Introducción

A. Antecedentes

El crecimiento de las redes locales en los últimos años ha permitido incrementar el flujo de información a grandes escalas, permitiendo con ello agilizar procesos educativos, personales y comerciales, pero también con ello nuevas amenazas y vulnerabilidades. En la actualidad es imprescindible la implementación de una red en cualquier sector, ya que la existencia de una empresa que no cuente con dicha infraestructura no le será posible garantizar su productividad ni mucho menos su existencia en el mercado.

Todo este tipo de actividades que involucran el uso de las computadoras y telecomunicaciones están relacionados con información, dado que la información es un bien al cual es asociado un valor, por lo tanto están sujetos a riesgos, impactando de manera económica, comercial, de prestigio y confianza y existencia de la organización, principalmente. En este escenario hay factores a tomar en cuenta, los equipos de cómputo y protocolos de comunicación empleados de manera inicial, no fueron creados con la seguridad en mente por *default*, así mismo la venta de equipo de cómputo de forma masiva, pone la capacidad de amenaza en manos de más personas, por esta razón no existe un momento en el que no importe la seguridad, para cualquier organización.

A pesar de la gran utilidad y todas las ventajas que ofrecen las redes no se puede dejar a un lado y mucho menos dar por hecho que la seguridad de la organización se encuentra en optimas condiciones, actualmente cada vez mas empresas reconocen tener incidentes de seguridad en sus organizaciones, lo que demuestra que es importante invertir en su seguridad, tomando en cuenta conceptos como administración, seguridad informática y todo lo que ello implica.

Dada la importancia de las redes y su indiscutible necesidad, han permitido el desarrollo de nuevas tecnologías así como una nueva forma de lucrar con la información ajena, de manera general se han mostrado las ventajas que éstas ofrecen, sin embargo, se deben tomar en cuenta ciertas cuestiones como garantizar que la información que circula a través de la red, así como aquella que es almacenada en un equipo final sea confiable, integra, disponible y confidencial.

Las instituciones actualmente están buscando mecanismos que permitan minimizar el riesgo al cual puedan estar expuestos, ya que no existe como tal un proceso que se debiera seguir y que con ello garantice o se considere una red 100% segura, pues la práctica demuestra lo contrario, aunque al implementar mecanismos de control, como lo son el uso de estándares de seguridad, políticas internas, legislación informática, respaldos, planes de contingencias, esquemas de seguridad perimetral, servicios de seguridad, recomendaciones de instituciones como NIST, SANS, ISO, entre otras, todo esto ayuda a reducir riesgos.

Mantener la información íntegra, disponible y de manera confidencial es de gran importancia para cualquier organización, ya que de ello depende que dicha organización cumpla con sus objetivos establecidos. Por otro lado, no es posible garantizar la seguridad global, pero sí es posible disminuir los riegos dentro de una red de área local, ¿cómo lograrlo?, existen distintas formas aunque como se mencionó, no necesariamente existe un camino, es decir, se pueden tener distintos esquemas de seguridad de acuerdo con las necesidades propias de cada organización.

B. Definición del problema

Considerando que día con día la mayoría de los servicios brindados por cualquier organización, se están migrando a entornos que involucran el uso de equipos de cómputo, servidores y redes de datos, también se deben considerar los múltiples ataques que sufren las organizaciones, enfocados al robo de información, falsificación, modificación, denegaciones de servicio, suplantaciones, vulnerabilidades en sistemas, uso de equipos de cómputo para actividades maliciosas, entre muchas otras, debido a un descuido o de manera intencional. Las organizaciones deben planear contar con un esquema de seguridad perimetral, basado en las necesidades de negocio y sus objetivos.

El hecho de implementar un esquema de seguridad perimetral, para el Colegio de Ciencias y Humanidades, tiene como objetivo proteger la red de la organización, partiendo de un análisis de riesgos que permita identificar los activos de mayor valor, realizar un inventario de la red actual, identificar amenazas, vulnerabilidades, ponderando los riesgos, buscando posteriormente plantear el diseño que permitirá minimizar riesgos.

Un esquema de seguridad perimetral para la red de una institución puede contemplar mecanismos de control de acceso, implementación de estándares, monitoreo, políticas, procedimientos, inventario de los equipos, firewall, IDS, IPS, DRP, prevención, auditorias, administración, detección y respuesta a incidentes, capacitación, entre muchos otros, ya que éstos en conjunto brindarán a la organización un nivel de confianza mayor, todo esto debe ser analizado y determinado a nivel directivo. Por estos motivos se busca seguir una metodología para implementar un esquema de seguridad. Cabe mencionar que mientras más controles se tengan, el nivel de confianza que alcanzará la institución será mayor, sin dejar de contemplar las vulnerabilidades de los controles que se agreguen.

El esquema que se analiza, desarrolla e implementa está basado en las necesidades de la Dirección General del Colegio de Ciencias y Humanidades, a la fecha es impredecible contar con un esquema de seguridad perimetral que proteja los servicios e información de la institución, como entidad central de los 5 colegios que la conforman, la información transmitida y almacenada tiene cierto grado de importancia. El esquema a diseñar puede ser aplicado a otras instituciones si no de manera total, sí parcialmente, ya que como se mencionó, la implementación depende directamente de los objetivos y activos de cada institución.

Al ser una institución educativa, se cree que sus activos principales caen en los registros escolares, base de datos de sus trabajadores, inventario, nómina, publicaciones educativas, servicios electrónicos brindados a la comunidad, así como garantizar la disponibilidad de los servicios tanto para académicos, administrativos y alumnos, buscando limitar las actividades que no tengan ninguna relación con la finalidad de la institución, tanto actividades internas como externas.

C. Objetivos

- Realizar un análisis de riesgos que permita priorizar necesidades de seguridad, con base en el NIST 800-30.
- Estudiar diferentes propuestas para ofrecer seguridad, tanto a nivel de red, transporte y aplicación.
- Elaborar un estudio de la infraestructura de red con que cuenta la Dirección General del Colegio de Ciencias y Humanidades, para determinar el esquema que permita administrar, auditar e identificar información relevante en el segmento de red, de manera centralizada implementado herramientas de software libre y propietario.
- Diseñar un esquema de seguridad perimetral para la Dirección General del Colegio de Ciencias y Humanidades, que permita minimizar los riesgos contra los ataques más frecuentes.
- Realizar la implementación del esquema de seguridad propuesto para la Dirección General del Colegio de Ciencias y Humanidades.

D. Contribuciones

- Realización de un primer análisis de riesgos para la institución, basado en el estándar NIST 800-30.
- Implementación en su conjunto de un primer esquema de seguridad perimetral para la institución.
- Implementación de controles, que permitan identificar y solucionar problemas en la red de manera clara y precisa.
- Desarrollo de políticas de uso de la red para la Dirección general del Colegio de Ciencias y Humanidades.
- Reducir los incidentes de seguridad relacionados con amenazas lógicas, así como físicas.
- Que este estudio sea una base para realizar una implementación de esquema de seguridad perimetral para cualquier otra organización, en particular para los planteles que conforman el colegio.

E. Estructura de la tesis

La tesis se divide en 5 capítulos:

Capítulo I. Conceptos básicos:

Se describen los conceptos básicos de redes, considerando los modelos OSI, TCP/IP y los protocolos de servicio más utilizados, considerando protocolos como DNS, HTTP, TELNET, SSH, DHCP, FTP, TFTP, SNMP, SMTP, entre otros.

Capítulo II. Conceptos generales de seguridad:

Cubre los conceptos generales de la seguridad, considerando sus principios, definiciones básicas, fases de un ataque, tipos de ataques, controles de seguridad y la importancia del análisis de riesgos.

Capítulo III. Mecanismos de seguridad en red:

muestra los mecanismos de seguridad que se pueden aplicar a una red, considerando tipos de estrategias, servicios, mecanismos de autenticación, factores relacionados a la seguridad física, cifrado, firewall, IDS, auditorias, monitoreo, seguridad en redes inalámbricas, sensores, estándares, políticas de seguridad y planes de contingencia.

Capítulo IV. Buenas prácticas de seguridad:

Observa las recomendaciones que se emiten de manera general en la seguridad de la información, por organizaciones con experiencia en la implementación de políticas, procedimientos, mecanismos y acciones, que permitan brindar un control efectivo en la organización.

Capítulo V. Propuesta de implementación, caso práctico:

Una vez comprendidos los conceptos y aspectos básicos de redes y seguridad la información, se realizará el análisis de riesgos basado en el estándar NIST 800-30 (Risk Management Guide for Information Technology Systems - Guía de Administración de Riesgos para Sistemas en Tecnologías de la Información), el cual será la base para la definición e implementación del esquema de seguridad perimetral.

Además el trabajo de tesis contiene un conjunto de apéndices que dan más detalle sobre algunos temas específicos, glosario, lista de acrónimos frecuentes, así como la bibliografía empleada para la realización de este trabajo.