UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNCACIÓN

ARTÍCULO CIENTÍFICO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA"

AUTOR: NORA ANGÉLICA PUERRES TREJO

DIRECTOR: ING. EDGAR MAYA

IBARRA –ECUADOR

2017

ARTÍCULO CIENTÍFICO

"SEGURIDAD PERIMETRAL Y SEGMENTACIÓN LÓGICA EN LA RED DE DATOS DEL INSTITUTO TECNOLÓGICO SUPERIOR JOSÉ CHIRIBOGA GRIJALVA DE LA CIUDAD DE IBARRA"

Autor- Nora Puerres Trejo, ***Coautor***- Ing. Edgar Maya.
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte (UTN), Ibarra – Ecuador
Autor: *napuerrest@utn.edu.ec*

1. Resumen

El proyecto de titulación se basa en el diseño e implementación de un Sistema de Seguridad Perimetral para la red de datos del Instituto Tecnológico Superior "José Chiriboga Grijalva "de la ciudad de Ibarra, con el objetivo primordial de mejorar la seguridad de la información en la institución educativa .

Como inicio del desarrollo del Sistema de Seguridad Perimetral, se realiza el levantamiento de la información de los activos informáticos físicos y lógicos de la institución con el objetivo primordial de evidenciar directamente la situación actual de red de datos , de esta manera se obtendrá las vulnerabilidades y amenazas, a las que se encuentra sometida la red lógica , con este antecedente se realiza el estudio del análisis de riesgo donde se utilizara la Guía del Instituto Nacional de estándares y tecnología NIST SP 800-30, y describir puntualmente los niveles actuales de seguridad de la información.

La parte de implementación del sistema de Seguridad Perimetral consta básicamente de la configuración del firewall en software libre, donde se definen las políticas de acceso o restricción que permita una defensa ante los ataques que puedan suscitarse en la red de datos, además la implementación y configuración del IPS y finalmente la creación de VLANs necesarias y que se ajusten a las necesidades de la red para un correcto funcionamiento de la segmentación lógica.

Con la evolución de las redes de datos en los últimos años, se puede evidenciar un crecimiento en el flujo de la información y en los servicios que estas brindan, puesto que son de carácter fundamental y necesario para cualquier tipo de proceso sea este de tipo comercial, gubernamental o educativo. Al encontrarse en estos grandes entornos se involucran el uso de equipos de cómputo u otros dispositivos que permita acceder a las redes de datos, que se encuentran susceptibles a cualquier tipo de ataque sea este de sustracción, falsificación o modificación de la información, denegación de servicios en las instituciones lo que conllevaría a pérdida de información y en algunos casos, perdidas económicas.

2. Introducción

El desarrollo y crecimiento del Instituto Tecnológico Superior José Chiriboga Grijalva ITCA, han permitido que su infraestructura tecnológica, crezca en gran medida, la misma que cuenta con una capacidad de acceso a Internet de 16 Mbps y una red de datos con direccionamiento

IPv4 clase B, estructurada a través de un Cableado Estructurado tanto de Fibra Óptica Furukawa 10gigabit dúplex optical, como también Cable UTP Categoría 6, los cuales se rigen en las normativas: EIA/TIA-568B. A su vez su Data Center se encuentra constituido por equipos Cisco tales como un Router HP A-MSR 900 perteneciente a TELCONET, un Router Cisco 881, un Switch Cisco 2950 capa 3, seis Switch SG200-26 y ochp Switch SG300-28, también contiene una Central 500 FXO de Voz IP, como también una Central HIK VISION de Cámaras IP además de ocho Servidores los cuales contienen grandes cantidades de información de suma importancia. A su vez cuenta con seis sistemas administrativos, una plataforma virtual en Moodle, cinco laboratorios informáticos y un espacio dedicado para libre acceso a consultas académicas para los estudiantes.

Actualmente el Instituto ITCA cuenta con una infraestructura de red funcional, pero no posee un buen sistema de seguridad para dicha red, por lo que se encuentra vulnerable ante ataques informáticos, de manera interna y externa; carece de una buena segmentación lógica que permita generar un mayor control de los accesos permitidos y denegados a determinada información, por lo cual el departamento de tecnología de la Institución ha visto urgente la implementación de un sistema de seguridad que proteja su red de datos.

El presente proyecto de titulación se basa en el bloqueo de las amenazas que se puedan presentar en la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva mediante la implementación de un Firewall basado en software libre además de la ejecución de políticas de seguridad y segmentación en base a la construcción de VLANs para la segmentación de la red.

En primera instancia se presenta los fundamentos teóricos, de seguridad de redes y las características para la implementación de la Seguridad Perimetral y la creación de VLANs en la red de datos del instituto.

Se realizará el levantamiento de la información, para evaluar la situación actual de la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva, de esta manera se obtendrá las vulnerabilidades y amenazas, a las que se encuentra sometida la red física y lógica de la red, esto se lo realizará en base a la metodología de análisis y gestión de riesgos NISTP SP 800-30 que comprende la caracterización de los sistemas, identificación de amenazas y vulnerabilidades y finalmente análisis y control de las mismas.

La parte de implementación del sistema de Seguridad Perimetral consta básicamente de la configuración del firewall, donde se definen las políticas de acceso o restricción que permita una defensa ante los ataques que puedan suscitarse en la red de datos, además la implementación y configuración del IPS y finalmente la creación de VLANs necesarias y que se ajusten a las necesidades de la red para un correcto funcionamiento de la segmentación lógica.

Después de realizar la parte de implementación del sistema de Seguridad Perimetral en la red de datos del Instituto Tecnológico Superior José Chiriboga Grijalva, se realiza un ataque simulado en la red de datos, dónde se verificará la funcionalidad de mismo.

3. Marco Referencial.

3.1 Contexto de la Institución

El Ministerio de Educación y Cultura mediante Acuerdo Ministerial Nº 3669 de fecha 5 de agosto de 1992, autoriza la transformación y funcionamiento del Instituto "José Chiriboga Grijalva" de la ciudad de Ibarra, provincia de Imbabura, con la finalidad de que otorgue los títulos de: Técnico Superior y el Título de Tecnólogo. (ITCA, 2015)

El Instituto Tecnológico Superior "José Chiriboga Grijalva" con su acrónimo ITCA se encarga de formar profesionales en distintas carreras de nivel tecnológico, teniendo presente los valores y el perfeccionamiento de habilidades y destrezas, con el objetivo de generar soluciones a los problemas y necesidades del país.

El Instituto Tecnológico Superior "José Chiriboga Grijalva" se encuentra ubicado en la ciudad Ibarra, entre las calles El Oro y 13 de Abril, como se muestra en la Figura 1.

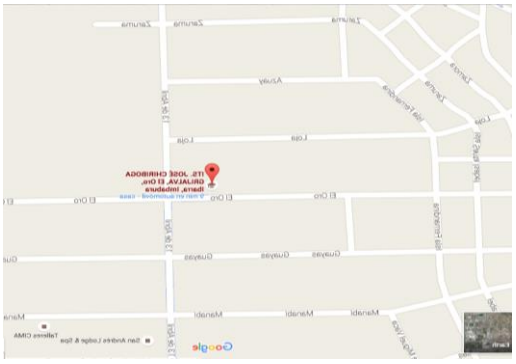

Figura 1. Ubicación Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Recuperado de https://www.google.com.ec/maps/place/ITS.+JOS%C3%89+CHIRIBOGA+GRIJALVA,+El+Oro,+Ibarra,+Imbabura

3.2 Marco teórico.

3.2.1 Seguridad perimetral

La seguridad perimetral es una rama de la seguridad informática que se ocupa de vigilar el perímetro o "borde" de la red, es decir, es una defensa ante las amenazas externas que intentan filtrarse. Se puede hacer una analogía con una muralla fortificada cuyo objetivo es restringir el paso a los enemigos, eso es básicamente lo que busca la seguridad perimetral, limitar los accesos solamente los paquetes confiables que circulan por la red y restringir aquellos que pueden hacer daño. (MAYORGA, 2008)

3.2.2 Objetivos de la seguridad perimetral.

Dentro de los objetivos de la seguridad perimetral se puede mencionar los siguientes:

- Proteger el perímetro de la red privada de datos ante las amenazas externas permitiendo sólo cierto tipo de tráfico en distintos segmentos de la red.

- Filtrar eficientemente todo tipo de acceso solicitado hacia la red privada, el tráfico entrante será dirigido a los sistemas adecuados dentro de la intranet.

- Reaccionar ante las amenazas antes de que estas puedan acceder a la red privada.

3.2.3 Perímetro de la red

Llamado también zona de frontera ya que aísla la red externa con la red interna donde se encuentran los hosts y los servidores de aplicación. Es considerada como la zona menos segura del sistema además de ser un punto con el

mayor tráfico a monitorizar, como se muestra en la figura 2.

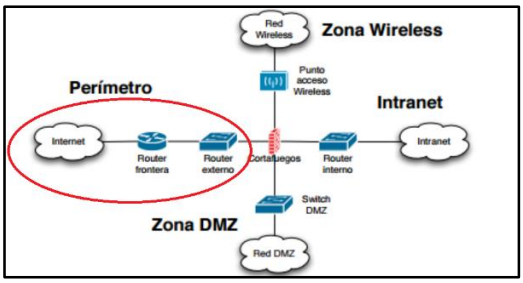

Figura 2. Topología de una red típica donde se visualiza la zona de perímetro de red

Fuente: Recuperado de http://www.ia.urjc.es

4. Evaluación de la situación actual de la red de datos

4.1 Situación actual de la red de datos del Instituto Tecnológico Superior "José Chiriboga Grijalva".

Tomando en cuenta que la institución educativa en los últimos cinco años ha realizado un importante cambio de espacio físico, por hoy cuenta con un nuevo edificio y con esto la capacidad ha aumentado, de tener en sus instalaciones mayor número de alumnos, docentes y personal administrativo. Por ende este tipo de usuarios necesitan a diario los servicios de la red de datos del instituto como: acceso a las aulas virtuales, ingreso de notas, correo institucional, facturación etc., con la finalidad de compartir recursos.

4.1Topología de red.

La topología de red del Instituto Tecnológico Superior "José Chiriboga Grijalva" se encuentra dividida en dos entornos, la topología física y la topología lógica.

4.1.1 Topología física.

En esta topología se evidencia el lugar físico donde se encuentran los equipos de usuarios finales, los dispositivos de red y el cableado que conforman la red de datos del instituto, como se muestra en la Figura 3.

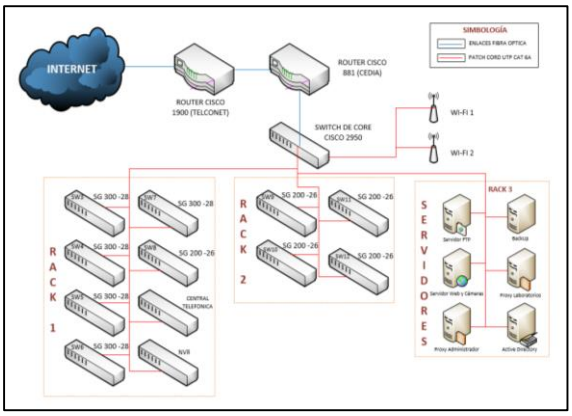

Figura 3. Topología física del Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Dirección de tecnología de la información ITCA

4.1.2 Topología Lógica

Dentro de esta topología se visualiza la forma de cómo se comunican los servicios y usuarios de capa de acceso con la infraestructura de red dentro de la topología física, como indica la Figura 4.

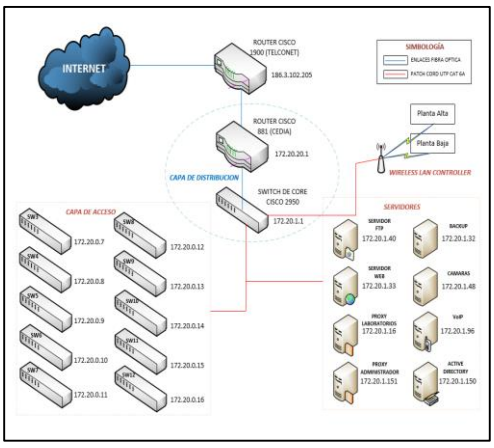

Figura 4. Topología lógica del Instituto Tecnológico Superior "José Chiriboga Grijalva"

Fuente: Dirección de tecnología de la información ITCA.

5. Análisis de riesgos en base a la metodología NIST SP 800 - 30

Para la realización del análisis de riesgo se utilizara la Guía del Instituto Nacional de estándares y tecnología NIST SP 800-30, con el fin de conocer los niveles actuales de seguridad de la información e identificar los requerimientos de seguridad en la red de Datos del Instituto Tecnológico Superior "José Chiriboga Grijalva".

5.1 Importancia del Análisis del riesgo.

El análisis de riesgo, se transforma en una herramienta importante para sustentar los incidentes de seguridad, así como también para justificar una posible inversión y orientar los recursos de manera costo-beneficiosa para cualquiera entidad. Este tipo de análisis nos permite determinar a qué nivel dentro de la organización y en qué áreas, la seguridad tendrá jurisdicción.

La metodología que se va a utilizar para la evaluación de riesgos en la red de Datos del Instituto Tecnológico Superior "José Chiriboga Grijalva", se ha tomado de la "Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información "publicada por NIST 800 en su publicación especial número 30.

La guía Americana Internacional descrita por el (NIST); Instituto Nacional de Normas y Tecnología con sus siglas en inglés (National Institute of Standards and Technology). Documento que fue creado en el año 2002, y se encarga de contribuir con el proceso que debe llevarse a cabo en la gestión de riesgos. Con la finalidad de gestionar, controlar y mitigar el riesgo que se pueda evidenciar, dentro de una organización.

Esta Guía está estructurada por cinco secciones, que se describen a continuación:

- Sección 1: Introducción,
- Sección 2: Visión de la Gestión de Riesgos
- Sección 3: Evaluación del Riesgo
- Sección 4: Mitigación del Riesgo
- Sección 5: Evaluación y Valoración.

De acuerdo al alcance de este proyecto solo se concentrará en la sección 3: Evaluación del Riesgo, como un precedente para el evidenciar tanto amenazas y vulnerabilidades que la red de datos del Tecnológico ITCA, presenta tomando en cuenta que esta guía ya define los pasos necesarios que deben complementarse para el análisis del riesgo.

Pasos de la metodología de evaluación del riesgo según la Guía NIST SP 800 - 30 La metodología de análisis y evaluación de riesgos está compuesta por nueve (9) pasos primarios, que se describen a continuación en la figura 5.

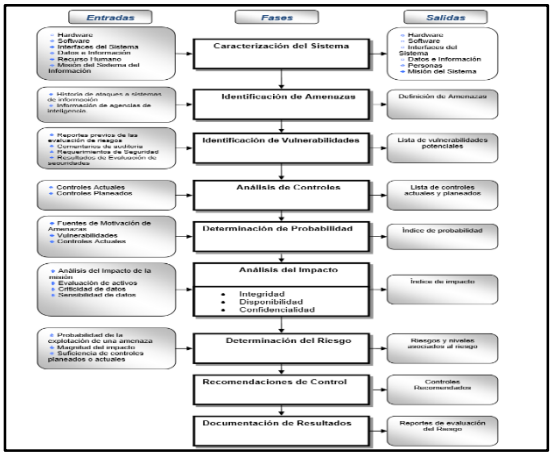

Figura 4. Metodología del análisis de riesgo

Fuente: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

5.2. Calculo del nivel de importancia (NI) para los activos dentro de la caracterización de sistemas del Tecnológico ITCA.

Se determina como nivel de importancia (NI) a cada grupo de activos dentro de la institución en base a tres factores que son: confidencialidad, integridad y disponibilidad. A continuación se describe a cada uno de los factores involucrados para dicho cálculo.

- Factor de Confidencialidad (Conf): la confidencialidad asegura que la información sea accesible solo para aquellos usuarios que estén autorizados, es decir, evita que la información sea usada por usuarios no autorizados.
- Factor de Integridad (Int): asegura que la información no sea falsa, también asegura exactitud y completitud, es decir, que los datos que se han recibido y/o se han recuperado sean exactamente los mismos que fueron enviados y/o almacenados, la información no debe tener alguna modificación.
- Factor de Disponibilidad (Disp): garantiza que la información se encuentre siempre disponible, que los usuarios autorizados pueden tener acceso a ésta información cuando lo requieran o la necesiten.

Para poder establecer el nivel de importancia (NI) de cada activo, primero se describe las escalas y el criterio que se va a utilizar para tal efecto. Las tablas 1, especifica la escala de importancia.

Tabla 1. Escala de valoración del factor Confidencialidad, Integridad y disponibilidad de los activos de información

FACTOR CONFIDENCIALIDAD (CONF)			FACTOR INTEGRIDAD (INT)	FACTOR DISPONIBILIDAD (DISP)
Nivel	Categoría	Descripción	Descripción	**Descripción**
1	**Bajo**	Puede ser revelado o proporcionado a cualquier persona	La modificación de su contenido no afectaría la entrega de servicios.	**En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser reducidas.**
		Consecuencia imperceptible	**Consecuencia imperceptible**	**Consecuencia imperceptible**
2	**Medio**	Puede ser revelado o proporcionado a sólo usuarios del Tecnológico ITCA	La modificación de su contenido tendría una afectación media en la entrega de servicios.	**En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser moderadas.**
		Consecuencia moderada	**Consecuencia moderada**	**Consecuencia moderada**
3	**Alto**	Puedes ser revelado solo a personal del Departamento de Sistemas del Tecnológico ITCA	La modificación de su contenido tendría una afectación media en la entrega de servicios.	**En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser altas**
		Consecuencia alta	**Consecuencia alta**	**Consecuencia alta**
4	**Muy alto**	Puede ser revelado sólo al personal autorizado del departamento de sistemas, si así se autoriza.	La modificación de su contenido afectaría de manera muy relevante en la entrega de servicios	**En caso de que la información no estuviese disponible, las consecuencias en la entrega de servicios podrían ser graves**
		Consecuencias graves	**Consecuencias graves**	**Consecuencias graves**

Fuente: Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

5.3 Resultado de la evaluación del riesgo

Para el resultado de la evaluación del riesgo se encuentran las vulnerabilidades que se asocian a cada una de las amenazas para los tres tipos de causas , la tabla 2 muestra en resumen cada amenaza y la vulnerabilidad que puedes ser explotada.

Tabla 2. Evaluación de amenazas/vulnerabilidades

TIPO	#	AMENAZAS	VULNERABILIDAD
TECNOLOGICAS	1	Daño del hardware	No existen los repuestos para el correcto funcionamiento del hardware, falta de presupuesto.
	2	Daño del software	No cuenta con un protocolo de actualización del software.
	3	Daño de los medios de trasmisión	No cuenta con políticas del manejo del cableado estructurado.
	5	Inhibición de los puertos	No cuenta con un protocolo de manejo de puertos.
	6	Falla eléctrica	Sobrecarga de energía Fallas del proveedor de suministro eléctrico. Tableros eléctricos expuestos.
	7	Falla del sistema de alimentación ininterrumpida (UPS)	No existe un protocolo de contención ante un corte inesperado de energía.
	8	Software no licenciado	No se encuentra con las licencias actualizadas.
	9	Software desactualizado	No cuenta con un protocolo de actualización de software.
	10	Daño del sistema de aire acondicionado	No cuenta con un protocolo de mantenimiento periódico.
	11	Ataque a la red	Acceso a la terminal de administración. Uso de contraseñas no robustas o por defecto.
	12	Falla de backup	No cuenta con una política de respaldo total o parcial de la información.

6. Diseño e implementación del sistema de seguridad perimetral en la red del instituto

En este capítulo se procederá con la configuración de los equipos necesarios para la implementación de la seguridad perimetral, así como para la IPS, Firewall y Segmentación lógica de la red.

6.1 Políticas de seguridad en la red.

La decisión de instalar un firewall puede estar influenciada por dos niveles de política de la red de datos como la distribución y uso del sistema.

- La política de acceso a la red define los servicios que se permitirán o negarán de manera explícita es la política de más alto nivel.
- También define cómo se utilizan los servicios la política de bajo nivel define cómo se restringirá en realidad el acceso y determinará los servicios especificados en la política de nivel superior.

Las dos políticas básicas en la configuración de un firewall y que cambian radicalmente la filosofía fundamental de la seguridad en la institución están dadas por:

- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.
- La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico Potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

6.2 Distribución lógica de la red del Tecnológico ITCA

Para lograr un correcto diseño de seguridad perimetral como primer paso se realiza la distribución de las Vlans de acuerdo al tipo de

servicios que se presenta y de acuerdo a las necesidades de la red.

Se han designado 16 Vlans con su direccionamiento IP y se han asignado de acuerdo a la dirección de red 172.20.0.1/24. La tabla 3 muestra el direccionamiento que se ha designado

Tabla 3. Distribución de las Vlans para la segmentación lógica

Numero de Vlan	Dirección IP	Mascara	Servicio
Vlan 1	172.10.1.0	255.255.255.0	**Por defecto**
Vlan 2	172.20.1.1	255.255.255.0	**Servidores**
Vlan 3	172.20.2.1	255.255.255.0	**Administrativos**
Vlan 4	172.20.3.1	255.255.255.0	**Sistemas**
Vlan 5	172.20.4.1	255.255.255.0	**Laboratorios**
Vlan 6	172.20.5.1	255.255.255.0	**Wireless**
Vlan 7	172.20.6.1	255.255.255.0	**Vigilancia**
Vlan 8	172.20.7.1	255.255.255.0	**Coordinadores**
Vlan 9	172.20.8.1	255.255.255.0	**Internet**
Vlan 10	172.20.9.1	255.255.255.0	**Laboratorio3**
Vlan 11	172.20.10.1	255.255.255.0	**Wireless-Estudiantes**
Vlan 12	172.20.11.1	255.255.255.0	**Wireless-Docentes**
Vlan 13	172.20.12.1	255.255.255.0	**- Wireless Administrativos**
Vlan 14	172.20.1.14	255.255.255.0	**Wireless-Invitados**
Vlan 15	172.20.15.1	255.255.255.0	**Cyber**
Vlan 16	172.2016.1	255.255.255.0	**CACMU**

Fuente: Basado en investigación teórica y práctica

6.3 Diseño del sistema de Seguridad Perimetral.

El diseño permite desarrollar la mejor solución que se acople a las necesidades para mejorar la seguridad de los activos de la red de datos del Tecnológico ITCA.

Para esto se han dividido la red en tres zonas la red WAN, red de la zona desmilitarizada DMZ y la red local LAN, La figura 6 muestra el diseño de Seguridad Perimetral.

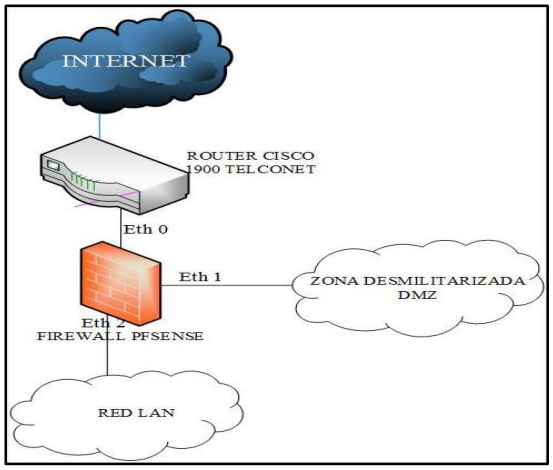

Figura 6 . Topología del diseño del firewall

Fuente: Basado en investigación teórica y práctica

6.4 Direccionamiento del diseño de seguridad perimetral del Tecnológico ITCA.

La tabla 4 muestra el direccionamiento propuesto, que se lleva acabo para el diseño del firewall.

Tabla 1. Direccionamiento del diseño de red

Red	Dirección IP	Mascara
Red WAN	192.168.X.X	**255.255.255.0**
Red DMZ	172.16.X.X	**255.255.255.0**
Red LAN	172.16.4.1	**255.255.255.0**

Fuente: Basado en investigación teórica y práctica

6.5 Principios y características de diseño.

El Firewall es colocado entre la red local LAN y la red WAN y por ende separa la red de la zona desmilitarizada DMZ

- **Objetivos:**
- Establecer un enlace controlado
- Proteger la red local de ataques
- Proveer un único punto de choque

Configuración de los equipos de red

Para la configuración del switch de Core se realiza un procedimiento establecido de la siguiente manera, la configuración completa en la tabla 5 muestra el resumen de la configuración de las Vlans.

- Configuración de Nombre
- Configuración de las contraseñas para ingreso de consola y telnet
- Configuración del Banner
- Configuración de VTP Server
- Configuración de las nuevas VLANs
- Configuración de la IP en las Interfaces de VLAN
- Configuración de los Enlaces de Troncal

Tabla 5. Resumen de la configuración de las Vlans

```
SW-ITCA-CORE#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
2    servidores                       active
3    Administrativos                  active
4    Sistemas                         active
5    Laboratorios                     active
6    Wireless                         active
7    Vigilancia                       active
8    Coordinadores                    active
9    Internet                         active
10   Laboratorio3                     active
11   W_Estudiantes                    active
12   W_Docentes                       active
13   W_Administrativos                active
14   W_Invitados                      active
15   Cyber                            active
16   CACMU                            active
1002 fddi-default                     active

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
5    enet  100005     1500  -      -      -        -    -        0      0
6    enet  100006     1500  -      -      -        -    -        0      0
7    enet  100007     1500  -      -      -        -    -        0      0
8    enet  100008     1500  -      -      -        -    -        0      0
9    enet  100009     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
12   enet  100012     1500  -      -      -        -    -        0      0
13   enet  100013     1500  -      -      -        -    -        0      0
14   enet  100014     1500  -      -      -        -    -        0      0
15   enet  100015     1500  -      -      -        -    -        0      0
16   enet  100016     1500  -      -      -        -    -        0      0
```

Fuente: Basado en investigación teórica y práctica

6.6. Implementación real del firewall Pfsense en la red del Tecnológico ITCA

La implementación del firewall se realiza con un nuevo direccionamiento es decir con las direcciones IP físicas reales en la red que se muestran en la tabla 6.

Tabla 6. Direccionamiento de la implementación firewall Pfsense

Red	Dirección IP	Mascara	gateway
Red WAN	186.3.X.X	255.255.255.0	186.3.X.X
Red DMZ	172.20.X.X	255.255.255.0	---------- ---
Red LAN	172.20.102.1	255.255.255.0	---------- ---

Fuente: Dirección de Sistemas Tecnológico ITCA

- Configuración de las interfaces del firewall Pfsense Real para la red LAN como se muestra en la imagen de la figura 7.

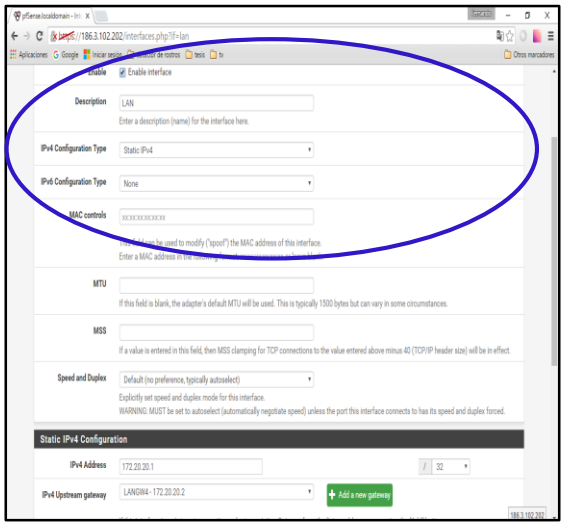

Figura 7. Configuración de interfaz LAN

Fuente: Pfsense versión 2.2.5

6.7 Sistema de prevención de intrusos (IPS).

El software de Pfsense incluye un paquete de instalación de un sistema de prevención de intrusos Snort. Se puede configurar para que simplemente registrar eventos y alertas de red detectados y/o bloquear las amenazas.

Este paquete está disponible para instalar desde System> Packages como se muestra en la figura 8.

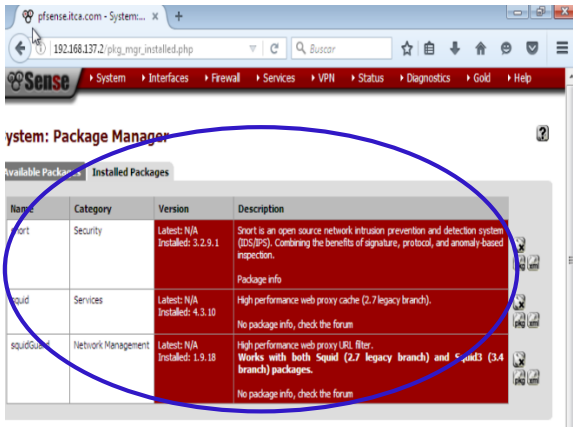

Figura 8 .instalación del software Snort

Fuente: Pfsense versión 2.2.5

Se crea automáticamente una lista de las direcciones IP que conforman el sistema Snort, se añaden las direcciones de red y subredes de la red LAN y DMZ como se muestra en la figura 9

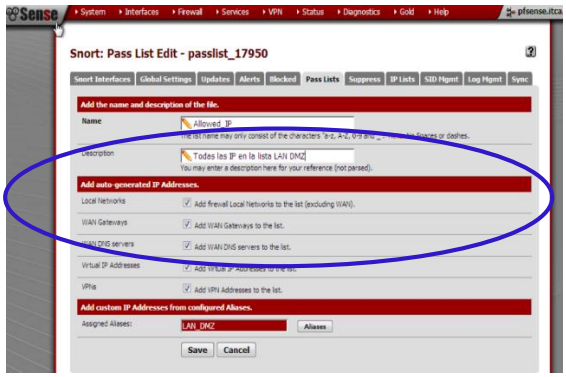

Figura 9. Creación de la lista de direcciones IP en Snort.

Fuente: Pfsense versión 2.2.5

7 Pruebas de verificación y funcionamiento del sistema de seguridad perimetral.

Se simularán varios ataques informáticos, para realizar las pruebas de funcionamiento y aplicabilidad los cuales demostrarán el correcto funcionamiento del sistema de Seguridad Perimetral.

7.1 Pruebas del servicio Squid

A continuación se realiza pruebas apegándose a las ciertas políticas de seguridad como por ejemplo la limitación, de la navegación a ciertas páginas.

7.2 acceso a internet a través de proxy Squid

La siguiente regla en, Squid permite el acceso a red de internet, la figura 10 muestra que el acceso a la red es exitoso para la página principal del navegador de Google Chrome.

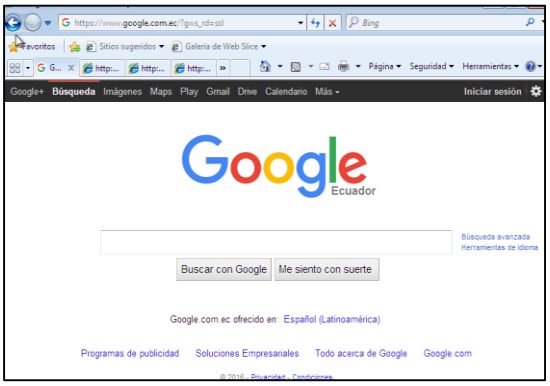

Figura 10 .acceso exitoso a Google

Fuente: Pfsense versión 2.2.5

7.2 Degación de las páginas de restringidas

Ya se había configurado anteriormente la restricción a las páginas de acceso a redes sociales, descargas y páginas pornográficas, las imágenes 11,12,13 y 14 muestran la negación de

acceso a estas páginas al tratar de abrir desde el navegador.

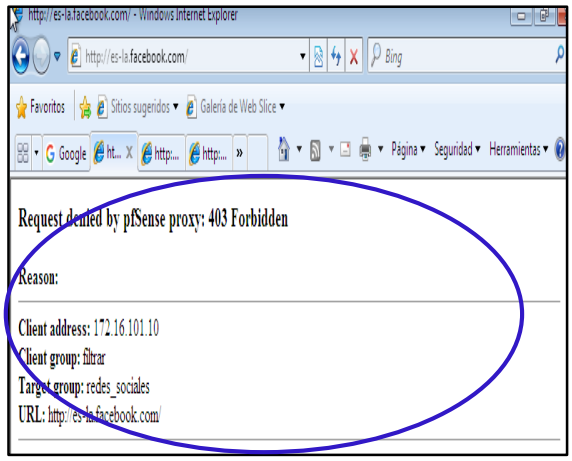

Figura 11. Restricción a la página de Facebook

Fuente: Pfsense versión 2.2.5

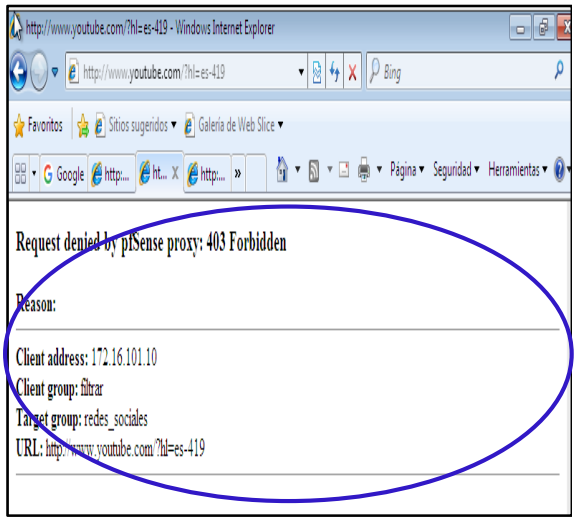

Figura 12 Restricción a la página de vide youtube

Fuente: Pfsense versión 2.2.5

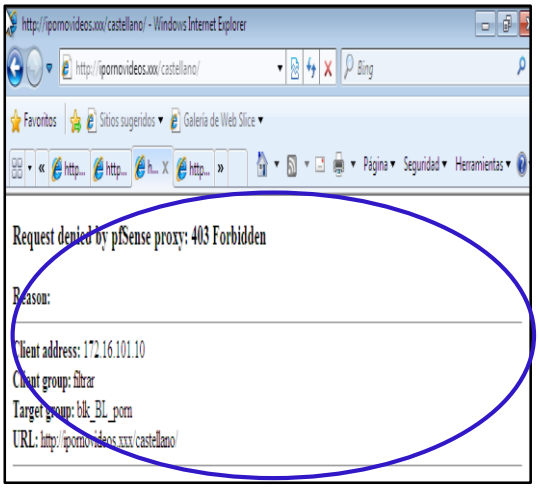

Figura 13. Restricción a la página pornografica

Fuente: Pfsense versión 2.2.5

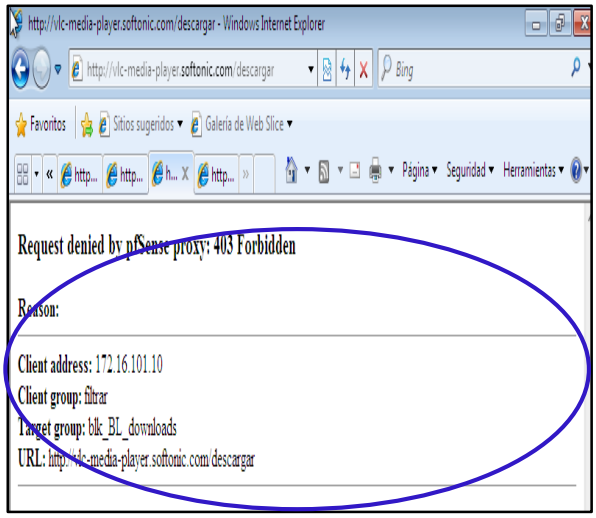

Figura 14. Restricción a la página de descargar softonic

Fuente: Pfsense versión 2.2.5

8 Conclusiones

Al culminar el proyecto de titulación se obtiene las siguientes conclusiones:

- La base teórica es de suma importancia para la realización del proyecto, se requiere la información suficiente sobre cuáles son las principales características de un Sistema de Seguridad Perimetral, de esta manera tener una idea clara de los procesos que se van a seguir para realizar un correcto diseño y finalmente la implementación del mismo de ser el caso requerido.

- El levantamiento de la información de la situación actual dela red del Tecnológico ITCA

Permite conocer a fondo toda la infraestructura existente tanto lógica como física, esta es una parte importante aquí se evidencia los activos de la red, permite verificar y dimensionar de la red y clasificar los activos que van a ser evaluados en el riesgo.

- En el estudio de la norma de evaluación del riesgo se utiliza la Guía del Instituto Nacional de Estándares y Tecnología NIST SP 800-30, con el fin de conocer los niveles actuales de seguridad de la información e identificar tanto amenazas y vulnerabilidades en la red de datos del Tecnológico ITCA, esta evaluación permite realizar un control del nivel del riesgo, y poder realizar el mejoramiento continuo de los sistemas.

- La gestión y evaluación de riesgos conlleva un esfuerzo adicional de los propietarios o administradores de la red ya que están definidos procesos específicos que deben seguirse en conjunto, y no es una actividad sencilla además los resultados se lo ven a largo plazo, por lo tanto se requiere de un alto compromiso de todo los involucrados dentro de la institución, para llevar a cabo la evaluación de riesgos y la implantación de controles.

- El estudio de la norma de evaluación del riesgo permite evidenciar las falencias de la red de datos del Tecnológico ITCA y permite verificar y concluir que no se ha implementado ningún sistema de seguridad perimetral, es una red plana es decir no está definido un modelo jerárquico. En cualquier momento la red puede ser blanco de un ataque informático esto puede ocasionar pérdida parcial o total de la información, costo económicos y más problemas que esta clase de ataques pueda desencadenar.

- Según las recomendaciones y conclusiones de la guía de evaluación del riesgo permite plantear el diseño del sistema de seguridad perimetral, para ello se divide la red en tres zonas específicas la red LAN, la red DMZ y la red WAN. Además de realizar la segmentación lógica de la red, esto permite separar a los usuarios por la naturaleza de servicios a los que necesitan acceder dentro de la institución.

- Se desarrolla la implementación del firewall Pfsense en la red Real del Tecnológico ITCA, donde se ha realizado configuración de los equipos necesarios en este caso el Swtich de core , además se realiza la segmentación lógica de la red, con la

creación de 16 Vlans que se ha clasificado de acuerdo a los requerimientos del administrador de red al mismo tiempo se realiza la configuración de proxy Squid para incrementar la rapidez de acceso a los servidores , y finalmente el Sistema de Prevención de Intrusos IPS en este caso Snort que en paquete incluido en el software Pfsense.

- En el presente trabajo de titulación se permitió unificar dos métodos de seguridad informática basados en software libre como son los Firewall y los IPS mediante Firewall Pfsense y Snort respectivamente, para el monitoreo y detección de ataques a la red de datos del tecnológico ITCA

- El desarrollo del análisis costo beneficio permite tener un precedente tanto de la infraestructura actual y de la necesaria tanto con su costo real para desarrollar el plan de puesta en marcha del sistema de seguridad perimetral para la red de datos del tecnológico ITCA

9 . Recomendaciones

Al culminar el proyecto de titulación se menciona las siguientes Recomendaciones:

- Para mejorar la estructura física y lógica de la red se recomienda realizar el modelo de red jerárquico contemplando el manejo de sus 3 capas: núcleo, distribución y acceso.

- En la actualidad las empresas o instituciones aún no tienen conciencia de la importancia de la implantación de una adecuada evaluación y gestión de los riesgos en los sistemas de información, la misma que va de la mano de una excelente toma de decisiones, se solicita tomar las medidas y acciones necesarias para llevar a cabo el plan de recuperación ante un ataque informático.

- En la infraestructura de red del Tecnológico ITCA, donde se evidencia que los equipos de red no poseen con la capacidad necesaria para dejar el sistema de seguridad perimetral en marcha puesto que al realizar aquello la red colapsaría y se recomienda como solución viable la adquisición del equipamiento necesario de Networking para la implementación del firewall de hardware.

- Es recomendable establecer un plan de contingencia ante los riesgos, se debe tener en cuenta la importancia de respaldar las bases de datos, configuraciones esenciales, información confidencial de los dispositivos y la capacidad de recuperase en el menor tiempo posible de un ataque.
- El diseño del firewall Pfsense así como todas las configuraciones necesarias son viables para cuando la institución desee continuar con el proceso de implementación total.

- Cabe mencionar que el uso de software libre en instituciones públicas o privadas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las redes de información, debido a que consume menos recursos de memoria, procesador y espacio en los equipos de red, permitiendo la reutilización de recursos y por ende disminución de gastos económicos que al utilizar un software propietario.

10. BIBLIOGRAFIA

Baltazar José, Campuzano Juan. (2011). *Diseño e Implemantación de un esquema de Seguridad Perimetral para redes de datos.* México, D.F: Universidad Autónoma de México.

educativo, P. (2014). *tiposde.org*. Obtenido de http://www.tiposde.org/informatica/131-tipos-de-servidores/

ITCA. (abril de 2015). *Instituti Tecnologico José Chiribiga Grijalva.* Obtenido de http://portalins.tecnologicoitca.edu.ec

MAYORGA, D. (2008). *ANALISIS,DISEÑO E IMPLEMTACIÓN DEL ESQUEMA DE SEGURIDAD PERIMETRAL PARA LA RED DE DATOS DE LA UISEK-ECUADOR (CAMPUS MIGUEL DE CERVANTES).* QUITO.

Microsoft Develoer network. (2005). MSDN Library. *Microsoft develoer network.*

MOLINA, E. (2012). *PROPUESTA DE SEGMENTACIÓN DE REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QoS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDA DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLATA NORTE.* Chiclayo.

Sanchez, J. (2012). *Instalación de un router/Appliance con funciones de firewall, VPN,potección de ataques,antiespam y antivirus perimetral con IpCop.* Colombia: Universidad de Caldas, Manizales, Colombia.

TORRES, R. J. (2014). *SEGURIDAD PERIMETRAL EN LA RED DE DISTRIBUCIÓN DE LA UNIVERSIDAD TECNICA DEL NORTE.* Ibarra.

ZAPATA. (s.f.).

Zapata, R. D. (2012). *Estudio de las técnicas de control de acceso a internet y su aplicación en la red de datos del colegio corina parral de la ciudad de Chimbo.* RIOBAMBA: Universidad Superior Politecnica de Chimborazo.

TESIS

Alulema Chiluisa, D. (2008). Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors, utilizando tecnología UTM (Unified Threat Management). (Tesis inédita de Ingeniería). Escuela Politécnica Nacional, Quito, ECU.

Astudillo Herrera, J & Jiménez Macías, A. & Ortiz Flores, F. (2011). Adaptación del IDS/IPS Suricata para que se pueda convertir en una solución empresarial. (Tesis inédita de Ingeniería). Escuela Superior Politécnica del Litoral, Guayaquil, ECU.

Vinueza Jaramillo, T. (2012). Honeynet virtual híbrida en el entorno de red de la Universidad Técnica del Norte de la ciudad de Ibarra. (Tesis inédita de Ingeniería). Disponible en el repositorio digital de la Universidad Técnica del Norte, Ibarra, ECU.

MICHILENA, M. A. (2013). METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN

DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO

AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA. Ibarra

LIBROS

PRESSMAN, S. Rogger; (2002). Ingeniería de Software. Quinta Edición. España.

Mc-GRAW-HILL/Interamericana de España

SOMMERVILLE, Ian; (2002). Ingeniería de Software. Sexta Edición. México.

Pearson Educación.

SOM, Cerezo Guillermo; (2002). Manual Imprescindible Visual Basic .NET.

Primera Edición. España. Anaya Multimedia S.A

BALENA, Francesco; (2003). Programación Avanzada con Microsoft VISUAL

BASIC .NET. Primera Edición. España. McGRAW-HILL/Interamericana de

España.

ROBINSON, Ed. James; BOND, Michael; (2003). Seguridad para Microsoft Visual

Basic .NET, Primera Edición. España. McGRAW-HILL/Interamericana de España.

BOTT, Ed. Siechert; (2003). Seguridad en Microsoft Windows XP. Primera

Edición. España. McGRAW-HILL/Interamericana de España.

GRATTON, Pierre; (1998). Protección Informática. Primera Edición. México.

Editorial Trillas, S.A de C.V.

GROFF, James R; WEINBERG, Paul N; (1991). Aplique SQL. Primera Edición.

México. McGRAW-HILL/Interamericana de México.