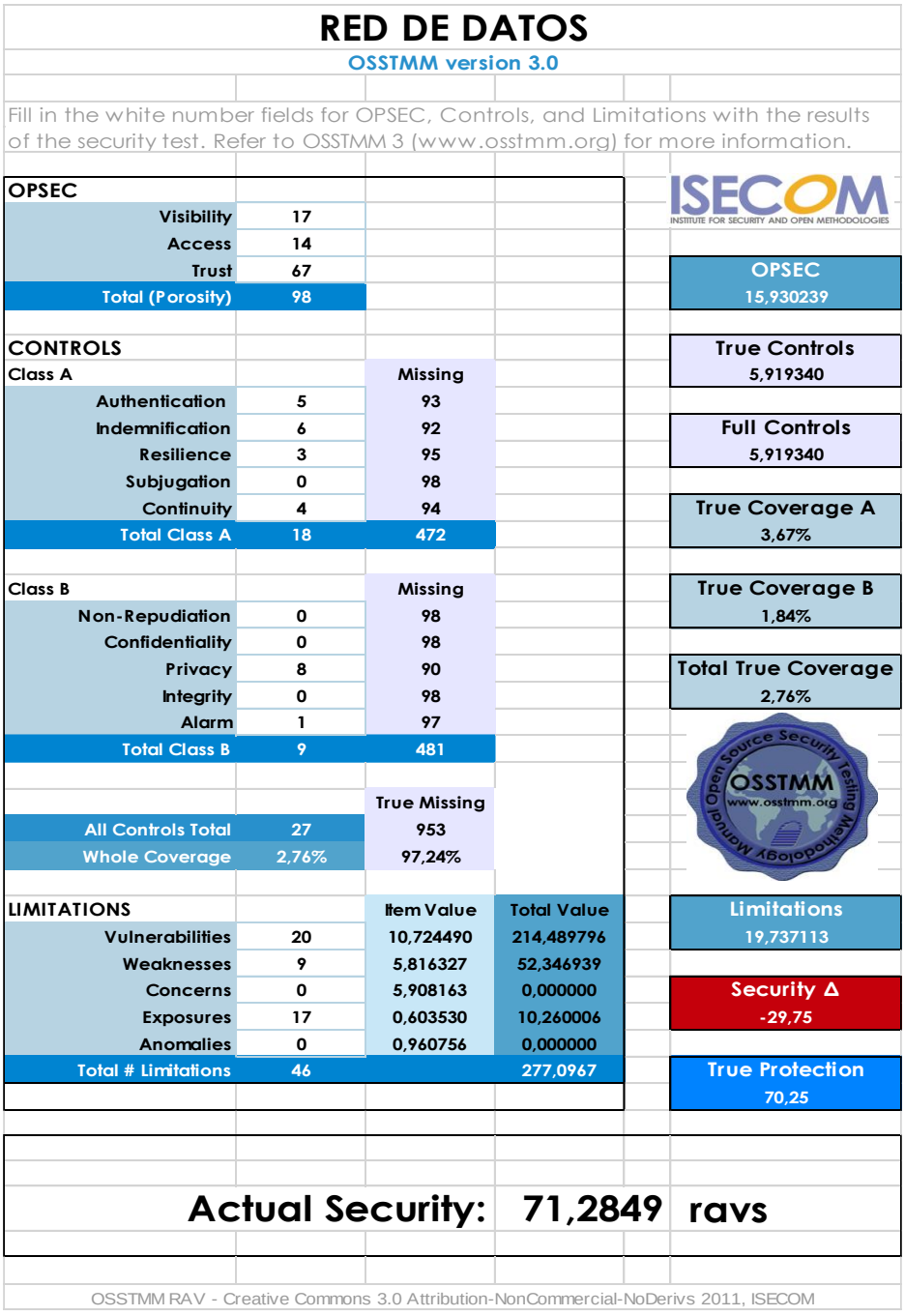
No se observaron anomalías durante el tiempo que se realizó el test de penetración, por lo tanto:

$$L_A = 0$$

D.2 CALCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir

de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática. (Herzog, OSSTMM 3.0)



RED DE DATOS

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	17		
Access	14		
Trust	67		
Total (Porosity)	98		
CONTROLS			
Class A		Missing	
Authentication	5	93	
Indemnification	6	92	
Resilience	3	95	
Subjugation	0	98	
Continuity	4	94	
Total Class A	18	472	
Class B		Missing	
Non-Repudiation	0	98	
Confidentiality	0	98	
Privacy	8	90	
Integrity	0	98	
Alarm	1	97	
Total Class B	9	481	
		True Missing	
All Controls Total	27	953	
Whole Coverage	2,76%	97,24%	
LIMITATIONS		Item Value	Total Value
Vulnerabilities	20	10,724490	214,489796
Weaknesses	9	5,816327	52,346939
Concerns	0	5,908163	0,000000
Exposures	17	0,603530	10,260006
Anomalies	0	0,960756	0,000000
Total # Limitations	46		277,0967

OPSEC 15,930239
True Controls 5,919340
Full Controls 5,919340
True Coverage A 3,67%
True Coverage B 1,84%
Total True Coverage 2,76%
Limitations 19,737113
Security Δ -29,75
True Protection 70,25

Actual Security: 71,2849 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

FIGURA D.6: Cálculo del RAVS en Canal Seguridad Física

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

ANEXO E

E SIMULACIÓN RED INTERNA

Una vez realizado el diseño de la Red de Datos, se realizará la simulación del mismo. Considerando que los equipos con los que se cuenta en el GADMOS son de tecnología 3COM, y el software de simulación de dichos equipos únicamente permiten realizar configuraciones básicas; la simulación del modelo propuesto se la realizará con un software propietario de otra empresa. Cabe destacar que a pesar de que las características y las configuraciones de los equipos sean diferentes, la funcionalidad presenta muchas similitudes.

En la simulación a realizar, se desarrollará la configuración de administración y seguridad en todos los switches, ya sean estos a nivel de acceso, distribución o núcleo.; dichas configuraciones se mostrará únicamente de uno de los switches de estas capas, recalcando que se debe realizar las mismas en todos los switches, cambiando el direccionamiento IP, acorde se muestra en las tablas siguientes.

De igual manera la configuración de las listas de acceso se realizará acorde al levantamiento de información previamente realizado en el capítulo 2 y en los Anexos A, B, C y D.

Previo al desarrollo de la simulación es necesario mostrar un diagrama topológico de red, y una tabla de direccionamiento del mismo. Esto se observa en el Figura y Tabla.

E.1 TOPOLOGÍA

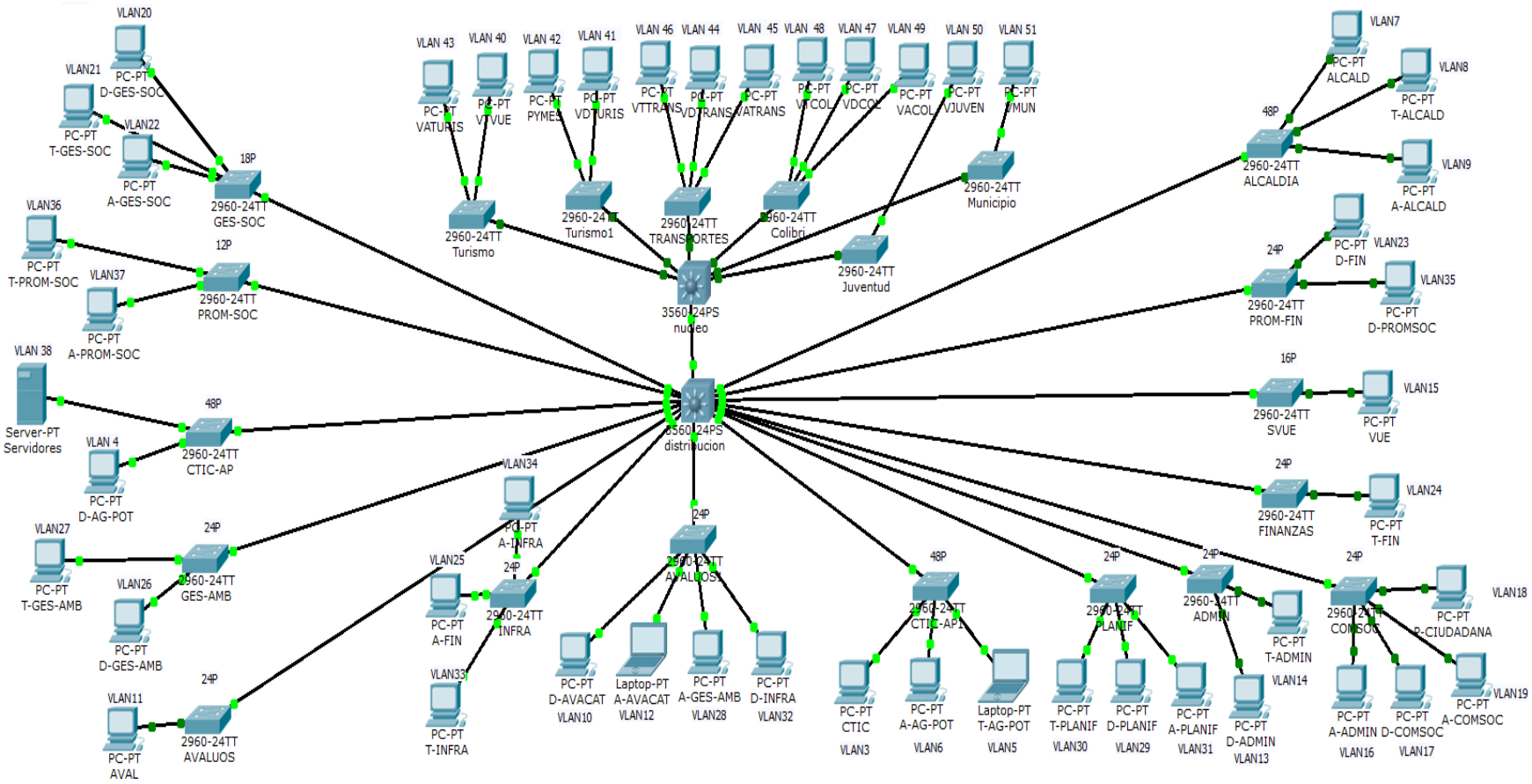


FIGURA E.1: Topología de Red

Fuente: Extraída de Cisco Packet Tracert.

E.2 TABLA DE DIRECCIONAMIENTO

TABLA E.1: Tabla de direccionamiento

Nombre del switch	Dirección IP de VLAN1	Máscara de subred	Nombres y números de VLAN	Asignación de puertos del switch
Switch GES-SOC	192.168.2.10	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.136	255.255.255.248	VLAN 20 VDGSI	fa0/1 -0/4
	192.168.1.208	255.255.255.240	VLAN 21 VTGSI	fa0/5-0/14
	192.168.3.114	255.255.255.248	VLAN 22 VAGSI	f0/15-0/18
Switch PROM-SOC	192.168.2.11	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.1.240	255.255.255.240	VLAN 36 VTPSP	fa0/1 -0/8
	192.168.3.146	255.255.255.248	VLAN 37 VAPSP	fa0/9 - 0/12
Switch CTIC-AP	192.168.2.12	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.4.0	255.255.255.192	VLAN 38 VSERV	fa0/1 -0/20
	192.168.2.96	255.255.255.248	VLAN 4 VDAP	fa0/21-0/24
Switch GES-AMB	192.168.2.13	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.1.128	255.255.255.224	VLAN 27 VTGAMB	fa0/1 -0/20
	192.168.2.152	255.255.255.248	VLAN 26 VDGAMB	fa0/21-0/24
Switch AVALUOS	192.168.2.14	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.3.0	255.255.255.224	VLAN 11 VTAVAL	fa0/1-0/24
Switch INFRA	192.168.2.15	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.3.64	255.255.255.240	VLAN 25 VAFIN	fa0/1 - 0/12
	192.168.1.224	255.255.255.240	VLAN 33 VTINFRA	fa0/13 - 0/20
	192.168.3.138	255.255.255.248	VLAN 34 VAINFRA	fa0/21-0/24
Switch Varios1	192.168.2.16	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.112	255.255.255.248	VLAN 10 VDAVAL	fa0/1 -0/4
	192.168.3.82	255.255.255.248	VLAN 12 VAAVAL	fa0/5-0/8
	192.168.3.122	255.255.255.248	VLAN 28 VAGAMB	fa0/9 - 0/12
	192.168.2.168	255.255.255.248	VLAN 32 VDINFRA	fa0/13 - 0/16
Switch CTIC-AP1	192.168.2.17	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.64	255.255.255.224	VLAN 3 VADMIN	fa0/1 - 0/14
	192.168.1.176	255.255.255.240	VLAN 5 VTAP	fa0/15 - 0/20
	192.168.3.66	255.255.255.248	VLAN 6 VAAP	fa0/21-0/24
Switch PLANIF	192.168.2.18	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.1.160	255.255.255.240	VLAN 30 VTPLAN	fa0/1 - 0/14
	192.168.2.160	255.255.255.248	VLAN 29 VDPLAN	fa0/15 - 0/18
	192.168.3.130	255.255.255.248	VLAN 31 VAPLAN	fa0/19 - 0/22
Switch ADMIN	192.168.2.19	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.120	255.255.255.248	VLAN 13 VDADMIN	fa0/1 -0/4
	192.168.1.96	255.255.255.224	VLAN 14 VTADMIN	fa0/5 -0/24

Switch COMSOC	192.168.2.20	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.1.192	255.255.255.240	VLAN 18 VTCXS	fa0/1 -0/12
	192.168.3.106	255.255.255.248	VLAN 19 VACXS	fa0/13 -0/16
	192.168.2.128	255.255.255.248	VLAN 17 VDCXS	fa0/17 -0/20
	192.168.3.90	255.255.255.248	VLAN 16 VAADMIN	fa0/21-0/24
Switch ALCALDIA	192.168.2.21	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.104	255.255.255.248	VLAN 7 VALCAL	fa0/1 - 0/8
	192.168.1.64	255.255.255.224	VLAN 8 VTALCAL	fa0/9 - 0/20
	192.168.3.74	255.255.255.248	VLAN 9 VAALCAL	fa0/21-0/24
Switch PROMFIN	192.168.2.22	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.144	255.255.255.248	VLAN 23 VDFIN	fa0/1 -0/4
	192.168.2.176	255.255.255.248	VLAN 35 VDPSP	fa0/5 -0/8
Switch VUE	192.168.2.23	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.2.144	255.255.255.248	VLAN 15 VVUE	fa0/1 -0/16
Switch Finanzas	192.168.2.24	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.1.0	255.255.255.192	VLAN 24 VTFIN	fa0/1-0/24
ENTES EXTERNOS				
Switch TURISMO	192.168.2.25	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.144	255.255.255.240	VLAN 40 VTVUE	fa0/1 -0/14
	192.168.5.160	255.255.255.240	VLAN 43 VATURIS	fa0/15-0/24
Switch TURISMO1	192.168.2.26	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.64	255.255.255.224	VLAN 42 VPYMES	fa0/1 -0/20
	192.168.5.200	255.255.255.248	VLAN 41 VDTURIS	fa0/21 - 0/24
Switch TRANSPORTES	192.168.2.27	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.128	255.255.255.240	VLAN 46 VTTRANS	fa0/1 -0/14
	192.168.5.192	255.255.255.248	VLAN 45 VATRANS	fa0/15 -0/20
	192.168.5.208	255.255.255.248	VLAN 44 VDTRANS	fa0/21-0/24
Switch COLIBRI	192.168.2.28	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.176	255.255.255.240	VLAN 48 VTCOL	fa0/1 -0/10
	192.168.5.216	255.255.255. 248	VLAN 47 VDCOL	fa0/11 -0/14
	192.168.5.224	255.255.255.248	VLAN 49 VACOL	fa0/15-0/18
Switch JUVENTUD	192.168.2.29	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.0	255.255.255. 192	VLAN 50 VJUVEN	fa0/1-0/24
Switch MUNICIPIO2	192.168.2.30	255.255.255.192	VLAN 2 Native	GigabitEthernet 1/1
	192.168.5.96	255.255.255. 224	VLAN 51 VMUN	fa0/1-0/24

Fuente: Elaborada por Andrea Zura

E.3 DESARROLLO

E.3.1 CONFIGURACIÓN DE ADMINISTRACIÓN BÁSICA DEL SWITCH

Este es un proceso que se debe realizar en todos los switches, sean estos de capa acceso, distribución o núcleo.

- Configurar el nombre del host

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Ges-Soc
```

- Configurar la contraseña EXEC privilegiado

```
Ges-Soc#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ges-Soc(config)#enable secret redgadmo2912
```

- Configurar contraseñas de terminal virtual y de consola

Se debe exigir una contraseña para acceder a la línea de consola. Incluso el Modo EXEC del usuario básico puede proporcionar información importante a un usuario malintencionado. Además, las líneas vty deben tener una contraseña antes de que los usuarios puedan acceder al switch de manera remota. (CISCO Networking Academic)

```
Ges-Soc(config)#enable password vlans2912
Ges-Soc(config)#line console 0
Ges-Soc(config-line)#password vlans2912
Ges-Soc(config-line)#login
Ges-Soc(config-line)#exit
Ges-Soc(config)#line vty 0 15
Ges-Soc(config-line)#password cisco
Ges-Soc(config-line)#login
Ges-Soc(config-line)#exit
```

- Configurar la encriptación de contraseñas

```
Ges-Soc(config)#service password-encryption
```

- Configurar el mensaje MOTD.

```
Ges-Soc(config)#banner motd &Acceso autorizado solo para Administradores&
```

- Configurar un servicio de traducción de nombres

```
Ges-Soc(config)#no ip domain-lookup
```

- Configure la gateway predeterminada en cada switch.

```
Ges-Soc(config)#ip default-gateway 192.168.2.1
```

E.3.2. CONFIGURACIÓN DE EQUIPOS TERMINALES

- Configurar las interfaces Ethernet en los equipos PC host

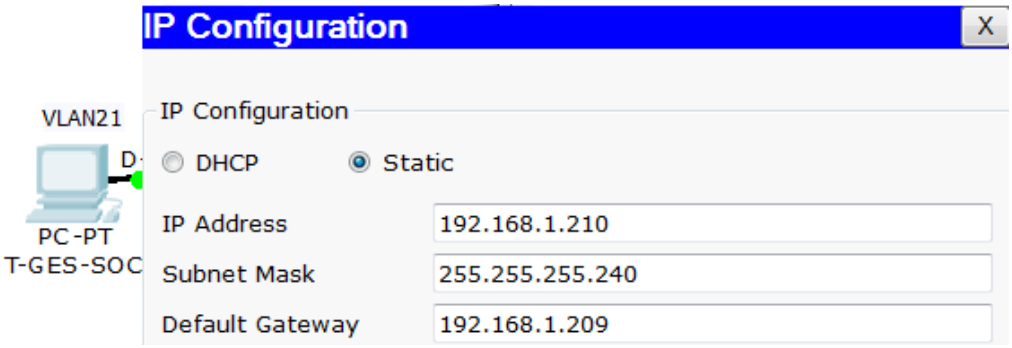


FIGURA E.2: Configuración IP host de acceso

Fuente: Extraído de Cisco Packet Tracert

E.3.3 CONFIGURACIÓN EN SWITCH CAPA ACCESO

- Habilitar los puertos del usuario en los switches de acceso en el modo de acceso

```
Ges-Soc#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ges-Soc(config)#interface range fa0/1-4
Ges-Soc(config-if-range)#switchport mode access
Ges-Soc(config-if-range)#no shutdown
Ges-Soc(config-if-range)#interface range fa0/5-14
Ges-Soc(config-if-range)#switchport mode access
Ges-Soc(config-if-range)#no shutdown
Ges-Soc(config-if-range)#interface range fa0/15-18
Ges-Soc(config-if-range)#switchport mode access
Ges-Soc(config-if-range)#no shutdown
Ges-Soc(config-if-range)#exit
```

- Configurar VTP

Antes de realizar la configuración de VTP se muestra en la tabla los modos de funcionamiento VTP de todos los switches que intervienen en la topología.

TABLA E.2: Distribución VTP en switches de acceso

Nombre del switch	**Modo funcionamiento VTP**	**Dominio VTP**	**Contraseña VTP**
Switch GES-SOC	Cliente	Gadmo	vlans2912
Switch PROM-SOC	Cliente	Gadmo	vlans2912
Switch CTIC-AP	Cliente	Gadmo	vlans2912
Switch GES-AMB	Cliente	Gadmo	vlans2912
Switch AVALUOS	Cliente	Gadmo	vlans2912
Switch INFRA	Cliente	Gadmo	vlans2912
Switch Varios1	Cliente	Gadmo	vlans2912
Switch CTIC-AP1	Cliente	Gadmo	vlans2912
Switch PLANIF	Cliente	Gadmo	vlans2912
Switch ADMIN	Cliente	Gadmo	vlans2912
Switch COMSOC	Cliente	Gadmo	vlans2912
Switch ALCALDIA	Cliente	Gadmo	vlans2912

Switch PROMFIN	Cliente	Gadmo	vlans2912
Switch VUE	Cliente	Gadmo	vlans2912
Switch Finanzas	Cliente	Gadmo	vlans2912
Switch Distribución	Servidor	Gadmo	vlans2912

Fuente: Elaborado por Andrea Zura

- Configurar VTP en todos los switches según la tabla.

```
Ges-Soc(config)#vtp mode client
Setting device to VTP CLIENT mode.
Ges-Soc(config)#vtp domain Gadmo
Domain name already set to Gadmo.
Ges-Soc(config)#vtp password vlans2912
Password already set to vlans2912
Ges-Soc(config)#end
```

- Configurar puertos de enlaces troncales

```
Ges-Soc(config)#interface range GigabitEthernet1/1-2
Ges-Soc(config-if-range)#switchport mode trunk
Ges-Soc(config-if-range)#switchport trunk native vlan 2
Ges-Soc(config-if-range)#no shutdown
Ges-Soc(config-if-range)#exit
```

- Configurar la dirección de la interfaz de administración

```
Ges-Soc(config)#interface vlan 2
Ges-Soc(config-if)#ip address 192.168.2.10 255.255.255.192
Ges-Soc(config-if)#no shutdown
Ges-Soc(config-if)#end
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

- Asignar puertos del switch a las VLAN

```
Ges-Soc(config)#interface range fa0/1-4
Ges-Soc(config-if-range)#switchport access vlan 20
Ges-Soc(config-if-range)#interface range fa0/5-14
Ges-Soc(config-if-range)#switchport access vlan 21
Ges-Soc(config-if-range)#interface range fa0/15-18
Ges-Soc(config-if-range)#switchport access vlan 22
Ges-Soc(config-if-range)#end
Ges-Soc#
%SYS-5-CONFIG_I: Configured from console by console
```

E.3.4. CONFIGURACIÓN EN SWITCH CAPA DISTRIBUCIÓN

- Configurar VTP en todos los switches según la tabla.

```
SW-DISTRIBUCION(config)#vtp mode server
Device mode already VTP SERVER.
SW-DISTRIBUCION(config)#vtp domain Gadmo
Changing VTP domain name from NULL to Gadmo
SW-DISTRIBUCION(config)#vtp password vlans2912
Setting device VLAN database password to vlans2912
SW-DISTRIBUCION(config)#end
```

- Configurar puertos de enlaces troncales

```
SW-DISTRIBUCION(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
SW-DISTRIBUCION(config-if-range)#switchport trunk native vlan 2
SW-DISTRIBUCION(config-if-range)#no shutdown
SW-DISTRIBUCION(config-if-range)#end
```

- Configurar el servidor VTP con las VLAN.

```
SW-DISTRIBUCION(config)#vlan 2
SW-DISTRIBUCION(config-vlan)#name Native
SW-DISTRIBUCION(config-vlan)#vlan 3
SW-DISTRIBUCION(config-vlan)#name VADMIN
SW-DISTRIBUCION(config-vlan)#vlan 4
SW-DISTRIBUCION(config-vlan)#name VDAP
SW-DISTRIBUCION(config-vlan)#vlan 5
SW-DISTRIBUCION(config-vlan)#name VTAP
SW-DISTRIBUCION(config-vlan)#vlan 6
SW-DISTRIBUCION(config-vlan)#name VAAP
SW-DISTRIBUCION(config-vlan)#vlan 7
SW-DISTRIBUCION(config-vlan)#name VALCAL
```

- Configurar la dirección de la interfaz de administración

```
SW-DISTRIBUCION(config)#interface vlan 2
SW-DISTRIBUCION(config-if)#ip address 192.168.2.2 255.255.255.192
SW-DISTRIBUCION(config-if)#exit
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
```

- Activar enrutamiento IP

```
SW-DISTRIBUCION(config)#ip routing
```

- Configurar la interfaz de enlaces troncales

```
SW-DISTRIBUCION(config-if)#interface vlan 3
SW-DISTRIBUCION(config-if)#ip address 192.168.2.65 255.255.255.224
SW-DISTRIBUCION(config-if)#no shutdown
SW-DISTRIBUCION(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up
SW-DISTRIBUCION(config-if)#interface vlan 4
SW-DISTRIBUCION(config-if)#ip address  192.168.2.97 255.255.255.248
SW-DISTRIBUCION(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up
SW-DISTRIBUCION(config-if)#interface vlan 5
SW-DISTRIBUCION(config-if)#ip address 192.168.1.177 255.255.255.240
SW-DISTRIBUCION(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to up
SW-DISTRIBUCION(config-if)#interface vlan 6
SW-DISTRIBUCION(config-if)#ip address 192.168.3.67 255.255.255.248
SW-DISTRIBUCION(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan6, changed state to up
```

- Configurar enlaces

```
SW-DISTRIBUCION(config)#interface GigabitEthernet 0/1
SW-DISTRIBUCION(config-if)#no switchport
SW-DISTRIBUCION(config-if)#ip address 192.168.5.233 255.255.255.252
SW-DISTRIBUCION(config-if)#no shutdown
```

E.3.5 CONFIGURACIÓN EN SWITCH CAPA NÚCLEO

- Configurar VTP en todos los switches según la tabla.

```
SW-NUCLEO(config)#vtp mode server
Device mode already VTP SERVER.
SW-NUCLEO(config)#vtp domain Gadmo
Domain name already set to Gadmo.
SW-NUCLEO(config)#vtp password vlans2912
Password already set to vlans2912
SW-NUCLEO(config)#end
```

- Configurar puertos de enlaces troncales

```
SW-NUCLEO(config)#interface range GigabitEthernet0/1-2
SW-NUCLEO(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
SW-NUCLEO(config-if-range)#switchport trunk native vlan 2
SW-NUCLEO(config-if-range)#no shutdown
SW-NUCLEO(config-if-range)#end
```

- Activar enrutamiento IP

```
SW-NUCLEO(config)#ip routing
```

- Configurar el servidor VTP con las VLAN.

```
SW-NUCLEO(config)#vlan 40
SW-NUCLEO(config-vlan)#name VTVUE
SW-NUCLEO(config-vlan)#vlan 41
SW-NUCLEO(config-vlan)#name VDTURIS
SW-NUCLEO(config-vlan)#vlan 42
SW-NUCLEO(config-vlan)#name VPYMES
SW-NUCLEO(config-vlan)#vlan 43
SW-NUCLEO(config-vlan)#name VATURIS
SW-NUCLEO(config-vlan)#vlan 44
SW-NUCLEO(config-vlan)#name VDTRANS
SW-NUCLEO(config-vlan)#vlan 45
SW-NUCLEO(config-vlan)#name VATRANS
SW-NUCLEO(config-vlan)#vlan 46
SW-NUCLEO(config-vlan)#name VTTRANS
SW-NUCLEO(config-vlan)#vlan 47
SW-NUCLEO(config-vlan)#name VDCOL
SW-NUCLEO(config-vlan)#vlan 48
SW-NUCLEO(config-vlan)#name VTCOL
SW-NUCLEO(config-vlan)#vlan 49
SW-NUCLEO(config-vlan)#name VACOL
SW-NUCLEO(config-vlan)#vlan 50
```

- Configurar la dirección de la interfaz de administración

```
SW-NUCLEO(config)#interface vlan 2
SW-NUCLEO(config-if)#ip address 192.168.2.2 255.255.255.224
SW-NUCLEO(config-if)#no shutdown

SW-NUCLEO(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

- Configurar la interfaz de enlaces troncales

```
SW-NUCLEO(config)#interface vlan 40
SW-NUCLEO(config-if)#ip address 192.168.5.145 255.255.255.240
SW-NUCLEO(config-if)#no shutdown
SW-NUCLEO(config-if)#interface vlan 41
SW-NUCLEO(config-if)#ip address 192.168.5.201 255.255.255.248
SW-NUCLEO(config-if)#no shutdown
SW-NUCLEO(config)#interface vlan 42
SW-NUCLEO(config-if)#ip address 192.168.5.65 255.255.255.224
SW-NUCLEO(config-if)#no shutdown
SW-NUCLEO(config-if)#interface vlan 43
SW-NUCLEO(config-if)#ip address 192.168.5.161 255.255.255.240
SW-NUCLEO(config-if)#no shutdown
```

- Configuración de enlaces

```
SW-NUCLEO(config)#interface GigabitEthernet 0/1
SW-NUCLEO(config-if)#no switchport
SW-NUCLEO(config-if)#ip address 192.168.5.234 255.255.255.252
SW-NUCLEO(config-if)#no shutdown
```

- CONFIGURAR RIP

```
SW-NUCLEO(config)#router rip
SW-NUCLEO(config-router)#version 2
SW-NUCLEO(config-router)#network 192.168.5.232
SW-NUCLEO(config-router)#network 192.168.2.0
SW-NUCLEO(config-router)#network 192.168.3.0
SW-NUCLEO(config-router)#network 192.168.4.0
SW-NUCLEO(config-router)#network 192.168.5.0
```

E.3.6 CONFIGURACIÓN EN SWITCH ENLACES EXTERNOS

- Configuración básica de administración.

```
Switch(config)#hostname TURISMO
TURISMO(config)#exit
TURISMO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TURISMO(config)#enable secret redgadmo2912
TURISMO(config)#enable password vlans2912
TURISMO(config)#line console 0
TURISMO(config-line)#password vlans2912
TURISMO(config-line)#login
TURISMO(config-line)#exit
TURISMO(config)#line vty 0 15
TURISMO(config-line)#password cisco
TURISMO(config-line)#login
TURISMO(config-line)#exit
TURISMO(config)#service password-encryption
TURISMO(config)#banner motd &Acceso autorizado solo para Administradores&
TURISMO(config)#no ip domain-lookup
TURISMO(config)#ip default-gateway 192.168.2.2
%SYS-5-CONFIG_I: Configured from console by console
```

- Habilitar los puertos del usuario en los switches de acceso en el modo de acceso

```
TURISMO(config)#interface range fa0/1-14
TURISMO(config-if-range)#switchport mode access
TURISMO(config-if-range)#no shutdown
TURISMO(config-if-range)#interface range fa0/15-24
TURISMO(config-if-range)#switchport mode access
TURISMO(config-if-range)#no shutdown
```

- Configurar VTP.

Antes de realizar la configuración de VTP se muestra en la tabla los modos de funcionamiento VTP de todos los switches que intervienen en la topología.

TABLA E.3: Distribución VTP enlaces externos

Nombre del switch	Modo funcionamiento VTP	Dominio VTP	Contraseña VTP
Switch Turismo	Cliente	Gadmo	vlans2912
Switch Turismo1	Cliente	Gadmo	vlans2912
Switch Transporte	Cliente	Gadmo	vlans2912
Switch Colibrí	Cliente	Gadmo	vlans2912
Switch Juventud	Cliente	Gadmo	vlans2912
Switch Municipio	Cliente	Gadmo	vlans2912
Switch Núcleo	Servidor	Gadmo	vlans2912

- Configurar VTP en todos los switches según la tabla.

```
TURISMO(config)#vtp mode client
Setting device to VTP CLIENT mode.
TURISMO(config)#vtp domain Gadmo
Changing VTP domain name from NULL to Gadmo
TURISMO(config)#vtp password vlans2912
Setting device VLAN database password to vlans2912
TURISMO(config)#end
```

- Configurar puertos de enlaces troncales y diseñar la VLAN nativa para los enlaces troncales.

```
TURISMO(config)#interface range GigabitEthernet1/1-2
TURISMO(config-if-range)#switchport mode trunk

TURISMO(config-if-range)#switchport trunk native vlan 2
TURISMO(config-if-range)#no shutdown
TURISMO(config-if-range)#end
```

- Configurar la dirección de la interfaz de administración

```
TURISMO(config)#interface vlan 2
TURISMO(config-if)#ip address 192.168.2.25 255.255.255.192
TURISMO(config-if)#no shutdown
TURISMO(config-if)#end
%LINK-5-CHANGED: Interface Vlan2, changed state to up
```

- Asignar puertos del switch a las VLAN

```
TURISMO(config)#interface range fa0/1-14
TURISMO(config-if-range)#switchport access vlan 40
TURISMO(config-if-range)#interface range fa0/15-24
TURISMO(config-if-range)#switchport access vlan 43
TURISMO(config-if-range)#end
```

E.3.7 CONFIGURACIÓN DE SEGURIDAD BÁSICA DEL SWITCH

- Habilitar seguridad en los puertos del switch

```
Ges-Soc(config)#interface range fa0/1-18
Ges-Soc(config-if-range)#switchport port-security
Ges-Soc(config-if-range)#interface range GigabitEthernet1/1-2
Ges-Soc(config-if-range)#switchport port-security
```

- Configurar la cantidad máxima de direcciones MAC.

```
Ges-Soc(config-if)#interface fastethernet 0/1
Ges-Soc(config-if)#switchport port-security maximum 1
```

- Configurar el puerto para agregar la dirección MAC a la configuración en ejecución

```
Ges-Soc(config)#interface fastethernet 0/1
Ges-Soc(config-if)#switchport port-security mac-address sticky
Ges-Soc(config-if)#interface fastethernet 0/5
Ges-Soc(config-if)#switchport port-security mac-address sticky
Ges-Soc(config-if)#interface fastethernet 0/15
Ges-Soc(config-if)#switchport port-security mac-address sticky
```

- Configurar el puerto para que se desactive automáticamente si se infringe la seguridad del puerto.

```
Ges-Soc(config-if)#interface fastethernet 0/1
Ges-Soc(config-if)#switchport port-security violation shutdown
Ges-Soc(config-if)#interface fastethernet 0/5
Ges-Soc(config-if)#switchport port-security violation shutdown
Ges-Soc(config-if)#interface fastethernet 0/15
Ges-Soc(config-if)#switchport port-security violation shutdown
```

E.3.8 CONFIGURACIÓN DE SSH EN LOS SWITCHES

```
Ges-Soc(config)#ip domain-name gadmo.com
Ges-Soc(config)#username security privilege 15 password vlans2912
Ges-Soc(config)#crypto key generate rsa
How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

Ges-Soc(config)#ip ssh time-out 30
*mar 1 3:58:37.179:  RSA key size needs to be at least 768 bits for ssh version
2
*mar 1 3:58:37.179:  %SSH-5-ENABLED: SSH 1.5 has been enabled
Ges-Soc(config)#ip ssh authentication-retries 3
Ges-Soc(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
Ges-Soc(config)#line vty 0 15
Ges-Soc(config-line)#transport input ssh
Ges-Soc(config-line)#login local
Ges-Soc(config-line)#logging on
Ges-Soc(config)#logging console
```

ANEXO F

F INSTALACIÓN Y CONFIGURACIÓN DEL IDS-IPS

Como se había mencionado en el capítulo tres, la plataforma utilizada para la implementación del sistema de detección de intrusos es SELKS, además se describió los requisitos previos a la instalación. Una vez instalado el sistema operativo, en la máquina virtual; tendremos la pantalla mostrada en la figura F-1.

FIGURA F.1: Pantalla de Inicio de SELKS

Fuente: Extraído de la pantalla de escritorio de SELKS

Para iniciar con la instalación y configuración es necesario desactivar la tarjeta de red, que será el sniffing del sistema de detección y prevención de intrusos; de tal manera que éste funcione de la manera más adecuada.

Es necesario verificar el estado de la interfaz de red que será el sniffing, en este caso la *eth1;* para ello se usa el comando **ehtool -k eth1.**

Se muestra dicha configuración en la figura F-2.

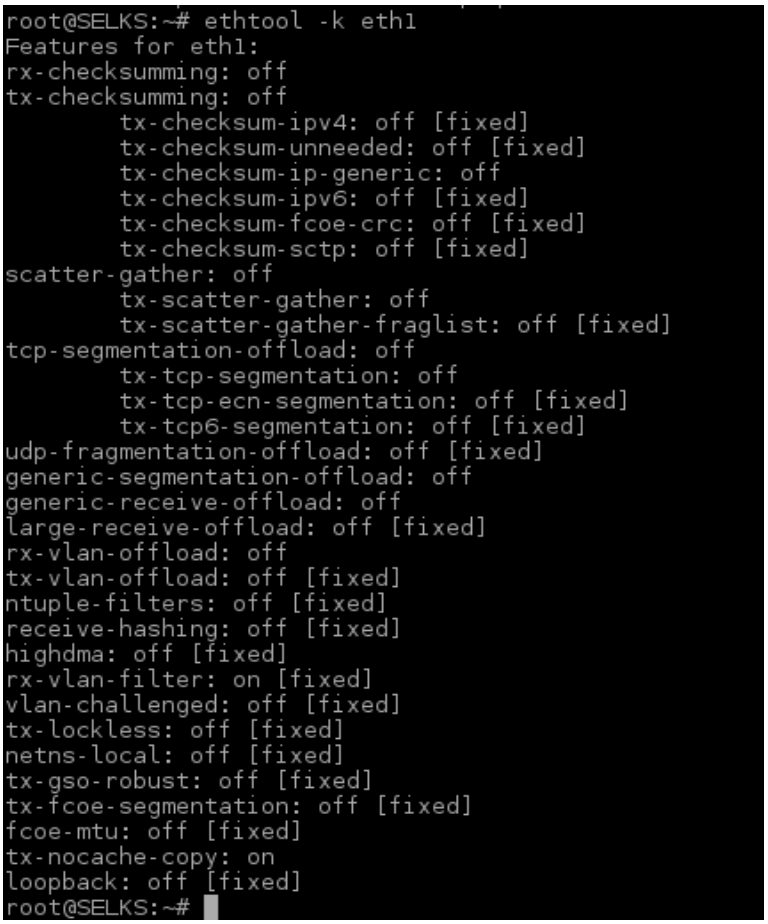


FIGURA F.2: Estado de la interfaz que funcionará como snnifing

Fuente: Extraída del terminal de SELKS

Conociendo el estado de la interfaz de red, se procede a configurarla, para que funcione como un snnifer, y permita monitorear de mejor manera la red.

Para ello a nivel de root, escribimos:

/opt/selks/Scripts/Setup/reconfigure-listening-interface_stamus.sh

FIGURA F.3: Configurar la interfaz snnifer

Fuente: Extraída del terminal de SELKS

Pedirá que se indique la interfaz que deseamos funcione como un snnifer; en este caso la eth1.

Se presentará después datos de la configuración realizada.

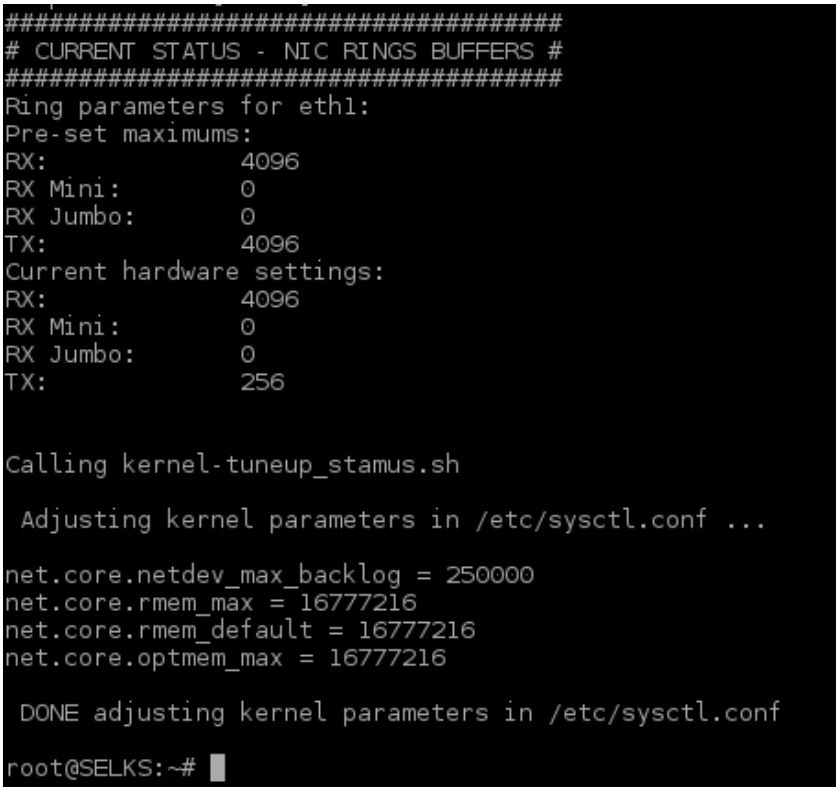


FIGURA F.4: Estado de interfaz snnifer

Fuente: Extraída del terminal de SELKS

F.1 Configuración de Suricata IDS-IPS

En la plataforma SELKS, ya viene instalado previamente Suricata; para comprobar que versión de este IDS-IPS se está corriendo, será necesario digitar el comando*:*

Suricata --build-info

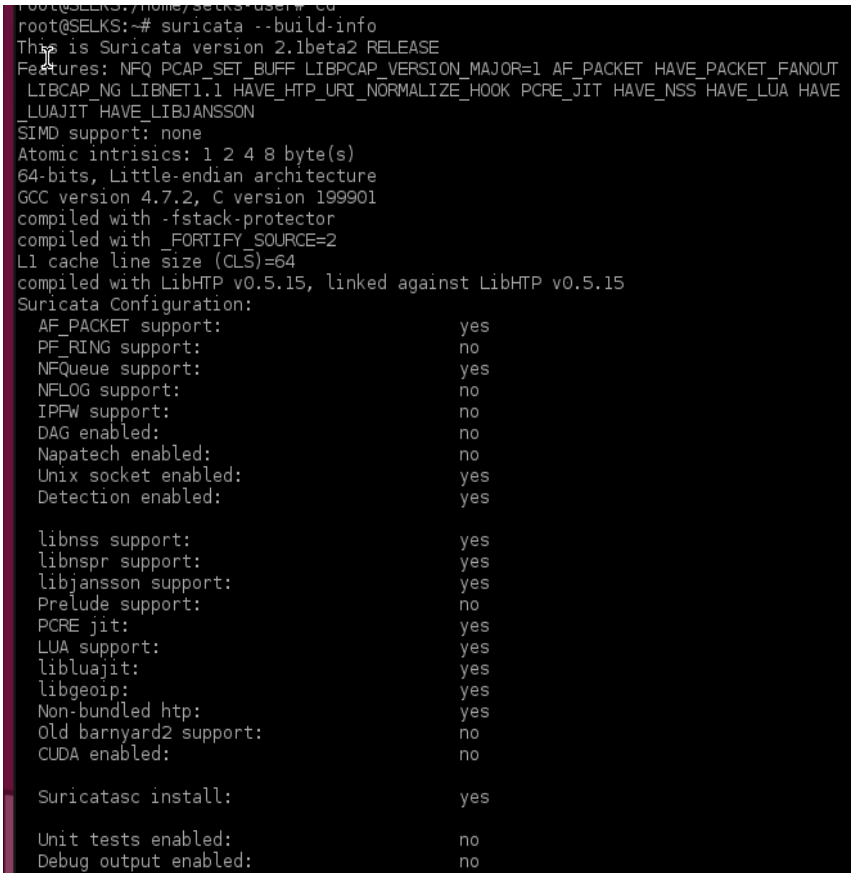


FIGURA F.5: Comprobación de la versión instalada de Suricata IDS-IPS

Fuente: Extraída del terminal de SELKS

Consideraciones básicas de configuración

Existen varias recomendaciones rápidas para mejo el r rendimiento en el tráfico de alta velocidad que se podría considerar ajustando ciertos valores del scrip **suricata.yaml**

Para ello, es necesario editar el script, en el directorio: /etc/suricata/suricata.yaml.

Las variables relativas a la transmisión vienen pre-establecidas con un valor bajo, ay que incrementarlo para obtener mejores resultados.

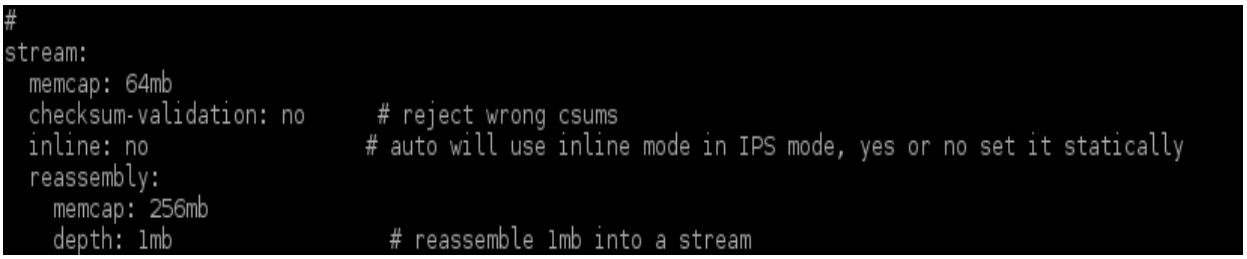


FIGURA F.6: Edición del parámetro stream en el archivo suricata.yaml

Fuente: Extraída del terminal de SELKS

El siguiente capo a editar son los tiempos de espera específicos para los flujos.; aquí puede especificar los tiempos de espera que los flujos de activos esperarán para tránsito y el transporte desde el estado actual a otro, en cada protocolo.

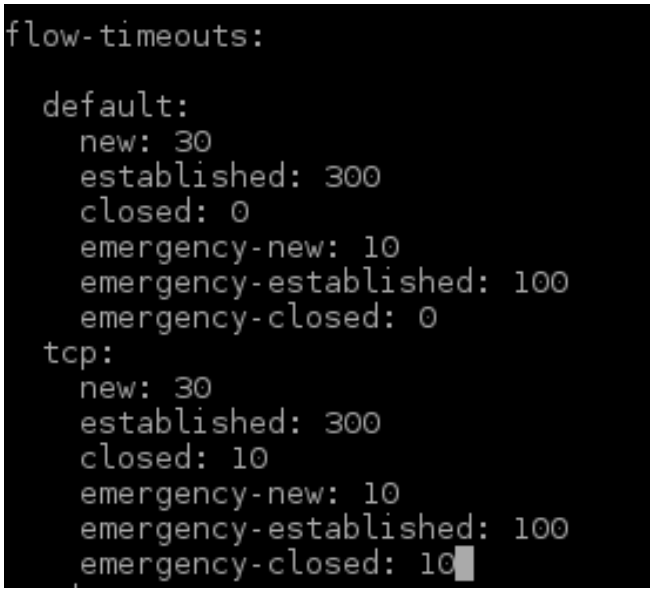


FIGURA F.7: Edición del parámetro flow-timeouts en el archivo suricata.yaml

Fuente: Extraída del terminal de SELKS

El motor de detección se basa en grupos internos de firmas, el cual nos permite especificar el perfil que desea utilizar para ellos, para gestionar la memoria de una manera eficiente manteniendo un buen rendimiento. Para la palabra clave de perfil puede utilizar las palabras de “baja”, “media”, “alta” o “personalizados”. En este caso se ha optado por el perfil alto.

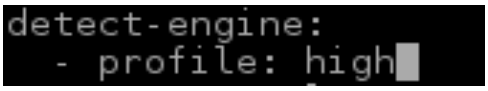


FIGURA F.8: Edición del parámetro detect-engine en el archivo suricata.yaml

Fuente: Extraída del terminal de SELKS

El valor máximo de paquetes pendientes viene establecido por defecto en 1024, pero esto desencadena un problema ya que puede causar cierta pérdida de paquetes debido a que se acumula de la firma después de que los hilos de captura de paquetes han comenzado a trabajar. Es por eso que no se recomienda dejarlo en el valor predeterminado. Es por ello que dicho valor se ha incrementado.

FIGURA F.9: Edición del parámetro max-pending en el archivo suricata.yaml

Fuente: Extraída del terminal de SELKS

Una vez instalado Suricata, lo vincularemos con Scirius; Elasticsearch, Kibana y Logstash para aprovechar todas las ventajas de la plataforma SELKS.

F.1.1 ENLAZAR SURICATA CON SCIRIUS

Lo primero que se hará será la instalación de Scirius, una aplicación escrita en Django[6]. Se puede instalar como cualquier otra aplicación Django.

La forma más fácil de instalar las dependencias es utilizar pip:

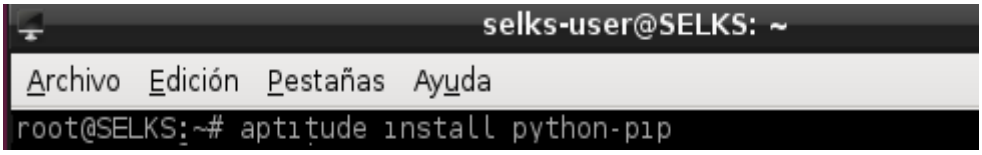


FIGURA F.10: Instalación de Python-pip

Fuente: Extraído del terminal de SELKS

A continuación, se debe instalar Django y las dependencias

FIGURA F.11: Instalación de Django y sus dependencias

Fuente: Extraído del terminal de SELKS

[6] Django es un framework web de código abierto escrito en Python que permite construir aplicaciones web más rápido y con menos código. http://django.es/

Una vez instalada, se puede poner en marcha el servicio.

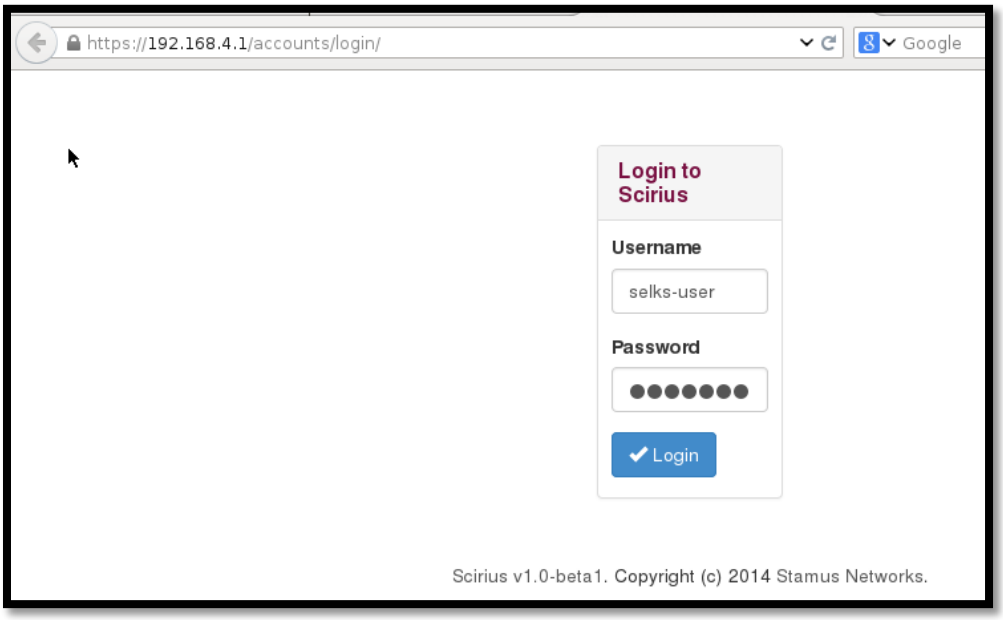


FIGURA F.12: Puesta en Marcha Scirius

Fuente: Pagina inicial desde el servidor de Scirius

Ahora enlazaremos Suricata con Scirius, considerando que éste está generando un solo archivo de reglas con todas las reglas activadas. Al editar el objeto Suricata, es necesario configurar el directorio donde desea que este archivo a ser generado y los archivos asociados del conjunto de reglas que se desea copiar.

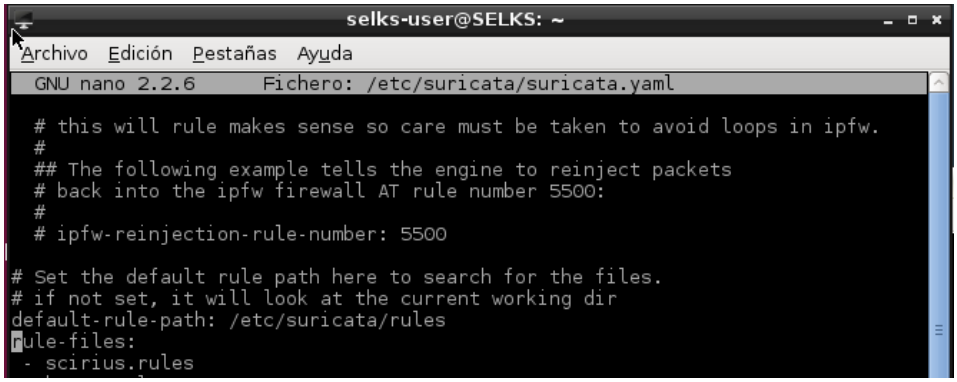


FIGURA F.13: Archivo configuración de ruta de reglas Scirius

Fuente: Extraído del terminal de SELKS

F.1.2 ENLAZAR SURICATA CON ELASTICSEARCH

Esta aplicación permitirá obtener información acerca de las firmas utilizadas por Suricata; además puede obtener gráfica y detalles sobre una norma específica.

Para configurar la conexión Elasticsearch, puede editar settings.py o crear un archivo en el directorio local_settings.py Scirius para configurar la función.

Se debe editar este archivo poniendo la variable USE_ELASTICSEARCH en verdadero y la variable ELASTICSEARCH_ADDRESS utilizando el formato IP: puerto.

```
# Elastic search

USE_ELASTICSEARCH = True
ELASTICSEARCH_ADDRESS = "192.168.4.1:9200"
```

FIGURA F.14: Edición de variables elasticsearch

Fuente: Extraído del terminal de SELKS

Se puede poner en marcha y observar la interacción con Suricata

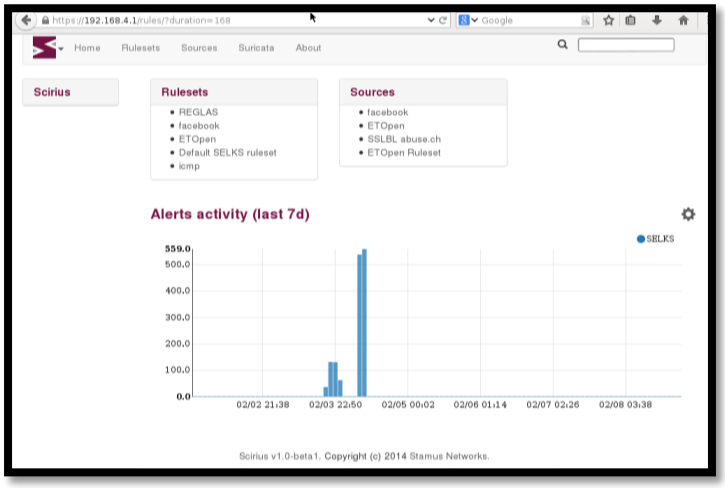


FIGURA F.15: Puesta en Marcha elasticsearch

Fuente: Pagina inicial desde el servidor de SELKS

F.1.3 ENLAZAR SURICATA CON KIBANA

Para configurar la conexión Kibana, puede editar settings.py o crear un archivo en el directorio local_settings.py Scirius para configurar la función.

```
# Kibana
USE_KIBANA = True
# Use django as a reverse proxy for kibana request
# This will allow you to use scirius authentication to control
# access to Kibana
KIBANA_PROXY = False
# Kibana URL
KIBANA_URL = "http://192.168.4.1:9292"
```

FIGURA F.16: Edición de variables kibana

Fuente: Extraído del terminal de SELKS

Se puede poner en marcha y observar la interacción con Suricata

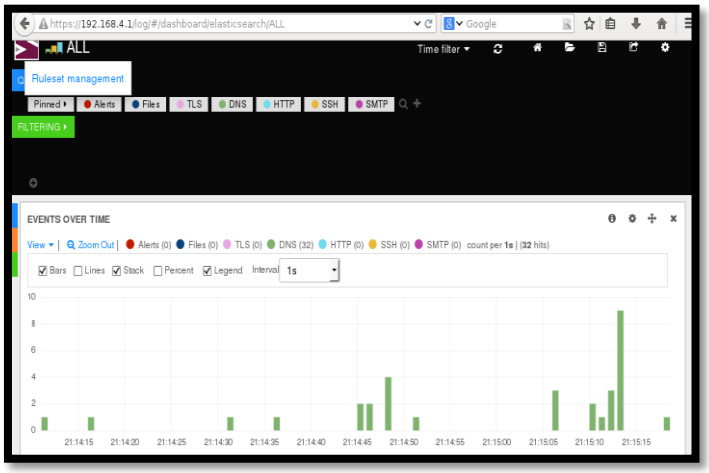


FIGURA F.17: Puesta en Marcha kibana

Fuente: Pagina inicial desde el servidor de SELKS

F.2 ADMINISTRACIÓN DE REGLAS

Un conjunto de reglas está hecho de componentes seleccionados de diferentes fuentes. Una fuente es un conjunto de archivos que proporcionan información a Suricata. (StamusNetworks, s.f.)

F.2.1 CREAR FUENTES

Para crear una fuente ir a fuentes -> Add (Añadir estar en el menú Acciones en la barra lateral). A continuación, establezca los diferentes campos y haga clic en Enviar.

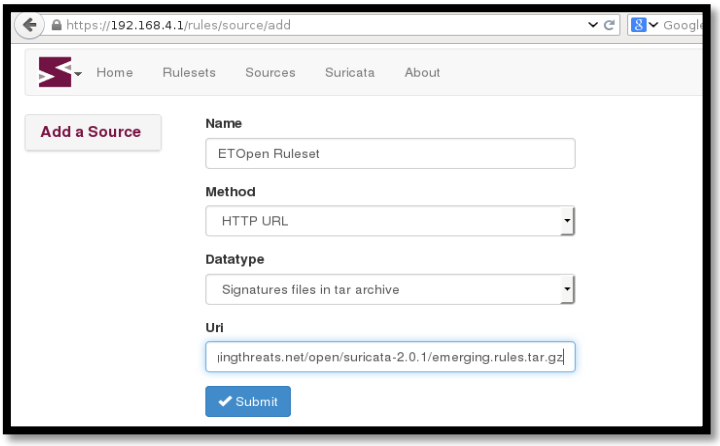


FIGURA F.18: Insertar fuentes en SELKS

Fuente: Pagina inicial desde el servidor de SELKS

F.2.2 CREAR CONJUNTOS DE REGLAS

Para crear un conjunto de reglas ir a Ruleset -> Add (Añadir estar en el menú Acciones en la barra lateral). A continuación, establezca el nombre del conjunto de reglas y elegir qué fuentes utilizar y haga clic en Enviar.

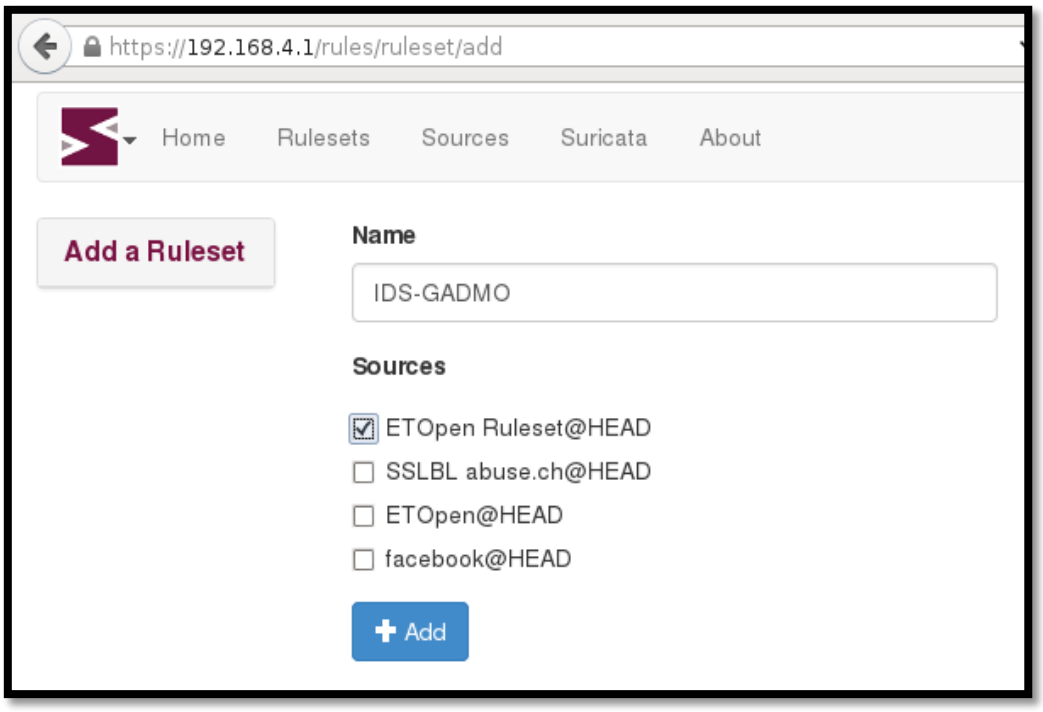


FIGURA F.19: Crear reglas Suricata

Fuente: Pagina inicial desde el servidor de SELKS

ANEXO G

G.1 MODELO DE TRÍPTICO DESTINADO A LOS USUARIOS DEL GADMO

El tríptico presentado a continuación, ha sido entregado a los Directores de los diversos Departamento, los cuales a su vez, han entregado copia del mismo con memo, a cada uno de los funcionarios de la entidad, de esta manera, se busca dar a conocer las principales Políticas de Seguridad de la Información propuestas en el “Manual de Políticas y Procedimientos de la Información”, desarrollados en este proyecto.

Además se presenta el documento de certificación de haber realizado la socialización del “Manual de Políticas y Procedimientos de la Información”

GOBIERNO AUTONOMO
DESCENTRALIZADO
MUNICIPAL DE OTAVALO

CERTIFICADO

De mi consideración:

Me permito en certificar por medio del presente que la señorita ANDREA YOMAIRA ZURA CHALÁ portadora de la cedula de identidad 100319306-5, ha llevado a cabo el proceso de entrega y socialización del MANUAL DE NORMAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, como parte de su trabajo de titulación de pregrado "**MODELO DE SEGURIDAD DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED PERIMETRAL Y RED INTERNA EN BASE A LA NORMA ISO/IEC 27002 EN LA RED DE DATOS DEL GADMO**"; proceso que se ha realizado satisfactoriamente, en las instalaciones de nuestra institución, obteniendo los mejores resultados del mismo.

Es todo cuanto puedo certificar, la peticionaria puede hacer uso del presente para los fines consiguientes.

Atentamente,

Wilman Garcés
Coordinador TIC´s

Dirección: García Moreno # 505 / **Telf:** 06 2 920 - 460 / 06 2 924 - 566
Fax: 06 2 920 - 404 / www.otavalo.gob.ec
OTAVALO - ECUADOR

Nuevo OTAVALO ADMINISTRACIÓN 2014 - 2019

Sobre el Uso del Servicio de Internet

- El uso del servicio de internet debe ser exclusivamente para actividades del GADMO.
- Las autoridades del GADMO podrán suspender el servicio de internet o cancelar la cuenta de correo electrónico por mal manejo, sin perjuicios de imponer las sanciones correspondientes según la gravedad de la falta.
- Es responsabilidad grave de cada usuario proteger su clave de acceso personal a la cuenta de correo, manteniéndola en estricto secreto, con la finalidad de evitar que cualquier otra persona la utilice para fines contrarios a lo establecido por el Manual de Normas y Procedimientos.

Sobre el Cumplimiento de las Políticas de Seguridad

- La CTIC será responsable de supervisar el cumplimiento de las políticas y lineamientos del GADMO
- En caso de infracciones leves de las normas y cualquier otro requisito de seguridad serán juzgados y sancionados por el Alcalde y/o Director Administrativo previo al informa técnico del Coordinador TIC'S.
- Se considerarán como infracciones graves al reglamento las siguientes:

a) Enviar mensajes para la difusión de noticias o correo electrónico sin identificar plenamente a su autor o autores, o enviar anónimos;

b) No hacer un uso racional, eficiente y considerado de los recursos disponibles tales como: el espacio en disco, memoria, red informática, entre otros;

d) Acceder a cualquier tipo de comunicaciones ente usuarios, como los CHAT, NEWS GROUP, MESSENGER, CORREO PERSONAL, etc.

e) Descargar archivos o correo electrónico sin la debida precaución de revisión de virus informáticos.

f) Intentar apoderarse de claves de acceso de otros usuarios, acceder y/o modificar archivos de otro usuario, y en especial los pertenecientes a la Municipalidad u otras Instituciones.

Si deseas obtener más información acerca de las políticas de seguridad de la información, acude a la Coordinación de TIC's y exige la revisión del Manual de Normas y Procedimientos; es tu deber y tu derecho el acceso al mismo.

CTIC

Coordinación de TIC's

Elaborado por: Andrea Zura Ch.

Autora de : "Manual de Normas y Procedimientos de Seguridad de Información en base a la Norma ISO /IEC 27002"

chazy_agav@yahoo.com

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL OTAVALO

Extracto del Manual de Nomas y Procedimientos de Seguridad de la Información

OBJETIVO

El presente documento tiene como propósito establecer un proceso eficaz para la gestión de los incidentes de la seguridad de la información, mediante políticas, objetivos y actividades plasmado en un Manual de Normas y Procedimientos, mismo que permitirá una formación, educación y concienciación adecuada de todos los usuarios de los activos informáticos del Gobierno Autónomo Descentralizado del Cantón Otavalo

NORMATIVA

El presente documento se realizó en base a la Norma NTE INEN-ISO/IEC 27002; la misma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información

Sobre la Políticas de Seguridad de la Información

El manual de Políticas de Seguridad de la Información se deberá comunicar de manera pertinente, accesible y comprensible para todos los usuarios de los activos del GADMO.

Sobre la Educación, formación y concienciación sobre la seguridad de la información

- En caso de necesitarlo, será responsabilidad de cada usuario solicitar capacitación al personal de la Coordinación de TIC's , en cuanto al manejo de paquetes informáticos, con el propósito de evitar fallas que pongan en riesgo la seguridad de la información.
- No será permitido en ningún momento la instalación y desinstalación d software en los equipos informáticos, sin previa consulta al personal autorizado en mantenimiento.
- Será responsabilidad de cada usuario, realizar respaldos d sus datos, acorde a la importancia de los mismos.
- Se presentará notificaciones inmediatas a la Coordinación de TIC's en caso de cualquier falla en los sistemas, o por mala manipulación de software o hardware de los equipos.

Sobre la ubicación y protección de los equipos

- **Se deberá evitar consumir alimentos y/o ingerir líquidos mientras se manipula equipos de cómputo, debido a que esto puede ocasionar un daño en el equipo.**
- **El usuario deberá tener cuidado de no pisar o maltratar los cables de conexiones tanto**

Sobre la Protección contra código malicioso y móviles.

- Se recomienda no descargar, adquirir o utilizar software de dudosa procedencia, o de fuentes no confiables.
- Todas las estaciones de trabajo, y servidores deberán tener instalado software antivirus activo y con sus respectivas actualizaciones..
- Antes de usar archivos provenientes de medios ópticos o electrónicos, y descargas de correos electrónicos todos los usuarios deberán realizar detección y reparación de códigos maliciosos.

Sobre el Uso de contraseñas

- El personal de trabajo de la Coordinación de TIC's emitirá una charla de las buenas prácticas de la seguridad en la selección y el uso adecuado de contraseñas.
- Evitar conservar registros de las contraseñas en papeles o archivos que están a la vista de cualquier usuario.
- Es responsabilidad del usuario el cambio periódico de contraseñas, evitando la reutilización de contraseñas antiguas. En caso de no saber hacerlo pedir asesoría en CTIC's.

La protección de tu información depende de ti. Haz un buen uso de tu contraseña.