ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"DISEÑO DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED DE LA UNIVERSIDAD SAN GREGORIO DE PORTOVIEJO"

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL GRADO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MILTON ALBERTO BALDA MACÍAS

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a mi familia por el apoyo que siempre me han concedido en cada desafío que he afrontado a nivel profesional y personal.

A los profesores y profesoras del MSIA que compartieron todo sus conocimientos y habilidades en el área de la seguridad informática.

A mis compañeros de clases del MSIA que trabajaron con entrega en la elaboración de los proyectos.

A la Universidad San Gregorio de Portoviejo por el apoyo brindado para realizar la maestría.

DEDICATORIA

El presente trabajo está dedicado ante todo a DIOS y a mis padres, quienes han sido el pilar fundamental de mi vida.

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenin Freire

DIRECTOR DEL MSIA

_____

Mgs. Nestor Arreaga

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

_____

Mgs. Robert Andrade

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

La seguridad en la actualidad es una parte fundamental en las empresas o instituciones existentes en nuestro país y el mundo. Las empresas deben salvaguardar la información, por este motivo el presente trabajo plantea una mejora en la seguridad de la infraestructura de red de la Universidad San Gregorio de Portoviejo, ya que en dicha institución se procesa información valiosa. Teniendo en cuenta el gran número de estudiantes que asistente a la institución y así mismo los empleados que laboran en ella, es indispensable que la institución cuente con sistemas de seguridad para evitar cualquier percance o daño que pueda suceder.

Para la realización del presente trabajo se realiza un análisis del estado actual de la infraestructura de red de la institución y una vez realizado lo anterior, se realiza el diseño de la seguridad de la infraestructura de red de la institución.

Todos estos análisis y diseño contribuirán en las mejoras de seguridad para la institución, para que en un futuro la institución esté preparada en el caso de sufrir un ataque de hacking o daños por software malicioso.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

BROADCAST	Transmisión de datos recibida por todos los dispositivos de la red.
DAN	Departamento de Admisión y Nivelación.
DHCP	Servidor de direcciones IP dinámicas.
DMZ	Zona desmilitarizada.
FIREWALL	Cortafuego diseñado para impedir el acceso no autorizado.
HARDENING	Proceso para la reducción de riesgo de seguridad.
IP	Protocolo de Internet.
IPTABLES	Herramienta de cortafuegos.
IDS	Sistema de detección de intrusos.
MOODLE	Software para aula virtual.
NIDS	Sistema de detección de intrusos basado en la red.
ROUTET	Enrutador de paquetes de red.
USGP	Universidad San Gregorio de Portoviejo.
VLAN	Red de área local virtual.
WAP2-PERSONAL	Sistema de seguridad de red inalámbrica.
WIFI	Punto de acceso de red inalámbrico.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En este documento se describe el análisis y diseño de la seguridad de la infraestructura de red de la Universidad San Gregorio de Portoviejo.

Se realiza el análisis del problema que contempla la infraestructura de red de la universidad y se da la justificación para dar solución al mismo.

Posteriormente se recaba la información para analizar el estado actual de la infraestructura de red de la universidad y se plantea las medidas de seguridad que se deben implementar para mejorar la seguridad de la infraestructura de red de la universidad.

Finalmente se describe los beneficios que la institución adquiere en el momento que implemente las medidas de seguridad planteadas para que la institución esté preparada en el caso de sufrir un percance de seguridad.

CAPÍTULO 1

GENERALIDADES

La tendencia, cada vez más dominante, hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones, e incluso, de las empresas, ha situado a la seguridad de los sistemas de información como un elemento en todo el desarrollo de la sociedad. [1]

Por tal motivo las empresas en la actualidad deben de tener en gran consideración que la seguridad en la infraestructura de red es primordial para que las operaciones que se llevan a diario sean ejecutadas con seguridad.

1.1. DESCRIPCIÓN DEL PROBLEMA

La Universidad San Gregorio de Portoviejo es una Institución de Educación Superior creada el 14 de diciembre del 2000, mediante Decreto Legislativo # 200-33.

La USGP ha tenido un crecimiento paulatino de la infraestructura de red debido al incremento de departamentos y oficinas en los diferentes edificios de la universidad. Dicho incremento ha provocado que la infraestructura de red haya sido creada de forma descontrolada para cubrir las áreas que necesitan soluciones de la misma para distribuir en los diferentes departamentos el servicio de Internet, telefonía IP, los sistemas informáticos para el control de docentes y matriculación de los estudiantes.

La infraestructura de red no cuenta con una correcta configuración de software y hardware adecuados para afrontar cualquier tipo de intromisión maliciosa, ya que no cuenta con áreas desmilitarizadas, cortafuegos, sistemas de detección de intrusos, grupo de trabajo, asignación correcta de IP dinámicas o estáticas.

La no existencia de un área adecuada para infraestructura de servidores, esto ha causado que los servidores que se encuentra dispersos en los diferentes edificios o departamentos del campus universitario. Los

servidores proveen el servicio de Intenet, proxy, web, base de datos, repositorios de tesis y bibliotecario, etc.

El acceso a la Internet por medio de redes Wifi es un servicio que se brinda a la comunidad universitaria pero dichas redes Wifi se encuentran sin protección de claves y en ciertos casos están protegidas con claves de seguridad WAP2-Personal.

A pesar del crecimiento de la infraestructura de red que ha surgido en la USGP, no se ha considerado el riesgo que esto conlleva si no se tiene en cuenta la seguridad de dicha infraestructura. Por tal motivo se realiza el presente diseño para dar solución a las falencias de la seguridad en la infraestructura de red de la USGP.

1.2. SOLUCIÓN PROPUESTA

En la actualidad las redes informáticas son parte fundamental de las instituciones, ya que ellas nos proveen de los diferentes servicios necesarios para poder comunicarnos de forma interna y externa a la organización. Una parte fundamental para que las comunicaciones funcionen de forma adecuada, sin temor a que la organización sea expuesta a algún fallo es la seguridad en su infraestructura de red. La

infraestructura de red es la que se encuentra expuesta directamente a las interconexiones internas y externas de la organización.

Es necesario diseñar la seguridad de la infraestructura de red para determinar los puntos críticos en los que se debe brindar protección y seguridad. Dicha protección y seguridad debe permitir que los beneficiados con los diferentes servicios que brinda la universidad puedan realizar sus tareas de forma segura.

Una vez determinado los diferentes puntos críticos de la infraestructura de red se debe diseñar el diagrama de seguridad de la red ubicando el hardware o software necesario para brindar seguridad en las áreas vulnerables de la infraestructura de red, determinando la zona desmilitarizada, grupos de trabajos, asignación de direcciones IP tanto estáticas como dinámicas, asignación correcta de cortafuegos y sistemas de detección de intrusos. Esto permitirá mejorar la seguridad donde se encuentra inmerso los diferentes servicios de Internet, proxy, web, base de datos, repositorios de tesis y bibliotecarios, telefonía IP, etc.

Se debe determinar un área donde se encuentren alojados los diferentes servidores que se encuentran dispersos en la universidad, realizando un adecuado diseño organizado de la seguridad de la infraestructura de red.

Se debe determinar los mecanismos de seguridad adecuados para las diferentes zonas Wifi que existen en el campus universitario.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ALCANCE

El presente trabajo se desarrolla en el estudio de la seguridad de la infraestructura de red de la Universidad San Gregorio de Portoviejo y se divide en dos fases, la primera es el análisis del estado actual de la infraestructura de red de acuerdo a su seguridad y la segunda fase se desarrollara el diseño de seguridad de la infraestructura de red en base a los datos obtenidos del análisis de la red.

2.2. ORGANIZACIÓN

La Universidad San Gregorio de Portoviejo basa su existencia en la acción planificada y conjunta con estudiantes, catedráticos, empleados, trabajadores, autoridades y fundamentalmente con el apoyo decidido de

la comunidad manabita que ve en ella el propósito de brindar profesionales altamente capacitados y con criterio humanista acorde a las exigentes y avanzadas normas académicas de la educación superior actual. [2]

Misión

Somos una universidad innovadora que contribuye al desarrollo de la sociedad, a través de la generación de conocimientos y la formación de profesionales competentes; comprometida con la investigación, la ciencia, la tecnología, la cultura y los valores.

Visión

Universidad líder en la excelencia académica, la investigación y la innovación; promotora del desarrollo, la cultura, la identidad y el pensamiento; sustentada en el humanismo, la solidez institucional, los valores y la vinculación con la colectividad.

La Universidad San Gregorio de Portoviejo tiene una población de 200 profesores y personal administrativo, y 2300 estudiantes.

La Universidad San Gregorio de Portoviejo se encuentra conformada por 4 edificios, distribuidos de la siguiente forma:

- Edificio Administrativo
- Edificio #1

- Edificio #2
- Edificio #3

Edificio Administrativo

El Edificio Administrativo es el edificio principal de la universidad donde se encuentra asignada un área para los servidores y salida hacia la Internet. En dicho edificio encontramos los departamentos de rectora, vicerrectorado, financiero, policlínico, admisión y nivelación, bienestar universitario, dirección general académica, evaluación institucional, talento humano, jurídico, biblioteca general y digital.

Edificio #1

En el edificio #1 se encuentra un servidor para la distribución del servicio de Internet en los diferentes puntos de trabajo. En este edificio funcionan las carreras de Odontología, Derecho y Finanzas.

Edificio #2

En el Edificio #2 se distribuye el Internet con a través del servidor que se encuentra en el edificio #1. En este edificio laboran las carreras de Auditoria y Contabilidad, Gestión Empresarial, Marketing, Arquitectura y Diseño Gráfico.

Edificio #3

En el edificio #3 se encuentra un servidor para la distribución del Internet en el edificio y en el laboran las carreras de Educación Inicial, Ciencias de la Computación y Ciencias de la Comunicación.

En la siguiente figura podemos apreciar los diferentes edificios de la Universidad San Gregorio de Portoviejo.

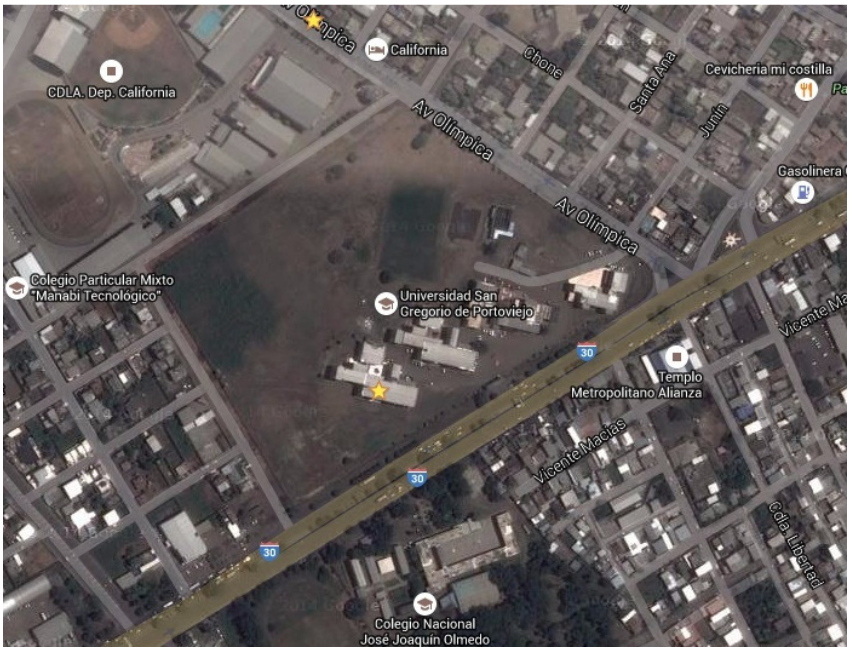

Figura 2.1. Vista satelital de la USGP a través de Google Map.

Estructura de la organización

El organigrama estructural de la organización lo podemos apreciar en la siguiente figura.

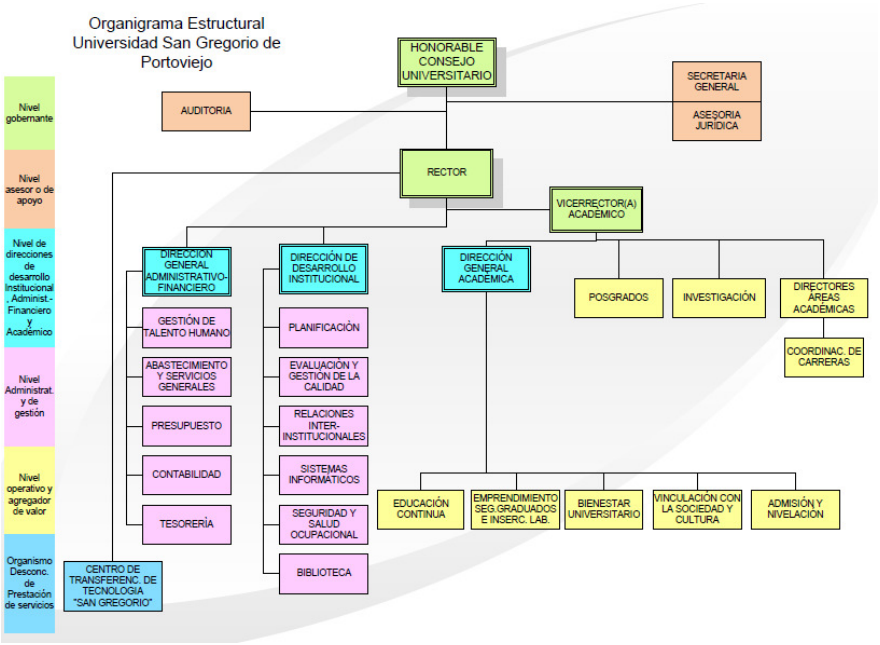

Figura 2.2. Estructura organizacional de la USGP [7]

En la figura 2.2 se puede apreciar que el departamento de Sistemas Informáticos se encuentra en conexión directa con el departamento de Dirección de Desarrollo Institucional.

El departamento de Sistemas Informáticos es el encargado de administrar la infraestructura de red, servidores, telefonía IP y dar soporte técnicos a los diferentes puestos de trabajos.

Debido a que dicho departamento no cuenta con especialistas en seguridad, por tal motivo, la infraestructura de red cuando se diseñó no se consideró las seguridades necesarias que ella debe tener para evitar acontecimiento negativos que puedan afectar a la universidad.

2.3. ESTADO ACTUAL DE LA INFRAESTRUCTURA DE RED DE LA ORGANIZACIÓN

Para conocer el estado actual de la infraestructura de red se analizó la red física, lógica y servidores, obteniendo como resultado el diagrama de actual de la infraestructura de red de la universidad.

2.3.1. RED FÍSICA

La red física de la USGP está distribuida en 4 edificios los cuales se interconectan por fibra óptica. Para conocer dicha red vamos a detallar por cada edificio los puntos de red, switch, router y tipo de cableado.

Puntos de Red

En el Edificio Administrativo encontramos diversos departamentos en el cual existen diferentes puntos de red que se talla a continuación:

Tabla 1. Puntos de red del Edificio Administrativo.

DEPARTAMENTO DEL EDIFICIO ADMINISTRATIVO	PUNTOS DE RED
Rectorado	1
Vice rectorado	1
Secretaria de rectorado	7
Financiero	9
Departamento de Admisión y Nivelación	4
Bienestar Universitario y Policlínico	5
Vinculación con la Sociedad	1
Jurídico	2
Planificación Institucional	2
Dirección General Académica	2
Evaluación Institucional	4
Talento Humano	3
Centro de Transferencia de Tecnología	15
Biblioteca General	20
Biblioteca Virtual	6
Bunker de servidores	3

Total	**81**

Puntos de red del Edificio #1

Tabla 2. Puntos de red del Edificio #1.

DEPARTAMENTO DEL EDIFICIO #1	**PUNTOS DE RED**
Oficinas de las carreras	15
Aulas de estudiantes	35
Laboratorio de informática #1	25
Laboratorio de informática #2	25
Laboratorio de informática #3	25
Sala de profesores	15
Bunker	4
Total	**141**

Puntos de red del Edificio #2

Tabla 3. Puntos de red de Edificio #2.

DEPARTAMENTO DEL EDIFICIO #2	**PUNTOS DE RED**
Oficinas de las carreras	15
Aulas de estudiantes	35
Sala de Profesores	15

Bunker	4
Total	**69**

Puntos de red del Edificio #3

Tabla 4. Puntos de red del Edificio #3.

DEPARTAMENTO DEL EDIFICIO #3	**PUNTOS DE RED**
Oficinas de las carreras	12
Aulas de estudiantes	35
Laboratorio de informática #1	25
Laboratorio de informática #2	25
Laboratorio de informática #3	20
Laboratorio de informática #4	20
Laboratorio de informática #5	13
Sala de profesores	15
Bunker	4
Total	**169**

En total podemos contabilizar que en la universidad existen 460 puntos de red.

Teléfonos IP

En la universidad se encuentran distribuido en los diferentes departamentos y puestos de secretarias los teléfonos IP modelos Yealink Sip T20 en un total de 50 puntos, distribuidos de la siguiente forma:

Tabla 5. Distribución de teléfonos IP por edificio

LUGAR	**# Teléfonos IP**
Edificio Administrativo	22
Edificio #1	7
Edificio #2	13
Edificio #3	8
Total	**50**

Switch

En la universidad existen diferentes switch distribuidos en los edificios, pero, solo existe dos switch administrable Cisco SG300-28 Gigabit de 24 puertos, que se encuentra en el bunker de servidores. En la siguiente tabla se detalla los switch:

Tabla 6. Número de switch distribuido en los diferentes edificios.

LUGAR	# Switch
Bunker de servidores	2
Edificio Administrativo	3
Edificio #1	6
Edificio #2	8
Edificio #3	8
Total	**27**

Router

La universidad cuenta con un router Cisco 1905 que es el que permite la comunicación hacia el internet. Dicho router es de la empresa proveedora de internet.

Router Inalámbrico

En la universidad existen router inalámbricos para proporcionar conectividad a los diferentes equipos que se conectan por este medio. Existe en cada edificio zonas Wifi para que los estudiantes se puedan conectar a la red. La seguridad de autentificación en los router es WAP2-Personal. [3]

En la siguiente tabla podemos apreciar la distribución de los router inalámbricos.

Tabla 7. Número de router inalámbricos distribuidos en los diferentes edificios.

LUGAR	**# Router Inalambricos**
Edificio Administrativo	6
Edificio #1	4
Edificio #2	4
Edificio #3	4
Total	**18**

Cableado

En la USGP el cableado que se ha utilizado para realizar la conexión principal entre edificios es de fibra óptica multimodo y la conexión interna para los diferentes puntos de red el cableado es UTP de categoría 6.

Computadores

En la universidad existen alrededor de 445 computadoras distribuidas en los diferentes puestos de trabajos, aulas de clases

y laboratorios, dichas computadoras trabajan con el sistema operativo Microsoft Windows 7 Profesional.

Las computadoras no cuentan con antivirus licenciado, ya que trabajan con versiones gratuitas y que no son tan eficaces al momento de detectar archivos que contengan software malicioso.

2.3.2 RED LÓGICA

En la USGP existen tres redes lógica que son la red administrativa, estudiante y telefonía IP. Dichas redes están distribuidas por 3 servidores que proveen el servicio DHCP a todos los edificios de la universidad y un servidor Asterisk para la distribución de la telefonía IP. Existen nueve IP Publicas para los diferentes servicios que proveen los servidores de la universidad. En la siguiente tabla se detalla la red lógica y sus IP:

Tabla 8. Distribución de IP de acuerdo a la red lógica.

Red Lógica	IP
Administrativa	128.121.61.0/24
Estudiante	192.168.50.0/24 192.168.51.0/24
Telefonía IP	192.168.1.0/24

IP Publicas	186.42.197.150 186.42.197.151 186.42.197.152 186.42.197.153 186.42.197.154 186.42.197.155 186.42.197.156 186.42.197.157 186.42.197.158

En la siguiente tabla se describen las características de los servidores.

Tabla 9. Distribución del servicio DHCP a los diferentes edificios.

Servidor	**Distribución**
Servidor 1 – DHCP (bunker servidores)	Provee el servicio DHCP para los edificios administrativo, edificio #2 y edificio #3
Servidor 2 – DHCP (bunker edificio 1)	Provee el servicio DHCP para el edificio #1

Servidor 3 – DHCP (bunker edificio 3)	Provee el servicio DHCP para los laboratorios de informática del edificio #3

Estas son las únicas redes lógicas que existen en la USGP, ya que no existen los grupos de trabajos y autentificación por servidor radius para las zonas wifi.

2.3.3. INFRAESTRUCTURA DE SERVIDORES

En la USGP existen diferentes servidores para dar servicios de base de datos, web, aula virtual, sistemas informáticos de pago del personal, matriculación y notas del estudiante.

Tabla 10. Descripción de servidores

Servidor	Función	Hardware	Ubicación
Base de datos. Sap SyBase - 1	El servidor provee el servicio de base de datos para la aplicación de matriculación	Servidor Hp Proliant DL380G5, Intel Xeon S5000 3Ghz,	Bunker de servidores, edificio administrativo

	y notas de los estudiantes	4GB de ram y 2x72GB disco duro SCSI	
Base de datos. Sap SyBase - 2	El servidor provee el servicio de base de datos para el sistema de pago de docente y empleados.	Servidor Hp Proliant DL320e gen8 v2, Intel Xeon 3.2Ghz, 4GB de ram y 500GB disco duro SATA	Bunker de servidores, edificio administrativo
Proxy y DHCP - 1	Servidor que distribuye ip dinámicas para el edificio	Desktop Intel Core I3, 4GB de ram y 1 TB	Bunker de servidores, edificio administrativo

	administrativo, edificio #2 y #3.	de disco duro	
Proxy y DHCP - 2	Servidor encargado para la distribución del servicio de Internet con IP dinámicas.	Desktop Intel Core I3, 4GB de ram y 1 TB de disco duro	Bunker edificio #1
Proxy y DHCP - 3	Servidor encargado para la distribución del servicio de Internet con IP dinámicas.	Desktop Intel Core I3, 4GB de ram y 1 TB de disco duro	Bunker edificio #3
Servidor Web y aula vitual - DAN	Servidor Web donde se encuentra	Desktop Intel Core I5, 8GB de	Departamento de Admisión y

	alojada página del DAN y el sistema de aula virtual basado en Moodle	ram y 2 TB de disco duro	Nivelación – Edificio Administrativo
Servidor del Sistema Bibliotecario	Servidor Web donde se encuentra alojada la aplicación bibliotecaria.	Servidor HP Prollant ML310E Gen 8 V2 Intel Xeon 3.1 Ghz, 8GB de ram y 1 TB de disco duro SATA	Biblioteca General – Edificio Administrativo
Servidor de telefonía IP	Servidor que distribuye el servicio de	Servidor Xorcom XE3056	Bunker de servidores.

	telefonía IP en la universidad.	es una PBX basada en Asterisk con cuatros puertos PRI, parta la telefonía IP.	

2.3.4. DIAGRAMA ACTUAL DE LA INFRAESTRUCTURA DE RED

En el presente subcapítulo se podrá apreciar el diagrama de red de cada edificio de la universidad y un diagrama general.

El primer diagrama que se visualizara es del edificio administrativo podemos observar la conexión a Internet, el área de servidores y la distribución de la red en los diferentes pisos del edificio.

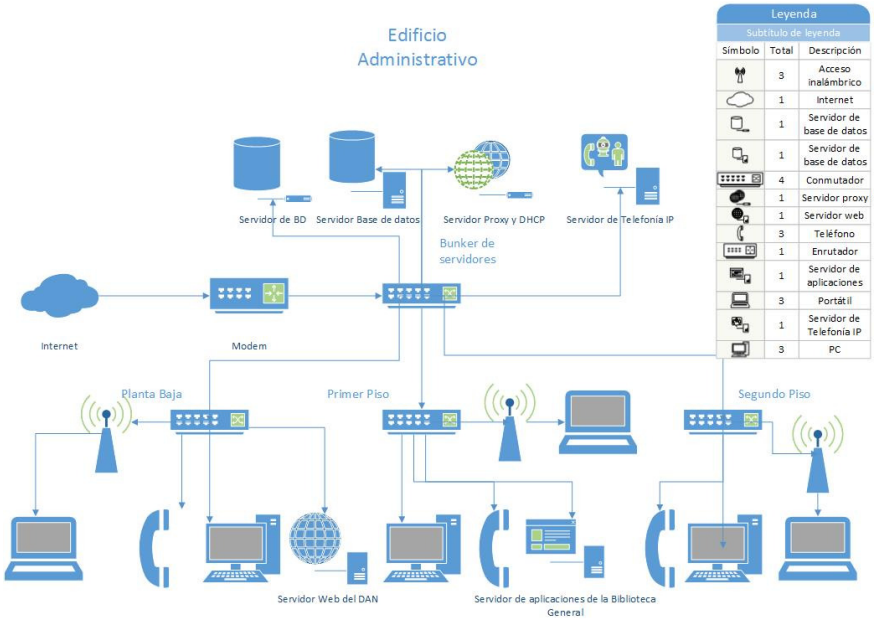

Figura 2.3. Diagrama de red del edificio administrativo.

En el siguiente diagrama podemos apreciar la distribución de la red en el edificio #1

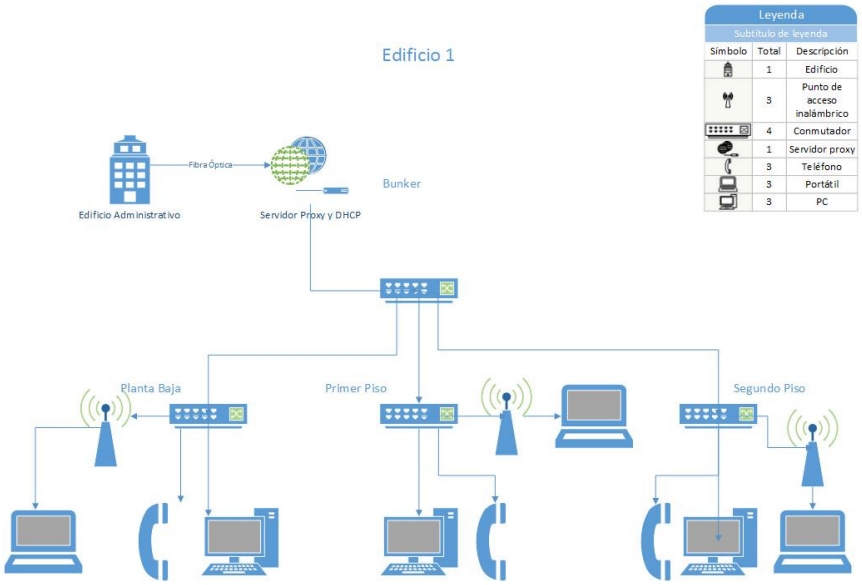

Figura 2.4. Diagrama de red del edificio #1

En el siguiente diagrama podemos apreciar la distribución de la red en el edificio #2

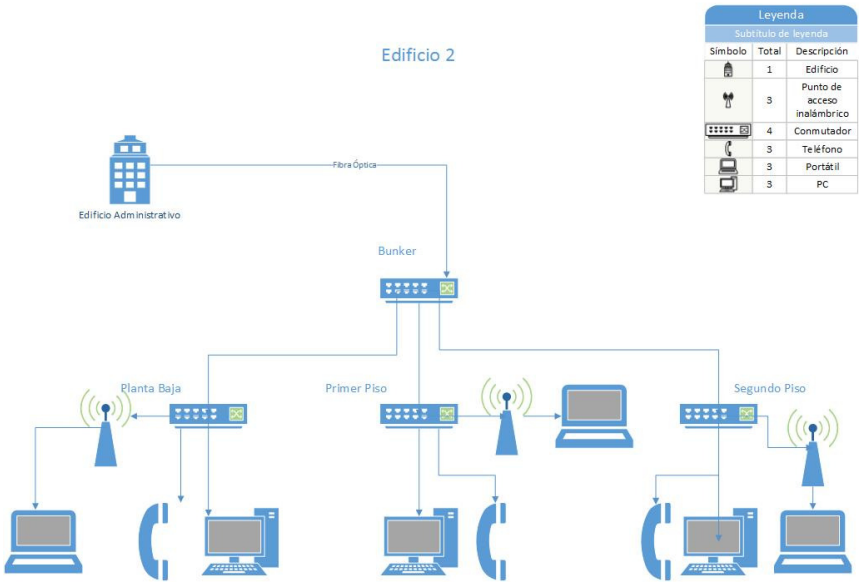

Figura 2.5. Diagrama de red del edificio #2

En el siguiente diagrama podemos apreciar la distribución de la red en el edificio #3.

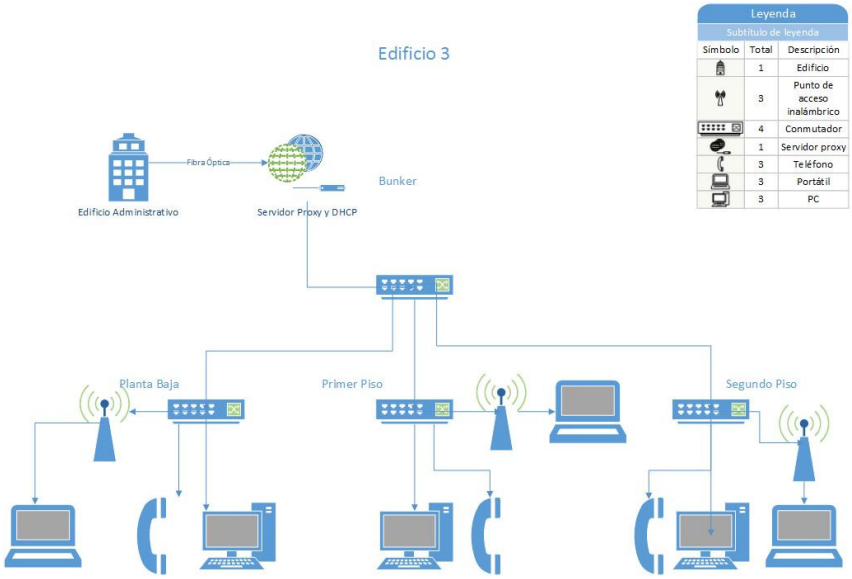

Figura 2.6. Diagrama de red del edificio #3.

El siguiente diagrama es una vista general de la infraestructura de red de la USGP, donde se aprecia el área de servidores y la distribución de la red hacia los diferentes edificios.

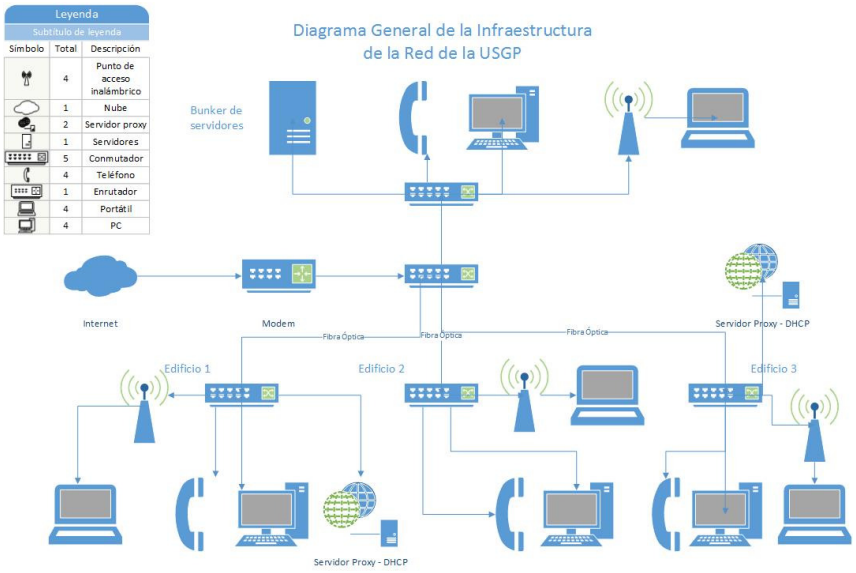

Figura 2.7. Diagrama general de la infraestructura de red de la USGP.

2.3.5. IDENTIFICACIÓN DE VULNERABILIDADES

Una vez realizado el análisis de la red lógica, red física e infraestructura de servidores; se tiene como resultado algunos puntos clave en donde se debe mejorar la seguridad de la red.

Los puntos vulnerables que se han encontrado por su carencia en la infraestructura de red, son:

- Firewall
- NIDS
- Vlans
- DMZ
- Servidor radius
- Antivirus licenciado

En el siguiente capítulo se analizarán los puntos anteriormente citados.

2.4. DISEÑO DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED DE LA ORGANIZACIÓN

En este capítulo se analiza los puntos clave para la seguridad de la infraestructura de red de la USGP.

2.4.1. DISEÑO DE SEGURIDAD DE LA RED FÍSICA

El tener acceso físico a la red es el mayor logro del hacker. Con acceso físico y suficiente tiempo, se puede lograr lo que sea en cuestión de extracción y modificación de datos. [4]

Por lo anteriormente mencionado la infraestructura de red debe contar con:

- Firewall
- NIDS
- Router

- Switch

Ahora analizaremos cada uno de ellos.

Firewall

Medio eficaz de protección de un sistema local o de red de los sistemas de las amenazas de seguridad basadas en la red, mientras que ofrezcan acceso al mundo exterior a través de WAN`s o Internet. [5] En la red de la USGP se debe implementar un firewall.

NIDS

El NIDS analiza el tráfico de red en tiempo real para evitar ataques de red que sean un riesgo potencial para la organización. En la red de la USGP se debe implementar 3 NIDS.

Router

Dispositivo de capa 3 que permite el encaminamiento de paquetes de la red. En la red de la USGP se debe implementar un router para la distribución de la red en los diferentes edificios.

Switch

Equipo que permite el intercambio de segmentos de la red y trabaja de acuerdo con la dirección MAC del host de destino. En la red de la USGP se debe implementar 18 switch administrables.

2.4.2. DISEÑO DE SEGURIDAD DE LA RED LÓGICA

En esta parte se analiza las vulnerabilidades desde el punto de vista lógico.

VLan

La implementación de VLan en los switches limita el libre tránsito de un hacker si penetra la red. Las Vlan reducen significativamente el dominio del broacast de paquetes, por lo que el hacker solamente puede ver los paquetes que fluyen dentro de la VLan donde se encuentra, reduciendo así el riesgo de que detecte otras IPs vulnerables. [4]

En la USGP se debe implementar la Vlan para tener un mejor control y distribución de la red virtuales, para atenuar algún suceso de seguridad que pueda suscitarse.

DMZ

Todos los servicios de correo, web, ftp, proxy, VoIP, o cualquier otro servidor que tenga un IP pública, debe estar en la red perimetral, también conocida como la DMZ.

Servidor Radius

En la universidad el acceso de red a través de wifi se lo realiza sin mayor control, ya que no existe autentificación de usuario. Por tal motivo es necesario la implementación de autentificación a través de un servidor Radius.

Antivirus

Los antivirus tiene como fin neutralizar las amenazas que intentan acceder a los privilegios de nuestro computadores, por dicho motivo se debe utilizar antivirus de software licenciados ya que hay una mayor actualización diaria en estos tipos de antivirus.

2.4.3. INFRAESTRUCTURA DE SERVIDORES

En esta parte se determinan las mejoras de seguridad que se debe implementar en el área de servidores.

Proxy

Se debe tener la implementación de un servidor proxy par tener un mayor control de acceso cuando una PC realiza peticiones a otras PC.

DHCP

El servidor DHCP nos permite la asignación automática y dinámica de IPs, pero para un mayor control se debe determinar las IPs que se van a asignar en cada PC.

IPTables

Las reglas de Iptables son fundamentales para la configuración de un cortafuego a nivel de software, ya que ellas permiten determinar los puertos de entrada y salida que deben estar abiertos o cerrados, y el redireccionamiento de los paquetes de la red de acuerdo a las solitudes que en ella surgen.

Servidor de Base de Datos

Los servidores de base de datos que son parte fundamental de la institución ya que en ellos reposa información valiosa deben estar dentro de una zona desmilitarizada para su mayor seguridad.

Servidor Web

Los servidores web que son los que normalmente tienen acceso directo a la Internet por el uso de IP públicas, ellos deben tener una buena configuración aplicando hardening para evitar cualquier intromisión no deseada. [6]

Servidor de Telefonía IP

El servidor de telefonía IP nos permite la comunicación internet, por lo tanto se debe tener en consideración dentro de la DMZ para mayor seguridad.

2.4.4. DIAGRAMA DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED

En esta parte se explica los diagramas de seguridad de la infraestructura de red para la USGP y se conocerán las mejoras que se deben realizar.

En el edificio administrativo que es donde se encuentra el bunker o área de servidores es donde se realizará las configuraciones más importantes para la seguridad de red. En el siguiente grafico podemos apreciar que se debe implementar NIDS, DMZ, firewall y switch administrables.

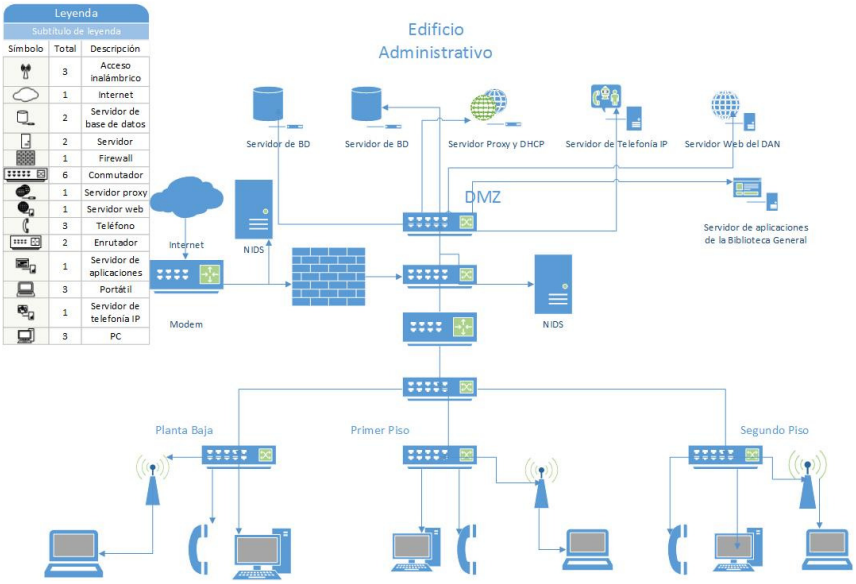

Figura 2.8. Diagrama de seguridad de red del edificio administrativo.

El siguiente diagrama de seguridad de red que podemos analizar es del edificio #1. En este diagrama podemos apreciar la utilización de switch administrables para la configuración de Vlan.

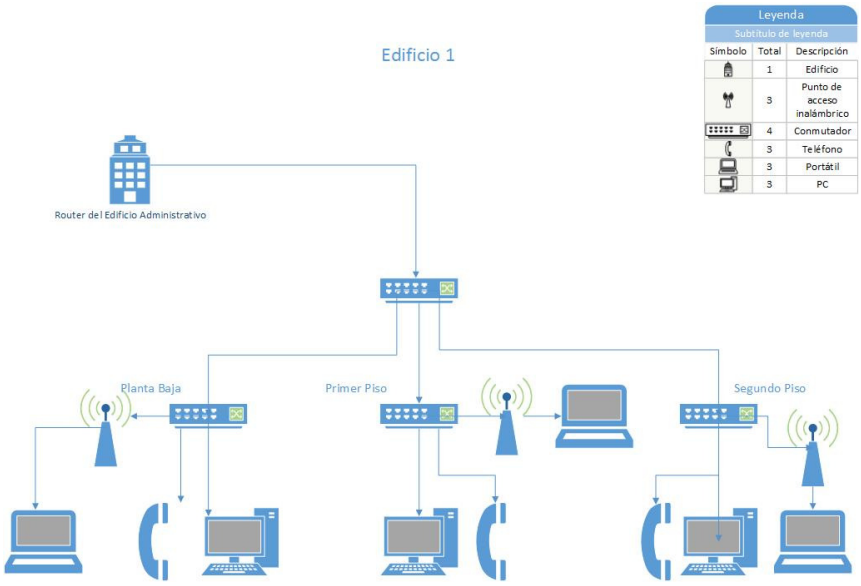

Figura 2.9. Diagrama de seguridad de la infraestructura de red del edificio #1

El siguiente diagrama de seguridad de red que podemos analizar es del edificio #2. En este diagrama podemos apreciar la utilización de switch administrables para la configuración de Vlan.

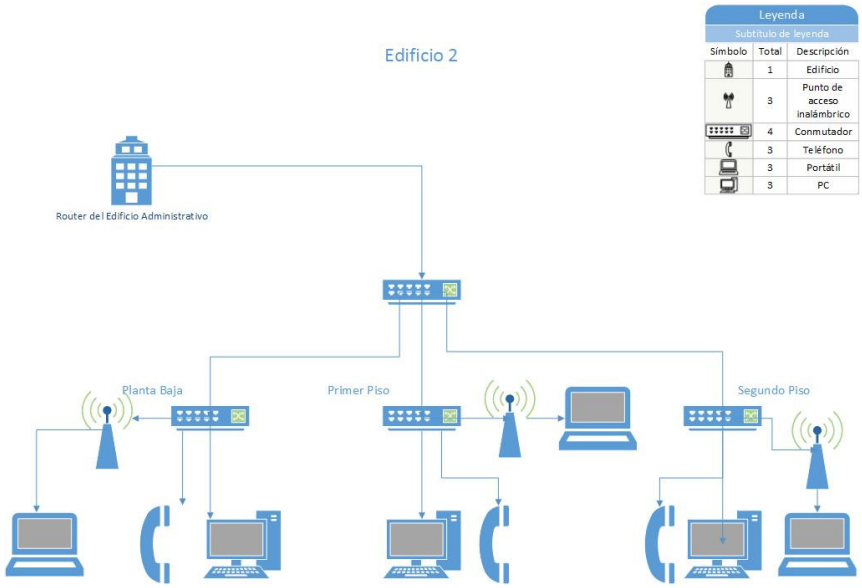

Figura 2.10. Diagrama de seguridad de la infraestructura de red del edifcio #2

El siguiente diagrama de seguridad de red que podemos analizar es del edificio #3. En este diagrama podemos apreciar la utilización de switch administrables para la configuración de Vlan.

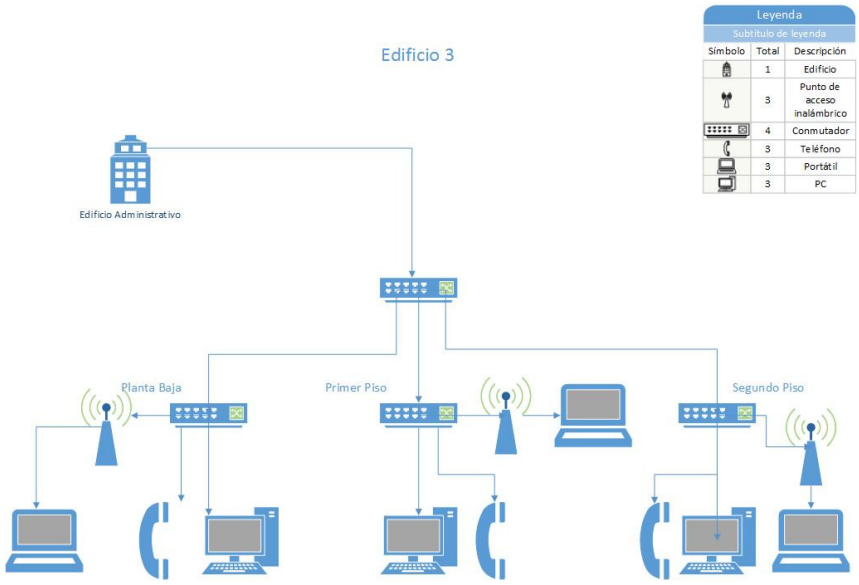

Figura 2.11. Diagrama de seguridad de la infraestructura de red del edificio #3.

El siguiente diagrama de seguridad de red analizaremos la configuración de Vlan para cada edificio de la USGP. En el diagrama podemos apreciar la utilización de 4 switch administrables y la creación de 5 Vlan para la virtualización de la red.

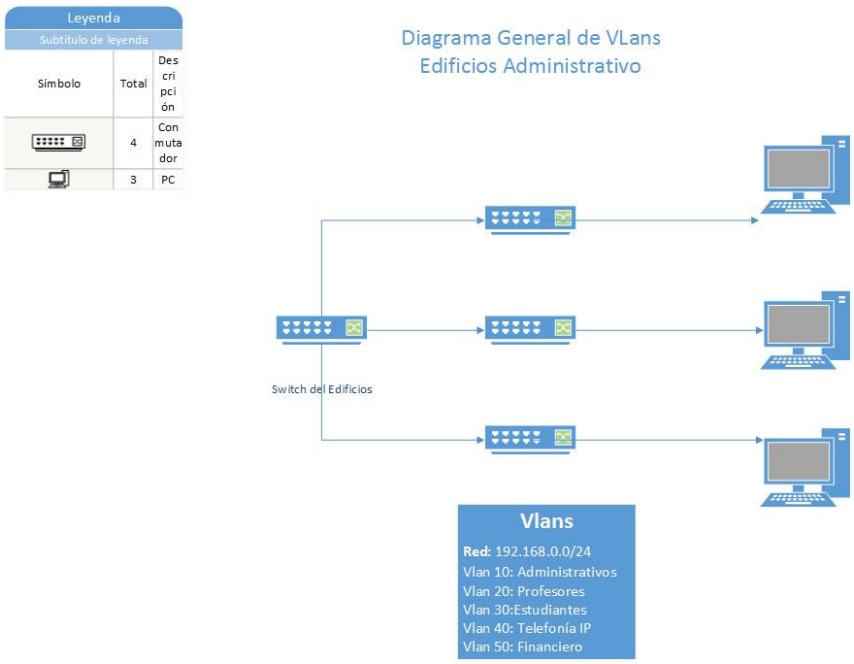

Figura 2.12. Diagrama de Vlan del edificio administrativo.

En el diagrama podemos apreciar la utilización de 4 switch administrables y la creación de 5 Vlan para la virtualización de la red del edificio #1.

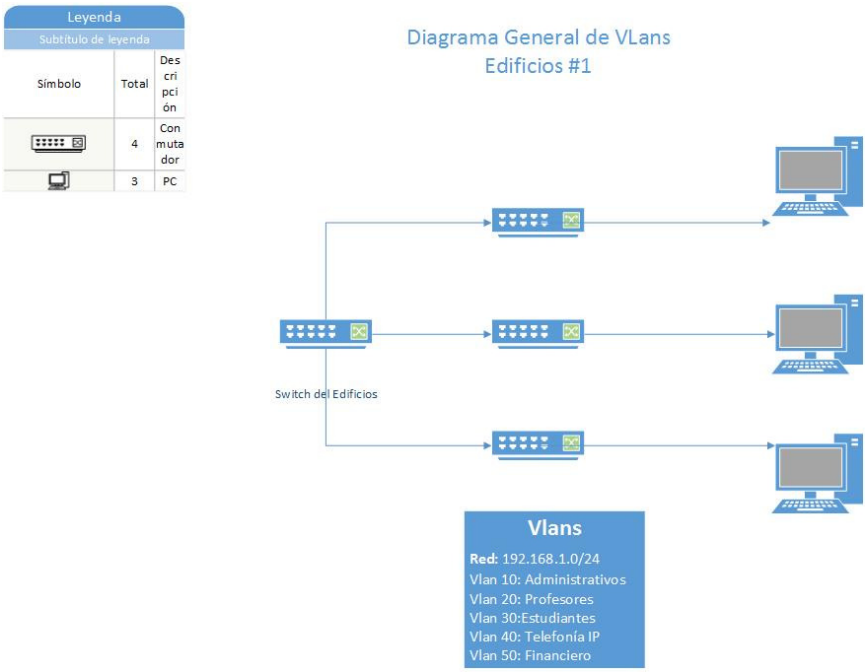

Figura 2.13. Diagrama de Vlan del edificio #1.

En el diagrama podemos apreciar la utilización de 4 switch administrables y la creación de 5 Vlan para la virtualización de la red del edificio #2.

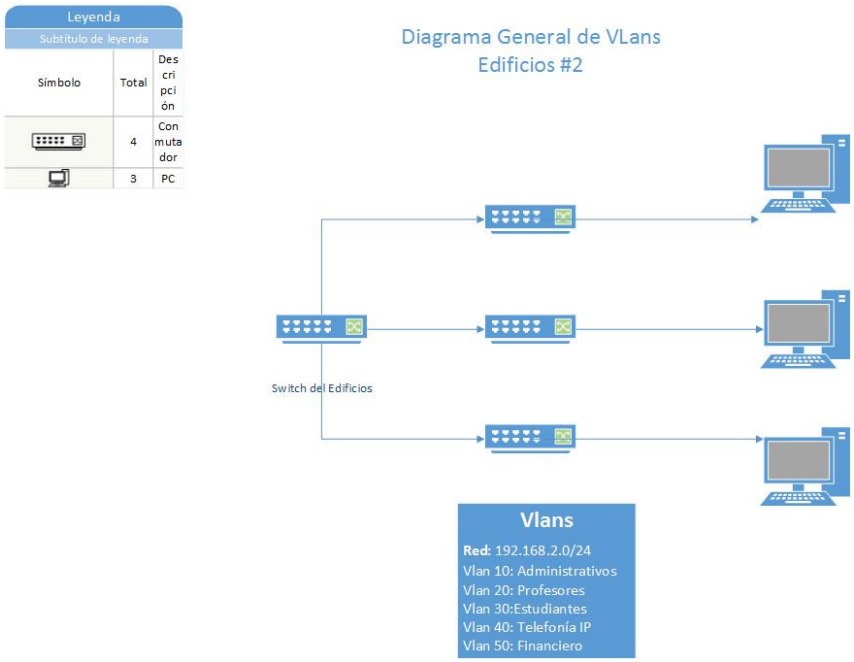

Figura 2.14. Diagrama de Vlan del edificio #2.

En el diagrama podemos apreciar la utilización de 4 switch administrables y la creación de 5 Vlan para la virtualización de la red del edificio #3.

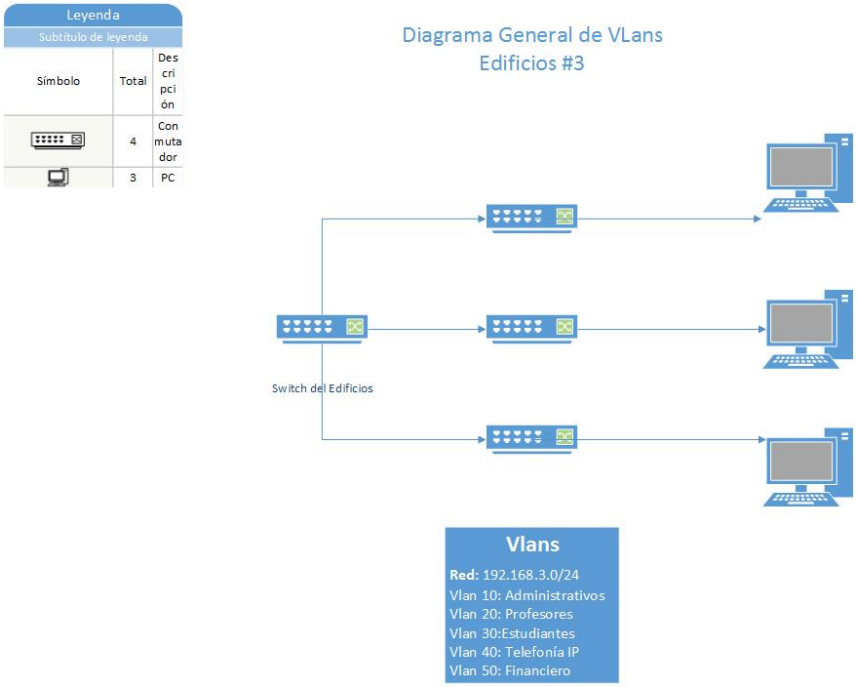

Figura 2.15. Diagrama de Vlans del edificio #3.

Finalmente el siguiente es el diagrama general de la infraestructura de la red de la USGP. Donde se puede apreciar el diseño y localización del firewall, NIDS, DMZ, switch administrable y router.

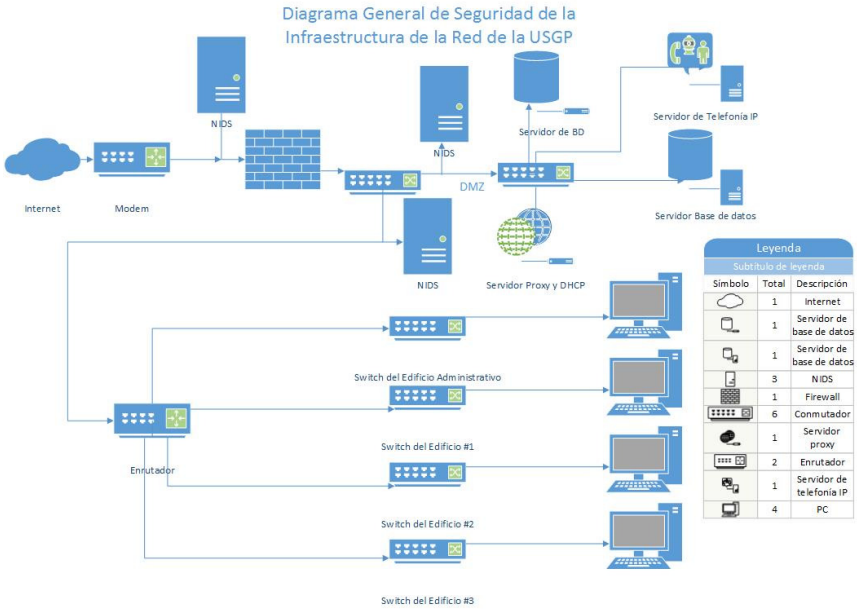

Figura 2.16. Diagrama general de seguridad de la infraestructura de red de la USGP.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 MEJORAS EN LAS ÁREAS VULNERABLES DE LA INFRAESTRUCTURA LA RED

Dentro de las mejoras de las áreas vulnerables de la infraestructura de seguridad de la red de la USGP tenemos que se recomienda la implementación de equipos y configuraciones lógicas para atenuar cualquier suceso de intromisión que puede sufrir la institución.

Entre las mejoras que tenemos es la implementación de un firewall para evitar la intromisión y filtración de cualquier paquete que lleve el intento de vulnerar la seguridad o introducir algún código dañino que pueda afectar gravemente los equipos de la red.

La implementación de 3 NIDS para que nos alerte de cualquier anomalía que puede haber en la red.

La implementación de DMZ para los diferentes servidores que existen en la USGP, evitando que las infiltraciones que pueden sufrir los servidores no lleguen hasta la red local.

La configuración de Vlans para evitar que en el caso de que un individuo intente tener acceso a toda red a través de un punto de red se encuentre con la barrera de que la red está virtualizada y así no podrá comprometer el resto de las redes LAN.

La utilización de un servidor radius mejoraría la seguridad en los puntos de acceso inalámbrico de la red, teniendo registro de la conectividad que se realiza a diario dentro de la institución.

En el mejor de los casos lo ideal sería que todas estas implementaciones se realicen para que red actual se transforme en una red segura en la cual se pueda trabajar sin tener el riesgo que la información se comprometida por alguna intromisión.

3.2 DISMINUCIÓN DE INCIDENTES DE SEGURIDAD DE LA RED

La disminución de incidentes de seguridad de la red se puede llevar a cabo mediante el mejoramiento de ciertas áreas y configuraciones para tener mayor seguridad en que si un usuario llega a descargar un software malicioso este sea detectado por el antivirus y que no afecte al sistema operativo de la PC, para ello el sistema operativo también debe encontrar actualizado con los parches de seguridad más actuales.

El sistema operativo es la parte principal a nivel de software del computador, por tal motivo el sistema operativo se debe encontrar actualizado para evitar que haya una intromisión por los fallos de seguridad del sistema operativo.

El antivirus cumple un papel fundamental en la seguridad de la información de las PC de los usuarios finales para evitar que cualquier intento de vulneración dañe la información que se encuentra reposando en la PC.

La configuración de Vlan para tener un mejor control de la red y evitar que un usuario con conocimientos básicos de informática pueda ingresar y ver toda la red de universidad. Gracias a las Vlan esto se puede evitar ya que ellas solo mostraran la red virtual en la que se encuentra conectado el usuario y no podrá acceder ni interferir en las otras redes virtuales. Las Vlan son fundamentales en este tipo de

institución ya que en ella se encuentran laborando diferentes tipos de profesionales y estudiantes. Las Vlan permiten dividir la red de forma virtual o lógica, definiendo el uso aplicación de la red para las áreas determinadas a través de las Vlan.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La infraestructura de red actual se encuentra expuesta y vulnerable ante cualquier ataque a la que pueda sufrir de forma interna o externa.
2. La red se encuentra distribuida de forma desorganizada, se deben hacer arreglos para tener mejoras, previo a cualquier cambio que se quiera realizar en un futuro.
3. El personal debe estar altamente capacitado para cualquier evento de seguridad que pueda suceder.
4. Las zonas wifi deben ser mejoradas con la implementación de un servidor radius para la autentificación seguro de la red.

RECOMENDACIONES

1. Los diferentes host de la universidad trabajan con el sistema operativo Microsoft Windows 7 y para mayor seguridad se recomienda que el sistema operativo este licenciado para permitir las actualizaciones de parches de seguridad.
2. Se recomienda la utilización de antivirus de software licenciado ya que estos tienen mayor soporte y actualización diarias, a diferencias de las versiones gratuitas.
3. Se recomienda que en los sistemas operativos se aplique hardening para atenuar cualquier comprometimiento de los equipos en el caso de alguna intromisión en la red.
4. La alta gerencia debe tomar en cuenta que la seguridad de la infraestructura de red es una parte muy importante para mantener en buen resguardo la información que circula a través de los servidores y la red lan.

BIBLIOGRAFÍA

[1] J. A. Bertolín, Seguridad de la Información, Madrid: Parainfo, 2008.

[2] U. S. G. Portoviejo, «www.sangregorio.edu.ec,» 2015. [En línea]. Available: http://www.sangregorio.edu.ec/paginas.php?id=1#.VbGpdPkjMsV.

[3] A. S. Tanenbaum, Redes de Computadoras, Mexico: Pearson Educación, 2003.

[4] S. C. Reynoso, Los 27 Controles Críticos de Seguridad Informática, 2012.

[5] Cisco, CCNA Security, EEUU: Cisco Press, 2012.

[6] K. Astudillo, Hacking Ético 101, Guayaquil, 2013.

[7] U. S. G. Portoviejo, «www.sangregorio.edu.ec,» 2015. [En línea]. Available: http://www.sangregorio.edu.ec/uploads/paginas/organigramainstitucional%281%29.png.