DEFINICIÓN DE UN MODELO DE SEGURIDAD PARA LA RED DE INVESTIGACIÓN DE TECNOLOGÍA AVANZADA DE LA UNIVERSIDAD DISTRITAL "FRANCISCO JOSÉ DE CALDAS" RITA-UD

DECIDING ON A SECURITY MODEL FOR THE ADVANCED-TECHNOLOGY AND RESEARCH NETWORK AT UNIVERSIDAD DISTRITAL (RITA-UD)

Abstract
One of the most important aspects of networking involves the protection of Information. This paper identifies the most important aspects to be considered when defining a security model for the Advanced-Technology and Research Network at Universidad Distrital (RITA-UD) based on the implementation of ISO27001 and NTC-ISO /IEC17799 standards. The final design is a proposal to implement a Cisco ASA5520 Firewall.

Keywords: Integrity, confidentiality, availability, information security, ISMS.

Resumen
Uno de los aspectos más importantes dentro de las networking se relaciona con la protección de la información. Este trabajo permite identificar los aspectos más importantes a considerar en la definición de un modelo de seguridad para la red de investigación de tecnología avanzada de la Universidad Distrital Francisco José de Caldas RITA-UD basado en la aplicación de las normas ISO27001 y NTC-ISO/IEC17799.El diseño final obtenido es una propuesta para la implementación de un Firewall Cisco ASA5520.

Palabras clave: Integridad, confidencialidad, disponibilidad, seguridad de la información, SGSI.

Danilo E. Rodriguez
Estudiante de Ingeniería Electrónica de la Universidad Distrital "Francisco José de Caldas".
dadtear@hotmail.com

Carlos A. Junca
Estudiante de Ingeniería Electrónica de la Universidad Distrital "Francisco José de Caldas".
carlos.a.junca@hotmail.com

Hector C. Manta
Ingeniero Electrónico, MSc. en Ciencias de la Información y las Comunicaciones de la Universidad Distrital "Francisco José de Caldas".
hcmantac@udistrital.edu.co

Diego F. Rocha
Ingeniero Electrónico, MSc (c) en Ciencias de la Información y las Comunicaciones de la Universidad Distrital "Francisco José de Caldas".
dfrochaa@correo.udistrital.edu.co

Tipo: Artículo de reflexión

Fecha de Recepción: Febrero 7 de 2011
Fecha de Aceptación: Mayo 10 de 2011

1. INTRODUCCIÓN

En ambientes empresariales e institucionales actuales, cobra mucha importancia el hecho de tener una red segura, rápida y confiable. De hecho, estudios revelan y comprueban los grandes costos que se están presentando por concepto de pérdidas de tiempo en las conexiones de los usuarios a los servicios provistos por la red, y especialmente, por accesos no autorizados y ataques externos o internos a las redes.

Para hacer frente a los problemas anteriormente mencionados en redes de datos, es indispensable definir de manera clara y precisa la topología de la red y los servicios asociados a esta, de tal forma que respondan a unos criterios de diseño adecuados y se guíen bajo rigurosos estándares de calidad.

Además es de suma importancia definir un modelo de seguridad compatible con la red que permita tener un control completo en materia de acceso tanto de usuarios como de información.

La red RITA-UD conectada a la red externa RUMBO, presenta las mismas características de una red privada conectada al servicio de Internet. En consecuencia, se debe poseer un modelo de seguridad que permitaque la red RITA-UD tenga un uso racional de los servicios que presta a los diferentes usuarios conectados y disminuya los costos asociados a tiempos perdidos por demoras en la red.

Esto se logra a partir del diseño e implementación del modelo de seguridad, que aquí se plantea, estructurado mediante la definición y/o ajuste de las políticas, normas y procedimientos de seguridad existentes dentro de la Universidad Distrital, aplicando los parámetros establecidos en la norma ISO27001 y las recomendaciones contenidas en la NTC-ISO/IEC 17799, de tal forma que se garantiza la prestación de todos los servicios a todos sus funcionarios y estudiantes, de manera que la información está disponible en el momento requerido, tienen acceso sólo las personas autorizadas y se conserva íntegra y no se ve alterada en forma descontrolada e inadecuada, ya sea, por agentes internos o externos a la red.

2. REDES ACADÉMICAS

En razón al desarrollo comercial que ha tenido Internet, en primera instancia pensado y diseñado con fines académicos y de intercambio de información, se han venido desarrollando, a nivel mundial, diferentes proyectos con el objetivo de implementar una serie de redes con fines académicos que permitan retomar la idea inicial de internet y establecer un efectivo mecanismo de colaboración científica y de tecnología, que se mantenga al margen de información de tipo comercial que es el tipo de información predominante en la actualidad.

El objetivo de la creación de las redes académicas es llegar a interconectar organizaciones a nivel mundial que se encarguen de permitir que las networks nacionales puedan establecer conexión con redes colegas en el resto del planeta.

Para lograr este objetivo de trabajo conjunto, las diferentes Redes Regionales establecen consorcios que permiten su interconexión a través de enlaces interoceánicos de muy alta velocidad (de orden superior a los 10 Gbps) alcanzando de esta forma un verdadero entorno de cooperación global.
En Colombia la red de investigación que nos representa a nivel mundial se llama RENATA (Red Nacional de Tecnologías Avanzadas) e inmersa en ella se encuentra la red distrital llamada RUMBO (Red Universitaria Metropolitana de Bogotá). La Universidad Distritalestá desarrollando RITA-UD (Red de Investigación y Tecnología Avanzadade la Universidad Distrital)que se encargará de conectarse a RUMBO y a su vez a Colombia y el mundo.

3. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un SGSI (sistema de gestión de la seguridad de la información) o en inglés ISMS (Information Security Management System) es un conjunto de políticas de administración de la seguridad de la información. El término es utilizado principalmente por la norma ISO/IEC 27001 y es el concepto principal sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Los aspectos claves de un SGSI son, para la organización, el diseño, implantación, mantenimiento y mejora de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información [1].

Al igual que todos los sistemas de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno [2].

Debido a que certificar un nivel de aseguramiento de la información total es virtualmente imposible, incluso si se dispusiera de recursos ilimitados; el propósito de un sistema de gestión es, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y las tecnologías. Teniendo en cuenta este estándar de seguridad y los diferentes riesgos, se planteó el diseño del perfil de seguridad.

4. METODOLOGÍA DE DISEÑO

El diseño del perfil se elabora con la seguridad necesaria para proteger la infraestructura y proporcionar un ambiente seguro para el intercambio de información. Existen una serie de tecnologías de seguridad de red y productos que están estratégicamente en toda la red para proteger a los empleados y a los activos de una empresa, y así garantizar la confidencialidad de los datos sensibles, y la disponibilidad e integridad de los sistemas y de los datos.

La Universidad no es inmune a la violencia, robo, vandalismo y otras amenazas. La adopción de la colaboración en red y tecnologías basadas en Internet también abre la posibilidad de una serie de amenazas cibernéticas.

Entender la naturaleza y la diversidad de estas amenazas, y cómo pueden evolucionar con el tiempo, es el primer paso hacia una estrategia de seguridad exitosa. Las siguientes son algunas de las amenazas comunes a cualquier entorno que el diseño contrarresta:

Servicio de Interrupción: Las interrupciones a la infraestructura, aplicaciones y otros recursos del negocio causadas por botnets, gusanos, malware, adware, spyware, virus, denegación de servicio (DoS), y ataques de capa 2.

Abuso de la red: El uso de aplicaciones no autorizadas; compartir archivos punto a punto, el abuso de mensajes instantáneos y acceso a contenidos no relacionados con el negocio.

Acceso no autorizado: Las intrusiones, los usuarios no autorizados, escalada de privilegios y acceso no autorizado a los recursos restringidos.

Pérdida de datos: El robo o fuga de datos privados y confidenciales de los servidores, mientras están en tránsito, o como resultado de los programas espía, malware, los registradores de claves, virus, etc.

Robo de identidad y fraude: Fraude de personal en los servidores y los usuarios finales a través de phishing y spam de correo electrónico.

El diseño del perfil se basa en una arquitectura de red validada y diseñada en torno a las operaciones de negocios y consideraciones técnicas. Reconociendo el hecho de que los costos son un factor común que limita a todos los diseños de redes, las topologías de la arquitectura y las plataformas fueron seleccionadas cuidadosamente para aumentar la productividad y reducir los costos globales.

Se adoptóla topología de trabajo mostrada en la Fig. 1, que sirve de base para el diseño del modelo de seguridad que se propone.

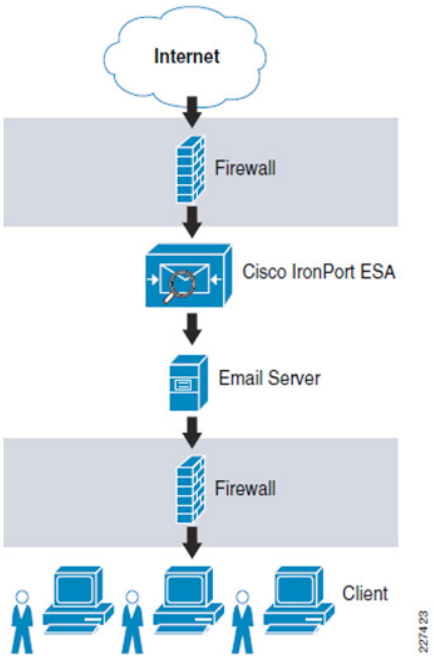

Fig. 1. Topología tomada de CISCO, como base del diseño del modelo propuesto [3].

5. DISEÑO DEL MODELO

Para el diseño del modelo de seguridad propuesto, se realizó un estudio previo del estado de las redes en la Universidad llegando a resumir esta información con la elaboración de las tablas de riesgos por áreas, dentro de las cuales están el personal de la Universidad, los usuarios finales, los accesos, etc. Un ejemplose muestra en la tabla 1.

Tabla 1. Niveles de riesgo en estudio.

Amenaza	Vulnerabilidad	Nivel de riesgo
Mal uso de las instalaciones de gestión de la información	Personal desmotivado o descontento	8
	Falta de mecanismos de vigilancia	8
	Falta de supervisión en horario extra laboral	8
Acceso no autorizado	Falta de mecanismo de vigilancia	8
	Inadecuado control lógico de acceso	8
	Inadecuado control físico de acceso	8

La información extraída de las tablas se resume en gráficos de barras (Fig. 2) con el ánimo de realizar un estimativo de los principales riesgos que afectarían a la red RITA-UD en producción.

Fig. 2. Resultados de los estudios de riesgos para la red RITA-UD.

Se utilizó una matriz de riesgos definida a base de hacer un análisis de los posibles ataques y otras vulnerabilidades de la red.

Teniendo en cuenta lo anterior, se definen claramente tres zonas de seguridad en la red RITA-UD. Una zona de alto riesgo o zona roja, una zona de riesgo medio o zona amarilla y finalmente una zona de bajo riesgo o zona verde. Estas tres zonas nos permiten dividir el trabajo de gestión de la seguridad de acuerdo al tipo de usuarios que se tendrán en la red.

Zona de alto riesgo o zona roja: En esta zona estarán ubicados todos aquellos usuarios que ingresan vía la red RUMBO o vía Internet. Esta zona es de alto riesgo por la enorme dificultad de controlar el tipo de ingreso a la red.

Zona de medio riesgo o zona amarilla: También es conocida como zona desmilitarizada o DMZ (por sus siglas en inglés). Su función principal es poder brindar servicios tanto a usuarios de la zona de alto riesgo como de la zona de bajo riesgo permitiendo el tráfico restringido desde estas zonas a la DMZ.

Zona de bajo riesgo o zona verde: Aquí se ubican los estudiantes, profesores y en general, todos los usuarios internos de la red RITA-UD. Estos usuarios tienen acceso autorizado hacia la DMZ y hacia la zona de alto riesgo. Este sector debe tener un esquema de interconexión robusto que permita a los usuarios tener alta disponibilidad de los servicios de red. En esta zona se propone utilizar un esquema de redundancia que atienda esta necesidad.

En la Fig. 3 se muestra el diagrama del diseño del esquema de seguridad de la red RITA-UD de acuerdo a lo requerido por el análisis de riesgos.

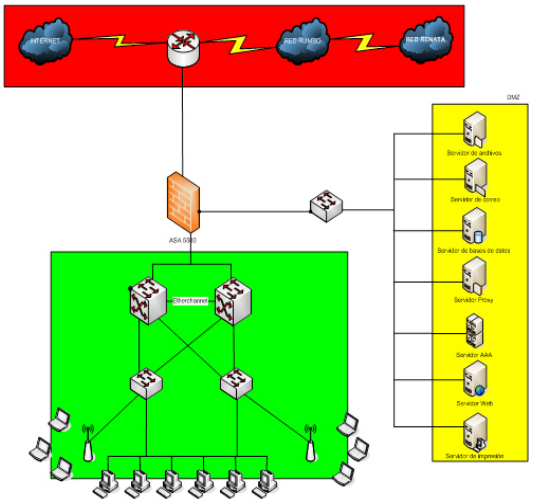

Fig.. 3. Diseño propuesto.

6. DIRECCIONAMIENTO DE LA RED

En la práctica, el direccionamiento se convierte en un tema clave para separar el tráfico entre los diferentes sectores de la red o sus segmentos.

La propuesta que se presenta consiste en la asignación de diferentes VLAN (Virtual LAN) que permitan un adecuado control del tráfico desde el Firewall. De esta manera se podrá tener una red en la que la configuración de reglas de tráfico se puedan manejar de la forma más práctica y ágil posible.

Las VLAN que se plantean son:

- VLAN 200 INTERNET_TELEFONICA. Permitirá la conexión del router de Internet con el Firewall. El direccionamiento de esta VLAN es de acuerdo al rango de direcciones que entregue el ISP. Aún no se ha entregado este rango. Para efectos prácticos de prototipo se utilizará la dirección 129.225.192.41.
- VLAN 300 RUMBO. Permitirá la conexión del router, por el que llega la red RUMBO, con el Firewall. El direccionamiento de esta VLAN es 190.15.10.0 /24 de acuerdo a dato entregado a la Universidad Distrital por la red RUMBO.

- VLAN 10 DMZ_RITA_UD. Esta LAN virtual separar el direccionamiento de todos los dispositivos de la DMZ. Para efectos prácticos se propone el siguiente rango de direcciones: 10.10.10.0 /24 lo que permitirá la asignación de hasta 254 direcciones IP. El direccionamiento es estático, es decir, se manejarán solo direcciones fijas asignadas por el Profesional de Seguridad.
- VLAN 20 INSIDE RITA_UD. garantizará asignar direcciones a todos los usuarios finales de la zona de bajo riesgo. El direccionamiento planteado para este segmento de red es 10.10.20.0 /23 lo que nos permitirá un crecimiento importante a nivel de usuario final. Las direcciones serán asignadas a cada cliente en el momento de la autenticación a través de un servidor AAA.
- VLAN 30 WIRELESS. Este segmento de la red está dedicado a los usuarios inalámbricos a quienes se les podría aplicar reglas de ingreso diferentes utilizando el estándar 802.1x y otras consideraciones. El direccionamiento asignado es 10.10.30.0/24. Las direcciones serán asignadas a cada cliente en el momento de la autenticación a través del servidor AAA.
- VLAN 99 GESTION. Se dedicará a los usuarios administradores de los equipos activos de red. El direccionamiento asignado es 10.10.99.0 /24.
- VLAN 40 GUEST. Esta sección se les asignará a los usuarios invitados, para quienes se restringirá el acceso. El direccionamiento asignado es 10.10.40.0 /24. El acceso a este segmento será administrado de una forma menos restrictiva debido a su restringido nivel de acceso.

7. GESTIÓN DE CAMBIOS

Todas las personas son elementos claves para la solución de seguridad propuesta, ya que ante cualquier control físico o lógico que se configure siempre un ser humano podrá encontrar una forma de evitarlo, eludirlo o subvertirlo. Esto implica que debe considerar a las personas en las etapas de desarrollo, implementación y puesta en marcha de una configuración o de cualquier cambio en la misma. Es por eso que se debe evaluar el efecto que el cambio tendrá en los usuarios finales, los diseñadores, programadores, desarrolladores, gestores e implementadores que tengan que ver con el proceso.

Cuando una persona ingresa a la red, debe ser claro cuál es su perfil en la organización y que permisos de acceso tendrá, para que la información a la que accede sea la necesaria y suficiente para el desarrollo normal de sus actividades.

Para construir la matriz de perfiles con sus responsabilidades se proponen una serie de elementos generales que permitirán establecer los diferentes accesos a la red como se muestran en la tabla 2.

Tabla 2. Matriz de perfiles.

Perfil	Derechos	Responsabilidad	Rotación prevista
Estudiante/ Usuario básico de consulta	Criticidad: Baja Significancia de las tareas: Baja Sensibilidad: Baja	El perfil exclusivamente consulta documentos en el servidor de trabajos de investigación publicados a todos los que quieran leerlos	Alta
Investigador	Criticidad: Alta Significancia de las tareas: Alta Sensibilidad: Media	Tiene acceso a los documentos de su investigación propia y a los documentos de acceso público	Media
Profesor/ Asesor	Criticidad: Alta Significancia de las tareas: Alta Sensibilidad: Alta	Tiene acceso a todos o algunos de los documentos de los diferentes investigadores	Bajas

Como parte del diseño se elaboraron los formatos de control de cambios para la gestión del SGSI basados en ITIL (Infrastructure Technology Information Library) que fueron los que se plantearon para la imple-

mentación por parte de la Universidad.

8. IMPLEMENTACIÓN

Para la ejecución del modelo, se utilizó el Firewall ASA 5520 de la familia ASA5500 de Cisco, en el cual se implementaron unas reglas de denegación de servicios ICMP y se obtuvieron unas gráficas de tráfico en la red, mediante el ASDM o herramienta de configuración grafica de la cual se muestra una impresión de pantalla en la Fig 4.

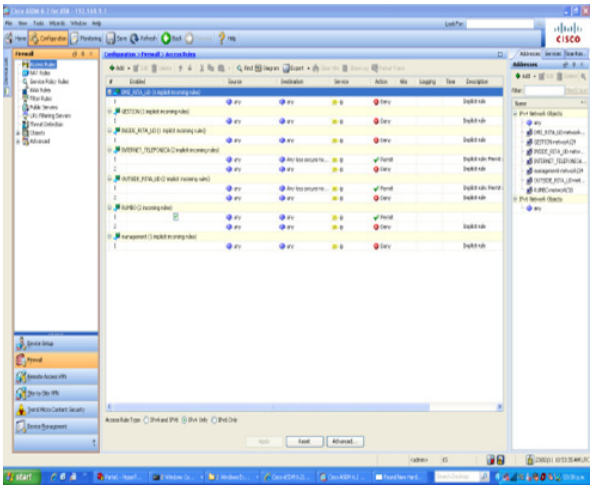

Fig. 4. Interfaz ASDM del ASA 5520 de CISCO.

9. CONCLUSIONES

Sería muy útil la implementación de un sistema de control de acceso físico a los dispositivos situados en las instalaciones de la Universidad, para garantizar la seguridad de los elementos físicos de la red.

Es indispensable adoptar la estructura organizacional propuesta que permita el control del activo de la información, para que esté siempre protegido y tenga un custodio que pueda responder por ella.

La red RITA-UD es una red de información que se enfrentará cada vez con más amenazas de seguridad procedentes de una amplia gama de fuentes, que incluyen fraudes asistidos por computador, espionaje, sabotaje, vandalismo, virus, Spyware, Botnets, etc. Por ello es importante considerar una constante capacitación del personal encargado de la administración de la seguridad, especialmente de los roles de Profesional de Seguridad, administrador de datos y custodio de datos ya que el modelo de seguridad no puede ser estático, sino que debe ser tan dinámico como las amenazas que se pueden recibir.

La dependencia de los sistemas con los servicios de información implica que las organizaciones son más vulnerables a las amenazas de la seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. En la implementación se minimizó lo más posible el acceso a las redes públicas desde las redes privadas.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería estar apoyada en una administración y unos procedimientos adecuados. El diseño planteado permite la identificación de los controles que deberían instalarse en una planificación cuidadosa y con una atención adecuada al detalle. La administración de la seguridad de la información en este diseño garantiza la participación de todos los involucrados en la red, especialmente la dirección, los usuarios finales y otros usuarios externos a la red RITA-UD.

La información es un activo que, como otros activos importantes de la red RITA-UD, tiene valor para la organización y requiere, en consecuencia, una protección adecuada. El modelo de seguridad de la información propuesto, la protege de una amplia gama de amenazas, para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad IT debe estar implementada y manejada en concordancia con los requeri-

mientos de la Universidad; y documentada como un conjunto de procedimientos, estándares y prácticas conforme a las recomendaciones realizadas en el diseño planteado.

En los planes de seguridad del diseño planteado se deben tomar en cuenta las necesidades de la Universidad, definidas por medio de una evaluación y valoración de vulnerabilidades, proyecciones industriales de amenazas y políticas actuales y procedimientos.

La implementación de este Modelo de Seguridad contribuye no sólo con el uso adecuado y seguro de la información sino con el prestigio de la Universidad Distrital, pues facilita la implementación de políticas que salvaguarden su reputación sobre el adecuado uso de la información, evita ser fuente de ataques desde el mundo exterior y ser pionera en Colombia en la implementación de este tipo de planes en el sector educativo.

Referencias Bibliográficas

[1] ICONTEC, Sistemas de gestión de la seguridad de la información. Normas NTC-ISO/IEC 17799 y NTC-BS 7799-2.

[2] ISO27001 el portal de ISO 27001 ISO 27001: Sistemas de Gestión de la Seguridad de la Información, [en línea]. Consultado en Enero de 2010, disponible en: http://www.iso27000.es/iso27000.html#section3a>

[3] M. Pueblas; S.Gyurinda; J.Strik; R.Kachalia;H. Rahul, Small Enterprise Design Profile Reference Guide. CISCO, Capitulo 5, 2010.

[4] CISCO, Fundamentos de seguridad de redes, Cisco press, p.p. 37 – 42, marzo del 2006.

[5] J. Harrington, Manual práctico de seguridad de redes, Editorial Anaya, p.p 125 – 129, 2006.

[6] J. Green, The irwin handbook of the telecommunications, quintaedición, McGraw hill, p.p 128-135, 2006.

[7] D. Comer, Internet working with TCP/IP, editorial Prentice hall, p.p 38 - 45, 2006.