SEGURIDAD EN LAS REDES LAN Y WLAN DE LOS LABORATORIOS UNIVERSIDAD MINUTO DE DIOS SEDE GARCIA HERREROS (GIRARDOT)

DAIVER HALYD TERREROS DAZA
JORGE ELIECER NUÑEZ CARDOSO

CORPORACION UNIVERSITARIA MINUTO DE DIOS

FACULTAD DE INGENIERIA
PROGRAMA TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA
GIRARDOT
2008

SEGURIDAD EN LAS REDES LAN Y WLAN DE LOS LABORATORIOS UNIVERSIDAD MINUTO DE DIOS SEDE GARCIA HERREROS (GIRARDOT)

DAIVER HALYD TERREROS DAZA
JORGE ELIECER NUÑEZ CARDOSO

Proyecto para Optar el titulo de Tecnólogo en Redes de Computadores y Seguridad Informática

Director
MAURICIO RODRÍGUEZ GARCÍA
Ingeniero Sistemas

CORPORACION UNIVERSITARIA MINUTO DE DIOS
FACULTAD DE INGENIERIA
PROGRAMA TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMATICA
GIRARDOT
2008

Nota de aceptación

4.5

_Ing._Efrain Masmela Téllez_____
Presidente del Jurado

_Ing. Mauricio Rodríguez García___
Jurado

__Ing. Fernanda Ismelda Mosquera_
Jurado

___Ing. Armando Darío Tovar____
Jurado

Girardot, Marzo 06 2009

AGRADECIMIENTOS.

Los autores expresan sus agradecimientos a:

A la Universidad Minuto de Dios y a todo su plantel docente de la Carrera Tecnología en redes de computadoras y seguridad informática por brindarnos los medios y conocimientos necesarios para acceder a una formación académica que nos permitirá desempeñarnos profesionalmente en el futuro próximo.

En especial queremos agradecerle todo el apoyo recibido y buena predisposición totalmente desinteresada, por nuestros profesores quienes nos guiaron durante todo este proceso ofreciéndonos sus conocimientos y horas de su tiempo.
Finalmente un agradecimiento especial al ingeniero Mauricio Rodríguez García, el cual nos guió en nuestros primeros años universitarios.

DEDICATORIA

Nosotros los estudiantes de la Universidad Minuto de Dios, quienes nos unimos para desarrollar este proyecto aportando trabajo voluntario con amor y desinterés, queremos dedicar este trabajo a nuestros familiares, novias y amigos, quienes nos acompañaron durante estos largos años de travesía universitaria, apoyándonos, aconsejándonos y brindándonos su incondicional afecto. Respetamos y fomentamos la oportunidad que tenemos de dar y aprender. Hacemos todo con las mejores intenciones, trabajando responsablemente con respeto y humildad, A todos ellos muchas gracias.

CONTENIDO

LISTA DE CUADROS.

LISTA DE FIGURAS.

INTRODUCCIÓN

En el presente proyecto se evidencia una serie de acontecimientos y contenidos, los cuales han llevado por parte de este grupo estudiantil, a la investigación y el desarrollo de los factores de riesgo que se pueden o no presentar en una Red, ya sea esta de carácter publica o privada, así como las medidas, que se tomaran para su buen desempeño y funcionamiento.

Con respecto al tema de su seguridad, el cual es el primordial objetivo en la culminación de este proyecto, estos contenidos y acontecimientos de carácter investigativo y productivo se vincularán con la gestión de la seguridad y los aspectos legales, en continua evolución, relacionados con el uso de las nuevas tecnologías y los problemas suscitados por ellas. Además de una vertiente claramente teórica, en la cual se consolidan los resultados propios de la elaboración y desarrollo, de este proyecto que demostrara el desempeño y las capacidades investigativas y laborales, por parte de sus desarrolladores.

1. PLANTEAMIENTO DEL PROBLEMA

Durante el desarrollo e implementación de nuevos laboratorios para los estudiantes de las Tecnologías en Redes-electrónica e Ingeniería Civil es donde hay que observar y tener en cuenta una inquietud bastante importante de este, su seguridad, en cuanto al manejo de la información que allí se genere, esta es la parte donde radica el problema, ya que mucha de la información y procesos que se lleven acabo en este laboratorio quedaran guardados en este lugar, lo cual implicara que tanto entes internos como externos tengan un control sin restricciones alguna forma, en este caso es cuando se debe implantar medidas de seguridad que con lleven a un manejo mucho mas ordenado y seguro de la información.

1.1 DESCRIPCION DEL PROBLEMA

Día tras día han ido evolucionando las redes informáticas, y así mismo también han aumentado cada vez más los riesgos de vulnerabilidad a ataques contra ella (hackers, crackers), debido a esto y a la importancia de la información, las empresas, universidades, organizaciones privadas y del estado han elaborado estrategias que permiten mantener seguras las redes ante cualquier tipo de ataque que lleve como objetivo el robo o modificación de la información y la denegación de servicios, entre estos métodos preventivos encontramos la utilización de firewall de alta confiabilidad, que cumple no solo con funciones típicas de un firewall, si no que también utiliza propiedades de otros sistemas como lo es el Proxy, que me permite hacer filtrado de spam, black list, bloqueo de algunos protocolos como lo es el p2p, pop, telnet, FTP, SMTP, entre otros, que no están siendo utilizados por el momento en la Universidad Minuto de Dios.

De no utilizar este tipo de métodos, las consecuencias para la red tanto inalámbrica como cableada serian catastróficas, pues todo mundo tendría permisos para ingresar a dicha red y utilizar varios de sus servicios (Internet, información), que daría como resultado una red lenta, vulnerable, insegura, no estable, etc. Pues así como a crecido Internet, en estos momentos cualquier persona no tiene que tener muchos conocimientos en cuanto a las redes para poder tratar infiltrarse en una de ellas, pues en la Internet se tiene al alcance de las manos y sin ninguna restricción, software, que permite hacer por ejemplo una denegación de servicios haciendo unos cuantos clicks. O en el caso de que el ataque no sea solamente por personas de afuera (outsider) si por usuarios del mismo establecimiento (insider) por ejemplo la instalación de software tipo spiware (keyloger, spoofing, pishing) que permitirían fácilmente conseguir información confidencial entre otras (claves de e-mail, cuentas bancarias, ingreso a páginas no autorizadas entre otras).

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo implementar una medida de seguridad para los laboratorios que se construirán en la Corporación Universitaria Minuto de Dios?

2. JUSTIFICACIÓN

Debido a los riesgos del uso indebido de la red (que en el momento se encuentra desprotegida y con muy pocos controles de seguridad) para personas extrañas o de la misma universidad, que pretendan desestabilizar o cometer actos que van en contra de los principios o reglas de la Universidad Minuto de Dios, es necesaria la implementación de métodos que solucionen este tipo de problemas a nivel de redes LAN y WLAN, y que hagan de esta una red más segura y estable.

La implantación de políticas de seguridad en los laboratorios de la Universidad Minuto de Dios es de suma importancia, además, de esta forma se ayuda a los estudiantes de las facultades de redes e informática a que aprendan a implementar las distintas medidas de seguridad utilizadas actualmente, en muchas empresas e instituciones, publicas y privadas.

El desarrollo de este proyecto beneficia y fortalece la seguridad en los laboratorios de la Universidad Minuto de Dios, así mismo obviamente beneficiara a los usuarios que soliciten los servicios de red (Administración, estudiantes, docentes y directivos).

El proyecto es viable a nivel económico, debido a la financiación por parte de la Universidad Minuto de Dios para la compra del firewall (software Mikrotik RouterOs), lo que implica únicamente la implementación y configuración del Mikrotik (firewall), en el cual sus gastos son lo de menos, pues es única y explícitamente talento humano, que es donde entra a jugar el papel de los estudiantes de Tecnología en Redes de Computadores y Seguridad Informática Jorge Eliécer Núñez Cardoso y Daiver Halyd Terreros Daza.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar una medida de seguridad que permitan al correcto funcionamiento de la red Lan y Wlan de los laboratorios de de la Universidad Minuto de Dios.

3.2 OBJETIVOS ESPECIFICOS

1. Instalar un firewall que me permita defender, administrar, supervisar y controlar posibles ataques que lleven como objetivo la denegación de servicios (spam, spoofing, pishing, boombing, malware, gusanos, troyanos, spiware, entre otros) en los laboratorios de redes Uniminuto.

2. Configurar e implantar RADIUS en el firewall para la autenticación de usuarios Uniminuto en la red Wlan.

3. Establecer permisos independientes para administradores, grupos, invitados u otros.

4. Autenticar usuarios por medio de filtrado MAC.

5. Configurar el servidor Proxy, para evitar el ingreso a paginas no autorizadas.

6. Balancear la velocidad de carga y descarga de datos desde y hacia la internet.

4. MARCO REFERENCIAL

4.1 MARCO HISTORICO

Tomando como gran referencia a Los piratas informáticos, que ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Llegando al año 2000, los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida. Sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas.

Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan. Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Pero el lema es viejo: hecha la ley, hecha la trampa. Los medios de comunicación masivos prefieren tildarlos de delincuentes que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se intrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones. Pero he aquí la gran diferencia en cuestión. Los Crackers (crack = destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc.

Esos son los Crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema.

4.2 MARCO LEGAL

En la proposición y la realización de todo acto, o proyecto, por parte de una persona o personas, es necesario tener en cuenta, que estamos regidos por una sociedad, la cual ha decretado un sin numero de artículos, leyes y estatutos que son de esencial importancia, pues estas rigen gran parte de nuestra vida y los actos que nos llevaran a una completa o parcial armonía, es por eso que a continuación daremos a conocer algunas de estas leyes, las cuales son esenciales, para la solución de problemas legales, con respecto a la realización de este proyecto.

LEY 527 DE 1999 (agosto 18) Diario Oficial No. 43.673, de 21 de agosto de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones

ARTICULO 1o. AMBITO DE APLICACION. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;
b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo.

ARTICULO 2o. DEFINICIONES. Para los efectos de la presente ley se entenderá por:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
b) Comercio electrónico. Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

c) Firma digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.
d) Entidad de Certificación. Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.
e) Intercambio Electrónico de Datos (EDI). La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.
f) Sistema de Información. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

ARTICULO 3o. INTERPRETACION. En la interpretación de la presente ley habrán de tenerse en cuenta su origen internacional, la necesidad de promover la uniformidad de su aplicación y la observancia de la buena fe.
Las cuestiones relativas a materias que se rijan por la presente ley y que no estén expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspira.

ARTICULO 4o. MODIFICACION MEDIANTE ACUERDO. Salvo que se disponga otra cosa, en las relaciones entre partes que generan, envían, reciben, archivan o procesan de alguna otra forma mensajes de datos, las disposiciones del Capítulo III, Parte I, podrán ser modificadas mediante acuerdo.

ARTICULO 5o. RECONOCIMIENTO JURIDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

4.2.1 Restricciones legales.

En algunos países existen muchas restricciones legales para el comercio electrónico y aplicaciones informáticas, lo que impide la evolución del desarrollo de las aplicaciones y la implementación de software de seguridad para los negocios en línea. Desgraciadamente, no sólo se enfrenta el problema técnico sino el legal porque cuando se utiliza una firma electrónica autorizada por las empresas involucradas en una transacción, por ejemplo, no se puede probar en un juicio que esta firma es auténtica. No existe una autoridad certificadora, éste es uno de los problemas más serios.

No se puede considerar que la seguridad sea cuestión de una sola cosa, ya que hay muchos elementos y soluciones en la infraestructura de informática de una empresa. Por ejemplo, muchas de las claves en la criptología son fácilmente descifrables, debemos ver otras alternativas de tecnología de otros países de Europa, Israel, Rusia y no sólo en las soluciones americanas que presentan también muchas restricciones legales para su importación.

Algunas medidas para hacer frente al creciente problema de la falta de seguridad son: entre ellas la importancia de evaluar su vulnerabilidad interna y hacerse conscientes de que sí bien existen muchas violaciones externas y muchas soluciones tecnológicas, existe un porcentaje muy alto de inseguridad interna como resultado de problemas organizacionales. Esto enmarca la importancia de contar con políticas internas específicas que cuenten con el apoyo de los altos directivos, así como la existencia de un responsable en la seguridad interna cuyas decisiones de protección se realicen en función de problemáticas específicas y no sujetas a ajustes económicos.

4.3 MARCO INSTITUCIONAL.

El centro de educación profesional y tecnológica (Universidad Minuto de Dios), cumplirá con la formación de comunidades humanas y cristianas que permitan el desarrollo integral y profesional de la persona, este es el compromiso principal de la Universidad Minuto de Dios, pues su fundador el Padre Rafael García Herrera, siempre supuso una fuerte convicción con la educación y formación de todas las comunidades en general.

La formación de profesionales compenetrados por la filosofía Minuto de Dios y por ende comprometidos con el desarrollo de la persona y de las comunidades, ha generado la existencia de esta institución de educativa, la cual con el paso del tiempo y el esfuerzo de sus integrantes ha logrado desarrollarse y posicionarse como una de las instituciones mas conocidas y respetadas en la comunidad.
Es por esto que gracias a sus avances en materia de educación y formación se le ha logrado tener establecidos los siguientes estatutos:

ARTICULO 1: Nombre: La Institución regulada por los presentes Estatutos se denomina UNIMINUTO-CORPORACION UNIVERSITARIA MINUTO DE DIOS.

PARAGRAFO 1: Una vez obtenga de las autoridades correspondientes y conforme a las normas vigentes, el reconocimiento institucional de Universidad se denominará UNIMINUTO-UNIVERSIDAD MINUTO DE DIOS

PARAGRAFO 2: UNIMINUTO corresponde a la sigla que utiliza la Corporación Universitaria Minuto de Dios para identificar en todos sus actos y de manera

exclusiva sus servicios. El uso de la sigla y del logosímbolo siempre va acompañado de la denominación del tipo de institución universitaria a que corresponde de conformidad con la Ley.

ARTICULO 2: La Corporación Universitaria Minuto de Dios deriva su nombre de la obra social "El Minuto de Dios", fundada en Colombia por el Sacerdote Eudista RAFAEL GARCIA- HERREROS.

ARTICULO 3: La Corporación Universitaria Minuto de Dios tiene como Fundadores a la Corporación El Minuto de Dios, al Centro Carismático Minuto de Dios y a la Congregación de Jesús y María (Padres Eudistas)

ARTICULO 4: NATURALEZA JURIDICA. La institución ha sido creada como entidad docente e investigativa, de derecho privado, que participa de la naturaleza jurídica de corporación consagrada en el Código Civil Colombiano, constituida como persona jurídica autónoma de utilidad común y sin ánimo de lucro.

ARTICULO 5: CARACTER ACADEMICO. La Corporación Universitaria Minuto de Dios es una Institución de Educación Superior con el carácter de Institución Universitaria. Podrá transformarse en Universidad de conformidad con las leyes de la República de Colombia.

ARTICULO 6: DOMICILIO. Para todos los efectos legales la Corporación Universitaria "MINUTO DE DIOS" tiene su domicilio en la ciudad de Bogotá, Distrito Especial, República de Colombia.

PARÁGRAFO: La Corporación Universitaria Minuto de Dios podrá crear Seccionales, Sedes, Facultades y Programas en cualquier otro lugar de la República de Colombia, de conformidad con las normas prescritas y las contenidas en los presentes Estatutos.

ARTICULO 7: DURACIÓN. La Corporación Universitaria Minuto de Dios tendrá duración indefinida, pero podrá disolverse y liquidarse de acuerdo con las causales previstas en la Legislación Colombiana y en estos Estatutos.

4.3.1 Misión.

La Corporación Universitaria Minuto de Dios es una institución universitaria de educación superior, inserta en el sistema educativo colombiano, con un modelo de educación alternativo que, desde la perspectiva del Evangelio y del pensamiento social de la Iglesia, de la Espiritualidad Eudista, de la renovación en el Espíritu y de la filosofía de la Organización Minuto de Dios: Forma

profesionales responsables, técnicamente competitivos, éticamente orientados y socialmente comprometidos.

Promueve el desarrollo integral de las personas, las comunidades y las organizaciones, fomentando en ellas sus potencialidades, en términos de actitudes humanas, cristianas, ciudadanas y de servicio a la sociedad.

Contribuye en la construcción de una nación más justa, democrática, participativa y solidaria, que respete los valores culturales propios y ajenos.

4.3.2 Visión.

La Corporación Universitaria Minuto de Dios, en el año 2007, será reconocida por: Formar parte del sistema socio-educativo Minuto de Dios y estar orientada por los Eudistas.

Ofrecer un modelo educativo alternativo, centrado en el estudiante.

Tener estudiantes con un claro proyecto de vida fundamentado en valores, con espíritu creativo, solidario y con fuerte responsabilidad social.

Contar con un cuerpo docente bien calificado, innovador y comprometido con el desarrollo personal y profesional de los estudiantes.

Ofrecer programas académicos de calidad, acreditados o en proceso de acreditación.

Realizar investigaciones aplicadas que contribuyan efectivamente a la solución de problemas específicos de personas, comunidades, organizaciones y regiones.

Propiciar, desde su comunidad académica, una proyección social relevante para Colombia.

Ofrecer profesionales responsables, conscientes de sus deberes y derechos como ciudadanos y con alta responsabilidad social.

Tener una comunidad de egresados comprometidos con su Alma Mater y con el desarrollo de Colombia.

Ofrecer servicios educativos en varias regiones de Colombia, siempre orientados al desarrollo local y regional.

Prestar sus servicios educativos en los diversos ciclos, grados, modalidades y niveles de formación.

Propiciar el intercambio de estudiantes y docentes en el ámbito nacional e internacional.

Aportar conocimientos y acumular experiencias en Organizaciones de la Sociedad Civil (OSC).

Promover Alianzas y Redes con el fin de racionalizar los recursos, generar nuevos conocimientos y colaborar en la superación de la pobreza.

Promover el acceso y la permanencia de estudiantes en la Educación Superior, a partir de facilidades de pago, precios justos y métodos de educación innovadores.

Poseer talento humano con “mucho espíritu”: Ético, solidario, sencillo, servicial, cualificado y con habilidades colaborativas.

Generar espacios que promueven el bienestar de la comunidad universitaria y estimulen el sentido de pertinencia y compromiso con la institución.

Poseer una cultura de planificación sólida y una operación (estructura y procesos) eficiente.

Contar con unidades de gestión auto sostenibles y una alta eficiencia en las unidades de apoyo.

Ser innovadora en la búsqueda de recursos financieros diferentes a los provenientes de las matriculas.

Tener la planta física y la infraestructura adecuadas y suficientes.

Mantener relaciones cordiales y transparentes con los proveedores.

4.4 MARCO TEÓRICO.

Los requerimientos en la seguridad de la información de la organización han sufrido dos cambios importantes en las últimas décadas. Previo a la difusión en el uso de equipo de información la seguridad de la misma era considerada como valiosa para la organización en las áreas administrativas, por ejemplo el uso de gabinetes con candado para el almacenamiento de documentos importantes.

Con la introducción de las computadoras la necesidad de herramientas automatizadas para la protección de archivos y otra información almacenada fue evidente, especialmente en el caso de sistemas compartidos por ejemplo sistemas que pueden ser acezados vía telefónica o redes de información. El nombre genérico de las herramientas para proteger la información así como la invasión de Hackers es la seguridad computacional.

El segundo cambio que afectó la seguridad fue la introducción de sistemas distribuidos así como el uso de redes e instalaciones de comunicación para enviar información entre un servidor y una computadora o entre dos computadoras. Las medidas de seguridad de redes son necesarias para proteger la información durante su transmisión así como para garantizar que dicha información sea auténtica.

La tecnología utilizada para la seguridad de las computadoras y de las redes automatizadas es la encripción y fundamentalmente se utilizan la encripción convencional o también conocida como encripción simétrica, que es usada para la privacidad mediante la autentificación y la encripción public key, también conocida como asimétrica utilizada para evitar la falsificación de información y transacciones por medio de algoritmos basados en funciones matemáticas, que a diferencia de la encripción simétrica utiliza dos claves para la protección de áreas como la confidencialidad, distribución de claves e identificación.

El uso creciente de la tecnología de la información en la actividad económica ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados, con una relación de terminales por empleado que aumenta constantemente en todos los sectores industriales. Ello proviene de la importancia que la información y su gestión poseen en la actividad de cualquier empresa.

Cuando se estudia el ámbito de la información que un puesto de trabajo genera se encuentran modelos de distribución que indican que alrededor de un 90% de la información generada tiene como destino el propio departamento, un 75% está destinada a un punto distante no más de 200 metros del punto de generación, y hasta un 90% queda dentro del propio edificio, lo que sólo le concede un 10% a la información dirigida a destinos remotos. Independientemente del carácter estimativo de las cifras anteriores es evidente que un esquema de distribución como el mencionado, incita a acciones contundentes a optimizar la difusión de la información que se mueve en un ámbito local.

La reubicación física de los puestos de trabajo es una realidad connatural con el dinamismo de las empresas actuales. Esta movilidad lleva a unos porcentajes de cambio anual entre un 20 y un 50% del total de puestos de trabajo. Los costos de

traslado pueden ser notables (nuevo tendido para equipos informáticos, teléfonos, etc.). Por tanto, se hace necesaria una racionalización de los medios de acceso de estos equipos con el objeto de minimizar dichos costos. Las Redes de Área Local han sido creadas para responder a ésta problemática.

El éxito de las LAN reside en que cada día es mayor la cantidad de información que se procesa de una manera local, y a su vez mayor el número de usuarios que necesitan estar conectados entre sí, con la posibilidad de compartir recursos comunes. Por ejemplo, acceder a una base de datos general o compartir una impresora de alta velocidad.

El crecimiento de las redes locales a mediados de los años ochenta hizo que cambiase nuestra forma de comunicarnos con las computadoras y la forma en que los ordenadores se comunicaban entre sí. La importancia de las LAN reside en que en un principio se puede conectar un número pequeño de ordenadores que puede ser ampliado a medida que crecen las necesidades. Son de vital importancia para empresas pequeñas puesto que suponen la solución a un entorno distribuido.

4.4.1 Seguridad en cómputo.

Es posible enunciar que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

Existe una medida cualitativa para la Seguridad que dice "Un sistema es seguro si se comporta como los usuarios esperan que lo haga.

4.4.1.1 Propiedades de la información que protegen la seguridad informática.

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

4.4.1.1.1 Privacidad.

La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la Privacidad es la Divulgación de Información Confidencial.

4.4.1.1.2 Integridad.

La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

4.4.1.1.3 Disponibilidad.

La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o “tirar” el servidor.

4.4.2 Tipos de redes

Según el lugar y el espacio que ocupen, las redes, se pueden clasificar en dos

tipos:

Redes LAN (Local Área Network) o Redes de área local

Redes WAN (Wide Área Network) o Redes de área amplia

4.4.2.1 LAN - Redes de área local. Es una red que se expande en un área relativamente pequeña. Éstas se encuentran comúnmente dentro de una edificación o un conjunto de edificaciones que estén contiguos.

Así mismo, una LAN puede estar conectada con otras LANs a cualquier distancia por medio de línea telefónica y ondas de radio.

Pueden ser desde 2 computadoras, hasta cientos de ellas. Todas se conectan entre sí por varios medios y topología, a la computadora(s) que se encarga de llevar el control de la red es llamada "servidor" y a las computadoras que depende n del servidor, se les llama "nodos" o "estaciones de trabajo".

Los nodos de una red pueden ser PC´s que cuentan con su propio CPU, disco duro y software y tienen la capacidad de conectarse a la red en un momento dado; o pueden ser PC´s sin CPU o disco duro y son llamadas "terminales brutas", las cuales tienen que estar conectadas a la red para su funcionamiento.

Las LAN´s son capaces de transmitir datos a velocidades muy rápidas, algunas inclusive más rápido que por línea telefónica; pero las distancias son limitadas.

4.4.2.2 WAN - Redes de área amplia. Es una red comúnmente compuesta por varias LANs interconectadas y se encuentran en una amplia área geográfica. Estas LANs que componen la WAN se encuentran interconectadas por medio de líneas de teléfono, fibra óptica o por enlaces aéreos como satélites.

Entre las WANs mas grandes se encuentran: La ARPANET, que fue creada por la Secretaría de Defensa de los Estados Unidos y se convirtió en lo que es actualmente la WAN mundial: INTERNET, a la cual se conectan actualmente miles de redes universitarias, de gobierno, corporativas y de investigación.

4.4.3 Topologías de redes

La topología de una red, es el patrón de interconexión entre nodos y servidor, existe tanto la topología lógica (la forma en que es regulado el flujo de los datos), como la topología física (la distribución física del cableado de la red).

Las topologías físicas de red más comunes son:

Estrella.

Bus lineal

Anillo.

4.4.3.1 Topología de estrella.

Red de comunicaciones en que la que todas las terminales están conectadas a un núcleo central, si una de las computadoras no funciona, esto no afecta a las demás, siempre y cuando el "servidor" no esté caído.

4.4.3.2 Topología bus lineal.

Todas las computadoras están conectadas a un cable central, llamado el "bus" o "backbone". Las redes de bus lineal son de las más fáciles de instalar y son relativamente baratas.

4.4.3.3 Topología de anillo.

Todas las computadoras o nodos están conectados el uno con el otro, formando una cadena o círculo cerrado.

4.4.4 Componentes de una red

De lo que se compone una red en forma básica es lo siguiente:

4.4.4.1 Servidor (Server).

El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información.

Muchos de los servidores son "dedicados", es decir, están realizando tareas específicas, por ejemplo, un servidor de impresión solo para imprimir; un servidor de comunicaciones, sólo para controlar el flujo de los datos...etc. Para que una máquina sea un servidor, es necesario que sea una computadora de alto rendimiento en cuanto a velocidad y procesamiento, y gran capacidad en disco duro u otros medios de almacenamiento.

4.4.4.2 Estación de trabajo (Workstation).

Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable.

Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya dentro, se añade al ambiente de la red.

4.4.4.3 Sistema operativo de red.

Es el sistema (Software) que se encarga de administrar y controlar en forma general la red. Para esto tiene que ser un Sistema Operativo Multiusuario, como por ejemplo: Unix, Netware de Novell, Windows NT, etc.

4.4.4.4 Recursos a compartir.

Al hablar de los recursos a compartir, estamos hablando de todos aquellos dispositivos de Hardware que tienen un alto costo y que son de alta tecnología.

En estos casos los más comunes son las impresoras, en sus diferentes tipos: Láser, de color, plotters, etc.

4.4.4.5 Hardware de red.

Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serían básicamente las tarjetas de red (NIC-> Network Interfase Cards) y

el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos.

4.4.5 Transmisión de datos en la red

La transmisión de datos en las redes, puede ser por dos medios:

4.4.5.1 Terrestres. Son limitados y transmiten la señal por un conductor físico.

a) Cable par trenzado: Es el que comúnmente se utiliza para los cables de teléfonos, consta de 2 filamentos de cobre, cubiertos cada uno por plástico aislante y entrelazados el uno con el otro, existen dos tipos de cable par trenzado: el "blindado", que se utiliza en conexiones de redes y estaciones de trabajo y el "no blindado", que se utiliza en las líneas telefónicas y protege muy poco o casi nada de las interferencias.

b) Cable coaxial: Este tipo de cable es muy popular en las redes, debido a su poca susceptibilidad de interferencia y por se gran ancho de banda, los datos son transmitidos por dentro del cable en un ambiente completamente cerrado, una pantalla sólida, bajo una cubierta exterior. Existen varios tipos de cables coaxiales, cada uno para un propósito diferente.

c) Fibra óptica: Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen enormes capacidades de transmisión, del orden de miles de millones de bits por segundo. Además de que los impulsos luminosos no son afectados por interferencias causadas por la radiación aleatoria del ambiente. Actualmente la fibra óptica está remplazando en grandes cantidades a los cables comunes de cobre.

4.4.5.2 Aéreos. Son "ilimitados" en cierta forma y transmiten y reciben las señales electromagnéticas por microondas o rayo láser.

4.4.6 Seguridad en redes

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la aparición, y más aun, desde la globalización de Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

De lo anterior, los administradores de red han tenido la necesidad de crear políticas de seguridad consistentes en realizar conexiones seguras, enviar y recibir información encriptada, filtrar accesos e información, etc.

No obstante lo anterior, el interés y la demanda por Internet crecen y crece y el uso de servicios como World Wide Web (WWW), Internet Mail, Telnet y el File Transfer Protocol (FTP) es cada vez más popular.

El presente trabajo piensa dar una visión global acerca de los problemas de seguridad generados por la popularización de Internet, como las transacciones comerciales y financieras seguras, el ataque externo a redes privadas, etc.

Se trataran temas como el uso de firewalls, de llaves publicas (criptografía) y los niveles de seguridad establecidos en la actualidad.

4.4.6.1 Aplicaciones posibles en una empresa.

Tenemos que tener en cuenta que nuestra Intranet, esté o no conectada con el exterior es muy probable que alguien quiera entrar a ella. No importa lo pequeña o el poco valor que para nadie pueda tener. Simplemente un usuario mal intencionado puede intentar atacarla. Este será el primer punto de trabajo para tener segura nuestra red.

En el momento que estamos seguros que nadie puede entrar desde nuestra propia red, si esta está conectada a Internet o a otra red solo nos tendremos que preocupar de que lo que salga o entre de nuestra red sea lo que nosotros queramos que salga o entre. Básicamente estos son los conceptos que tenemos que tener muy claros desde el principio. No debemos dar mas importancia a la seguridad externa que a la interna. De nada nos servirá tener un Firewall perfectamente configurado si luego nuestros usuarios hacen lo que quieren entre ellos.

Tener siempre localizados todos los posibles problemas es algo que deberemos estudiar. Tener la posibilidad de escanear cualquier utilización de la red.

Siempre y antes de hacer cualquier tipo de trabajo con respecto a la seguridad de una red hay que sentarse a planear el trabajo a realizar. Tener muy claro desde el principio todo es fundamental para conseguir un trabajo "limpio". Evitando después "apagar fuegos". Una cosa es que deje de funcionar un servidor y por falta de previsión no haya nadie para repararlo y otra cosa es enterarnos que han entrado y se han llevado datos confidenciales de nuestra empresa.

Cada vez más se tiende a utilizar los recursos que nos proporciona Internet para nuestro negocio. Cualquier red, por pequeña que sea tendrá la necesidad urgente de utilizar e-mail, Web, ftp, etc. por motivos técnicos o estéticos. O en el peor de los casos, nuestra propia red da información a todo el que la quiera en Internet.

Cuando instalamos un router, un proxy y servidores de servicios Internet en nuestra red, abrimos una puerta al exterior. Cuando instalamos un módem para que uno de nuestros usuarios se conecte a la red interna, trabajando en forma remota desde cualquier sitio. Cuando nuestra red tiene que fusionarse con otra en otra delegación, etc.

Reglas generales para evitar intromisiones:

9	Mínimos espacios por donde salir o entrar.
10	Mínimos recursos accesibles desde fuera.
11	Mínima importancia de datos con posibilidad de robo.
12	Máximos controles entre nuestra red y la red exterior.

Evidentemente la única regla que no se puede cambiar es la primera. Si la importancia de los recursos que dejamos accesibles aumenta, también tendrá que aumentar los recursos que se necesiten para asegurar dichos recursos.

Pongamos por ejemplo que nuestra empresa quiere hacer "comercio electrónico", tomando pedidos por medio de métodos de pago electrónicos. Tendremos en nuestro poder números de tarjetas de crédito y datos confidenciales de clientes. Nuestra empresa tendrá que hacer marketing para darse a conocer en la red, y ese mismo marketing servirá para que gente inquieta quiera intentar sacar datos de los que compran en nuestra empresa virtual.

En este caso podemos dejar solo a la vista el servidor Web, donde nos podrán leer datos confidenciales, pero siempre entrando por un estrecho lugar en el que se encuentra un firewall. Nuestro servidor estará certificado y registrado por todos los sistemas de cifrado que se encuentren en el mercado "Verisign, Integrión, RSA, SSL etc..." y todo el que entre o salga estará auditado por el Firewall.

Hay que tener en cuenta que muchas veces no solo damos servicios de Web, y los damos de e-mail, ftp, das, tftp, cgi etc.. Todo esto es posible que algún día nos dé problemas por lo que auditaremos absolutamente todo.

4.4.6.2 Niveles De Seguridad.

De acuerdo con los estándares de seguridad en computadoras desarrollado en el libro naranja del Departamento de Defensa de Estados Unidos, se usan varios

niveles de seguridad para proteger de un ataque al hardware, al software y a la información guardada.

4.4.6.2.1 Nivel D1.

Es la forma más elemental de seguridad disponible, o sea, que el sistema no es confiable. Este nivel de seguridad se refiere por lo general a los sistemas operativos como MS-DOS, MS-Windows y System 7.x de Apple Macintosh. Estos sistemas operativos no distinguen entre usuarios y tampoco tienen control sobre la información que puede introducirse en los discos duros.

4.4.6.2.2 Nivel C1.

El nivel C tiene dos subniveles de seguridad: C1 y C2. El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad disponible en un sistema típico Unix. Los usuarios deberán identificarse a sí mismos con el sistema por medio de un nombre de registro del usuario y una contraseña para determinar qué derechos de acceso a los programas e información tiene cada usuario.

4.4.6.2.3 Nivel C2.

Junto con las características de C1, el nivel C2 tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso de algunos archivos basados no sólo en permisos, sino en niveles de autorización. Además requiere auditorias del sistema. La auditoria se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema. La auditoria requiere autenticación y procesador adicional como también recursos de disco del subsistema.

4.4.6.2.4 Nivel B1.

El nivel B de seguridad tiene tres niveles. El nivel B1, o protección de seguridad etiquetada, es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultra secreta. Parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

4.4.6.2.5 Nivel B2.

Conocido como protección estructurada, requiere que se etiquete cada objeto como discos duros, terminales. Este es el primer nivel que empieza a referirse al

problema de comunicación de objetos de diferentes niveles de seguridad.

4.4.6.2.6 Nivel B3.

O nivel de dominios de seguridad, refuerza a los dominios con la instalación de hardware. Requiere que la Terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

4.4.6.2.7 Nivel A.

Nivel de diseño verificado, es el nivel más elevado de seguridad. Todos los componentes de los niveles inferiores se incluyen. Es de distribución confiable, o sea que el hardware y el software han sido protegidos durante su expedición para evitar violaciones a los sistemas de seguridad.

4.4.6.2.8 Criptografía.

La criptografía robusta sirve para proteger información importante de corporaciones y gobiernos, aunque la mayor parte de la criptografía fuerte se usa en el campo militar. La criptografía se ha convertido en un gran negocio últimamente ya que es una de las pocas defensas que pueden tener las personas en una sociedad vigilante.

4.4.6.3 Terminología básica.

El mensaje es llamado plaintext ó cleartext.

La codificación del mensaje es llamada encriptamiento.

El mensaje encriptado es llamado texto cifrado.

El proceso de recuperar el texto original del texto cifrado es llamado desencriptamiento.

El encriptamiento y el desencriptamiento requieren el uso de una llave y un método de codificación de tal forma que el método de encriptamiento pueda ser modificado únicamente por el usuario.

El criptoanálisis es la ciencia de descubrir el contenido de los mensajes cifrados.
La criptografía trata el manejo de los mensajes de seguridad, firmas digitales, dinero electrónico, etc.

La criptología es una rama de las matemáticas que se encarga de estudiar las bases de los métodos criptagráficos.

4.4.6.3.1 Algoritmos básicos de criptografía.

Todos los algoritmos modernos utilizan una llave para el encriptamiento y desencriptamiento, un mensaje puede ser desencriptado únicamente si la llave de encriptamiento hace juego con la llave de desencriptamiento, para efectos prácticos pueden o no ser la misma; aunque el algoritmo las ve como la misma.

Hay dos tipos de algoritmos básicos de encriptamiento. El algoritmo simétrico o llave secreta y el asimétrico o llave publica, con la diferencia que el simétrico utiliza la misma llave o una derivada de la original y el asimétrico usan llaves deferentes para el encriptamiento y el desencriptamiento y la llave secundaria en derivada de la primer. Los algoritmos simétricos pueden ser divididos en bloques y cadenas cifradas, las cadenas cifran bit a bit y los bloques cifran grupos de bits (64 normalmente) como una unidad simple.

Los cifrados asimétricos pueden tener la llave de desencriptamiento pública, pero la de encriptamiento es privado.

4.4.6.3.2 Firmas digitales.

Son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave publica; son utilizados principalmente para verificar la autenticidad del mensaje o la de una llave publica. En una estructura distribuida se necesita una llave principal o raíz de conocimiento publico y cada grupo define un grupo de llaves particulares autenticables con la llave principal este es el concepto que maneja los sistemas PGP.

4.4.6.3.3 Algoritmos de mezcla de funciones y por generación de números aleatorios.

En los algoritmos por mezcla de funciones se definen por el usuario o de forma automática una secuencia de funciones de encriptamiento determinada de modo que la única forma de desencriptar el mensaje sea corriendo la misma rutina con sus correspondientes llaves en el encriptamiento por generación de números aleatorios se generan una serie de llaves numéricas de forma aleatoria que son usadas de forma automática por el ente de encriptamiento y el de desencriptamiento. Hay sistemas de criptografía que son teóricamente inviolables pero que en la realidad no se puede probar, un sistema de criptografía robusto puede ser implementado de forma sencilla en la que la habilidad del creador es el que determina su confiabilidad, las llaves pueden ser halladas por la fuerza

pasando todas las posibles combinaciones de las mismas así las llaves de 32 bits toman 232 pasos para ser barridas por completo; se ha determinado que las llaves de 128 bits son lo suficientemente confiables como para no requerir de mas bits en la llave.

Aunque la longitud de la llave no es el punto más relevante en la seguridad del criptograma ya que este puede roto de otra forma.

4.4.6.4 Firewalls.

Un firewall es un sistema o un grupo de sistemas que decide que servicios pueden ser accesados desde el exterior (Internet, en este caso) de un red privada, por quienes pueden ser ejecutados estos servicios y también que servicios pueden correr los usuarios de la intranet hacia el exterior (Internet). Para realizar esta tarea todo el tráfico entre las dos redes tiene que pasar a través de él.

El firewall solo dejar pasar el tráfico autorizado desde y hacia el exterior. No se puede confundir un firewall con un enrutador, un firewall no direcciona información (función que si realiza el enrutador), el firewall solamente filtra información. Desde el punto de vista de política de seguridad, el firewall delimita el perímetro de defensa y seguridad de la organización. El diseño de un firewall, tiene que ser el producto de una organización conciente de los servicios que se necesitan, además hay que tener presentes los puntos vulnerables de toda red, los servicios que dispone como públicos al exterior de ella (WWW, FTP, telnet, entre otros) y conexiones por módem (dial-in módem calling).

4.4.6.4.1 Beneficios de un firewall.

Los firewalls manejan el acceso entre dos redes, si no existiera todos los hosts de la intranet estarían expuestos a ataques desde hosts remotos en Internet. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador de la red escogerá la decisión si revisar estas alarmas o no, la decisión tomada por este no cambiaría la manera de operar del firewall.

Otra causa que ha hecho que el uso de firewalls se halla convertido en uso casi que imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones CIRD (o direcciones sin clase), las cuales salen a Internet

por medio de un NAT (Network address traslator), y efectivamente el lugar ideal y seguro para alojar el NAT ha sido el firewall.

Los firewalls también han sido importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido mas en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor ancho de banda.

Finalmente, los firewalls también son usados para albergar los servicios WWW y FTP de la intranet, pues estos servicios se caracterizan por tener interfaces al exterior de la red privada y se ha demostrado que son puntos vulnerables.

4.4.6.4.2 Limitaciones del firewall.

La limitación mas grande que tiene un firewall sencillamente es el hueco que no se tapa y que coincidencialmente o no, es descubierto por un hacker. Los firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo dejara pasar. Pero este no es lo más peligroso, lo verdaderamente peligroso es que ese hacker deje "back doors" es decir abra un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el firewall "no es contra humanos", es decir que si un hacker logra entrar a la organización y descubrir passwords o se entera de los huecos del firewall y difunde la información, el firewall no se dará cuenta.

Es claro que el firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus.

4.4.6.4.3 Componentes de un firewall.

•Un enrutador que sirva única y exclusivamente de filtro de paquetes.
•Un servidor proxy o gateway a nivel de aplicación (debido al costo, implementado comúnmente en una maquina linux).
•El gateway a nivel de circuito.

4.4.6.5 Cómo diseñar una política de seguridad para redes.

Antes de construir una barrera de protección, como preparación para conectar su red con el resto de Internet, es importante que usted entienda con exactitud qué recursos de la red y servicios desea proteger. Una política de red es un

documento que describe los asuntos de seguridad de red de una organización. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

5. METODOLOGÍA DE DESARROLLO

5.1 PARTICIPANTES.

ESTUDIANTES DE TECNOLOGÍA EN REDES DE COMPUTADORES Y SEGURIDAD INFORMÁTICA:

JORGE ELIECER NUÑEZ CARDOSO, estudiante de la Corporación Universitaria Minuto de Dios, sexto semestre de Tecnología en Redes de Computadores y Seguridad Informática 2008-II.

DAIVER HALYD TERREROS DAZA, estudiante de la Corporación Universitaria Minuto de Dios, sexto semestre de Tecnología en Redes de Computadores y Seguridad Informática 2008-II.

5.2 MATERIALES.

En el desarrollo del proyecto se observara y vera la evidencia en la red de computadores de los laboratorios de la Universidad Minuto de Dios sede Girardot, donde se instalara el firewalle (MIKROTIK RouterOs), además será donde se desarrollara los laboratorios o practicas de ataques a la red y obviamente la configuración y puesta en marcha del Mikrotik, se harán uso de las herramientas y dispositivos de los laboratorios antes mencionados como lo son el switche, el router, probador de cables, "ponchadora", y el uso de servicios como el de Internet.

CANT.	DESCRIPCIÓN	VALOR UNITARIO	VALOR TOTAL
2	Resmas de Papel	$ 9.000	$ 18.000
100	Fotocopias	$ 100	$ 10.000
500	Impresiones	$ 200	$ 100.000
60hr	Sevicio de Internet	$ 800	$ 48.000
4	CD's	$ 1.000	$ 50.000
50 hr	Instalación del Mikrotik	$ 50.000 hr	$ 2'500.000
		TOTAL	**$ 2'726.000**

5.3 PROCEDIMIENTO.

Para el desarrollo del presente proyecto se ha tenido en cuenta la utilización de el siguiente modelo o ciclo vital, en este caso el ciclo de vida lineal, puesto que es el más utilizado en el desarrollo de proyectos e investigaciones, además este modelo permite que en sus diferentes fases de evolución y desarrollo, se cumplan a cabalidad una sola vez y sin margen de errores, todas las actividades planteadas, en orden jerárquico para que en el momento de verificar el desempeño del producto, este no presente fallas.

5.3.1 Diagnostico situacional.

Actualmente la corporación Universitaria Minuto de Dios, se encuentra en el desarrollo y construcción de nuevos laboratorios "Laboratorios para los alumnos de Tecnología en Redes, Tecnología en Electrónica, y Laboratorio para alumnos de Ingeniería Civil", los cuales serán terminados de construir antes del año 2009, y cuya infraestructura contara con mas de 20 equipos, los cuales servirán de apoyo para los estudiantes de estas especialidades, pero como se sabe para los laboratorios es necesario implantar una seguridad, a nivel de software claro, y es por tal motivo que se ve en la necesidad de desarrollar e implementar medidas de seguridad, para proteger la información y el acceso de sus usuarios y/o directivos, pues las medidas no se han desarrollado ni planeado, pues los laboratorios están en proceso de desarrollo.

5.3.2 Descripción de las actividades.

Las actividades para dar comienzo a la ejecución de este proyecto, están divididas en módulos, módulos que están presentes en el siguiente plan de actividades y cuyo fin es proporcionar una visión mucho mas amplia de lo que se realizara durante la ejecución de este proyecto, es primordial y relevante dar a conocer que en estas actividades se ha tomado el modulo dos(2) y tres(3) como los más importantes, en el desarrollo de este proyecto pues son las fases en las que hay que tener en cuenta y fijar las necesidades que ha de llevar la configuración de esta Red y sus laboratorios.

Modulo 1. Revisión Producto (Software Mikrotik).

N°	Actividad	Descripción	Responsables
1	Revisión producto entregado por la Universidad (Verificar que contenga los	En el momento de entrega del producto, este será verificado, para poder establecer que cumpla sus características aparentes y	**Mauricio Rodríguez Jorge Núñez**

	elementos especificados en la orden de compra).	su categoría.	**Daiver Terreros.**
2	Pruebas iníciales a nivel de funcionalidad (Verificación que el software funcione, su desempeño y las capacidades que pueda realizar).	Se llevara a cabo la pertinente configuración e instalación a nivel de red, esto con la finalidad de observar y verificar que sus funciones son las requeridas.	**Mauricio Rodríguez Jorge Núñez Daiver Terreros.**
3	Configuración de software (Mikrotik) a nivel de direccionamiento IP.	Se realizara la respectiva configuración a nivel de direccionamiento, para establecer funciones y permisos pertinentes en el momento en que el software este en funcionamiento.	**Mauricio Rodríguez Jorge Núñez Daiver Terreros.**

Modulo 2 . Configuración y selección de complementos y procesos para el funcionamiento del software.

N°	Actividad	Descripción	Responsables
1	Configuración e instalación de complementos para Mikrotik (Establecer que complementos serán acordes para la seguridad y administración de la Red.	Se hará un listado y revisión de los diferentes complementos que se implantaran y configuraran para controlar y brindar la seguridad en la Red.	**Jorge Núñez Daiver Terreros.**
2	Determinación y establecimiento de procesos a seguir en la configuración de el Mikrotik (Filtrado, Controlo de acceso, Control ancho de banda, Listas de acceso, Listas negras).	Se otorgaran las funciones que estará desempeñando el software para la red y su seguridad.	**Jorge Núñez Daiver Terreros.**

Modulo 3 . Pruebas Funcionamiento del Software.

N°	Actividad	Descripción	Responsables
1	Verificación del funcionamiento, rendimiento y funcionalidad del software en la Red.	Se verificara mediante pruebas, a nivel de práctica, si los parámetros establecidos cumplen con la configuración propuesta.	**Jorge Núñez Daiver Terreros.**

Modulo 4 . Entrega de Producto.

N°	Actividad	Descripción	Responsables
1	Entrega de Producto (Software ya configurado, contraseñas usadas y explicación de acceso y configuración de funciones).	Se hará la entrega del producto en funcionamiento, al igual que contraseñas usadas para esto, además se dará una explicación de cómo acceder y modificar las funciones.	**Jorge Núñez Daiver Terreros.**

5.3.3 Planificación.

Las actividades o módulos se han planeado, de acuerdo a las necesidades y orden jerárquico, que se debe tener en cuenta en el momento de hacer un análisis y configuración de un producto, en este caso el software Mikrotik.

5.3.4 Análisis.

En la planificación de las actividades, y teniendo en cuenta que lo primero que se debe establecer a la hora de la adquisición de un producto es revisar sus capacidades y desempeño, en este caso para la Red y para su seguridad, se ha visto un poco estancado la realización de este proyecto, pues durante la adquisición de este producto se han detectado fallas como:

- No contaba con su respectivo manual de configuración, manual (Mikrotik) que es necesario para determinar y evitar cualquier anomalía que se pueda presentar a nivel presente o futuro.

- No poseía su antena para los usuarios inalámbricos.

- Además presenta fallas a nivel de sistema operativo.

Lo cual es causal de grandes [37] inconvenientes y retrasos en el desarrollo de este proyecto, por lo tanto se ha avanzado en la realización de este proyecto con las herramientas disponibles en el mercado y la Universidad (Demostraciones de el Sistema Operativo).

5.3.5 Diseño.

La finalidad de este proyecto es la configuración del Firewall Mikrotik RouterOS, el cual brindara los servicios de seguridad, así como otros adicionales, para la protección e integridad de la red en los laboratorios, como este Router posee tres salidas Ethernet, una vez listo, este se conectara a nuestros swichs, para que este se encargue de darles la salida a internet y protección a los usuarios de la Red, otra de las salidas se destinara para la parte inalámbrica, y finalmente su ultima Ethernet será destinada para nuestro Router, la cual le otorgara salida a internet.

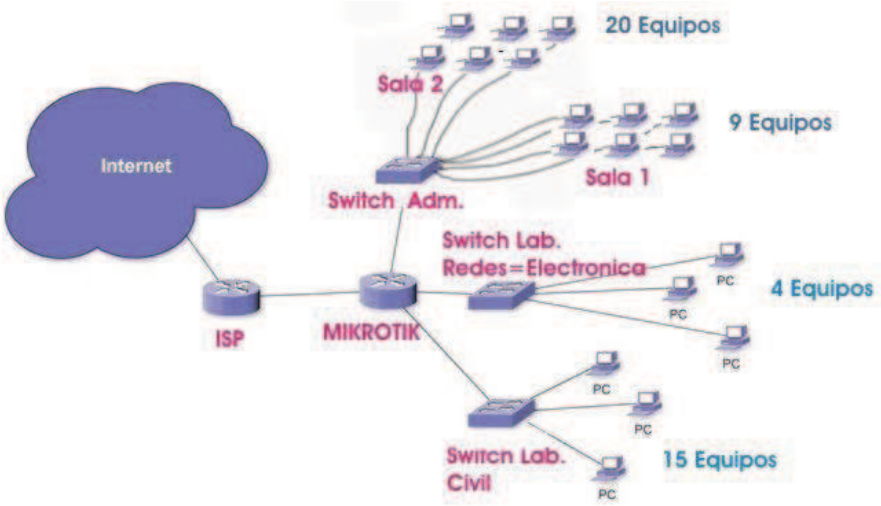

Fig. 1 Diseño para Red Cableada.

Fig. 2 Diseño para Red Inalámbrica.

5.3.6 Desarrollo.

El desarrollo de estas actividades se ha determinado, y ha comenzado teniendo en cuenta el orden de los módulos establecidos en el plan de actividades, cada actividad cuenta con un tiempo establecido, el cual está fijado en el cronograma, para el desarrollo de este proyecto.

5.3.7 Documentación.

Durante el desarrollo parcial de las actividades del modulo 1, la documentación de estas ha sido nula, pues no se encuentra la necesidad de establecerla, pues esta ya se ha evidenciado, y ve reflejada con la orden de compra del producto (Software Mikrotik), para esto solamente es necesario comparar la orden de compra del producto, con las características de este.

Cotización de los siguientes artículos (Mikrotik y complementos):

ROUTER BOARD 433……	$590.000
TARJETA MINIPCI 2.4, 5GHZ…….	$160.000
CAJA ORIGINAL MIKROTIK……	$99.000

MINIPIGTAIL UF.L ‘RPSMA… $39.000
ANTENA 5DBI OMNI.... $30.000

Los valores NO incluyen el IVA
Tiempo de Entrega 1 semana
Garantia 3 meses

Incluye Mikrotik Routr OS L4

Pero por consiguiente para las actividades que se desarrollan a partir del modulo 2, es necesario llevar una documentación, documentación que será fijada y presentada como anexo, esto con el fin de dejar prueba de la culminación de las actividades, en este caso, el manual para su configuración.

6. CONCLUSIONES

Del análisis y los resultados se concluye que la Universidad Minuto de Dios debería hacer una reestructuración de su red informática. Debido a el constante crecimiento en cuanto a los usuarios, además el conocimiento de estos mismos crece cada vez mas en cuanto a las nuevas formas de evasión de la seguridad.

Una de la mas grande de las satisfacciones, que obtuvimos en el trascurso de este proyecto, se evidencia en los conocimientos obtenidos, y los resultados que deseábamos para la configuración de este RouterOS, en este caso:

- Se definió la configuración de las interfaces. Asignando nombres, direcciones de IP a las mismas y definición de las Vlan.

- Para la implementación de la seguridad en la red se utilizó el sistema operativo Mikrotik RouterOS basado en Linux. El mismo convierte una PC Standard en un router dedicado de alto rendimiento.

- Se configuró el servidor de DHCP para cada una de las sub redes. En el cual se definieron los pools de ip para cada una. También la asignación de direcciones de IP fijas a partir de direcciones MAC de los servidores.

- Se configuró un servidor NTP para sincronizar la hora dentro de toda la red.

- También se configuro un cliente NTP para sincronizar la hora de la red con otros servidores de tiempo.

- Se configuró un servidor de Web Proxy para optimizar la utilización de los recursos hacia Internet. En el mismo se configuro politicas de bloqueo de tráfico hacia ciertas páginas al igual que el bloqueo de descarga de ciertos archivos.

- Se realizaron políticas de control de ancho de banda para los clientes P2P y mensajera.

- Se implemento políticas de firewall como bloqueo de p2p, bloqueo del Msn Messenger, redireccionamiento de puertos y bloqueo de paquetes no deseados.

- Se configuró un Hot Spot en el RouterOS mediante el cual los usuarios se autentican mediante un servidor Radius.

7. GLOSARIO.

Black-list: es una lista donde se registran las direcciones IPs que generan spam de forma voluntaria o involuntaria, Las blacklist son libres de tal forma que alguno de manera malintencionada puede añadir IPs *inocentes* e impedir que lleguen correos válidos.

Crackers: Individuo con amplios conocimientos informáticos que desprotege, piratea programas o produce daños en sistemas o redes.

Criptología: Es el estudio de los criptosistemas, sistemas que ofrecen medios seguros de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo. Sus áreas principales de estudio son la criptografía y el criptoanálisis, pero también se incluye la esteganografía como parte de esta ciencia aplicada.

DHCP: Dynamic Host Configuration Protocol. Método que asigna automáticamente direcciones IP a clientes de una red.

DNS: Domain Name System. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Encripción: (Cifrado, codificación), La encriptación o encripcion es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Hackers: Expertos en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones, generalmente están solucionando problemas o fallas en los sistemas.

Firewall: Literalmente " Muro de Fuego". Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

Firmas digitales: Es un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje, garantizar que no se pueda modificar su contenido.

Ftp : File Transfer Protocol. Protocolo de Transferencia de Ficheros. Uno de los protocolos de transferencia de ficheros mas usado en Internet.

Gateway: Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red. En Español: Pasarela.

HotsPot: (punto caliente). Los Hotspots son los lugares que ofrecen acceso Wi-Fi, que pueden ser aprovechados especialmente por dispositivos móviles como notebooks, PDAs, consolas, para acceder a internet.

Informática: Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos y sistemas informáticos.

IP: Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de Internet. También se refiere a las direcciones de red Internet.

IPIP: Instituto de Prevención del Delito e Investigación Penitenciaria.

IPsec: (IP security). Conjunto de protocolos para la seguridad en comunicaciones IP mediante la autentificación y/o encriptación de cada paquete IP.

Keylogger: Registrador de pulsaciones de un teclado que se incorporan físicamente en un teclado para registrar todas las pulsaciones que se realizan sobre el mismo.

La Internet: Conocida como la red de redes, pues se trata de una de las redes más grandes con un estimado de mil cien millones de usuarios, la cual para funcionar utiliza el conjunto de protocolos TCP/IP.

LAN: Local Area Network. Red de Area Local. Red de ordenadores de reducidas dimensiones. Por ejemplo una red distribuida en una planta de un edificio.

Licencia: El conjunto de permisos que un desarrollador da para la distribución, uso o modificación de la aplicación que desarrolló o posee. Puede indicar en esta licencia también los plazos de duración, el territorio donde se aplica.

LINUX: Versión Shareware del conocido sistema operativo *Unix*. Es un sistema multitarea multiusuario de 32 bits para PC.

Mikrotik: Es una compañía de Letonia que manufactura principalmente routerboards (Placas Ruteadores) o encaminadores es conocido por el software que lo controla el RouterOS.

NTP: Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

Plaintex: Sistema de composición de textos de alta calidad, en particular para aquellos que contienen una gran cantidad de expresiones matemáticas creado por Donald Knuth.

P2p: (peer-to-peer sharing). Red descentralizada que no tiene clientes ni servidores fijos, sino que tiene una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red.

Pishing: El phishing es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc. El objetivo más común, suele ser la obtención de dinero del usuario que cae en la trampa.

Pop: (Post Office Protocol) Protocolo de Oficina de Correos. Protocolo utilizado para recibir correo electrónico.

Pptp: Es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

Una VPN es una red privada de computadores que usa Internet para conectar sus nodos. PPTP ha sido crackeado o descifrado, no debería usarse donde la privacidad de los datos sea importante.

Proxy: El Proxy es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

Router: Enrutador, encaminador. Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

RouterOs: Es un sistema operativo basado en Linux, Permite a los usuarios convertir un ordenador personal PC en un router, lo que permite funciones como firewall, VPN Server y Cliente, Gestor de ancho de banda, QoS, punto de acceso inalámbrico y otras características comúnmente utilizado para el enrutamiento y la conexión de redes.

Routing: Routing o encaminamiento, se refiere a la selección del camino en una red de computadoras por donde se envían datos.

SMTP: Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles).

Software: En computación, todo programa o aplicación, programado para realizar tareas específicas.

Spam: Se llama así al "bombardeo" con correo electrónico, es decir, mandar grandes cantidades de correo o mensajes muy largos.

Spiware: Software espía. Cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando. Es un tipo de malware que por lo general se introduce y opera en las PCs sin que el usuario lo advierta.

Spoofing: Este hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Telnet: Conexión a un Host en la que el ordenador cliente emula un Terminal de manera que se configura como Terminal virtual del ordenador servidor.

Tracert: Utilidad que traza el camino que hace un paquete desde una computadora hasta un otra en internet (generalmente un servidor), mostrando el tiempo que tarda en ir de un lado al otro y los saltos (hops) que da durante el camino.

Unix: Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas más conocidos como MS-DOS están basadas en este sistema muy extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

User-manager: Es un administrador de usuario es un sistema de gestión que pueden utilizarse para: HotSpot users; PPP (PPtP/PPPoE) users; DHCP users; Wireless users; RouterOS users.

Vlan: Es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único

conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.

WAN: (Wide Area Network - Red de Área Extensa). WAN es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso en el ámbito planetario.

Winbox: Es una aplicación de redes para Windows, que envía y recibe e-mails utilizando los protocolos más conocidos en Internet. Más técnicamente, Winbox es un estándar POP3, IMAP 2, 3 y 4, SMTP y opcionalmente (activándolo desde el archivo winbox.ini) es un simple NNTP (para leer News de Usenet), Finger, Buscador de IPs, Time y cliente Echo.

WLAN: Wireless Local Area Network Red de comunicación inalámbrico por radio frecuencia alternativa a las LAN con cables.

WWW: WEB o W3 World Wide Web. Telaraña mundial, para muchos la WWW es Internet, para otros es solo una parte de esta. Podríamos decir estrictamente que la WEB es la parte de Internet a la que accedemos a través del protocolo http.

BIBLIOGRAFÍA

- Mikrotik 2008. “Documentation Site”: http://www.mikrotik.com/testdocs/ros/2.9/ (citado 10 Noviembre, 2008).

- Mallery, John; Zann, Jason; Kelly, Patrick. ”Blindaje de Redes”. 1ra Edicion.
España. Anaya Multimedia. (720 pag)

- Mikrotik 2007. “Manual de referencia”. <http://www.mikrotik.com/testdocs/ros/2.9/> (citado 10 de noviembe, 2008)

- Mikrotik 2009: http://www.mikrotik.com/
(citado 10 Noviembre, 2008).

- Prabhaker Mateti: http://www.yoled.com/ys_htm_art_portscan.php
(citado 12 Noviembre, 2008).

- Red Hat Enterprise Linux 4: Manual de seguridad: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-server-ports.html
(citado 12 Noviembre, 2008).