COLEGIO GIMNASIO MODERNO

AUTORES:
JEISSON CARDONA
JOHN ALEXANDER CIFUENTES

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERIA
TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA
BOGOTA D.C.
2011

ANALISIS DE LA SEGURIDAD INTERNA DEL COLEGIO GIMNASIO MODERNO

AUTORES:
JEISSON CARDONA
JOHN ALEXANDER CIFUENTES

Asesor:
JULIO CESAR PINTO DEL BASTO
Mcs. En Comunicaciones.

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERIA
TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA
BOGOTA D.C.
2011

Nota de Aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, Diciembre de 2010.

AGRADECIMIENTO

Primero a Dios ya que nos ha dado la oportunidad de crecer profesionalmente, de tener la fortuna de estudio y caminos abiertos para un mejor futuro.

Para realizar este proyecto es muy importante destacar nuestros más sinceros agradecimientos a toda la parte de docencia de la universidad ya que en el trayecto de esta carrera han infundido diferentes pautas para el crecimiento profesional y personal de nosotros. Ha sido importante la paciencia de la facultad para la realización de este proyecto el cual ha pasado por muchas etapas para lograr su finalización.

A nuestras familias por inculcarnos los diferentes valores los cuales se ven reflejados en la larga realización de este proyecto, el apoyo ha sido incondicional para logremos el tan anhelado titulo.

DEDICATORIA

La dedicatoria de este proyecto es de manera general para todas las personas que participaron y que de alguna u otra forma aportaron ideas, impartieron conocimientos y fueron consientes del esfuerzo realizado, la idea principalmente ha sido luchar por un mismo propósito y es obtener el éxito en nuestras vidas.

CONTENIDO

GLOSARIO

Antivirus: Programa cuya finalidad es prevenir las infecciones producidas por los virus informáticos así como curar las ya producidas.

Autenticación: Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad.

Banda Ancha: Técnicamente es la diferencia en hertzios (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. Además es la cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado, por ejemplo, 33,6 Kbps (miles de bits por segundo).

Byte: Conjunto significativo de ocho bits que representan un carácter, por ejemplo la letra "a", en un sistema informático.

Clientes Ligeros o Livianos: Forma parte de una arquitectura cliente-servidor, donde el cliente depende del servidor para el procesamiento de tareas.

Confidencialidad: Garantizar que nadie pueda entender la información que fluye, por medio de una encriptación.

DMZ: Zona Desmilitarizada, donde se encuentran los servidores públicos de una red (Mail, Web Server).

DNS (Sistema de Nombres de Dominio): El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas anfitriones *(hosts)* de Internet basándose en los nombres de éstos. El estilo de los nombres de host utilizado actualmente en Internet es llamado nombre de dominio.

Estrella Extendida: Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de switches. Esta topología puede extender y dar cobertura de la red.

FTP (Protocolo de Transferencia de Ficheros): Protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de una red.

Firewall (cortafuegos): Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

Gateway (pasarela): Punto de una red que actúa como punto de entrada a otra red.

Hacker (pirata): Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Los *hackers* proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos.

Hardware (equipo físico, hardware, maquinaria): Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

IP (Protocolo Internet): Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet.

Integridad: Garantizar la información que se ha enviado sea la misma.

Intranet: Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

LAN (Red de Área Local) Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de Gbps (gigabits por segundo).

MAC: Control de Acceso Mandatario, forma común como se puede acceder a un recurso de un sistema, pocos controles.

Malware (malgramas, malware, programas malignos, software maligno): Cualquier programa cuyo objetivo sea causar daños a ordenadores, sistemas o redes y, por extensión, a sus usuarios.

Moodle: es un sistema de gestión de cursos, que ayuda a crear comunidades de aprendizaje en línea.

Nodo: Punto de conexión de una red.

Phishing: Es un término caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos ordenadores deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos.

Proxy: Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (*firewall* o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

Puerto: En los protocolos TCP/IP es un punto de conexión lógica. También es un punto de conexión física de un ordenador para enlazar con otros dispositivos como, por ejemplo, módems o impresoras.

Router (direccionador, encaminador, enrutador): Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento.

Seguridad Informática: Proteger información de las redes y los activos de la misma.

Servidor: Sistema que proporciona recursos (por ejemplo, servidores de ficheros, servidores de nombres). En Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la Red.

Software (componentes lógicos, programas, software): Programas o elementos lógicos que hacen funcionar un ordenador o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos del ordenador o la red.

Spyware: Son unos pequeños programas cuyo objetivo es mandar información, del usuario, por medio del internet. Usualmente estas acciones son llevadas a cabo sin el conocimiento del usuario, y consumen ancho de banda, en donde la computadora se pone lenta, etc.

Switch: Dispositivo de red que filtra y envía las tramas basadas en la dirección fuente y destino de cada trama, también es capas de interconectar dos o más segmentos de red haciendo ver solo una y dando un buen rendimiento y seguridad de la red interconectada (LANs).

TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet) Sistema de protocolos, definidos en RFC 793, en los que se basa buena parte de Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en destino, mientras que el segundo se responsabiliza de dirigirla adecuadamente a través de la red.

Transsiver: Conversor de fibra óptica a UTP.

TrojanHorse (Caballo de Troya, troyano) Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia (de ahí su nombre).

Virus: Programa cuyo objetivo es causar daños en un sistema informático y que a tal fin se oculta o disfraza para no ser detectado. Estos programas son de muy diversos tipos y pueden causar problemas de diversa gravedad en los sistemas a los que infectan. Hoy día se propagan fundamentalmente mediante el correo electrónico.

Vlan: Es un conjunto de dispositivos de una o más LANs que son configurados de tal forma que se pueden comunicar, haciendo las ver como si fuera una sola, cuando en realidad están localizados en un segmento diferente de LAN. Esto es porque VLANs están basadas en las conexiones lógicas en lugar de las físicas y es por eso que son extremadamente flexibles. Además sirven para administrar redes.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

WAN (Red de Área Amplia) Red de ordenadores conectados entre sí en un área geográfica relativamente extensa. Este tipo de redes suelen ser públicas, es decir, compartidas por muchos usuarios.

WPA (Acceso Protegido WiFi) Protocolo de seguridad para redes Wifi, utilizando claves dinamicas, para identificar usuarios de una red y establecer los privilegios de acceso.

WWW (World Wide Web) (Telaraña Mundial, Malla Mundial, WWW) Sistema de información distribuido, basado en hipertexto. La información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y es fácilmente accesible a los usuarios mediante los programas navegadores.

RESUMEN

Este proyecto realiza un estudio para mejorar la seguridad perimetral del Colegio Gimnasio Moderno, actualmente existen diferentes riesgos internos los cuales se presentan en el mal manejo de la información, no tener definido una topología de red y políticas de seguridad, para esto se presentaran alternativas de actualización del sistema de seguridad, un diseño para mejorar la red y políticas de seguridad con el objetivo de garantizar el acceso indebido de la información.

ABSTRACT

This project conducted a study to improve the security perimeter of the College GimnasioModerno, currently there are different internal risks which are described in the mishandling of information, have not defined a network topology and security policies to be presented this alternative security system upgrade, designed to improve network and security policies with the objective of ensuring the improper access of information.

INTRODUCCIÓN

Este proyecto da a conocer la parte de seguridad tecnológica interna que actualmente tiene el Colegio Gimnasio Moderno en Bogotá, este Colegio esta divido por varias dependencias en las cuales transfieren bastante información sin precaución alguna, la seguridad en redes se hizo para prevenir perdida, mal uso y alteración de la información por personas malintencionadas, este proyecto quiere enfatizar en que los usuarios tengan conciencia que lo que hagan a diario con la información puede ser perjudicial para muchas personas.

Sean realizado pruebas de seguridad en los servidores y equipos de cómputo detectando varios problemas como lo son puertos abiertos en los servidores, detección de intrusos, virus en los equipos e información no protegida por parte de los usuarios.

Para el proceso de seguridad no solo se toman medidas hacia los usuarios sino también a la parte de software y hardware que tiene el Colegio, es importante ir actualizando los recursos tecnológicos los cuales ayudan bastante a un proceso de seguridad, el proyecto muestra las alternativas del cambio de seguridad que tendría el Colegio, mirando los servicios que ofrece, las ventajas y desventajas, los costos y los valores agregados de cada solución. Este proceso genera que se haga varias capacitaciones a todo el personal del Colegio para que se rijan ciertos parámetros de seguridad y así el trabajo a diario sea más confiable.

1. ASPECTOS GENERALES

1.1 Descripción del problema

La infraestructura de telecomunicaciones que actualmente posee el colegio Gimnasio Moderno, presenta desorganización a nivel de topología lógica y topología física de la red, hecho que incide directamente sobre la seguridad de la información y hace vulnerable los procesos institucionales.

La red del Colegio Gimnasio Moderno está diseñada en una topología de árbol y no se encuentra totalmente estructurada, debido a falta de aspectos administrativos de la red, tanto a nivel físico, lógico y de seguridad.

1.1.1. Descripción actual de la Red:

Está compuesta por un servidor principal el cual tiene instalado Windows Server 2003 R2, este equipo se conecta a un switch TREDNET de 24ptos (administrable). y mediante la asignación de la IP como puerta de enlace los demás equipos acceden a Internet, la interconexión de los edificios del Colegio se realiza por medio de fibra óptica multimodo, para que luego los switch sean los encargados de extender la red y puedan comunicarse con las demás dependencias.

Los Access Points tiene habilitado el DHCP para cualquier equipo que se conecte a ellos, permitiendo el acceso a la LAN y con ello el servicio de Internet, a pesar de que los equipos inalámbricos tienen seguridad WPA los riesgos de seguridad son muy altos ya que no tienen una configuración que los permita aislarlos de la LAN, además el Colegio no cuenta con los recursos suficientes para cambiar estos dispositivos por unos más actuales.

El Campus educativo del colegio Gimnasio Moderno, está compuesto por 6 edificaciones distribuidas en un área de **6 Hectáreas** entre las direcciones Calle 76 - 74 y Cra. 9 - 11.

La red por edificación esta descrita de la siguiente manera:

- **EDIFICIO PRINCIPAL (A):** Tiene dos pisos y un altillo, así:

  Primer piso:
  17 equipos: 15 administrativos y 2 académicos
  Un switch donde entra la cascada del switch principal del edificio.

  Segundo Piso
  22 equipos: 9 administrativos y 13 académicos.
  Allí se encuentra alojado el rack con 2 switchTrendnet de 24 administrables capa 2 con módulos de fibra de Gigabit, además es donde se comunican los demás edificios, también cuenta con un Access Point Dlink.

  Altillo:
  1 Access Point DLink.

A. En este edificio se encuentra la conexión principal donde está ubicado el modem que provee el servicio de Internet y el servidor que da la salida a Internet.
En el primer piso hay 7 equipos y 2 servidores el del antivirus y el otro contiene el programa de cartera y de biblioteca.

- 9 equipos: 7 administrativos y 2 académicos.

En el segundo piso hay un 2 rack uno de ellos con el modem de Telmex Huawei y un Gateway AlliedTelesyn es el encargado de convertir la conexión de fibra en UTP, además hay 2 switchs uno Trendnet administrable capa 2 con módulo de fibra Gigabit, este comunica al edifico principal donde se interconectan los demás edificios, y un 3Com administrable de nivel 2, en el otro rack cuenta con 2 switchs uno Trendnet 24 puertos y el otro Encore de 16 puertos y van en cascada por UTP con uno de los switch del otro rack, en este piso hay 22 equipos y 2 de ellos son servidores uno el Web y el otro maneja el programa contable, en 2 de las salas se encuentran los clientes ligeros llamados Office Start de estos hay 48, para así ampliar la capacidad de los recursos y los usuarios.

- 22 equipos: 2 administrativos y 20 académicos.

12 equipos de los académicos tienen los clientes ligeros, para así ampliar las estaciones a un total de 60 usuarios.

B. El edificio de Primaria cuenta con 10 equipos donde 2 de ellos manejan Office Start para ello hay 8 clientes ligeros, también se encuentra un rack con un switch administrable Trendnet capa 2 y con modulo de fibra Gigabit, donde se conecta al switch del edificio Principal, esto en el primer piso.

- 10 equipos: 2 administrables y 8 académicos.

En el segundo piso hay 3 equipos, en el tercer piso no hay ningún equipo.

- 3 equipos: 3 académicos.

C. El Centro Cultural cuenta con una sola planta donde va un rack, con un switch administrable de nivel 2, modulo de fibra, marca Trendnet este switch se conecta con el edificio Principal y la Piscina y cuenta con 12 equipos.

- 12 equipos: 8 administrables y 4 académicos.

D. Este edificio cuenta en el primer piso con 5 equipos y 4 Office Start, un switchTrendnet administrable, de capa 2 y modulo de fibra Gigabit, donde va comunicado con el edificio Principal, además cuenta con un Access Point DLink.

- 5 equipos: 4 administrables y 1 académico.

En el segundo piso hay 2 equipos y en el tercero 3.

- 5 equipos: 5 académicos.

E. La Piscina cuenta con 4 equipos y un rack con un switch administrable de capa 2, con modulo de fibra Gigabit marca Trendnet.

- 4 equipos: 3 administrables y 1 académico.

Cantidad de equipos.

EDIFICIO	ACADEMICOS	ADMINISTRATIVOS	TOTAL	OFFICE START
PRINCIPAL	15	24	39	0
FACULTAD	22	9	31	48
PRIMARIA	11	2	13	8
CULTURAL	4	8	12	0
BACHILLERATO	6	4	10	4
PISCINA	1	3	4	0
TOTAL	**59**	**50**	**109**	**60**

TABLA No. 2

Direccionamiento IP:

Dirección clase C (192.200.200.xxx) y una mascara (255.255.255.0) para todos los equipos administrativos y académicos, al igual que los Access Point.

Los clientes ligeros llamados Office Start manejan una dirección Clase C (192.100.100.xxx) y una mascara (255.255.255.0).

El servidor WEB cuenta con una dirección IP clase B (190.114.15.144) y una máscara de red (255.255.0.0).

Se sabe que la seguridad de información es un tema bastante complejo y lo más importante, por eso se requiere de tiempo y dedicación para conocer todas las falencias y accesos indeseados a dicha información, el Colegio al tener varios edificios hace que este en constante riesgo las bases de datos y la transferencia de archivos que es el trabajo diario de los usuarios.

El Colegio ha visto que la seguridad de red es uno de los puntos críticos, ya que la tecnología ha venido avanzando a través de los días, y con un ejemplo muy claro encontramos riesgos que representan el conocimiento de ciertas personas indebidas con información clave ya que por medio de ellos se puede generar ataques informáticos, acceso a hackers, intrusiones dentro de la red, el robo de información, contenidos malintencionados como virus, gusanos, troyanos, spyware, phishing y demás clases de malware.

Se deben tener en cuenta los siguientes aspectos a optimizar en la infraestructura de la red nivel de Seguridad:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información.
- Seguridad física y ambiental
- Control de acceso
- Gestión de incidentes en la seguridad de la información.

Instalaciones del Colegio

- **A.** Edificio Principal
- **B.** Edificio Facultad
- **C.** Edificio Primaria
- **D.** Centro Cultural
- **E.** Edificio Bachillerato
- **F.** Piscina

2. ANTECEDENTES

2.1. Internos

El Colegio Gimnasio Moderno desde sus inicios en 1995 ha venido mejorando su infraestructura Tecnológica a nivel de hardware y software, Sin embargo la escalabilidad de la red no ha sido planificada y las mejoras se han realizado por partes. En el año 2004 se implementó un servidor principal con Windows Server 2003, el cual actualmente carece de políticas de respaldo y de acceso limitado.

Desde la implementación anterior, no se ha actualizado al personal administrativo en el buen uso de los recursos informáticos y en el cuidado consiente de la información procesada y almacenada en el sistema. Ya que está conformada por Bases de datos personales, administrativos y académicos; que son puntos de riesgo en la actividad diaria de la entidad educativa.

En la descripción del problema se evidencia como varios la red no cuenta con una estructura definida y como algunos puertos se encuentran abiertos, permitiendo filtrado de paquetes; y un posible ataque informático.

3. OBJETIVOS

3.1. Objetivo General

Diseñar un sistema de seguridad interno, que garantice una red fiable para la solución a los problemas de transferencia y seguridad de los datos en el Colegio Gimnasio Moderno.

3.2. Objetivos Específicos

- Realizar un diagnostico completo a la estructura, configuración y políticas de seguridad de la red del Gimnasio Moderno.

- Investigar cuáles son las alternativas de seguridad existentes en la actualidad para entidades educativas.

- Evaluar cuál es la mejor alternativa de solución a los problemas de velocidad y seguridad de la red del Gimnasio Moderno de acuerdo a los criterios y costos que el Colegio tenga.

- Capacitar a todos los usuarios del Colegio Gimnasio Moderno en todo lo referente a seguridad informática.

4. ALCANCES Y LIMITACIONES

4.1. Alcances

Con este proyecto se busca dar respuesta a los requerimientos red que presenta el colegio Gimnasio Moderno, entre los cuales tenemos el rediseño de la red , bajo una estructura de Vlans, configuración de firewalls, configuración de Listas de Acceso (ACL), Actualización de políticas y recomendaciones de seguridad a nivel lógico y físico.

4.2. Limitaciones

Los recursos presupuéstales destinados por el colegio son un 10**%,** del presupuesto anual; (**aprox $ 100.000.000)** siendo insuficientes para la implementación en soluciones de seguridad, la cual debe darse de manera actualizada y progresiva. Por lo anterior el Colegio debe utilizar en lo posible las mismas herramientas que tienen actualmente.

El Colegio Gimnasio Moderno tomara el proyecto como alternativa para la solución a sus problemas de seguridad internos mas no será un proyecto que se ejecutara de forma inmediata.

5. JUSTIFICACIÓN

El proyecto está enfocado para realizar un estudio general del manejo interno que se hace a toda la información que tiene el Colegio Gimnasio Moderno, esta red es controlada y gestionada por el mismo Colegio, el cual está en un proceso de mejoramiento en diferentes conceptos de tecnología, se pretende realizar un plan de organización en la transmisión de información, mensajería multimedia, acceso seguro a Internet y servicio Web interno.

La seguridad no es solamente implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información.

Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

La seguridad informática se ha convertido en un factor importante en el diseño e implementación de las redes, que el mismo administrador de la red debe estar constante supervisión de las medidas de seguridad con el fin de tener una red confiable y estable a los posibles ataques informáticos.

6. MARCO REFERENCIAL

Temáticas generales:

6.1 VLAN

Sus siglas internacionales VIRTUAL LOCAL AREA NETWORKS, es la alternativa actual que la gran mayoría de empresas están adecuando en su infraestructura de red, logrando organización, estabilidad, seguridad y administración de diferentes grupos de trabajo.

[1]La **VLAN** se conforman de grupos de dispositivos en una LAN que se configuran usando un software de administración de modo que se puedan comunicar como si estuvieran conectados al mismo cable cuando, de hecho, están ubicados en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son muy flexibles.

[2]**TIPOS DE VLAN**

VLAN de puerto central

Es en la que todos los nodos de una VLAN se conectan al mismo puerto del switch.

VLAN Estáticas

Los puertos del switch están ya preasignados a las estaciones de trabajo.

Por puerto

Se configura por una cantidad “n” de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Para la Figura 1 tendríamos en el Switch 9 puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3 como la tabla lo indica

Por dirección MAC

Los miembros de la VLAN están especificados en una tabla por su dirección MAC.

Por protocolo

Asigna a un protocolo una VLAN. El switch se encarga de dependiendo el protocolo por el cual venga la trama derivarlo a la VLAN correspondiente

[1] CISCO, 2007-2008, CCNA Exploration 1, Glosario.
[2] http://www.textoscientificos.com/redes/redes-virtuales

Por direcciones IP

Está basado en el encabezado de la capa 3 del modelo OSI. Las direcciones IP a los servidores de VLAN configurados. No actúa como router sino para hacer un mapeo de que direcciones IP están autorizadas a entrar en la red VLAN. No realiza otros procesos con la dirección IP.

VLAN Dinámicas (DVLAN)

Las VLAN dinámicas son puertos del switch que automáticamente determinan a que VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados. Cuando un puesto de trabajo pide autorización para conectarse a la VLAN el switch chequea la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas y automáticamente se configura el puerto al cual corresponde por la configuración de la VLAN. El mayor beneficio de las DVLAN es el menor trabajo de administración dentro del armario de comunicaciones cuando se cambian de lugar las estaciones de trabajo o se agregan y también notificación centralizada cuando un usuario desconocido pretende ingresar en la red.

VENTAJAS GENERALES DE LA VLAN

- Facilidad de cambios en el switch para cualquier grupo de trabajo
- Bajo costo en la implementación.
- Reduce tráfico innecesario y aumenta el rendimiento en la red.
- Mayor seguridad a la información de cada grupo de trabajo
- Facilidad en la administración de las VLANs

6.2 ESTRELLA EXTENDIDA

Las topologías se crearon para definir un estilo de interconexión entre varios computadores y así transferir información de un lugar a otro como por ejemplo la topología estrella se caracteriza por tener un dispositivo principal donde se conecta las diferentes estaciones para luego distribuir información entre las mismas.

La **estrella extendida** se utiliza cuando existen varias subredes teniendo un crecimiento considerable con las estaciones conectadas, teniendo dispositivos principales en cada subred para la comunicación entre si.

Principalmente las ventajas de esta topología es que el cableado es más corto, extiende longitud y el tamaño de la red, además busca siempre mantener información local.

6.3 ISO 27002

Esta norma es utilizada en las empresas para la seguridad de información tanto interna como externa que se maneje en la red. Al tener varios controles genera diferentes alternativas de solución minimizando al máximo las probabilidades de ser afectados por robo, daño o pérdida de información.

[3]Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

[4]Las clausulas de ISO 27002 son:

• **Introducción**

Conceptos generales de seguridad de la información y SGSI.

• **Campo de aplicación**

Se especifica el objetivo de la norma.

• **Términos y definiciones**

Breve descripción de los términos más usados en la norma.

• **Estructura del estándar**

Descripción de la estructura de la norma.

• **Evaluación y tratamiento del riesgo**

Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

• **Política de seguridad:**

Documento de política de seguridad y su gestión.

• **Aspectos organizativos para la seguridad:**

Organización interna; organización externa.

• **Gestión de activos:**

Responsabilidad sobre los activos; clasificación de la información.

• **Seguridad ligada a los recursos humanos:**

Anterior al empleo; durante el empleo; finalización o cambio de empleo.

[3] http://iso27000.wik.is/Area_Normas
[4] http://iso27000.wik.is/Area_Normas/ISO%2f%2fIEC_27002

• **Seguridad física y del entorno:**

Áreas seguras; seguridad de los equipos.

• **Gestión de comunicaciones y operaciones:**

Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.

• **Control de accesos:**

Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

• **Adquisición, desarrollo y mantenimiento de sistemas de información:**

Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.

• **Gestión de incidentes de seguridad:**

Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.

• **Gestión de continuidad del negocio:**

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

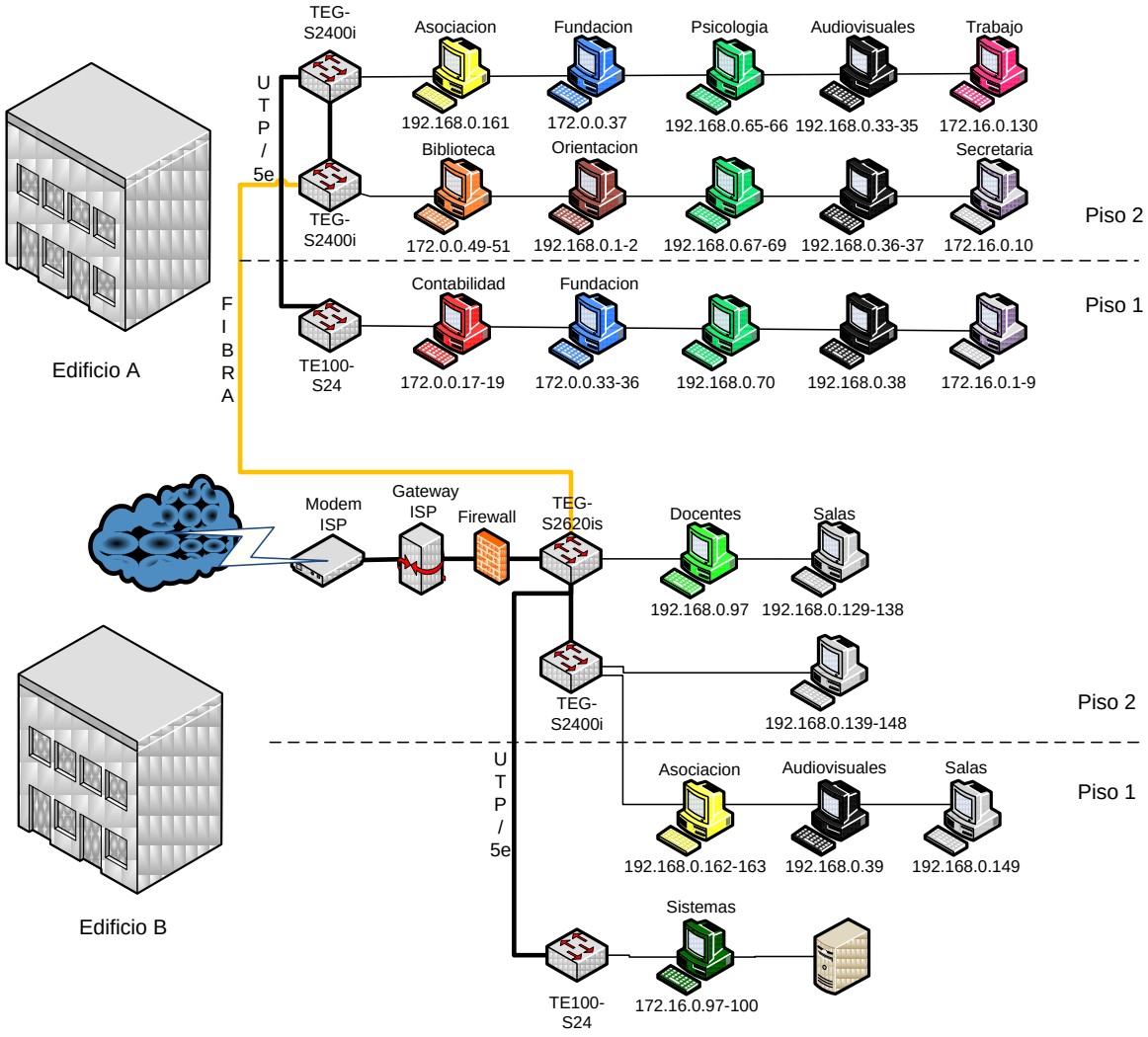
• **Conformidad:**

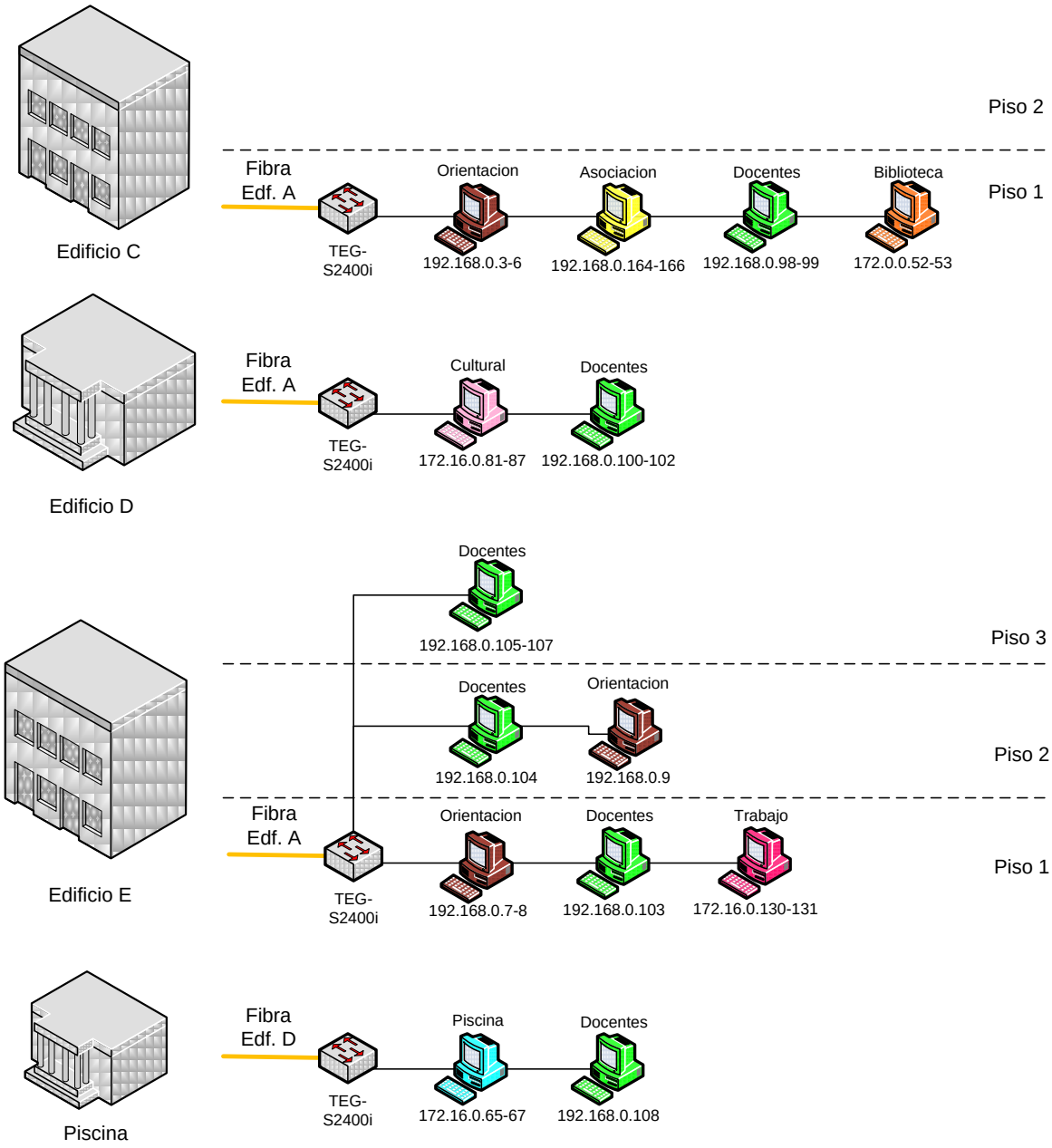
Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

7. DISEÑO DE INFRAESTRUCTURA DE RED

7.1 Diseño Físico

- El cableado horizontal y vertical de toda la red, va en cable UTP Cat. 5e, tx voz y datos con velocidad hasta 1000Mb/s.
- La comunicación de los edificios va por fibra óptica, a módulos de 1000M.
- Swicth TrendNet.




Piso 2
Fibra
Edf. A
Orientacion
Asociacion
Docentes
Biblioteca
Piso 1
TEG-
S2400i
192.168.0.3-6
192.168.0.164-166
192.168.0.98-99
172.0.0.52-53
Edificio C
Fibra
Edf. A
Cultural
Docentes
TEG-
S2400i
172.16.0.81-87
192.168.0.100-102
Edificio D
Docentes
192.168.0.105-107
Piso 3
Docentes
Orientacion
192.168.0.104
192.168.0.9
Piso 2
Fibra
Edf. A
Orientacion
Docentes
Trabajo
Piso 1
TEG-
S2400i
192.168.0.7-8
192.168.0.103
172.16.0.130-131
Edificio E
Fibra
Edf. D
Piscina
Docentes
TEG-
S2400i
172.16.0.65-67
192.168.0.108
Piscina

- **Caracteristicas de los servidores**

Servidor Web.

- HP Proliant ML-150
- Procesador Intel Xeon de 1.86GHz
- Memoria de 1GB
- Disco Duro de 250GB
- Tarjeta de Red Gigabit Ethernet 10/100/1000

Servidor Antivirus.

- IBM NetVista
- Procesador Intel Pentium IV 2.8GHz
- Memoria de 1.25GB
- Disco Duro 80GB
- Tarjeta de Red Intel PRO/100 VE Network Connection

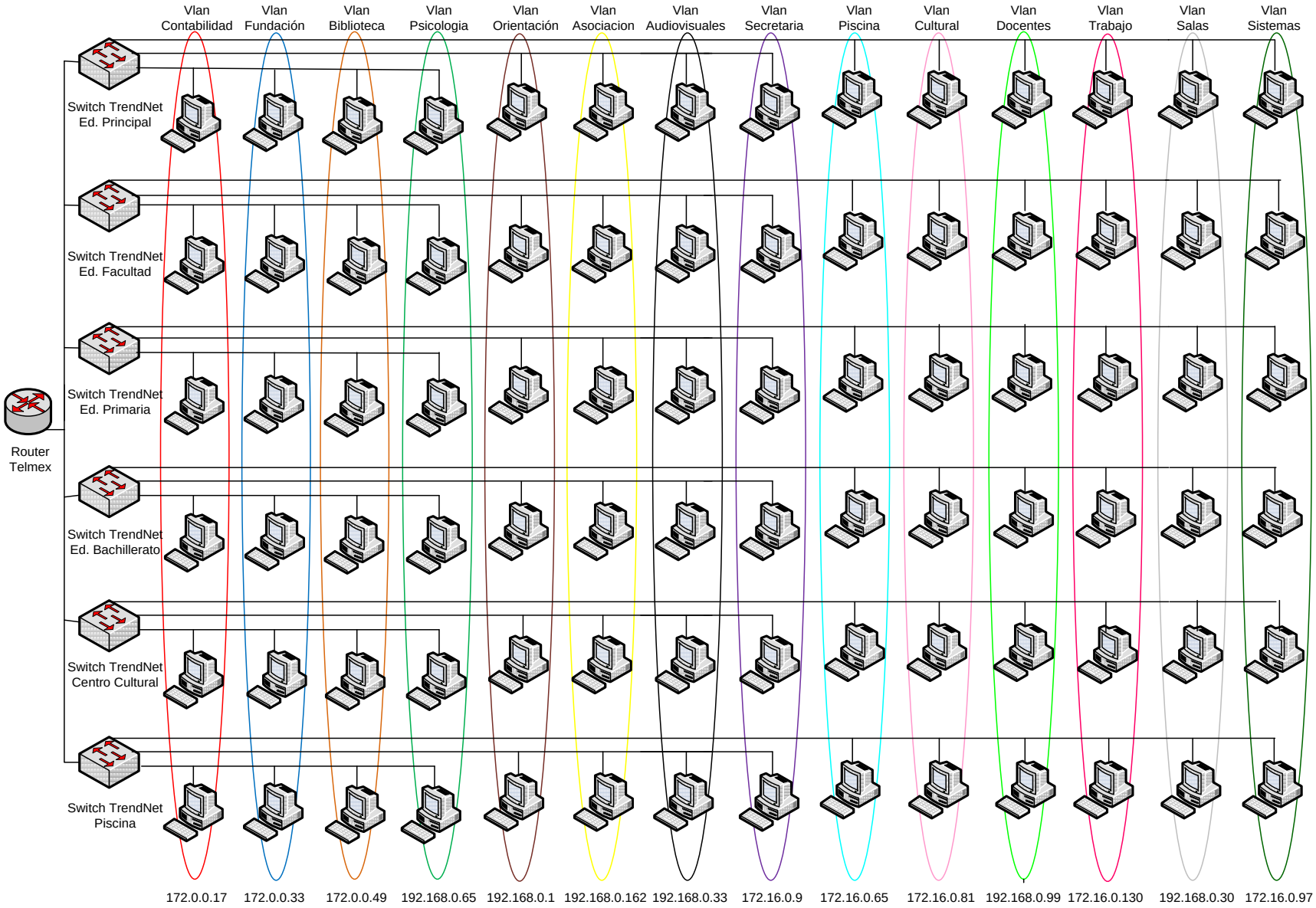
7.2 Diseño lógico y esquema de direccionamiento

9 subredes para el área administrativa que tendrán el siguiente rango de direcciones IP 172.16.0.0 con una mascara 255.255.255.240.

AREA ADMINISTRATIVA	Dirección de subred	Direcciones de host	Dirección de Broadcast
SECRETARIA	172.16.0.0	172.16.0.1-14	172.16.0.15
CONTABILIDAD	172.16.0.16	172.16.0.17-30	172.16.0.31
FUNDACION	172.16.0.32	172.16.0.33-46	172.16.0.47
BIBLIOTECA	172.16.0.48	172.16.0.49-62	172.16.0.63
PISCINA	172.16.0.64	172.16.0.65-78	172.16.0.79
CULTURAL	172.16.0.80	172.16.0.81-94	172.16.0.95
SISTEMAS	172.16.0.96	172.16.0.97-110	172.16.0.111
SERVER	172.16.0.112	172.16.0.113-126	172.16.0.127
TRABAJO	172.16.0.128	172.16.0.129-142	172.16.0.143

Para el área academica se va a tener un rango de clase C con la siguiente dirección IP 192.168.0.0 y una mascara de red 255.255.255.224.

AREA ACADEMICA	Dirección de subred	Direcciones de host	Dirección de Broadcast
ORIENTACION	192.168.0.0	192.168.0.1-30	192.168.0.31
AUDIOVISUALES	192.168.0.32	192.168.0.33-62	192.168.0.63
PSICOLOGÍA	192.168.0.64	192.168.0.65-94	192.168.0.95
DOCENTES	192.168.0.96	192.168.0.97-126	192.168.0.127
SALAS	192.168.0.128	192.168.0.129-158	192.168.0.159
ASOCIACION	192.168.0.160	192.168.0.161-190	192.168.0.191


Vlan Contabilidad
Vlan Fundación
Vlan Biblioteca
Vlan Psicologia
Vlan Orientación
Vlan Asociacion
Vlan Audiovisuales
Vlan Secretaria
Vlan Piscina
Vlan Cultural
Vlan Docentes
Vlan Trabajo
Vlan Salas
Vlan Sistemas
Switch TrendNet Ed. Principal
Switch TrendNet Ed. Facultad
Switch TrendNet Ed. Primaria
Switch TrendNet Ed. Bachillerato
Switch TrendNet Centro Cultural
Switch TrendNet Piscina
Router Telmex
172.0.0.17
172.0.0.33
172.0.0.49
192.168.0.65
192.168.0.1
192.168.0.162
192.168.0.33
172.16.0.9
172.16.0.65
172.16.0.81
192.168.0.99
172.16.0.130
192.168.0.30
172.16.0.97

7.3 Serie TZ SonicWALL

La serie **SonicWALL TZ** es la plataforma ideal de seguridad total para oficinas domésticas y para sucursales y oficinas pequeñas o remotas. Proporciona a las organizaciones una facilidad de uso para redes básicas y una flexibilidad para redes con necesidades complejas. Como plataforma altamente escalable, la serie TZ protege su inversión e integra todas las funciones en una sola solución asequible que incluye firewall de inspección profunda de paquetes, seguridad inalámbrica 802.11b/g, tecnologías de reconexión/recuperación, Gateway antivirus, anti-spyware, prevención de intrusiones, filtrado de contenido y prestaciones VPN IPSec. Los modelos de la serie TZ ofrecen diversas configuraciones de nodos y hardware, y permiten agregar prestaciones y funcionalidad.

Los dispositivos de la serie TZ poseen la certificación ICSA y se pueden gestionar de forma remota y sencilla como parte de un entorno multicortafuegos y VPN mediante una interfaz Web, o a través del Sistema de gestión global de SonicWALL (GMS).

Como opcional el equipo TZ 190, están disponible como solución el paquete de TotalSecure, que combina el hardware y todos los servicios necesarios para garantizar la protección completa de la red contra una amplia variedad de amenazas, como virus, spyware, gusanos, troyanos, keyloggers y demás amenazas maliciosas. El resultado es una solución de Gestión unificada de amenazas (UTM) con un nivel de seguridad excepcional y capacidad para proteger la red contra las amenazas emergentes. Serie TZ 190 de SonicWALL

Características del TZ 190

El TZ 190 es una plataforma de seguridad con enfoque multicapa que proporciona acceso inalámbrico, además incluye un módem analógico que pueden utilizarse como conexión WAN principal o secundaria, estas soluciones incluyen tecnologías de reconexión/recuperación automatizadas, un firewall de inspección profunda de paquetes y acceso LAN inalámbrico 802.11b/g opcional.

Gracias al potente sistema operativo SonicOS Enhanced de SonicWALL, la serie TZ 190 ofrece funciones avanzadas de continuidad del negocio y prestaciones de red como reconexión ISP, NAT basado en políticas, gestión basada en objetos y DDNS. Al integrar antivirus en pasarela, anti-spyware, prevención de intrusiones y antispam en tiempo real, la serie TZ 190 de SonicWALL ofrece un nivel de seguridad superior, garantizando la máxima protección contra cualquier tipo de amenazas maliciosas, ya sean internas o de Internet.

8. ANALISIS Y RECOMENDACIONES PARA LA SEGURIDAD DE INFORMACION

- MATRIZ DE PRIORIZACION

Esta matriz se realizo con las especificaciones de la norma **ISO 270002** la cual cuenta con 11 controles para la revisión de la seguridad de información en redes.

Se califico todos los controles de la norma donde **1** es MALO y **5** es EXCELENTE.

DOMINIOS	OBSERVACIONES	CALIFICACION
Política de seguridad	El colegio no cuenta con políticas de seguridad establecidas, ni documentación de la red general.	1
Aspectos organizativos para la seguridad	No todas las áreas de la empresa cuentan con una implementación de red adecuada ni condiciones de seguridad industrial óptimas.	3
Gestión de activos	El colegio cuenta con un inventario actualizado de los activos propios, realizando las modificaciones necesarias cada vez que exista un ingreso.	5
Seguridad física y del entorno	El colegio no cuenta con una infraestructura moderna que brinde la seguridad necesaria a cada una de las áreas y los equipos que se encuentran en ellas.	1
Gestión de comunicación y operaciones	El colegio resuelve a diario las diferentes solicitudes de soporte hechas a diario, además gestiona una protección contra virus, malware y demás código malicioso. Se realizan backups periódicamente. No se tiene documentación de las operaciones y soluciones brindadas a diario.	3
Control de accesos	El colegio no presenta una clasificación de acceso para las diferentes áreas tanto físicas como de red. Las redes inalámbricas se encuentran dentro de la misma red principal del colegio.	2
Gestión de incidentes de seguridad	Los usuarios no son responsables con la información generada a diario ya que no toman las medidas adecuadas de seguridad	1

- RECOMENDACION DECONTROLES DE LA NORMA **ISO 270002**

1. POLITICA DE SEGURIDAD.

1.1. Política de seguridad de la información.

Se crearan políticas por cada área dependiendo de las funciones que se realicen, estas políticas se basaran principalmente en la protección y el buen uso de la información. Cada política creada o modificada estará documentada en una bitácora.

1.1.1. Documento de política de seguridad de la información.

Se realizara un documento con todas las políticas planteadas para que la administración del Colegio apruebe y comunique a todas las personas

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

Se revisaran las políticas cuando estas no cumplan con los requisitos planteados y se llevara un control semestral para la revisión de las mismas.

2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION

2.1. Organización interna

2.1.1. Compromiso de la dirección con la seguridad de la información.

El administrador de la red tiene que distribuir las respectivas políticas de seguridad de la información, con el fin de fomentar su aplicación y cumplimiento por parte de los usuarios.

2.1.1.1 Coordinación de la seguridad de la información.

Realizar una respectiva evaluación por el área de sistemas para delegar las funciones respectivas de seguridad y a su vez reconocer que personas pueden realizar modificaciones en el sistema.

2.1.1.2. Asignación de responsabilidades relativas a la seguridad de la información.

Se deja claro a cada usuario que manipule información en el Colegio, debe seguir reglas como lo son: no dejar sesiones abiertas, no dejar claves en los escritorios, abrir siempre la información específica, no utilizar USB si no es autorizado por el área de sistemas.

2.1.1.3. Proceso de autorización de recursos para el procesado de la información.

Todo proceso en el sistema llevará un nivel de seguridad asignado en el servidor, cada área tendrá los usuarios correspondientes, como son: contabilidad, recursos humanos, sala de sistemas, etc, y se tendrá un administrador general para realizar modificaciones cuando sea necesario.

2.1.2. Acuerdos de confidencialidad.

La gran mayoría de información que tiene el Colegio son los datos personales de cada estudiante, por ser tan sensible la información solo personal autorizado podría copiar las bases de datos, los docentes solo pueden mirar los datos básicos como nombre, apellidos, identificación y e-mail.

2.1.3 Contacto con las autoridades.

Autoridades pertinentes, que manejen delitos informáticos.

2.1.4 Contacto con grupos de especial interés.

Realizar capacitaciones a la parte administrativa sobre cómo proteger la información de entidades educativas mínimo cada año.

2.1.5 Revisión independiente de la seguridad de la información.

Utilizar herramientas independientes que verifiquen políticas, procesos y procedimientos de seguridad.

2.2. Terceros

2.2.1. Identificación de los riesgos derivados del acceso de terceros

Prevenir los ataques externos que puedan afectar la red tanto de físicos como lógicos, revisando de manera permanente y aleatoria los procedimientos que se están ejecutando para mitigar los riesgos.

2.2.2 Tratamiento de la seguridad en la relación con los clientes.

Llevar un control de verificación de los estudiantes para el uso indebido de la información.

2.2.3 Tratamiento de la seguridad en contratos con terceros.

Personas externas deben cumplir con las normas establecidas de seguridad para ingresar o utilizar los servicios de la Institución.

3 SEGURIDAD FISICA Y AMBIENTAL.

3.2 Áreas seguras.

3.2.2 Perímetro de seguridad física.

Definir las áreas en las que ningún personal no autorizado ingrese, principalmente donde están ubicados los servidores y equipos en el área de sistemas.

3.2.3 Controles físicos de entrada.

Tener señalizado todas las áreas del Campus de Colegio, mantener las áreas restringidas siempre cerradas y tener las llaves en lugares seguros o por personal de seguridad experto. Alarma en el momento de forzar la puerta o sin quitar la clave.

3.2.4 Seguridad de oficinas, despachos, e instalaciones.

Lo recomendable es que en horarios fuera de trabajo no pueden permanecer funcionarios, personas no autorizadas y visitantes, además el personal de seguridad privada debe verificar que las oficinas se encuentren totalmente cerradas.

3.2.5 Protección contra las amenazas externas y de origen ambiental.

Tener señalizado lugares de evacuación a desastres naturales, tener varios puntos de extintores y realizar simulacros de prevención cada año.

3.2.6 Trabajo en áreas seguras.

Se deben tener políticas en la manipulación de partes tecnológicas por parte de estudiantes y personal administrativo para prevenir accidentes. Cualquier anomalía se debe informar al área de sistemas. TIA EIA-607 o 606a.

3.2.7 Área de acceso público y de carga y descarga.

Tener un lugar específico dentro de las instalaciones del colegios alejado del área de sistemas para evitar el ingreso no autorizado de personas.

3.3 Seguridad de los equipos

3.3.2 Emplazamiento y protección de los equipos.

Los equipos de cómputo deben estar ubicados en lugares no visibles para las personas tanto externas como internas, además todos los periféricos que componen un equipo de computo deben estar asegurados como mínimo con guayas. Cada dispositivo tecnológico para poder ser retirado del sitio debe llevar una orden de salida y ser registrado en la bitácora diaria.

3.3.3 Instalaciones de suministros.

Los servidores del Colegio deben estar conectados a una UPS con una duración mínima de 15 minutos si la corriente eléctrica fallara.

3.3.4 Seguridad del cableado.

El cableado estructurado como el cable eléctrico deben ir por canaleta y cuando sea de edificio a edificio por un respectivo tubo. Ningún cable debe estar al aire libre y la manipulación se realizara siempre por el área de sistemas.

3.3.5 Mantenimiento de los equipos.

Se realizará mantenimiento preventivo cada dos (2) meses y mantenimiento correctivo dos (2) veces al año.

3.3.6 Seguridad de los equipos fuera de las instalaciones.

Los equipos tecnológicos deben tener una póliza para protegerlos de los riesgos externos e internos.

3.3.7 Reutilización o retirada segura de los equipos.

Cuando los equipos se cambien por problemas físicos o por actualización siempre se debe realizar backups, para luego ser limpiado en su totalidad la parte de software, con esto preveemos que la información sensible sea utilizada.

3.3.8 Retirada de materiales propiedad de la empresa.

Siempre que se desee sacar propiedades de la empresa (equipos de computo, información o software legal), debe existir una orden de salida y llevar un registro o bitácora diaria.

4 CONTROL DE ACCESO.

4.2 Requisitos de negocio para el control de acceso.

4.2.2 Política de control de acceso.

El control de acceso debe estar dividido dependiendo de lo que se desee proteger, las restricciones se realizaran por dependencia.

4.3 Gestión de acceso de usuario

4.3.2 Registro de usuario.

Cada usuario perteneciente al Colegio debe estar creado en el servidor y pertenecer a grupo específico, este llevara nombre completo.

4.3.3 Gestión de privilegios

Los privilegios estarán filtrados por los grupos de red que pertenezcan al servidor, por ejem: Contabilidad no podrá ingresar a Recursos Humanos.Como ya sabemos los usuarios tienen un id y password como validación, este proceso se realizara en todo momento para el acceso a carpetas de red o información general la red.

4.3.4 Gestión de contraseñas de usuarios.

Cuando ingrese por primera vez el usuario debera colocar su propia contraseña, luego el mismo sistema pedirá cambio de contraseña cada 45 días, otra condición será que el usuario no pueda repetir contraseña.

4.3.5 Revisión de los derechos de acceso de usuario.

Trimestralmente se debe revisar los permisos que cada usuario tiene para acceder a la información del servidor.

4.4 Responsabilidades de usuario.

4.4.2 Uso de contraseña

El usuario debe establecer una contraseña con los parámetros exigidos y responsabilizarse de la misma.

4.4.3 Equipo de usuario desatendido.

4.4.4 Política de puesto de trabajo despejado y pantalla limpia.

Mantener el lugar de trabajo sin información que pueda causar futuros daños al colegio.

4.5 Control de acceso a la red.

4.5.2 política de uso de los servicios en red.

Capacitar a los usuarios de accesos restringidos en la red.

4.5.3 Autenticación de usuario para conexiones externas.

Se debe crear un usuario y contraseña especifico en cada área para el acceso remoto

4.5.4 Identificación de equipos en las redes.

Se deben registrar los equipos que siempre se autentican en el servidor para evitar que equipos externos puedan conectarse fácilmente a la red.

4.5.5 Diagnostico remoto y protección de los puertos de configuración.

4.5.6 Segregación de las redes.

El colegio estará segmentado por cada una de las dependencias y servicios que este ofrece

4.5.7 Control de la conexión a la red.

Mantener en constante revisión el acceso a redes compartidas para el ingreso indebido a la red.

4.5.8 Control de encaminamiento de red.

Tener siempre un flujo confiable entre los equipos de cada dependencia para evitar perdida.

4.6 Control de acceso del sistema operativo.

4.6.2 Procedimientos seguros de inicio de sesión.

Cada vez que se encienda el computador debe aparecer una ventana con nombre de usuario y contraseña, de esta forma podrá ingresar al sistema.

4.6.3 Identificación y autenticación del usuario.

Todo el personal administrativo, docente y estudiantil tendrá un único usuario para la autenticación en el sistema, este usuario previamente se creara en el servidor.

4.6.4 Sistema de gestión de contraseñas.

Siempre que se cree un nuevo usuario la persona tendrá que cambiar la contraseña en el primer inicio de sesión, esta debe tener letras mayúsculas y minúsculas, números y caracteres especiales. Si estas características no se cumplen el sistema no le permitirá ingresar al sistema.

4.6.5 Usos de los recursos del sistema.

Los equipos estarán configurados con los programas necesarios, como lo es el acceso a la intranet, office para la entrega de reportes y acceso a la web con restricciones.

4.6.6 Desconexión automática de sesión.

En el servidor principal se configuro para que las sesiones que permanezcan abiertas por más de 30 minutos se han cerradas automáticamente, previamente se le ha informado al usuario para que no se ha sorpresa.

4.6.7 Limitación del tiempo de conexión.

Se debe llevar un informe desde el servidor del tiempo que permanece el usuario conectado a la red, este tiempo se tomara desde el inicio de sesión hasta el cierre de la misma, los usuarios que permanezcan más de diez (10) horas diarias se les hará un seguimiento personal.

4.7 Control del acceso a las aplicaciones y a la información.

4.7.2 Restricción del acceso a la información.

En el servidor estará distribuido el acceso a las respectivas dependencias del Colegio, el personal que no corresponda a la dependencia correcta no tendrá los permisos para acceder a ella. En el servidor se crean grupos que corresponde a las dependencias y los usuarios serán añadidos respectivamente a donde correspondan.

4.7.3 Aislamiento del sistema sensible.

Todos los servidores y dispositivos importantes tendrán su cuarto informático aislado de las demás dependencias y solo personal del área de sistemas podrá acceder.

4.8 Ordenadores portátiles y teletrabajo.

4.8.2 Ordenadores portátiles y comunicaciones móviles.

El colegio internamente tendrá conexiones inalámbricas para que el personal visitante pueda en ciertos casos utilizar Internet, esta red será totalmente diferente a la red LAN.

4.8.3 Teletrabajo.

Los servicios de Internet deben estar administrados por el firewall que disminuye cualquier riesgo externo o interno a la red principal.

5 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION.

5.2 Notificación de eventos y puntos débiles de la seguridad de la información.

5.2.2 Notificación de los eventos de seguridad de la información.

Para cualquier eventualidad los canales de comunicación serán por correo corporativo, intranet y comunicación directa con el área de sistemas.

5.2.3 Notificación de puntos débiles de la seguridad.

El servidor tendrá logs los cuales serán revisados a diario para conocer incidencias en el sistema, además se tendrá en total comunicación con los usuarios de las dependencias para conocer cualquier anomalía que se presente en la red.

5.3 Gestion de incidentes de seguridad de la información y mejoras.

5.3.2 Responsabilidades y procedimientos.

Cada vez que exista una anomalía en la red será registrada en el sistema para que tenga un seguimiento desde el inicio hasta la solución, será asignada a una persona del área de sistemas el cual llevara el reporte de lo realizado al problema.

5.3.3 Aprendizaje de los incidentes de seguridad de la información.

Se debe tener un CRM el cual será alimentado por las incidencias que ocurran en la red, esto nos permitirá solucionar inconvenientes que se hayan presentado anteriormente de una forma rápida y eficaz.

5.3.4 Recopilación de evidencias

Siempre que suceda incidencias a la red que el área de sistemas no pueda solucionar las acciones se tomaran por las reglas establecidas legalmente por fornecía informática.

VENTAJAS Y DESVENTAJAS

- VENTAJAS

    - Analizar el tráfico de la red por medio de las Vlan.
    - Manipulación del cableado estructurado.
    - Se distribuye las políticas de seguridad dependiendo del sector o importancia de la información.
    - Se conoce los puntos críticos en los cuales la información puede ser vulnerable.

- DESVENTAJAS

    - Al reorganizar la red tanto hardware como software influye en que el colegio a parte de la solución tengan más costos.
    - El proceso de cambio de políticas de seguridad pueda retrasar algunos trabajos diarios del colegio

CONCLUSIONES

- El proyecto es una base importante para dar nuevas ideas de organización a lo que ya existe.
- Si se crean políticas internas como externas se puede lograr al máximo mitigar el riesgo de la información.
- La estructura de la red es la que permite la administración eficaz y solvente a los diferentes problemas.
- Actualización de la infraestructura de red con pocos recursos.