ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INFORMÁTICA:

"Estrategia para la implementación de políticas de seguridad en la red de computadoras de una institución financiera por medio de Active Directory"

Sustentante: Efrén Pereira Avendaño

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIADO EN INFORMÁTICA CON ÉNFASIS EN GESTIÓN DE RECURSOS TECNOLÓGICOS

San José – Costa Rica

Mayo 2005

DEDICATORIA

Esta tesis se la dedico a Dios, a mi mamá, mis hermanos, a mis compañeros de trabajo, jefes de departamento que tanto apoyo y superación me han brindado, mis profesores que me brindaron el entendimiento y conocimientos con los cuales puede surgir en esta difícil carrera, a Claudia , la persona más importante en mi vida que con su cariño, paciencia y comprensión me ha ayudado a superar todos los momentos difíciles y de sacrificio que tuve que pasar y muy especialmente a mi papá por ser un ejemplo de superación a seguir por el cual guardo un enorme respecto, cariño y gratitud.

AGRADECIMIENTOS

Agradezco a todas las personas que me ayudaron en la creación de este trabajo, en especial a Omar Quesada y Ruben Ching que fueron quienes me inspiraron para elegir el tema de tesis.

Agradezco a quienes amablemente han estado pendientes de mí y de esta importante etapa en mi vida y, sobretodo, agradezco a Dios por darme la fortaleza y entendimiento para superar esta prueba.

Adicional a lo anterior, agradezco al profesorado de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT) por su calor humano y excelencia en el cumplimiento de sus funciones.

PRESENTACION

El siguiente trabajo se inspira en la búsqueda continua de la excelencia en la atención al cliente, lo cual es un valor fundamental de las instituciones financieras.

Se busca mejorar la prestación continua de los servicios bancarios planteando una metodología por medio de la cual se apliquen políticas de seguridad en la infraestructura tecnológica que minimicen los riesgos de ataques informáticos y por ende posibiliten una robustez percibible en la prestación de servicios.

El trabajo de investigación es requisito para optar por el grado de Licenciatura en Ingeniería Informática en la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT).

CAPÍTULO 1
PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

El presente trabajo de investigación trata de recopilar información referente a la relevancia de implementar un adecuado esquema de seguridad en una institución financiera.

Dentro de los temas desarrollados se tratará de indagar las opciones más comúnmente implementadas en cuanto al establecimiento de políticas de seguridad y las mejores prácticas existentes en el mercado en las instituciones financieras existentes en el ámbito nacional.

La investigación se desarrollará tomando como base una de las instituciones financieras más importantes de Costa Rica. Se reserva el nombre de dicha empresa por cuestiones de protección de la información empresarial y controles internos de la misma.

La idea central del trabajo es plantear un esquema que garantice una infraestructura de seguridad robusta por medio de la cual la institución financiera mencionada obtenga beneficios tales como la protección de la información, y el aseguramiento de la integridad y disponibilidad de los recursos de red, sin dejar de lado la lógica de negocio de la misma. El propósito de la investigación es plantear un esquema de implementación que pueda ser utilizado por cualquier institución financiera.

El planteamiento del esquema antes mencionado abarca el análisis de la infraestructura de dominios en Active Directory, el análisis de distribución y clasificación de objetivos, la definición de políticas de seguridad según las mejores prácticas del mercado y la documentación de todo el proceso.

.

1.2 Justificación

Debido a la funcionalidad y auge que han tenido las redes de computadoras en casi cualquier organización y tomando en cuenta la complejidad y estructuración de la lógica de negocio de una entidad financiera en cuanto a perfiles y funciones específicas, se hace cada vez más difícil la administración y manejo de todos los recursos.

La gran cantidad de información relevante que manejan los usuarios, así como el factor económico involucrado en el consumo y utilización de recursos tecnológicos, hacen que sea necesario contar con una infraestructura de seguridad robusta que permita centralizar la gestión de la información clasificada sensible, recursos tecnológicos físicos y lógicos y la organización de perfiles y permisos según áreas específicas de trabajo predefinidas.

El propósito de este trabajo consiste en hacer una recopilación de los aspectos de seguridad más relevantes en redes de computadoras, usuarios y recursos de red en general, los cuales representen insumos sensibles a ser vulnerados en una empresa financiera, evaluar las herramientas de hardware y software más adecuadas para implementar una infraestructura de seguridad bien definida y hacer el análisis de una posible implementación a la medida de mecanismos de seguridad y configuraciones posibles utilizando Active Directory como orquestador de políticas de seguridad; todo esto, con la intención de que los resultados obtenidos sean de gran utilidad para las personas encargadas de evaluar o diseñar estrategias de seguridad, para la administración de recursos de red, administración de usuarios, grupos de trabajo y perfiles en general.

Según los manuales de seguridad de Microsoft, no existe una estrategia de seguridad estándar que pueda ser aplicada a un área de negocio específica; por el contrario, dadas las complejidades y la enorme cantidad de variables de ambiente que se pueden presentar de una organización a otra, la mejor forma de implementar seguridad es diseñando esquemas a la medida que se amolden a las características de la empresa.

Las herramientas tecnológicas para implementar un buen esquema de distribución y mantenimiento de seguridad, muchas veces están presentes en las empresas u organizaciones; sin embargo, por razones tales como falta de experiencia, desconocimiento, o simplemente el desinterés gerencial, dichas herramientas no son utilizadas o son subutilizadas.

Con esta investigación se pretende crear un modelo que se pueda seguir por parte de las instituciones financieras, de manera que el proceso de aseguramiento de su infraestructura tecnológica sea lo más sencilla posible, por lo menos en su punto más básico.

1.3 Planteamiento del problema

En la actualidad, las empresas financieras experimentan un acelerado proceso de modernización tecnológica debido a las presiones de mercado y la búsqueda de un posicionamiento efectivo en el mercado nacional.

Dado este afán por ser el número uno, tecnológicamente hablando, se han dado varios fenómenos en las empresas financieras, tales como el crecimiento desordenado de la tecnología, falta de planificación de la infraestructura, incompatibilidad entre plataformas tecnológicas y, por ende, los altos costos involucrados de integrar estas cajas negras.

Debido a los aspectos anteriores, todos los esfuerzos de las gerencias tecnológicas y de operaciones se han inclinado hacia la integración de tecnologías y la creación de nuevos servicios y sistemas, dejando de lado el tema de seguridad.

La utilización de buenas prácticas de seguridad está poco desarrollada en nuestro ambiente financiero, y este es un fenómeno que se generaliza en el resto de las áreas económicas del país. Hasta hace pocos años el tema de seguridad no era un aspecto relevante ni de misión crítica para las empresas; sin embargo, en nuestros tiempos se ha visto un incremento exponencial de ataques a sistemas y equipos de diversos sectores económicos.

La aparición de los hackers y crackers, los virus y las innumerables vulnerabilidades que aparecen diariamente en las plataformas tecnológicas actuales, nos hacen poner en duda la integridad y confidencialidad de nuestra información.

En el sector financiero nacional se ha hecho un enorme esfuerzo por lograr un nivel de seguridad básico para proteger los intereses empresariales; sin embargo, falta mucho camino por recorrer en esta materia.

Las infraestructuras tecnológicas actuales con que cuenta el sector financiero nacional necesitan una reorganización y planificación adecuada, ya que, debido al crecimiento desordenado que han sufrido, no se adecuan para aprovechar las herramientas actuales y así lograr una infraestructura de seguridad robusta que permita dar protección a los recursos empresariales.

1.4 Problema de investigación

¿Cómo implementar un esquema de seguridad por medio de Active Directory de manera que se facilite la configuración y manipulación de políticas de seguridad y permisos a sistemas, equipos y usuarios de manera centralizada?

1.5 Objetivos

1.5.1 Objetivo general de diagnóstico

- Describir la situación actual de las instituciones financieras del país en materia de seguridad, identificando las áreas de impacto más relevantes o sensibles a ataques, los riesgos inherentes y las posibles soluciones a implementar según las posibilidades actuales.

1.5.2 Objetivos específicos de diagnóstico

- Identificar los principales riesgos que pueden afectar a una empresa financiera si no cuenta con una infraestructura de seguridad para la protección de sus sistemas e información crítica.

- Identificar las principales políticas de seguridad y configuraciones que afectan a los objetos de Active Directory (recursos de red y usuarios).

- Identificar las principales técnicas de ataque a equipos y usuarios

- Identificar software y hardware especializados en materia de seguridad para la plataforma Microsoft.

- Identificar las mejores practicas y técnicas existentes en materia de seguridad de manera que se pueda proponer un modelo o infraestructura adecuado en Active Directory

1.5.3 Objetivo general de la propuesta

- Establecer un modelo de seguridad a la medida en Active Directory para una empresa financiera de manera que se defina una infraestructura de seguridad bien establecida que prevenga posibles ataques a la integridad de sus recursos de red, sistemas, usuarios, datos y equipos.

1.5.4 Objetivos específicos de la propuesta:

- Plantear una adecuada estructuración del Active Directory de manera que se optimice la administración de usuarios, equipos y recursos de red.

- Definir una estrategia de implementación de seguridad a nivel de Active Directory, de manera de que asegure una adecuada distribución de políticas de seguridad según la estructuración planteada.

- Generar plantillas y políticas de seguridad para que una institución financiera cuente con un adecuado plan de seguridad en su infraestructura de Active Directory.

- Generar referencias básicas en donde se describa como configurar y administrar la infraestructura de seguridad definida en el Active Directory.

CAPÍTULO 2
MARCO TEORICO

2.1 Seguridad

En los últimos años el tema de la seguridad ha sido altamente difundido entre las grandes empresas que utilizan tecnología como el pulmón de su negocio y cualquier otra organización que de una u otra forma hace uso de tecnologías de información.

Según Ardita, Julio (2002), la seguridad informática concierne a la protección de la información que se encuentra en una computadora o red de computadoras y también a la protección del acceso a todos los recursos del sistema.

El acelerado crecimiento de la tecnología y el surgimiento de la era del **Internet** han hecho que muchas empresas puedan extender sus fronteras comerciales y con ello lograr múltiples ganancias en sus operaciones. Sin embargo, proporcional al crecimiento tecnológico, también se ha dado un exponencial incremento de los **delitos informáticos**, los cuales atentan contra la integridad de los sistemas.

Según la Guía de Seguridad de Windows Server2003 (2004, p.03.), "Muchas organizaciones cometen el error de subestimar el valor de su ambiente de informática, generalmente porque excluyen los costos indirectos sustanciales".

Si una organización depende de la tecnología para continuar con sus operaciones y poder ser productiva, por ejemplo una Página Web de ventas en línea, un ataque podría causar grandes pérdidas tanto económicas como de imagen ante el mercado en el que se desarrolla.

El tema de seguridad en muchas organizaciones ha tenido muy poco avance dadas las características propias de cada industria y la complejidad asociada con su lógica de negocio. Según Alfaro, Elier (2004) los siguientes puntos son los responsables de dificultar la labor de aseguramiento en las empresas:

- Existencia de servidores con diversas funciones.
- Recursos limitados para implementar soluciones seguras.
- Utilización de sistemas antiguos.
- Carencia de experiencia en seguridad.
- Amenazas internas y externas.
- Acceso físico anula muchos procedimientos de seguridad

La carencia de recursos destinados a implementar seguridad y la falta de experiencia en el campo, provoca serias deficiencias en las plataformas tecnológicas de muchas organizaciones ya que se encuentran vulnerables ante cualquier ataque a sus sistemas.

Es importante señalar que la seguridad se basa en la protección y el aseguramiento de la información o sistemas, de manera que se garantice la **confiabilidad**, **integridad** y **disponibilidad** de los mismos; por lo cual, todos los esfuerzos en el establecimiento de una estrategia de seguridad deben estar basados en el logro de estas tres características.

2.2 Violaciones de Seguridad

En la actualidad el número de ataques a sistemas y equipos ha crecido exponencialmente; las amenazas presentes en los sistemas han evolucionado y se han vuelto más frecuentes, lo cual provoca grandes pérdidas financieras.

Durante el 2004, las pérdidas financieras por ataques a sistemas o equipos en los Estados Unidos alcanzan los $141.496.560, según un estudio realizado por el Computer Security Institute (CSI), apoyados por el Computer Intrusion Squad del FBI, (*1, 2004*)

Los sistemas de una empresa pueden ser víctimas tanto de ataques externos a la red (por Internet, correo electrónico u otro), como internos, es decir, ocasionados por un agente al interior de una empresa que no tenga acceso autorizado a los equipos, o bien utilice sus códigos de acceso a los sistemas con fines maliciosos.

Según un estudio de 2000 del Computer Security Institute(2004), los ataques de tipo interno, pueden alcanzar más del 80% de las incursiones maliciosas, ocasionadas generalmente por empleados descontentos.

Según Wong, William (2004), los ataques y técnicas más comunes realizadas contra equipos y sistemas se resumen en la tabla # 1:

Tabla # 1
Violaciones de Seguridad

TECNICAS DE ATAQUE	DESCRIPCIÓN
Ingeniería social	Los intrusos aprovechan la inocencia de los usuarios y por medio de mensajes atractivos o engañosos incitan al usuario a abrir archivos potencialmente peligrosos.
Creación de puertas traseras	Por medio de la ejecución de código maligno que abre puertos del computador o aprovecha alguna vulnerabilidad para dejar la puerta abierta para ataques posteriores.
Robo de direcciones de correo electrónico	Los conocidos correos de Spam que podrían contener código maligno o potencialmente peligroso para los sistemas
Motores de correo electrónico incrustados	Utilización de código oculto dentro de los correos electrónicos que se ejecutan en cuanto el usuario los accesa.
Explotar las vulnerabilidades del producto	Aprovechamiento de errores en el código del sistema operativo que pueden ser aprovechados por un atacante para apoderarse del computador o ejecutar código maligno en el mismo.
Explotar las nuevas tecnologías de Internet	Los intrusos informáticos se aprovechan de las novedosas herramientas con que cuenta Internet para realizar búsquedas minuciosas de sistemas vulnerables.

2.3 Tendencias en el Sector Financiero

A través del tiempo las empresas financieras han sido un pilar en la utilización de las tecnologías de la información, y, por ende, han estado en una constante búsqueda de técnicas, estrategias y mejores prácticas en el área de la seguridad informática.

Para una empresa financiera el nivel de confianza que el cliente perciba en el servicio que brinda es fundamental, ya que en última instancia la confianza es el principal producto que comercializa una institución de esta índole.

Si un atacante logra infiltrarse en los servidores institucionales de una organización financiera, dependiendo de la severidad de dicho ataque, se podrían dañar las operaciones de toda la organización y afectar los datos contables de todos sus clientes, lo cual causaría toda una catástrofe a nivel funcional de los sistemas de información y la reputación de la institución financiera.

Dada esta situación, el sector financiero debe evaluar el impacto que tendría un posible ataque en cada uno de sus componentes y evaluar el costo de asegurar cada uno de los componentes en comparación con las pérdidas cualitativas y cuantitativas que se tendrían con un posible ataque.

2.3.1 Análisis de Vulnerabilidades

Según la Guía de Seguridad de Windows Server2003 (2004, p.10.), “El análisis de vulnerabilidades, riesgo y exposición respecto a la seguridad implementada en la organización le informa sobre el equilibrio entre la seguridad y la capacidad de uso o probabilidad de ataque a las que están sujetos todos los sistemas de cómputo en un ambiente de red”.

Es por lo anterior que se deben implementar contramedidas que mitiguen dichas vulnerabilidades minimizando así el **riesgo** involucrado de contar con estos huecos de seguridad en nuestra infraestructura.

Cada componente de una infraestructura tecnológica es vulnerable a algún ataque y dependiendo de la complejidad y amplitud de esta infraestructura, el aseguramiento,

monitoreo y mantenimiento de cada uno de dichos componentes puede volverse inmanejable.

En todo sistema computacional, existen muchos elementos u objetos los cuales son comúnmente utilizados por los usuarios en un ambiente de red, tales como: impresoras, aplicaciones, bases de datos, servidores de archivos, etc.

La complejidad percibida en el manejo de dichos elementos depende de la demanda de los usuarios ante estos recursos, y de la facilidad que tengan los administradores de controlar y administrar el uso de dichos recursos.

2.3.2 Herramienta para la gestión de Seguridad (Active Directory)

La necesidad de contar con una herramienta robusta que ayude a controlar toda esta serie de recursos y elementos de red, hace que la empresa Microsoft introduzca en su producto al mercado un concepto llamado servicio de directorio, el cual, en su función más básica, se dedica a detallar atributos sobre objetos (*entiéndase por objeto todo elemento computacional o recurso presente en una red de computador*es), de manera que se obtenga un directorio de ellos, categorizado por atributos comunes, que le permite a los usuarios y administradores encontrar y manejar de una manera fácil y eficiente los objetos presentes en una infraestructura tecnológica por medio de atributos específicos.

Según Microsoft TechNet *(2004, par. 7.), un servicio de directorio puede:

- Reforzar la seguridad definida por los administradores para mantener la información segura ante intrusos.
- Distribuir un directorio a través de muchas computadoras en una red.
- Hacer duplicados del directorio para que esté disponible para más usuarios y sea resistente a las fallas.
- Separar un directorio en almacenes múltiples para permitir el almacenaje de un gran número de objetos.

** http://www.microsoft.com/latam/technet/articulos/199909/art05/*

Dada la diversidad de usos para esta herramienta, su utilización se puede adaptar tanto para propósitos administrativos como para usuario final.

El servicio de directorio se convierte en el eje sobre el cual gira un sistema computacional, ya que, conforme la infraestructura tecnológica va creciendo, aumenta la dependencia con esta herramienta y las bondades administrativas que permite.

2.3.2.1 Definición de Active Directory (AD)

Microsoft introduce a partir de su sistema Operativo Windows 2000 el Active Directory; el cual, "permite que las aplicaciones encuentren, utilicen y administren recursos de directorio en un ambiente de cómputo distribuido" (Guía de Seguridad de Windows Server2003, 2004, p.14.).

Active Directory es un servicio extensible y escalable que permite manejar eficientemente recursos de red. La tecnología del Active Directory se basa en protocolos estándares y tiene un diseño que ayuda a definir claramente la estructura de red de la organización.

2.3.2.2 Funciones de Active Directory

Según Serrano, José (2003), las funciones primordiales de Active Directory en una infraestructura de red son las siguientes:

- Punto Único: Por medio del AD se pueden gestionar los distintos objetos presentes en la infraestructura (usuarios, aplicaciones, dispositivos, etc)

- Repositorio centralizado: Se administra la seguridad de manera centralizada (autenticación, autorizaciones, delegación de permisos, etc)

- Plataforma Abierta: Concentra herramientas que ayudan al desarrollo o integración con otros sistemas.

- Organización Jerárquica: Presenta una estructura arbórea, con objetos en contenedores y contenedores en contenedores (estructura especificada para una mejor administración)

- Almacenamiento Orientado a Objetos: Soporta múltiples modelos de objetos, además de la información de los objetos (atributos). Adicional a esto enmarca la seguridad a nivel de objeto y atributo.

- Replicación Multi-Master: Soporta replicaciones múltiples de la información entre las diferentes estructuras del dominio, lectura – escritura completa por réplica y réplica optimizada automáticamente.

- Simplifica la gestión de Windows: Gestión y distribución automática de software, ficheros y control de impresoras.

- Refuerzo de la seguridad: Acceso único a los recursos de la red y configuración de Desktop de acuerdo con los servicios de seguridad de Internet y de las aplicaciones internas según lo requieran.

2.3.2.3 Estructura de Active Directory

Según Microsoft TechNet* (2004, par.12.), Existen varios conceptos relacionados con el Active Directory, en donde se definen estructuras lógicas y físicas para los componentes de red, dentro de los cuales se pueden mencionar los siguientes:

2.3.2.3.1 Objeto

Juego de nombres preciso de atributos que representan algo en concreto, como un usuario, una impresora o algún elemento de una aplicación. Los atributos mantienen datos que describen al sujeto que es identificado por el objeto del directorio. Los atributos de un usuario pueden incluir su nombre, apellido y dirección de correo electrónico.

2.3.2.3.2 Contenedor

Un contenedor es como un objeto en que tiene atributos y es parte del espacio para nombres del Active Directory. Sin embargo, a diferencia de un objeto, no representa algo en concreto. Es un contenedor para un grupo de objetos y otros contenedores.

2.3.2.3.3 Domain

Grupo de computadoras que comparten una base de datos común del directorio. Un dominio es un solo límite de seguridad de una red computacional de Windows NT, Windows 2000 y Windows 2003.

El Active Directory está compuesto de uno o más dominios. En una sola estación de trabajo, el dominio es la computadora misma. Un dominio puede conectar más de una ubicación física. Cada dominio tiene sus propias políticas de seguridad y relaciones de seguridad con otros dominios. Por lo general existen en la red equipos que hacen el papel de **Domain Controllers**, los cuales tienen la tarea de replicar la base de datos de Active Directory dentro de la red.

2.3.2.3.4 Domain Tree

Un Domain Tree comprende varios dominios que comparten un esquema común y configuración. Los dominios en un árbol están también vinculados por relaciones de confianza. El Active Directory es un conjunto de uno o más Domain Trees. Los Domain Trees pueden ser vistos de dos maneras. Una manera es las relaciones de confianza entre los dominios. La otra es el espacio para nombres del Domain Trees.

Windows 2000 establece las relaciones de confianza entre los dominios basándose en el protocolo de seguridad Kerberos. La confianza de Kerberos es transitiva y jerárquica, si el dominio A confía en el dominio B y dominio B confía en dominio C, dominio A confía también en el dominio C.

Grafico # 1.
Esquema de Relaciones de confianza en A.D,
Tomado de http://www.microsoft.com/latam/technet/articulos/199909/art05/, 2004

También se puede determinar el nombre único de un objeto siguiendo el camino hacia el espacio para nombres del Domain Tree, lo cual se realiza mediante una búsqueda intensa desde la raíz en la jerarquía completa.

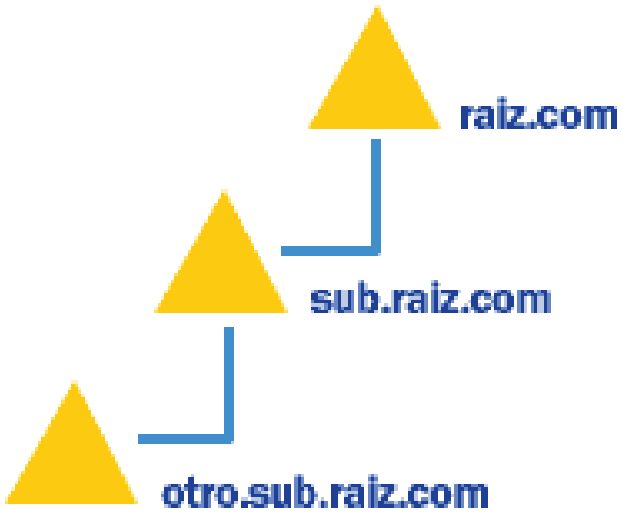

Grafico # 2.
Esquema de Espacio de Nombres en A.D,
Tomado de http://www.microsoft.com/latam/technet/articulos/199909/art05/, 2004

2.3.2.3.5 Domain Forest

Es un conjunto de uno o más Domain Trees. Todos los Domain Trees en un Domain Forest comparten un esquema común, configuración, y Catalogo Global. Todos los árboles, en un Domain Forest dado, confían uno en el otro vía relaciones de confianza Kerberos, las cuales son transitivas y jerárquicas.

A diferencia de un Domain Tree, un Domain Forest no necesita un nombre único. Un Domain Forest existe como un conjunto de objetos de referencia recíproca y relaciones de confianza Kerberos conocidas para los Domain Trees.

2.3.2.3.6 Organization Units (OU)

Organización de dominios que refleja a menudo el negocio o la estructura funcional de la compañía. (Microsoft TechNet, 2004, Párrafos 1 y 2).

Son contenedores en donde se pueden almacenar lógicamente objetos dentro de una infraestructura diseñada por Active Directory.

2.3.2.3.7 Sitio

Un sitio es una ubicación en una red que contiene servidores de Active Directory. Un sitio se define como una o más subredes TCP/IP bien conectadas. Este conjunto de subredes permite a los administradores configurar rápidamente y fácilmente el acceso al Active Directory.

El esquema del Active Directory es implementado como un conjunto de instancias de clase de objetos almacenados en el directorio. Es muy diferente a muchos directorios que tienen un esquema, pero los almacena como un archivo de texto para leerse al iniciar. Por ejemplo, las aplicaciones del usuario pueden leer el esquema para descubrir qué objetos y propiedades están disponibles.

CAPÍTULO 3
MARCO METODOLOGICO

3.1 Tipo de investigación

La investigación tiene un enfoque descriptivo ya que se hace una búsqueda exhaustiva de las características y propiedades comunes de las áreas tecnológicas involucradas en un proceso de aseguramiento.

Se busca una descripción de los principales métodos de ataques utilizados en contra de equipos y sistemas, así como de las técnicas utilizadas para frenar dichos ataques.

La definición de perfiles e implementaciones comunes en las empresas financieras en materia de seguridad es de suma importancia para establecer una solución común para este ámbito.

Por otro lado, también se realiza un estudio exploratorio en cuanto al establecimiento de una estrategia a la medida, que ayude a implementar seguridad por medio de Active Directory, tomando en cuenta las características propias de una empresa financiera.

3.2 Muestreo

La muestra será no probabilística ya que se requiere la opinión de expertos en el tema de seguridad y personas con conocimientos básicos-altos en el manejo y administración del Active Directory.

3.3 Población

Instituciones financieras. La investigación se realizará tomando como modelo una de las instituciones financieras más importantes del Costa Rica y se tratará de amoldar la estrategia planteada para ser adaptable a cualquier organización financiera.

3.4 Descripción del instrumento de recolección de datos

El instrumento utilizado para la recolección de datos para la investigación es el siguiente:

3.4.1 Entrevistas a expertos:

Se realizaron preguntas relacionadas con mejores prácticas sobre posibles implementaciones de seguridad a un consultor de Microsoft para Costa Rica y al administrador de Active Directory de una institución financiera de Costa Rica.

Con estas entrevistas se pretende obtener información de primera mano en cuanto a implementaciones presentes y más comúnmente utilizadas en las empresas económicamente activas; de manera que esta información pueda ser procesada y comparada con las mejores prácticas del mercado.

3.5 Alcances

Esta propuesta se basa en el planteamiento de una estructura de Active Directory aplicable para una institución financiera de manera que se pueda realizar una distribución adecuada de plantillas de seguridad.

En el transcurso de la propuesta se plantean varias recomendaciones en relación con el establecimiento de políticas de seguridad, roles y responsabilidades.

Este trabajo se enfoca en instituciones financieras que tengan su infraestructura tecnológica implementada bajo la plataforma Microsoft.

3.6 Limitaciones

Durante la recopilación de datos hubo limitaciones en cuanto a la colaboración de los encargados de seguridad de las varias instituciones financieras.

En la mayoría de los casos dichos encargados alegan que la información consultada es de carácter confidencial por lo que no participaron en la investigación.

Dado lo anterior, la investigación se centra en la opinión experta del proveedor y en el encargado de arquitectura de la institución modelo.

CAPÍTULO 4
DIAGNÓSTICO

4.1 Riesgos en el Sector Financiero

Para identificar los riesgos presentes en el ámbito de las entidades financieras, es necesario analizar antes cuales son los principales peligros presentes en el ambiente y las técnicas utilizadas por los intrusos informáticos para realizar sus actos delictivos.

Según Symantec (2004), las principales **vulnerabilidades** a las que se enfrentan las instituciones financieras (en porcentajes de más del 94% de las instituciones encuestadas), se refieren a vulnerabilidades básicas de router que podían poner en peligro la disponibilidad de los sistemas bancarios en línea.

Entre los riesgos específicos identificados, debidos a la configuración de los enrutadores, estaban los ataques de **negación del servicio** (DoS), el acceso no autorizado a los recursos de las redes y detalles reveladores acerca de los usuarios registrados en los sistemas, incluyendo el nombre de los mismos.

La encuesta también reveló que un tercio de las organizaciones financieras investigadas tenían al menos 10 fallos de seguridad.; además, en el transcurso del estudio, las organizaciones financieras mostraron un incremento constante de los riesgos en el firewall.

La encuesta llegó a la conclusión de que, en términos de riesgo por áreas, el sector financiero se comportaba "generalmente dentro del promedio" en comparación con los sectores de gobierno, **TI** y telecomunicaciones, manufacturas y jurídico.

Según la encuesta, los 10 riesgos principales descubiertos en el sector financiero en el año 2002 fueron los siguientes**:**

- El **router** de acceso a Internet permite el acceso al Protocolo de Mensajes para el Control de Internet Público (ICMP).
- Los servidores **DNS** permiten transferencia de zona desde cualquier equipo host.
- El router de Internet ofrece servicios misceláneos de red.
- El servidor Web anuncia tipos y versiones de software.

- Los servidores de correo electrónico soportan el protocolo sencillo y extenso de transferencia de correo (SMTP).

- El firewall para Internet ofrece servicios de administración y de redes privadas virtuales (VPN).

- El router de acceso a Internet tiene la vulnerabilidad de fuga de información.

- Los servidores de Internet utilizan secuencias numéricas de TCP predecibles.

- Los servidores DNS permiten consultas públicas recurrentes.

- El servidor Web admite únicamente autenticación básica.

4.1.1 Aumento de Intrusos Informáticos

Según Symantec (2004), en el "Estudio sobre Informes de Actividades Sospechosas (SAR)", publicado en octubre 2003 por la Red de Lucha contra los Delitos Financieros (Financial Crimes Enforcement Network, FinCEN), el número de Informes sobre Actividades Sospechosas (SAR) archivados bajo el título de "**intrusos informáticos**" está creciendo aceleradamente. Hubo 65 informes en el año 2000, 419 en 2001, 2.484 en 2002, y 3.605 al 30 de junio de 2003.

Se logró entender mejor el problema gracias a la encuesta reciente de Deloitte & Touche, la cual analizó el estado de la seguridad de Infraestructura Tecnológica (TI) en las 500 principales instituciones financieras del orden mundial.

La encuesta, publicada en mayo de 2003, descubrió que casi el 40 por ciento de estas empresas ha tenido un grave problema de seguridad de la TI durante el 2003, a pesar de que invierten mucho en normas y tecnologías de seguridad de TI.

Según Symantec (2004), las empresas financieras bajo su estudio realizan grandes esfuerzos en el tema de la seguridad informática:

- Las compañías de servicios financieros globales están utilizando típicamente entre el 6 y el 8 por ciento de sus presupuestos de TI para la seguridad de la información.

- Más de dos tercios de todos los encuestados informaron que las gerencias generales perciben la seguridad de TI como un "costo necesario del negocio", y no como un gasto discrecional.

- Cerca de la mitad (el 47%) de estas instituciones financieras han incrementado su personal de seguridad desde el 2001.

- Solamente el 19% afirmaron haber reducido su personal de seguridad como resultado de la depresión económica.

Este comportamiento hace pensar que las instituciones financieras finalmente han comprendido la importancia de contar con una infraestructura tecnológica no fragmentada en el ámbito de la seguridad; y por ende, han aunado esfuerzos en el reforzamiento de su plataforma de seguridad con programas de inversión y capacitación en el tema.

Es en este punto en el que se vuelve importante contar con un planeamiento estratégico que traiga a relucir una herramienta especializada en el manejo de seguridad y contar con un modelo de implementación de seguridad.

Para realizar este planteamiento se debe conocer a plenitud el rango de acción de los delitos informáticos y las consecuencias que traen, por lo cual se realiza una breve reseña de las implicaciones en el ámbito legal.

4.1.2 Orígenes de los Crímenes Informáticos

Según el grupo Grupo Mnemosine (2004), el ámbito informático nos permite distinguir dos grandes grupos de delitos informáticos: los delitos informáticos de carácter económico y los delitos informáticos que van contra la privacidad.

4.1.2.1 Delitos informáticos de carácter económicos

En este primer grupo se analizan todas aquellas conductas delictivas en las que, ya sea mediante el uso de un sistema informático como herramienta, o tomando al sistema informático como objeto de un ataque, se produce un perjuicio a un bien patrimonial de la organización.

4.1.2.2 Delitos informáticos en contra de la privacidad de la información

Los delitos informáticos que afectan la privacidad constituyen un grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano o empresa mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

La expansión del uso de la informática en el área financiera ha permitido la utilización de herramientas especializadas para la comisión de delitos que exceden el marco de los delitos patrimoniales y contra la privacidad.

4.1.3 Delitos Informáticos en el Ámbito Financiero

Según Quesada, Omar (2005), los delitos informáticos comunes en el ámbito financiero son los que se listan a continuación:

4.1.3.1 Fraudes cometidos a través de la manipulación de sistemas informáticos

Estas conductas consisten en la manipulación ilícita de datos contenidos en sistemas informáticos con el objeto de obtener ganancias indebidas.

4.1.3.2 Copia ilegal de software y espionaje informático

En este grupo se engloban las conductas dirigidas a obtener datos, en forma ilegitima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, estados financieros, estrategias del negocio, etc.

En muchos casos el objeto de un ataque a un sistema informático es obtener alguna ganancia ya que, por lo general, los mismos suele tener un importante valor económico.

4.1.3.3 Sabotaje informático

Consiste en el daño causado a sistemas informáticos, ya sea en sus elementos físicos (hardware) o en la información intangible contenida en sus programas.

4.1.3.4 Uso ilegitimo de sistemas informáticos ajenos

Esta modalidad consiste en la utilización sin autorización de los equipos y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido por empleados de los sistemas de procesamientos de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias de su trabajo.

4.1.3.5 Acceso a sistemas informáticos sin autorización:

Consiste en el acceso no autorizado a un sistema de datos a través de procesos de datos a distancia, cometidos sin intención fraudulenta ni de sabotaje o espionaje.

Según el CERT® Coordination Center (2004), en los últimos años se ha observado un elevado incremento en la actividad de los intrusos informáticos. El comportamiento de muchas empresas de diferentes áreas de mercado es optar por el cambio de tecnologías cerradas y englobadas en sus propias empresas para pasar a infraestructuras abiertas que hacen un uso intensivo de la comunidad del Internet.

Este comportamiento ha permitido que las técnicas de ataque utilizadas por los intrusos, sean cada vez más complejas y comunes en nuestro ambiente; la habilidad de las organizaciones e individuos para utilizar de forma segura el Internet ha sido muy pobre ya que la cultura informática históricamente no ha estado enfocada en el tema de la seguridad.

4.1.4 Amenazas e Impactos

Según J. M. Minguet Melian(2004), la diversidad de elementos de un sistema informático que pueden ser atacados, origina que las amenazas puedan deberse a muy diversas causas. A principios de los años ochenta un estudio del Gobierno sueco identificó 800 diferentes amenazas, aunque evidentemente con mayor o menor probabilidad de riesgo y con impactos muy variables.

La evolución de la tecnología informática y el creciente número de jóvenes expertos dedicados a vulnerar sistemas incrementa continuamente el riego presente en TI. Por ello la identificación de las posibles amenazas y el intento de tipificarlas es una labor muy ardua.

Complica la labor de clasificación el hecho de que el ataque a un sistema se suele producir mediante amenazas combinadas y con un propósito definido, en la mayoría de los casos, de obtener algún beneficio de tipo económico.

4.1.4.1 Tipos de Amenazas

Las amenazas que pueden afectar los recursos informáticos, los activos informáticos y el personal informático son básicamente los siguientes:

- Intercepción
- Modificación
- Interrupción y
- Generación

4.1.4.1.1 Intercepción

La Intercepción se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema.

Ejemplos: acceso a una base de datos, entrada a través de la red en un sistema informático ajeno, captura de paquetes por medio de un sniffer, etc

4.1.4.1.2 Modificación

La Modificación intenta cambiar en todo o en parte el funcionamiento del sistema. Es el tipo de amenaza más peligroso ya que puede ocasionar grandes daños en el sistema.
Ejemplos: cambios en el contenido de una base de datos, cambios en los datos de una transferencia bancaria, etc.

4.1.4.1.3 Interrupción

La Interrupción puede ser temporal o permanente e incluye la posibilidad de destrucción de recursos y activos. Es la más sencilla de detectar y la que presenta mayor dificultad para luchar contra ella, ya que muchas veces son accidentes naturales.

Ejemplos: interrupción de suministro eléctrico, incendios, errores de operación que afectan al S.O., etc.

4.1.4.1.4 Generación

La Generación se refiere a la adición de campos o registros en los activos, en la adición de líneas de código en los recursos lógicos, o a la introducción en el sistema de programas completos.

Ejemplos: virus informáticos, caballos de Troya, transacciones electrónicas falsas, introducción de datos en una base, etc.

4.1.4.2 Impactos

Cuando se produce un incidente de seguridad, es decir, cuando se materializa una amenaza, se produce una pérdida para la organización que es necesario valorar.

Es importante clasificar la naturaleza de las posibles pérdidas derivadas de un incidente, según orden de importancia, con el objeto de seleccionar las medidas preventivas a adoptar en cada caso.

.

4.1.4.2.1 Tipificación de las pérdidas

La importancia de las pérdidas depende del sector de la organización que afecta, dado que se pueden llegar a producir daños irreparables en las organizaciones.

Estadísticas recientes indican que una de cada tres empresas que han tenido un incidente de seguridad grave, han quebrado en el plazo máximo de 2 años.

Las pérdidas ocasionadas pueden ser de muy diferente naturaleza, tales como:

- Físicas: Incapacidades laborales, enfermedades profesionales.
- Materiales: Daños a recursos informáticos, robos de los mismos.
- Alteraciones de la normalidad: Interrupciones y retrasos en los procesos de producción, pérdidas de ingresos.
- Pérdidas de integridad: Alteraciones de la información y programas.
- Salidas indeseadas: de datos e informaciones, de programas.

La fuerte interdependencia entre los daños materiales, lógicos y humanos hace que la anterior tipificación no sea única, por lo que también se utilizan otras clasificaciones con base en la magnitud de las pérdidas, los activos afectados, etc.

La utilización de estas otras clasificaciones depende fundamentalmente de las prioridades de seguridad de cada organización.

4.1.4.2.2 Valoración económica

La valoración económica de las pérdidas o impacto exige tener en cuenta tanto los aspectos económicos tangibles (costo de reparaciones, reposición de recursos, responsabilidad civil, etc.) como los intangibles.

Ejemplos típicos de pérdidas intangibles son:

- Pérdida de imagen por errores o retrasos
- Disminución de ingresos potenciales por salida de información a la competencia.
- Pérdida de posición competitiva en el sector, etc.

Debe hacerse un esfuerzo especial por valorar económicamente estas pérdidas intangibles, aunque sea aproximadamente, ya que en muchas ocasiones sobrepasan sensiblemente las pérdidas tangibles.

4.2 Políticas de Seguridad y Configuraciones en el AD

El Active Directory (AD) es una parte integral de toda infraestructura tecnológica basada en la plataforma Microsoft; específicamente bajo los sistemas operativos Windows2000 o Windows2003.

Esta herramienta gestiona los servicios esenciales del sistema operativo para toda la red; además de brindar otra serie de valores agregados a la administración de la plataforma, incluyendo el punto de interés de este trabajo que se enfoca en la gestión de la seguridad.

A continuación se presenta el esquema lógico utilizado por Active Directory para orquestar todos los elementos configurados en una red común:

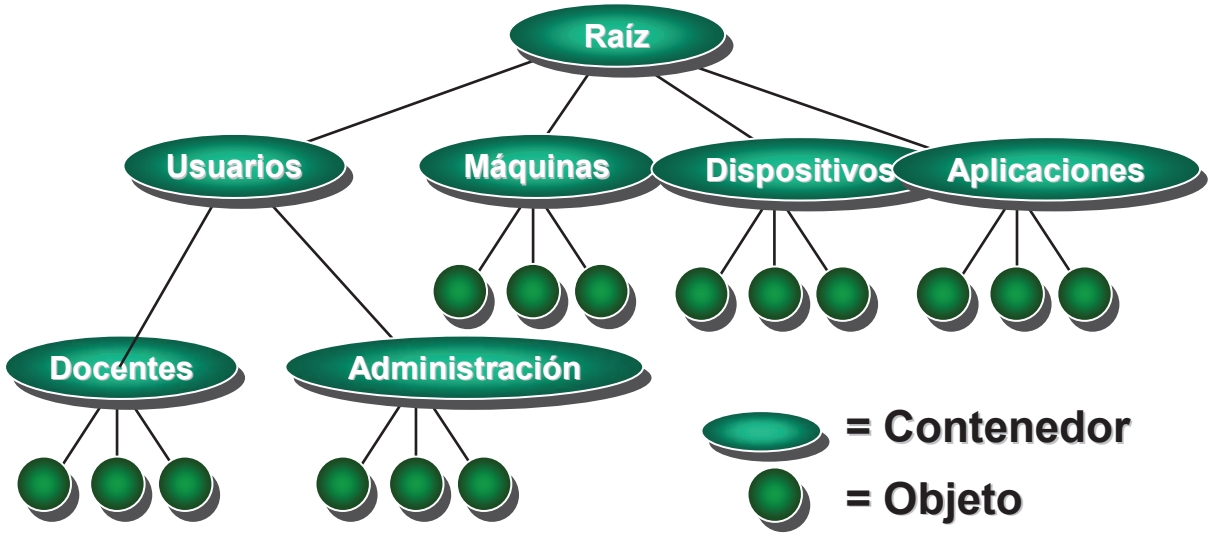

Grafico # 3.
Esquema de arquitectura para la administración de A.D,
Tomado de http://www.rediris.es/jt/jt2000/trans/jt2000-2-2.ppt, 2004

4.2.1 Configuración del AD

Según la guía de Seguridad de Windows Server2003 (2004, p.15.), al crear una arquitectura de Active Directory en cualquier organización, se debe tomar en cuenta el ámbito de administración de esta solución, ya que de esta medición dependerá en gran medida el éxito y efectividad de la implementación de seguridad de la organización.

En toda infraestructura tecnológica, se deben establecer los límites de la arquitectura de administración para gestionar de manera adecuada todos los elementos que conviven en ella; en el caso del Active Directory, estos límites se establecen automáticamente durante la instalación de Active Directory.

4.2.1.1 Límites de seguridad

Los límites de seguridad ayudan a definir la autonomía o el aislamiento de diferentes grupos dentro de la organización.

Por lo general, las infraestructuras tecnológicas implementadas en instituciones financieras son muy complejas, ya que albergan una gran cantidad de tecnologías, servicios y esquemas de trabajo; razón por la cual es difícil realizar un balance entre una infraestructura segura y una infraestructura funcional.

Para lograr exitosamente este equilibrio, se debe realizar un análisis formal de amenazas presentes en la organización y valorar las implicaciones de seguridad en cuanto a la criticidad de la información potencialmente vulnerable.

A partir de este punto es fácil para los mandos administrativos tomar la decisión de modificar la arquitectura de red de su ambiente para volverla más segura, o, si las amenazas presentes en el ambiente no son significativas, entonces tomar la decisión de convivir con ellas.

Ya una vez definidos los límites de administración e identificadas las amenazas puntuales que se quieren corregir o prevenir en la organización, se puede realizar un análisis de las posibles soluciones o acciones para atacar tales riesgos, y definir las acciones o contramedidas que se pueden implementar con una herramienta como Active Directory.

Dentro del análisis se mencionan las principales ventajas y métodos utilizados por AD para contrarrestar dichas amenazas.

4.2.1.2 Políticas de Seguridad y Configuración de Objetos

Los límites de seguridad son el punto de arranque que utiliza Active Directory para comenzar a evaluar los riesgos presentes en cualquier infraestructura.

El enfoque que se establezca se debe centrar en la configuración de la seguridad de los objetos contenidos dentro del límite indicado; para lo cual se pueden aprovechar cada una de las facilidades que presta el AD para su administración y aseguramiento.

Según la guía de Seguridad de Windows Server2003 (2004, p.15.), Active Directory brinda una serie de facilidades para la administración y configuración de elementos en cuanto a la seguridad de los mismos.

A continuación una descripción de las acciones permitidas por AD para subsanar estas debilidades de seguridad.

4.2.1.2.1 Restringir nivel de permisos

El AD permite limitar los privilegios de los usuarios u objetos en general, por medio de la configuración de niveles de seguridad.

Para este punto el AD se apoya en las **Directivas de Seguridad** (*conjunto de variables establecidas por medio de alguna "plantilla" que puede ser aplicado a un grupo de objetos*); de esta manera no se le permite a los usuarios la posibilidad de elegir o modificar aspectos de seguridad en sus equipos o aplicaciones.

Como se mencionó anteriormente, Active Directory presenta una organización jerárquica en la cual existen relaciones de herencia en cuanto a permisos y atributos de los objetos; esto facilita la aplicación de directivas de seguridad mediante el apoyo en las relaciones de herencia.

En primera instancia el AD plantea una estructura de directivas de grupo, en las cuales se presentan las siguientes opciones:

- Directivas Locales: Son aplicadas únicamente en los equipos que las tienen asignadas, independientemente del dominio al que pertenezcan.

- Directivas de Sitio: Se aplican a los equipos u objetos de un sitio específico presente en algún dominio.
- Directivas de Dominio: Se aplican a todos los usuarios u objetos del dominio.
- Directivas de la Unidad Organizativa (OU): Se aplican solamente a los usuarios u objetos contenidos en esa unidad organizativa en específico

Las directivas de seguridad establecidas en el AD se aplican de manera jerárquica, de forma que la prioridad se establece según la lista anterior, de menor a mayor; en donde las directivas locales tienen una prioridad menor que las de OU.

Por ejemplo, si un equipo está siendo afectado por una directiva de dominio, dicha directiva prevalecerá aunque contenga otra directiva local con alguna configuración específica.

En las directivas de seguridad se pueden delegar o quitar permisos sobre elementos de configuración como los siguientes:

- Configuración de aplicaciones
- Configuración del sistema (uso del **REGEDIT o REGEDT32**, Panel de Control, Local Security Policies, etc)
- Permisos de instalación de paquetes
- Cuotas de disco
- Utilización de dispositivos(CD-ROM, Floppy, UBS, Impresoras)
- Utilización de recursos de RED (Proxy, Carpetas Compartidas, Servidores de Archivos, Bases de Datos, etc)

En el **Anexo # 1 (**Administración y Configuración de Plantillas de Seguridad) se muestra como crear una directiva o plantilla de seguridad en donde se pueden realizar configuraciones para subsanar la seguridad de los elementos anteriores.

4.2.1.2.2 Configuración de Seguridad de Objetos

Adicional a lo anteriormente listado, AD permite la configuración de aspectos específicos de seguridad y permisos tales como los siguientes:

- Configuración del perfil de administrador:: Permite renombrar el perfil de administrador en los equipos que administra, de manera que sea más difícil de detectar para cualquier intruso.

- Configuración del perfil de huésped (GUEST): Una buena práctica en la configuración de los equipos es el renombrar y deshabilitar el usuario guest que se instala por default en el sistema operativo.

  Por medio de directivas de seguridad este proceso se puede hacer automático en todos los equipos a los que se les aplique la plantilla.

- Configuración de Servicios de Sistema: Las directivas de seguridad permiten deshabilitar o enviar configuraciones específicas a servicios del sistema operativo.

  Por ejemplo, se puede crear una directiva de seguridad que deshabilite en servicio IIS o Indexing Service en todas las estaciones de trabajo ya que son servicios innecesarios para las labores que se realizan sobre los mismos.

- Instalación de Software: Active Directory permite el envío de paquetes de seguridad por medio de Windows Scripting, los cuales son enviados a todas las estaciones o objetos ubicados dentro de los límites de administración del AD.

  Adicional a esto AD es el complemento para herramientas de terceros para la administración y distribución de paquetes de seguridad, service packs y actualizaciones en general, tales como **SMS**(System Management Server) o **SUS** (Security Update Service).

4.2.1.2.3 Restringir el acceso

Otra de las utilidades del AD es asignar o limitar el acceso de los usuarios a la red INTERNET y la red interna. Con esto se asegura que el usuario solo va a poder accesar lo que verdaderamente necesita en el desempeño de sus funciones.

Para restringir los accesos, Active Directory posibilita la creación de perfiles y roles de usuarios, a los cuales se les otorgan permisos específicos sobre objetos o recursos de red específicos.

Esta delegación de permisos se realiza por medio de directivas de seguridad. Ver **Anexo # 1** (Administración y Configuración de Plantillas de Seguridad).

Adicionalmente, AD utiliza LDAP para la autenticación de sus clientes.

4.2.1.2.3.1 Protocolo LDAP (Lightweight Directory Access Protocol)

El protocolo LDAP es un estándar derivado del X.500; el cual fue adoptado por el Active Directory de Microsoft para el manejo de autenticación de los clientes.

El estándar X.500 define de forma nativa un protocolo de acceso denominado DAP (Directory Access Protocol) que resulta muy complejo, además de pesado, en cuanto al procesamiento, porque está definido sobre la pila completa de niveles del OSI.

Como alternativa a DAP para acceder a directorios de tipo X.500, se creo el protocolo LDAP (Lightweight Directory Access Protocol), el cual ofrece un protocolo "ligero" casi equivalente, pero mucho más sencillo y eficiente, diseñado para operar directamente sobre TCP/IP.

El protocolo LDAP realiza sus conexiones y transferencias de información por medio de un subsistema de reglas básicas de codificación, las cuales según Microsoft Support (2005, par. 3.), son tramitadas entre el cliente y el servidor por medio de los puertos 389; el cual se utiliza para autenticación de usuarios o equipos mediante SASL (Simple Authentication and Security Layer), y el 636 que se utiliza para la transmisión segura de datos por medio del LDAP Security Sockets Layer (SSL).

El SASL (Simple Authentication and Security Layer) permite la configuración de seguridades de acceso tales como:

- Limite de tamaño permitido
- Tiempo de vida de sesiones
- Atributos y permisos de acceso
- Filtros de seguridad

4.2.1.2.3.2 Servicios de Windows para el control de accesos

Además de LDAP, Active Directory se puede aprovechar de servicios propios de Windows para otorgar seguridad en el acceso.

Existen específicamente cuatro servicios en Windows 2000 que pueden ser editados para otorgar o negar acceso a equipos específicos, los cuales se describen a continuación:

- **Access this Computer from de Network**: Permite otorgar a usuarios específicos el derecho de acceder por medio de la red al equipo en el que se configuren los permisos.
- **Deny Access to this Computer from de Network**: Deniega el derecho de acceso por medio de la red al equipo a usuarios especificados en la variable.
- **Log on Locally**: Permite iniciar sesión localmente a los usuarios especificados en la política.
- **Deny Logon Locally**: No permite el inicio de sesión a usuarios especificados en la política.

Todas las modificaciones y configuraciones de los servicios y atributos mencionados anteriormente se pueden realizar por medio de las plantillas de seguridad.

4.2.1.2.4 Filtrar el tráfico de correo electrónico

Para este punto AD se aprovecha de herramientas como Exchange o herramientas de terceros para evitar la propagación de software malicioso y SPAM.

El correo no deseado (SPAM) es una fuente potencial de propagación de software malintencionado como virus, gusanos, etc.

Muchas organizaciones tratan de proteger el correo electrónico corporativo instalando numerosos productos de seguridad, pero este enfoque es difícil de administrar y a menudo tiene efectos adversos sobre el rendimiento de los sistemas.

Para evitar estos problemas, las herramientas de filtrado de SPAM deben contar con las siguientes características:

- Protección multi niveles de filtrado para maximizar las detecciones
- Compatibilidad con Active Directory
- Niveles de confianza para los SPAM
- Protección contra virus, integrando sus acciones con el software antivirus
- Administración centralizada

El envío de SPAM es una técnica muy utilizada por los intrusos informáticos para tratar de vulnerar los sistemas y redes de computadoras realizando escaneos de direcciones o enviando software malintencionado que pueda comprometer la seguridad de la organización.

4.2.1.2.5 Minimizar el uso de claves estáticas

Por medio de políticas de seguridad delegadas a los distintos objetos del dominio, se utilizan mecanismos de control de acceso con autenticación robusta.

En la versión Windows NT 4.0 y en todas las versiones siguientes a esta, existe un apartado de Local Security Policies (Políticas Locales de Seguridad), en el cual se pueden realizar una serie de configuraciones referentes a políticas de seguridad de password. (Ver **Anexo # 2**, Configuración de Políticas de Seguridad de Passwords)

4.2.1.2.6 Actualizaciones de Seguridad

El Active Directory da la facilidad de distribuir software o scripts de seguridad para mantener los equipos de los usuarios debidamente actualizados y asegurados.

El Visual Basic Scripting (VBScript), permite desarrollar herramientas para el Active Directory que le permiten realizar una serie de operaciones masivas mediante una secuencia de comandos.

Por ejemplo, por medio de un VBScript se pueden cambiar masivamente los atributos de los objetos del AD.

Con las facilidades que brinda esta herramienta, se pueden programar secuencias de comandos que actualicen configuraciones de equipos masivamente o programe acciones que se realicen en cuanto los usuarios inicien sesión.

Otra de las facilidades que brinda el AD, es interactuar con herramientas de terceros tales como SMS, SUS, etc para la distribución de actualizaciones de seguridad tales como parches o services packs.

4.2.1.2.7 Limitar y controlar la utilización de dispositivos

Permite limitar a los usuarios la utilización de dispositivos periféricos tales como disqueteras, CDs, USB, Infrarrojo, etc, los cuales pueden ser utilizados por software malicioso para la infección de la red. (Ver **Anexo # 3**, Configuración de Seguridad en Dispositivos Perifericos)

4.3 Técnicas de Ataque a Equipos y Usuarios

Como se mencionó en el Marco Teórico, el número de ataques a sistemas y equipos ha venido en aumento en los últimos años. Esto ha provocado diversas reacciones en todas las organizaciones financieras.

Las instituciones financieras se han dado a la tarea de buscar métodos y técnicas innovadoras para fortalecer su seguridad; sin embargo, estas implementaciones no exoneran a la empresa de posibles ataques.

Según Theil, Ricardo (2004), "La tecnología es segura. El punto débil está en las personas".

Uno de los principales puntos débiles; que es ampliamente explotado por los intrusos informáticos, es la ignorancia o desconocimiento por parte de los empleados de la organización, acerca de las amenazas presentes en el ambiente informático.

La ingeniería social es una de las técnicas más comunes y efectivas utilizadas por los intrusos informáticos. Como ejemplo, y según indicó Theil, Ricardo (2004), el fraude más común en Brasil son los correos electrónicos falsos que solicitan a los clientes bancarios actualizar sus datos personales, y que permiten de esta manera a los criminales robar identidades y números de tarjetas de crédito; o bien, correos electrónicos que ofrecen premios por hacer que el usuario acceda una conexión web, pero que simultáneamente instalan programas para registrar su nombre y claves de Internet.

Así como el caso anterior, existen muchas otras técnicas enfocadas a vulnerar los sistemas o equipos. Es por ello que se hace necesario tener un panorama claro de los posibles ataques que se pueden realizar en una institución financiera, de manera que se pueda realizar un plan estratégico para atacar cada una de estas amenazas.

4.3.1 Tendencias en el ámbito del delito informático

Según el CERT® Coordination Center (2004), a continuación se describen las principales tendencias utilizadas para los ataques más comunes en nuestros días:

4.3.1.1 Primer Tendencia : Automatización y velocidad de las herramientas de ataque

El nivel de automatización y el grado de complejidad de las herramientas utilizadas por los intrusos informáticos hacen evidente el ingenio y las habilidades de estos individuos. Los ataques automatizados hacen referencia a las siguientes frases:

4.3.1.1.1 Escaneo de Víctimas Potenciales:

El escaneo extensivo ha sido muy común desde finales de los 90. Hoy las herramientas de exploración son más complejas y utilizan patrones de búsqueda más avanzados para maximizar el impacto y acelerar los resultados.

4.3.1.1.2 Sistemas comprometidos o vulnerables:

Anteriormente las técnicas utilizadas por los intrusos se basaban e escaneos extensivos en la red y una finalizadas estas exploraciones explotaban las vulnerabilidades existentes.

Este esquema ha cambiado en los últimos años, de manera que actualmente las herramientas de ataque explotan las vulnerabilidades como parte de su actividad de búsqueda, lo cual permite que la velocidad de propagación aumente considerablemente.

4.3.1.1.3 Propagación del ataque

Antes del año 2000 las herramientas utilizadas por los atacantes requerían que una persona iniciara el ataque y reiniciara ciclos de ataque adicionales; hoy las herramientas de ataque pueden reproducirse a si mismas.

Virus tales como CODE RED y NIMDA tienen la habilidad de reproducirse a si mismo a un punto tal que podrían lograr una infección global en menos de 18 horas.

4.3.1.1.4 Manejo coordinado de las herramientas de ataque

Desde 1999, con la llegada de las herramientas de ataque distribuidas, los atacantes han podido manejar y coordinar una gran cantidad de herramientas de ataques distribuidos desplegadas a través de muchos sistemas en el Internet.

Hoy las herramientas de ataques distribuidos son capaces de lanzar ataques de negación de servicio más eficientemente, buscando potenciales víctimas y comprometiendo sistemas vulnerables.

Las funciones de coordinación se aprovechan de protocolos de comunicaciones públicos tales como el Internet Relay Chat (IRC) y de mensajería inmediata (IM).

4.3.1.2 Segunda Tendencia: Incremento de la complejidad de las herramientas de Ataque

Sin duda alguna las técnicas utilizadas actualmente son más avanzadas que las utilizadas en el pasado. El código utilizado en las herramientas de ataque es cada vez más difícil de detectar a través de los sistemas firmados digitalmente tales como el software de antivirus y software para la detección de intrusos.

Existen tres características importantes que hacen a estas herramientas de ataque difíciles de detectar:

4.3.1.2.1 Naturaleza oculta

Las técnicas de los atacantes procuran ocultar la naturaleza de las herramientas utilizadas. Este ocultamiento de código hace que los expertos en seguridad pierdan tiempo valioso en el análisis de estas herramientas de ataque para entender su naturaleza, su comportamiento y analizar la vulnerabilidad que está explotando. Muchas veces este proceso lleva mucho tiempo en pruebas de laboratorio e ingeniería reversa.

.

4.3.1.2.2 Comportamiento dinámico

Las herramientas utilizadas en el pasado seguían un patrón de ataque en secuencias definidas. Las herramientas automatizadas de hoy pueden variar sus patrones de ataque y comportamientos basados en la selección al azar, trayectorias predefinidas o a través del manejo directo del intruso.

4.3.1.2.3 Modularidad de las herramientas de ataque

Las herramientas actuales pueden ser cambiadas rápidamente, aumentando o reemplazando porciones de código de la herramienta.

Esta situación provoca que los ataques sean desarrollados más rápidamente y que herramientas polimórficas evolucionen por sí mismas para ser diferentes en cada nuevo ataque.

Las herramientas de ataque se están desarrollando más comúnmente para ejecutarse en plataformas de múltiples sistemas operativos.

4.3.1.3 Tercer Tendencia: Descubrimiento acelerado de vulnerabilidades

Las vulnerabilidades descubiertas sobre la plataforma Microsoft crece más del doble cada año. Esto hace muy difícil la administración de la seguridad en los equipos, ya que continuamente se debe programar la aplicación de parches.

Adicional a esto, cada vez se descubren vulnerabilidades más complejas y dañinas para los sistemas; lo cual puede provocar que intrusos aprovechen estas vulnerabilidades antes de que los proveedores puedan corregirlas.

4.3.1.4 Cuarta Tendencia: Incremento en la permeabilidad de los Firewalls

Por lo general, los Firewalls son utilizados como el principal método de protección contra intrusos, sin embargo las nuevas tecnologías han sido diseñadas para penetrar fácilmente las configuraciones comunes de los Firewalls, con protocolos tales como IPP (Internet Printing Protocol), o el WebDAV (Web-based Distributed Authoring and Versioning).

La utilización de paquetes tales como los ActiveX, Java y JavaScript hacen difícil la implementación de seguridad ya que por su naturaleza oculta impide que software malicioso pueda ser descubierto.

4.3.1.5 Quinta Tendencia: Incremento de la amenaza asimétrica

La seguridad en Internet es altamente interdependiente. La exposición que tenga cada sistema del Internet a algún ataque depende, en gran medida, del estado de la seguridad del resto de los sistemas unidos al Internet.

Debido a los avances en la complejidad de los ataques, un solo intruso puede fácilmente emplear una gran cantidad de sistemas distribuidos para lanzar ataques devastadores contra una sola víctima.

4.3.2 Vulnerabilidades más utilizadas y técnicas de ataque

Existen varias causas por las cuales un sistema puede verse comprometido. Existen vulnerabilidades físicas y vulnerabilidades lógicas las cuales pueden ser aprovechadas por personas malintencionadas para realizar sus actos delictivos.

4.3.2.1 Vulnerabilidades físicas

Existe una gran cantidad de amenazas presentes en el ambiente informático que pueden afectar la integridad, disponibilidad y confidencialidad de la información, equipos y los sistemas.

Las amenazas físicas abarcan las siguientes situaciones:

- Accesos no autorizados a centros de procesamiento de datos
- Vulnerabilidades propias de equipos de comunicaciones o servidores
- Fallos de energía eléctrica o falta de aire acondicionado
- Accesos no autorizados a los armarios de almacenamiento de las cintas de Back-up.

Una persona malintencionada podría causar serios daños y pérdidas si materializa los riesgos presentes en las situaciones anteriores. Las personas que pueden causar daños se pueden clasificar en los siguientes grupos:

4.3.2.1.1 Empleados

Según Ardita, Julio (2002), más del 70% de los ataques a sistemas o equipos se producen internamente dentro de las empresas.

Los empleados de una empresa tienen acceso a información crítica que puede ser vulnerada fácilmente. Las principales causas por las cuales un empleado podría querer atacar un sistema son las siguientes:

- Robo de información confidencial para beneficio personal
- Fraude financiero
- Modificación de archivos críticos
- Sabotaje corporativo

Las fallas de seguridad producidas por empleados pueden ser intencionales por las causas anteriormente mencionadas, o pueden ser accidentes producidos por errores o desconocimiento.

Como ejemplo de esto, un empleado puede causar un grave problema de seguridad en alguna empresa con tan solo abrir un correo electrónico que contenga un virus.

4.3.2.1.2 Ex – Empleados

Generalmente estas son personas descontentas que quieren causar algún daño a la institución por razones personales o simplemente al conocer al detalle los sistemas que operan en la misma, se aprovechan de las debilidades que presentan para beneficio propio.

4.3.2.1.3 Hackers

Un **hacker** es un experto en el área tecnológica que disfruta de explorar los detalles internos de los sistemas informáticos.

No es una persona malintencionada; sin embargo, sus embates no benefician en nada la confiabilidad de un sistema de información, especialmente si estamos hablando de una institución financiera.

4.3.2.1.4 Crackers

Un **cracker** es una persona que ingresa en un sistema informático, de forma no autorizada, con intenciones de provocar daños o simplemente por la diversión de vulnerar un sistema.

4.3.2.2 Vulnerabilidades Lógicas

Así como existe una gran cantidad de amenazas físicas como las mencionadas anteriormente, existe también una gran variedad de amenazas lógicas que pueden causar serios daños a los sistemas.

Se clasifica como amenaza lógica a cualquier programa que pueda causar algún perjuicio a los sistemas.

Según J. M. Minguet Melian(2004), las amenazas lógicas se pueden clasificar en los siguientes grupos:

4.3.2.2.1 Virus

Son programas o secuencias de código que pueden modificar otros programas o insertarse dentro del código de otros ejecutables, esto con la finalidad de propagarse y liberar o ejecutar sus comandos malintencionados.

En la actualidad, el principal método de propagación que utilizan los **virus** son los correos electrónicos.

Algunos ejemplos de virus más reconocidos son: Viernes 13, Melissa, Love Letter, Back Orifice, The Tour of de Worm, y el Chernobyl.

4.3.2.2.2 Caballos de Troya

Los comúnmente llamados Troyanos, son instrucciones introducidas en la secuencia de código de otros programas y que realizan funciones no autorizadas, destruyen ficheros o capturan información mientras simulan efectuar funciones correctas.

4.3.2.2.3 Bombas Lógicas

Las bombas lógicas son un tipo de código malintencionado, introducido en un programa o aplicación, que se activa en determinadas condiciones tales como una fecha determinada, o la presencia o ausencia de un determinado dato en un registro.

Una bomba lógica puede estar inactiva por años y su efecto es la liberación de un virus o un troyano.

4.3.2.2.4 Remailers

Los Remailers son programas relacionados con la administración y gestión del correo electrónico, que pueden generar órdenes de envío de correos desde un origen a diversos destinatarios y a su vez, utilizar su libreta de direcciones para reenviarse a estos nuevos destinatarios, creando así una cadena de envíos. Actualmente es la manera más común de propagar virus

4.3.2.2.5 Electronic Mail Bombs

Los electronic Mail Bombs también son programas relacionados con el correo electrónico y permiten generar órdenes de envío de correos desde uno o varios orígenes, a un solo destinatario, generándole una gran cantidad de órdenes y mensajes, con el fin de bloquear su funcionamiento e impidiéndoles, por ejemplo, atender pedidos o responder consultas. A este efecto se le conoce como denegación de servicios (DoS).

Uno de los DoS más habituales consisten en la inhabilitación total de un determinado servicio o de un sistema completo, bien porque ha sido realmente bloqueado por el atacante o porque está tan degradado que es incapaz de ofrecer un servicio a los usuarios por la gran cantidad de peticiones que ha recibido por los electronic mail bombs.

4.3.2.2.6 Worms

Un **gusano** es un programa capaz de ejecutarse y propagarse por si mismo. . El gusano no necesita, a diferencia de los virus otro programa para funcionar y simplemente se va duplicando y ocupando memoria hasta que su tamaño desborda al sistema en que se instala, impidiéndole trabajar con normalidad.

En ocasiones los gusanos pueden dejar virus o troyanos insertados en el sistema en donde ataca.

4.3.2.2.7 Puertas Traseras (Back Doors)

Está técnica permite introducirse en los programas por puntos que no son los estándares o normales. En principio eran utilizados por los programadores para facilitar el proceso de pruebas, evitando tener que procesar todo el programa o sistema para probar algún módulo de código.

Si estas puertas falsas se mantienen en la versión operativa, bien de forma intencionada o por descuido; se crean agujeros en la seguridad de la aplicación que pueden ser utilizados por los hackers, crackers o software malintencionado para vulnerar el sistema.

4.3.2.2.8 Sniffers

Los Sniffers o rastreadores son programas que se ejecutan en una red informática y rastrean todas las transacciones que viajan por ella. El estudio de las tramas capturadas permite encontrar claves, passwords o números de tarjetas de crédito, que pueden ser utilizados de forma fraudulenta.

4.3.2.2.9 Software de Mensajería

Este tipo de programas son utilizados para el envío de mensajería entre usuarios de los sistemas. Si bien es cierto este no es software malintencionado, la falta de seguridad presente en su código y protocolos que utiliza hace que se vuelva un serio agujero de seguridad para cualquier infraestructura tecnológica.

Como ejemplo y según Symantec (2004), la mayor parte de las instituciones financieras utilizan la Mensajería Instantánea (IM) y la Interconexión Entre Abonados (P2P), ya que cada vez se están volviendo más populares entre sus empleados. Sin embargo, a diferencia del correo electrónico, IM y P2P a menudo tienen poca o ninguna seguridad instalada para protegerlos. De acuerdo con la última edición del Symantec Internet Security Threat Report (Informe sobre las amenazas a la seguridad en Internet emitido por Symantec), 19 de los 50 virus y gusanos más importantes utilizan las aplicaciones IM y P2P.

4.4 Hardware y Software especializados en seguridad

Bajo la plataforma Microsoft, existe una variedad de herramientas tanto propietarias como de terceros que fueron diseñadas para subsanar las debilidades presentes dentro de esta plataforma.

Se podría realizar una categorización de herramientas dependiendo de su funcionalidad, para lo cual se listan las siguientes categorías:

4.4.1 Software utilizado para la implementación de seguridad

4.4.1.1 Software Antivirus

Los antivirus son programas diseñados para la detección y prevención de virus y otros programas maliciosos conocidos.

Según Wikipedia (2005); un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus reconocidos.

Algunos antivirus cuentan con funciones avanzadas como la búsqueda de comportamientos típicos de virus (*técnica conocida como heurística*) o la verificación contra virus en redes de computadoras.

Algunos de los antivirus más reconocidos son los siguientes:

- Panda Software Antivirus
- Symantec Norton Antivirus
- Computer Associates eTrust InoculateIT
- McAfee Antivirus
- F-Secure Antivirus
- PC-Cillin

En general, las más grandes plataformas tecnológicas implementadas alrededor del mundo se encuentran ensambladas en la plataforma Windows; y tomando en cuenta que hoy por hoy Windows es el principal foco de ataques producidos por intrusos

informáticos, se hace necesario contar con algún tipo de protección contra programas malintencionados.

4.4.1.2 Parches de Seguridad

El tema de la seguridad en las empresas se está volviendo crítico en todos los niveles, ya que existen muchos sistemas e información crítica que está expuesta o vulnerable a ataques si no se cuenta con una adecuada política de aseguramiento.

Cada semana se descubren agujeros de seguridad o debilidades en los sistemas actuales, los cuales atentan contra la integridad, confiabilidad y disponibilidad de la información de las empresas.

Dichos agujeros de seguridad deben ser eliminados o según el caso minimizados con el fin de mitigar riesgos.

Según la Guía Microsoft de Gestión de Parches de Seguridad (2005, p.01.), “Microsoft se toma muy en serio las amenazas de seguridad, proporcionando rápidamente orientación y, cuando es necesario, parches de seguridad para las vulnerabilidades”.

La empresa Microsoft, libera parches de seguridad el segundo martes de cada mes para contrarrestar las vulnerabilidades descubiertas en su plataforma.

Dada la situación anterior y tomando en cuenta que las plataformas tecnológicas de las instituciones financieras, que son nuestro punto de estudio; son considerablemente grandes, se hace necesario contar con alguna estrategia de gestión de parches de seguridad.

Existen diversos productos en el mercado diseñados para la gestión de parches de seguridad y configuraciones, los cuales se describen a continuación:

4.4.1.2.1 System Management Server (SMS)

Esta herramienta fue diseñada por Microsoft y se especializa en realizar tareas automáticas y centralizadas en cuanto a la administración de infraestructuras tecnológicas.

Dentro de sus principales funciones se encuentran las siguientes:

- Distribución de Aplicaciones
- Gestión de Inventarios
- Gestión de Parches de Seguridad
- Administración de usuarios y equipos móviles

El SMS ayuda a la planificación, pruebas y distribución de aplicaciones y software especializado de una manera segura y eficiente por medio de puntos de distribución, lo cual permite abarcar un gran número de equipos. Adiciona a esto reduce costos operativos al realizar la administración de inventarios de forma centralizada.

4.4.1.2.2 LANDesk Server Manager

Este software ofrece altos niveles de seguridad y disponibilidad para servidores mediante herramientas de supervisión, evaluación de vulnerabilidades y distribución de parches. Además, contiene lógicas de análisis y predicción de errores de hardware y las herramientas para la recuperación rápida de equipos.

Dentro de sus principales funcionalidades se encuentran las siguientes:

- Detectar vulnerabilidades de seguridad y mantener los niveles de parches
- Supervisar el rendimiento del hardware y software en tiempo real y predecir errores de hardware
- Distribuir software, actualizaciones y herramientas mediante tecnología a petición bajo demanda
- Recuperar a través de la red, mediante el control remoto de la alimentación y las herramientas para la resolución de problemas, los equipos con IPMI que dejen de funcionar
- Configurar alertas sobre rendimiento, disponibilidad y recuperación

4.4.1.2.3 LANguard Network Security Scanner

Esta herramienta analiza la red mediante métodos potenciales que un intruso podría utilizar para atacarla. La detección de debilidades de seguridad se realiza mediante el análisis del sistema operativo y de las aplicaciones que se están ejecutando sobre los equipos de red. Las actualizaciones de seguridad se realizan escaneando la red y determinando los parches y service packs ausentes.

Sus principales características son las siguientes:

- Identifica debilidades de seguridad y recomienda la acción
- Rápido escaneo e identificación de puertos TCP y UDP
- Gestión de parches y service packs de toda la red
- Comprueba directivas de contraseñas
- Comprueba los programas que se inician automáticamente (Troyanos potenciales)
- Realiza un inventario de la red
- Proporciona una lista de recursos compartidos, usuarios (información detallada), servicios, sesiones, TOD (time of day) remoto e información del registro del equipo remoto (Windows)
- Detección de dispositivo SNMP, SNMP Walk para inspeccionar dispositivos de red como enrutadores, impresoras de red...
- Identifica todos los servicios Windows instalados.

4.4.1.2.4 Microsoft Software Update Services (SUS)

Esta herramienta también creada por Microsoft, está diseñado para simplificar el proceso de mantener sistemas basados en Windows con las últimas actualizaciones de seguridad (parches).

Los servicios de SUS del lado del cliente se basan en la tecnología del Windows Automatic Updates.

Las características principales de este software son las siguientes:

- Permite la actualización automática de parches de seguridad y services packs
- Permite la selección y aprobación de los parches de seguridad que se quieren instalar en los equipos
- Permite la sincronización entre servidores
- Administración remota
- Estatus de las actualizaciones

4.4.1.3 Services Packs (SP)

Los Service Packs son el conjunto acumulado de todos los parches de seguridad liberados y las correcciones para errores encontrados internamente desde la publicación del producto. Los Service Packs pueden contener también un número limitado de peticiones del cliente para cambios de diseño u otras características.

Adicional a esto, los Service Pack puede cambiar la lógica de los programas para agregarles funcionalidades de seguridad o lógica, como el SP2 de Windows XP que le adicionó un firewall personal a estaciones de trabajo.

En Microsoft Windows los Service Packs pueden ser descargados desde la página de Windows Update (http://windowsupdate.microsoft.com/) o bajando el archivo directamente desde http://www.microsoft.com/.

4.4.1.4 Antispyware

Los "spyware" son programas espía o parásitos, los cuales pueden entrar en algún equipo simplemente accesando algún enlace en Internet.

Estos programas permiten el robo de información abriendo agujeros al exterior. Algunos degradan las conexiones de red y el funcionamiento de los equipos ya que realizan envíos masivos de paquetería desde el equipo infectado, lo cual puede causar problemas de Negación de Servicio.

Algunos ejemplos de spyware son Gator, Xupiter o CoolWebSearch, los cuales se instalan en cuanto se accede a enlaces no seguros. Estos programas pueden instalar otros programas malintencionados, espíar la navegación web, o también robar los datos introducidos en formularios, documentos y claves de acceso. Envían secretamente la información a su base, donde se procesa y vende, sobre todo a empresas de correo basura.

En los últimos años, los spyware se han diseminado exponencialmente y también los programas que los detectan y eliminan, la mayoría gratuitos; por ejemplo, el Adware, Spybot, SywareBlaster y SpywareGuard.

Los programas Antispyware son relativamente nuevos, por lo cual se podría decir que todavía están en pañales. Hasta hace poco no eran capaces de detectar firmas específicas en ficheros, "cookies", o el registro de Windows. Aun no aplican mecanismos heurísticos, por lo cual la detección de spyware es deficiente.

4.4.1.5 Certificados Digitales

Los certificados son documentos electrónicos que contiene información de identificación del usuario o servidor, la cual es utilizada para verificar la identidad y ayudar a establecer un vínculo de seguridad mejorada.

Una persona o entidad dueña de un certificado, firma digitalmente la información que quiere transmitir de manera que cuenta con buenas garantías de seguridad con respecto a los siguientes elementos:

- **Autenticación:** el receptor tiene la seguridad que el emisor es quien asegura ser.
- **Confidencialidad del mensaje:** que solo lo pueda leer el destinatario.
- **Integridad del documento:** que no presente ninguna alteración
- **No repudio:** el mensaje una vez aceptado, no puede ser rechazado por el emisor.

Un certificado digital cuenta con una clave pública y una firma digital. Las claves públicas son emitidas y administradas por entidades emisoras de certificados (CA), las cuales son quienes firman digitalmente los certificados, asegurando su integridad y certificando la relación existente entre la clave pública contenida y la identidad del propietario. La CA es la que garantiza la validez de los certificados.

Por su parte una firma digital es la información que es incluida con un mensaje o es transmitida separadamente, la cual se utiliza para identificar y autentificar al emisor y la información del mensaje. Una firma digital también puede confirmar que el mensaje no haya sido alterado.

Para su correcto funcionamiento, los certificados digitales deben contener la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

4.4.1.6 IPSec (Internet Protocol Security)

IPSec es un protocolo utilizado en plataformas abiertas para obtener comunicaciones privadas seguras bajo redes que trabajan con IP (Internet Protocol).

Según Microsoft TechNet* (2004, par. 7.), IPSec ofrece privacidad, integridad, autenticidad y protección de los datos en una red en particular. El equipo emisor protege los datos antes de la transmisión y el equipo receptor los descodifica una vez que los ha recibido. IPSec se basa en claves criptográficas y se puede utilizar para proteger equipos, sitios, dominios, comunicaciones de aplicaciones, usuarios de acceso telefónico y comunicaciones de extranets.

Adicional a esto IPSec posibilita la implementación de controles de autenticación y encriptación en diferentes niveles de la plataforma tecnológica en la que se implemente; define los formatos de paquetes IP y la infraestructura relacionada para proporcionar una eficaz autenticación de principio a fin, integridad, protección contra reproducción y confidencialidad para el tráfico de red.

Es importante señalar que para la implementación de esta solución es necesario contar con un servicio de directorio bien definido, que posibilite la implementación de políticas adecuadas de seguridad según los ámbitos de los equipos en que se vayan a aplicar.

4.4.1.7 Detectores de Intrusos

La lógica de un sistema de detección de intrusos se basa en el escaneo continuo de la red con la finalidad de detectar actividades sospechosas provenientes desde el interior o exterior de la red.

Según Borghello, Cristian(2001), los sistemas de detección de intrusos se pueden dividir en los siguientes grupos según su función y comportamiento:

- **Host – Based IDS**: operan en un host para detectar actividades maliciosas en el mismo.
- **Network – Based IDS**: operan sobre flujos de información intercambiados en una red.
- **Knowledge – Based IDS:** sistemas basados en conocimientos.
- **Bahavior – Based IDS**: basados en el comportamiento de los usuarios para detectar actividades anómalas.

Un sistema detector de intrusos debería contar con las siguientes características:

- Funcionar sin la intervención humana
- Tolerante a fallos
- Consumir pocos recursos en la máquina cliente
- Observar desviaciones sobre el comportamiento estándar

Los sistemas de detección de intrusos ayudan a reaccionar oportunamente para evitar daños por ataques a la red. Es una herramienta muy útil, en cualquier arquitectura tecnológica, en cuanto a seguridad se refiere, ya que ayuda a prevenir ataques o, según el caso, a recoger evidencia sobre comportamientos inadecuados, lo cual dificulta el trabajo del intruso de eliminar sus huellas.

4.4.2 Hardware utilizado para la implementación de seguridad

4.4.2.1 Firewalls

Para nadie es secreto que en los últimos tiempos la creciente demanda de servicios en línea ha provocado que las empresas deban implementar una serie de servicios potencialmente vulnerables en sus plataformas tecnológicas tales como servicios FTP, Web Services (IIS), E-Mail, TELNET, etc.

Un Firewall es un sistema o grupo de sistemas que impone una serie de reglas básicas en las comunicaciones, dependiendo de las políticas de seguridad de la organización, entre la red privada (LAN) y la red pública (Internet).

El Firewall determina los servicios disponibles y controla quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información que provenga de algún ente externo deberá pasar a través del mismo, donde podrán ser inspeccionadas las tramas que ingresen a la red privada.

Los Firewalls pueden ser de software o de hardware por medio de routes.

4.4.2.2 Biometría

Según Borghello, Cristian (2001), la biometría se define como la parte de la biología que estudia de forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estáticos.

La biometría es una tecnología que realiza mediciones electrónicas y compara características únicas para la identificación de personas por medio de dispositivos especializados para este propósito.

La lógica de identificación de la biometría consiste en la comparación de características físicas de cada persona por medio de un patrón conocido el cual fue previamente registrado y almacenado en una base de datos

Los lectores biométricos identifican a la persona por medio del escaneo corporal de la misma, como las manos, ojos, huellas digitales, la voz, etc. Esto elimina la necesidad de contar con tarjetas de acceso.

Algunas de las mediciones biométricas que se pueden aprovechar para establecer un sistema de seguridad son las siguientes:

4.4.2.3 Emisión de calor:

Se mide la emisión del calor del cuerpo, con lo cual se crea un mapa de valores sobre la forma de la persona; esto se conoce como termograma.

4.4.2.3.1 Huella digital:

Las huellas digitales tienen la particularidad de ser únicas para cada persona, por lo cual es una de las mediciones más utilizadas por la biometría.

Una huella digital posee pequeños arcos, ángulos o remolinos diseñados de forma única para cada persona, las cuales son fácilmente digitalizadas.

4.4.2.3.2 Verificación de la voz:

Para esta medición, se realiza previamente una grabación de una o varias frases de la persona que se quiere identificar. Para esta medición la biometría se aprovecha de características de la voz tales como la entonación, diptongos, la agudeza y el timbre.

Este sistema tiene el problema que es sensible a factores externos tales como el ruido, enfermedades de la persona que afecten la voz o el envejecimiento de la misma.

4.4.2.3.3 Verificación de patrones oculares:

Las mediciones realizadas se basan en patrones del iris o de la retina del ojo. Es considerada como la técnica más segura de biometría; sin embargo, su principal enemigo es la desconfianza de la gente por los efectos negativos que le pueda traer el continuo escaneo del iris de sus ojos.

La aplicación de esta tecnología es práctica y muy segura, sin embargo su principal desventaja son los costos iniciales de adquisición.

4.5 Mejores Prácticas y Técnicas de Aseguramiento

En la actualidad toda organización está expuesta a debilidades o amenazas que se presentan en su infraestructura tecnológica debido a las vulnerabilidades propias de la tecnología.

Esta situación influye en la necesidad de contar con planes estratégicos concebidos para subsanar estas amenazas y conjuntamente justifican la decisión de adoptar diversas medidas para prevenir riesgos y minimizar sus consecuencias.

Los riesgos presentes en los sistemas informáticos están estrechamente relacionados con la evolución de la tecnología, lo cual obliga a frecuentes cambios en los métodos de protección y las medidas de seguridad con que cuenta el ambiente tecnológico, esto con la finalidad de anticiparse a las nuevas posibles amenazas.

4.5.1 Mejores prácticas para asegurar el entorno

Según J. M. Minguet Melian (2004), la protección de la infraestructura tecnológica se debe realizar por medio de defensas o medidas de seguridad administrativas, físicas y lógicas.

4.5.1.1 Medidas de Seguridad Administrativas

El primer paso para contar con un buen sistema de seguridad para la defensa y protección de la infraestructura tecnológica es que los mandos administrativos del departamento de Tecnología estén identificados con el tema de seguridad.

La creación de un ente regulador y responsable de la seguridad de la información y la plataforma tecnológica dentro de una organización, es fundamental para poder contar con un plan estratégico para el aseguramiento del ambiente informático.

Es importante que se generen políticas, procedimientos y estándares sobre las sanas prácticas de seguridad informática que se deban aplicar en toda la organización y, más importante aún es el seguimiento y controles que se debe realizar para velar por el cumplimiento de esta reglamentación por medio de auditorias internas o externas.

4.5.1.2 Defensas Físicas

Las defensas físicas abarcan las siguientes prácticas:

- Definir controles de acceso a los centros de cómputo o cualquier sitio que tenga acceso a equipo de cómputo o información crítica de la empresa.
- Contar con equipos de contingencia que garanticen la continuidad del negocio (equipos duplicados y aislados geográficamente).
- Los equipos de cómputo deben ser tolerantes a fallos (fuentes de poder redundantes, tarjetas de I/O redundantes, contratos de mantenimiento en caso de fallos).
- El centro de computo debe contar con piso falso y el cableado tanto eléctrico como de datos, debe estar protegido.
- El sitio en donde se ubiquen los equipos de cómputo debe contar con los siguientes componentes:
    - Sistema de aires acondicionados con controles de temperatura y humedad relativa del ambiente.
    - Equipos de contingencia para el caso de fallos de corriente (UPS, plantas eléctricas secundarias)
- Contar con un centro de procesamiento de contingencia en otra ubicación física.
- Sistema de cámaras de seguridad (circuito cerrado)

Las defensas físicas son una parte integral de cualquier plan de seguridad de TI, ya que brindan defensas tangibles sobre la protección con que se cuenta.

4.5.1.3 Defensas Lógicas

Las defensas lógicas consisten en la aplicación de políticas y procedimientos por medio de los cuales se resguarde el acceso a la información o los sistemas presentes en la infraestructura tecnológica, de manera que solamente puedan acceder a ellos las personas autorizadas a hacerlo.

Según Borghello, Cristian (2001), las defensas lógicas se establecen con los siguientes objetivos:

- Restringir el acceso a programas o archivos
- Que los usuarios tengan acceso solamente a lo que realmente necesiten

- Asegurar que los datos, archivos y programas sean utilizados correctamente y que esta utilización sea acorde con el procedimiento.
- Que la información transmitida sea recibida solamente por el destinatario al cual fue enviado.
- Que la información recibida sea la misma que la trasmitida.

En este punto es donde existe una mayor variedad de estándares y mejores prácticas en el mercado que pueden ser aplicables en un ambiente tecnológico abierto. La protección lógica va desde la configuración de seguridad en los equipos hasta la instalación de antivirus y firewalls o la implementación de cifrados de los datos.

Según Borghello, Cristian (2001), estos son los tipos de defensas lógicas que se pueden implementar bajo un esquema de mejores prácticas:

4.5.1.3.1 Controles de Acceso

Los controles de acceso son aplicables al sistema operativo, bases de datos y aplicaciones por medio de la autenticación con un usuario y password.

En un ambiente de red, el control de acceso asegura que los recursos tecnológicos presentes no van a sufrir modificaciones o accesos no autorizados, con lo cual se asegura la integridad de la información crítica y no crítica de la empresa.

Según el Nacional Institute for Standards and Technology (2005), se definen los siguientes requisitos mínimos de seguridad en cuanto al control de accesos:

4.5.1.3.1.1 Identificación y Autorización:

Previene el acceso de personas no autorizadas a los sistemas, bases de datos o aplicaciones. Permite dar un seguimiento de los controles de acceso y actividades de los usuarios por medio del registro y seguimiento de las acciones realizadas por lo mismos

En una infraestructura de red, es conveniente que los usuarios sean identificados y autenticados desde un punto central (servidor de autorizaciones), a partir del cual se otorgue o no el permiso para utilizar los recursos de red según el perfil que tenga asignado el usuario.

La administración de la identificación, autenticación y autorización de acceso abarca lo siguiente:

- Creación, manejo, seguimiento y cierre de las cuentas de usuario.
- Definición de roles, perfiles y permisos
- Revisión periódica de permisos de acceso
- Detección de actividades no autorizadas
- Mantenimiento de las cuentas de usuario (actualización de información y eliminación de cuentas innecesarias)

4.5.1.3.1.2 Roles o Perfiles

Se deben definir roles según las funciones de los usuarios, de manera que se pueda definir una lista de accesos comunes que pueden ser asignados a un grupo de usuarios en particular.

En el caso de una empresa financiera se podrían definir los siguientes roles dependiendo de las funciones que deben realizar los usuarios y los sistemas que deben acceder: Cajeros, Plataformistas, Área Administrativa, Crédito, Desarrolladores, etc.

4.5.1.3.1.3 Modalidad de Acceso

Se debe definir el nivel de permisos con que cuenten los usuarios a la hora de interactuar con la información. Se pueden delegar los siguientes permisos según el rol asignado al usuario y sus necesidades:

- **Lectura:** El usuario tiene permisos de leer o visualizar la información pero no puede alterarla.
- **Escritura:** Permite agregar, modificar o eliminar información
- **Ejecución:** Otorga el privilegio de ejecutar programas o aplicaciones
- **Borrado:** Permite eliminar información o recursos del sistema.

Para los permisos de Escritura y Borrado se debe definir muy claramente cuales van a ser las personas autorizadas de realizar estas funciones, ya que por si solos son permisos riesgosos.

4.5.1.3.1.4 Ubicación y Horario

El acceso de los usuarios puede estar determinado por la ubicación lógica o física del mismo; adicional a esto se pueden definir rangos de horas para el acceso a sistemas o equipos críticos. Esto ayuda a controlar que los accesos se realicen solamente cuanto sea necesario.

4.5.1.3.1.5 Palabras Clave:

Se utilizan para la autenticación de usuarios a nivel de sistema operativo, bases de datos o aplicaciones.

Es uno de los controles de acceso más eficientes y baratos; sin embargo, uno de los principales problemas con que cuentan las palabras claves es que, por lo general, a los usuarios se les hace difícil recordar claves complejas, por lo cual utilizan palabras fácilmente deducibles.

Para este punto es importante señalar los siguientes puntos que deben ser considerados a la hora de crear una política de utilización de passwords:

- **Complejidad del password:** Es importante que se establezcan características mínimas con que debe contar un password, de manera que se asegure hasta cierto grado la complejidad del mismo; por ejemplo, el largo en caracteres, la utilización de caracteres especiales y números.

  Según Quesada, Omar (2005), una buena práctica en el establecimiento de password es la utilización de “frases” en vez de palabras clave, ya que para las herramientas de hacking utilizadas actualmente se hace más difícil descifrar este tipo de contraseñas.

- **Caducidad y Control:** Es una buena práctica establecer un período de validez de los passwords, de manera que se obligue a los usuarios a realizar cambios periódicos. Adicionado a esto, es importante establecer políticas por medio de las cuales se le dificulte al usuario utilizar claves iguales a las utilizadas anteriormente y por medio del control se pueden establecer reglas que permitan controlar los intentos fallidos y bloquear las contraseñas. (Ver **Anexo # 2**, Configuración de Políticas de Seguridad de Passwords)

4.5.1.3.2 Herramientas de Seguridad

Existen herramientas que pueden ser utilizadas para asegurar el entorno tecnológico,; dentro de estas herramientas podemos mencionar las siguientes:

4.5.1.3.2.1 Encriptación

Por medio de esta técnica se asegura que la información que viaje dentro de la red no va a ser modificada o capturada por personas no autorizadas.

La encriptación posibilita un control estricto de acceso a la información ya que dicha información solo va a poder ser desencriptada por quienes posean la clave apropiada.

4.5.1.3.2.2 Listas de control de acceso (ACL)

Se debe definir un registro con los nombres de usuarios o grupo de usuarios a los cuales se les otorgaron permisos de acceso a un determinado recurso en el sistema, así como los permisos específicos (lectura, escritura, actualización o eliminación) que le fueron otorgados.

Estas listas pueden ser utilizadas para controlar los accesos a aplicaciones según los módulos que deban utilizar.

4.5.1.3.2.3 Utilización de Firewalls

La utilidad de este componente puede ser utilizado para controlar y filtrar el tráfico que existe entre dos redes de computadoras, comúnmente entre redes públicas y privadas.

Los **firewalls** permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que impide o previene la intromisión de atacantes a los sistemas de la organización.

4.5.2 Técnicas para el Aseguramiento

Los métodos de defensa antes mencionados son muy útiles para asegurar la infraestructura tecnológica ya que por medio de ellos se logra minimizar el riesgo de un posible ataque; sin embargo las defensas físicas y lógicas pueden dar una sensación de falsa seguridad en la organización ya que auque son muy importantes, no aseguran que los sistemas no sigan siendo vulnerables.

Recordemos que la mayoría de los agujeros de seguridad en una organización son ocasionados por las malas prácticas de usuarios de los sistemas internos. La ingeniería social es una técnica muy utilizada por los intrusos informáticos para tratar de vulnerar los sistemas, aprovechándose de estas malas prácticas de los usuarios.

Es por lo anterior que los administradores de la seguridad de la información deben probar técnicas innovadoras para contrarrestar las debilidades propias de la infraestructura. A continuación algunas de las técnicas utilizadas por los expertos en cuanto al aseguramiento de sus sistemas.

4.5.2.1 Vulnerar para proteger

Los intrusos informáticos intentan vulnerar los sistemas y aplicaciones buscando puntos débiles que puedan ser utilizados para ingresar en forma no autorizada a los mismos.

Estas técnicas de escaneo pueden ser utilizadas también con fines benéficos por los administradores de la infraestructura tecnológica para conocer las zonas vulnerables de los sistemas y así crear un plan de acción para corregir lo encontrado.

A esta técnica se le conoce como pruebas de penetración y como el nombre lo dice, su finalidad es tratar de vulnerar los sistemas para tratar de ingresar en ellos por medio de métodos no comunes.

Esta técnica es ampliamente utilizada por los responsables de seguridad de la información para tratar de entender las formas de ataque de los intrusos y así crear barreras cada vez más eficaces.

Herramientas tales como el Internet Nessus o el Internet Scanner (ISS) posibilitan realizar pruebas de penetración parametrizando las acciones, evaluaciones y ataques que se quieren realizar contra los equipos escaneados.

4.5.2.2 Administración de la Seguridad

La autenticación, autorización y auditoria son partes fundamentales de una adecuada administración de la seguridad. Todas las políticas institucionales enfocadas en seguridad deben tomar en cuenta estos tres puntos para que sea efectiva.

Los métodos utilizados más comúnmente para asegurar la autenticación, autorización y auditoria de la información y sistemas son los siguientes:

- **Sistemas de detección de intrusos:** Analizan bitácoras de los sistemas en busca de patrones de comportamiento sospechosos.

- **Sistemas de análisis de vulnerabilidades:** Escanean los equipos en busca de vulnerabilidades conocidas

- **Sistemas de protección a la integridad de la información:** Mediante criptografía verifican y aseguran que la información no sea alterada de manera no autorizada.

- **Sistemas de protección a la privacidad de la información:** Herramientas que por medio de criptografía se aseguran que la información no sea visible para que no tiene autorización.

4.5.2.3 Seguridad en protocolos y servicios

Todos los protocolos existentes son vulnerables en un mayor o menor porcentaje. Uno de los errores más comunes de las empresas es tener activos en sus equipos servicios que las aplicaciones realmente no requiere, lo cual produce un riesgo potencial, máxime si no se han realizado procesos de aseguramiento sobre estos servicios innecesarios.

Según Borghello, Cristian (2001), “es necesario seguir un consejo básico: minimizar el número de usuarios en la máquina y minimizar el número de servicios ofrecidos en ella”.

Los equipos dedicados a brindar un servicio en específico deberían contar solamente con los servicios necesarios para brindar dicho servicio.

4.5.2.4 Plantillas de Seguridad

Una plantilla de seguridad reúne un conjunto de políticas del sistema en donde se establece la configuración de los objetos que afecta.

En una infraestructura administrada por Active Directory, las plantillas de seguridad se pueden aplicar a nivel de dominio, de controlador de dominio, sitio, equipo local o por unidad organizacional (UO).

Esta división permite que se establezcan perfiles a los cuales se les pueden asignar permisos específicos, dependiendo de los recursos de red que deban utilizar, y especificar lo que los usuarios pueden hacer con esos recursos.

Todas las mejores prácticas y técnicas mencionadas anteriormente tienen un factor común: la utilización de un punto central de autenticación, a partir del cual se deben distribuir las políticas de seguridad que se quieran implementar.

Es en este punto en donde Active Directory se convierte en una poderosa herramienta por medio de la cual se pueden orquestar políticas de seguridad, mediante la utilización de perfiles comunes ordenados previamente en su infraestructura.

En la implementación de Active Directory se debe crear una estructura organizativa, acorde con las áreas de trabajo o tareas comunes, con el fin de establecer esta distribución de seguridad de manera eficiente. El planteamiento de la estructura ideal se realizará en el siguiente capítulo.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

5.1.1 Amenaza Presente

A través del diagnóstico de este trabajo se dieron varios datos estadísticos referentes a la creciente cantidad de ataques de índole tecnológico que están sufriendo grandes empresas a nivel mundial; adicional a esto, se mencionaron las grandes pérdidas económicas provocadas por dichos ataques.

Analizando esta situación desde otro punto de vista, ninguna gráfica o estadística mencionada puede estimar a ciencia cierta la pérdida de imagen y confiabilidad, de cara al usuario, que significan estos ataques. En el caso particular de las instituciones financieras, la pérdida de confianza y credibilidad puede perfectamente provocar la banca rota de la organización afectada, ya que los clientes no van a arriesgarse a tener su capital en una institución que demostró ser vulnerable.

El crecimiento del delito informático, sumado a la tendencia actual de automatización de las organizaciones, han hecho una necesidad el contar con una plataforma tecnológica robusta y un plan de seguridad empresarial definido para salvaguardar la integridad, disponibilidad y confidencialidad de la información, usuarios y sistemas.

5.1.2 Diseño Seguro

Históricamente, las organizaciones siempre han pensado en la operabilidad y la funcionalidad de las aplicaciones y sistemas que implementan, y nunca se han desgastado en indagar si dichas implementaciones son seguras.

Con el análisis realizado se concluye que ahora más que nunca el tema de seguridad debe estar de la mano con la operabilidad y funcionalidad de los sistemas, lo cual implica que los esfuerzos de asegurar la infraestructura no se un intento o iniciativa aislada de un departamento en la organización, sino que sea responsabilidad de todas las áreas de tecnología.

Existe la necesidad de crear conciencia dentro de la organización sobre los temas de seguridad y esto solamente se logra con programas de comunicación y capacitación que den a conocer las políticas y disposiciones institucionales sobre el tema.

5.1.3 Herramientas para el Aseguramiento

Existe una gran cantidad de herramientas desarrolladas exclusivamente para brindar seguridad a las infraestructuras tecnológicas. Dichas soluciones, tanto de hardware como de software, fortalecen puntos débiles en las plataformas y dominios tecnológicos, de manera que se minimizan los riesgos presentes en el ambiente hostil en el que vivimos.

Por lo general, estas herramientas existen en las organizaciones; sin embargo, son subutilizadas. Ello provoca que su verdadero valor, en cuanto al aseguramiento que pueden brindar, raramente se aprovecha.

5.1.4 Metodologías Utilizables

Existen muchas metodologías que pueden ser utilizadas para brindar seguridad a la organización, pero al igual que en el caso de las herramientas de seguridad a veces son subutilizadas o simplemente no son aplicadas.

Del presente trabajo se puede concluir que en el mercado existe un mundo de posibilidades en cuanto al aseguramiento de las plataformas tecnológicas, sin embargo, aún muchas empresas no le toman el interés que deberían, tomando en cuenta los riesgos actuales presentes.

5.1.5 Utilizar Active Directory

Si se toma como premisa que en el mundo financiero la mayoría de organizaciones poseen su infraestructura tecnológica basada en la plataforma Microsoft, la utilización de Active Directory es una buena opción para subsanar muchas de las vulnerabilidades y riesgos presentes en el ambiente informático, dadas las utilidades y facilidades que brinda.

5.2 RECOMENDACIONES

5.2.1 Implementar Active Directory

Las configuraciones de seguridad de Active Directory han demostrado subsanar el foco de algunos de los tipos de ataques mencionados en el diagnostico.

Para implementar seguridad por medio de Active Directory se recomienda lo siguiente:

- Establecer una estructuración de AD bien definida según la propuesta realizada.
- Definir políticas de seguridad en el nivel organizacional con la finalidad de contar con pautas por seguir que cuenten con el aval de la gerencia de la organización.
- Traducir dichas políticas en plantillas de seguridad que deberán ser aplicadas a todos los objetos presentes en el dominio tecnológico.
- Monitorear y controlar la adecuada aplicación de las políticas.
- Crear procesos de mejoramiento continuo para las políticas y configuraciones.

5.2.2 Complementar Active Directory con otras herramientas

La utilización y aseguramiento de la plataforma tecnológica por medio de Active Directory solamente es una pequeña parte del aseguramiento que se debe realizar por medio de plan de seguridad empresarial.

Paralelamente a la aplicación de plantillas de seguridad se deben implementar herramientas tales como **detectores de intrusos**, firewalls, **antivirus**, configuración segura de equipos de comunicaciones, certificados digitales etc que ataquen focos de posibles ataques que no se cubren con las configuraciones aplicadas con el AD.

5.2.3 Mejoramiento Continuo

Al implementar seguridad, se debe estar conciente que esta no es una labor estática. Las estrategias de aseguramiento deben estar sometidas a un proceso de mejoramiento continuo ya que día con día crecen los riesgos tecnológicos.

Para la plataforma Microsoft se recomienda la implementación del modelo MOF (Microsoft Operations Framework), bajo el cual se dan pautas a seguir para implementar seguridad y posteriormente mantenerse seguro.

CAPÍTULO 6

PROPUESTA PARA LA IMPLEMENTACIÓN DE SEGURIDAD CON ACTIVE DIRECTORY

6.1 Estructura del Active Directory

La confección y diseño de la infraestructura de Active Directory es el primer paso para poder realizar una buena planeación de distribución y control de seguridad en un ambiente de red en la plataforma Microsoft.

Como se mencionó anteriormente, las instituciones financieras cuentan con una infraestructura tecnológica muy compleja. Por esta razón se hace evidente la necesidad de contar con una estructura organizativa adecuada, que permita agrupar factores comunes entre los recursos de red, y poder así atacar las vulnerabilidades presentes en la infraestructura tecnológica, tomando en cuenta los atributos de la misma.

El diseño del Active Directory se va a convertir en un factor crítico de éxito en la implementación de seguridad utilizando esta herramienta. Ver **Anexo # 11**, Guía para la instalación de Active Directory.

La propuesta que se presenta a continuación, está enfocada hacia la creación de una estructura del Active Directory correcta para una institución financiera; la misma se basa en las mejores prácticas recomendadas por Microsoft para la implementación de Infraestructuras Tecnológicas basadas en AD.

Además, durante la propuesta de estructuración del AD, se tomará en cuenta las experiencias de los expertos entrevistados, a saber Omar Quesada de Biznet S.A; la cual es Partner Certificada de Microsoft para Costa Rica, y Ruben Ching, el cual es administrador de la Infraestructura de Active Directory para el Banco Nacional de Costa Rica.

Según la Guía de Seguridad de Windows Server2003 (2005), cuando se crea una arquitectura de Active Directory se recomienda considerar los siguientes puntos:

6.1.1 Establecer los límites del directorio

Los límites del AD definirán el bosque, el dominio, la topología del sitio y la delegación de permisos. Estos límites deben ser definidos en relación con las políticas y necesidades de la organización.

Para el caso específico de las instituciones financieras, se recomienda los siguientes límites en el AD:

- Un bosque único para toda la infraestructura tecnológica.
- Un dominio central que controlará la Casa Matriz de la institución financiera, las Oficinas y las Agencias de la misma. En caso de que se cuente con una infraestructura de red limitada en cuenta a la capacidad de los enlaces, se podría plantear la existencia de más de un dominio y hacer relaciones de confianza dentro del mismo bosque.
- División de la infraestructura de red en los OUs correspondientes según las características de los equipos y recursos presentes.
- División de Recursos de Red por departamentos y servicios.

6.1.1.1 Limites de seguridad

Es posible que la organización necesite considerar la división del control administrativo de los servicios y datos dentro del diseño de Active Directory, con el fin de tener un control más estricto de la seguridad que se debe manejar en el mismo.

El diseño de Active Directory planteado, requiere entender completamente los requisitos de la organización en cuanto a la autonomía y aislamiento de los servicios, así como en cuanto a la autonomía y aislamiento de los datos.

Es por esto que en la definición de la estructura del AD, se debe realizar una división de los recursos de red, según las características comunes de los servicios que brindan y los departamentos que soportan, según recomendó Quesada, Omar (2005) en su entrevista.

6.1.1.2 Límites administrativos

Según la estructuración realizada en relación con los servicios prestados y los departamentos soportados, Ching, Ruben (2005) recomienda definir los diferentes niveles de administración requeridos para gestionar los OUs; es por tal motivo que se deben definir los siguientes niveles de administración:

6.1.1.2.1 Administradores de servicios

Los administradores de servicios son los encargados de mantener y ejecutar servicios de los controladores de dominio; son responsables de asegurar la disponibilidad de los servicios.

Dependiendo de las necesidades organizacionales, los administradores de servicios se pueden dividir por funciones en otros grupos que quizá se necesite incluir en el diseño del Active Directory, a saber los siguientes:

- **Administradores de Dominio:** responsables de los servicios de directorio; estos administradores deben ser personas altamente confiables.
- **Administradores del DNS:** responsables de la administración del sistema de nombres del dominio. Su responsabilidad es plantear el diseño del DNS y administrar la infraestructura del mismo.
- **Administradores Locales (OUs):** responsables de administrar los datos almacenados dentro de la OU de Active Directory asignado.
- **Administradores de Servidores de Infraestructura:** responsables de la administración y diseño de servicios tales como WINS o DHCP.

6.1.1.2.2 Administradores de datos

Los administradores de datos son responsables de administrar datos almacenados en el AD o en estaciones de trabajo que se unen al AD. Estos administradores de datos no tienen control sobre la configuración o servicios del AD.

Algunas de las tareas diarias de los administradores de datos incluyen:

- Controlar un subconjunto de objetos en el AD
- Administrar las estaciones que son miembros del AD y los datos que residen en las mismas.

6.1.2 Estructura de las Unidades Organizacionales (OUs)

Los OUs ofrecen una manera fácil de agrupar usuarios, recursos y políticas de seguridad; también proporcionan un mecanismo efectivo para segmentar los límites administrativos.

Adicional a esto los OUs facilitan la aplicación de políticas de grupo (GPOs) con base en el rol del servidor o recurso por medio de plantillas de seguridad.

Según recomendó Quesada, Omar (2005) en su entrevista, en el caso de instituciones financieras es importante segmentar de una manera adecuada las equipos tomando en cuenta sus roles y funcionalidades.

Para este fin la propuesta plantea la creación de las siguientes Unidades Organizacionales:

6.1.2.1 OUs para la Administración de Servidores

Crear grupos administrativos proporciona a los administradores una manera de segmentar grupos de usuarios, grupos de seguridad o servidores en contenedores para una administración autónoma.

Para saber como crear los OUs ver **Anexo # 4**, Cómo crear Unidades Organizacionales en Active Directory.

Para este fin la Guía de Seguridad de Windows Server2003 (2005), recomienda crear los siguientes OUs con fines administrativos:

6.1.2.1.1 OU de Servidores Miembro

En este contenedor van a residir todos los servidores institucionales que brinden algún servicio a la organización.

Para el caso específico de las instituciones financieras, los servidores miembro se pueden subdividir en agrupaciones dependientes de la funcionalidad y servicio brindado por el servidor.

Es por lo anterior que se recomienda la siguiente subdivisión de OUs:

- OU de Servidores de Base de Datos
- OU de Servidores WEB
- OU de Servidores de Aplicaciones
- OU de Servidores de Archivos
- OU de Servidores de Impresión

En general el patrón tecnológico seguido por las instituciones financieras hace que esta división sea válida y cubra todas las áreas de su infraestructura. Los servicios bancarios en general no varían en relación con la tecnología, por lo cual se puede generalizar en relación con los grupos anteriormente establecidos.

En cada OU se debe aplicar una GPO (política de grupo) específica para cada rol, la cual se debe haber confeccionado tomando en consideración las características propias de cada grupo de servidores según las configuraciones que requieran para proporcionar un buen nivel de seguridad al mismo tiempo que mantienen su funcionalidad.

A continuación un gráfico que describe la topología de los servidores miembro

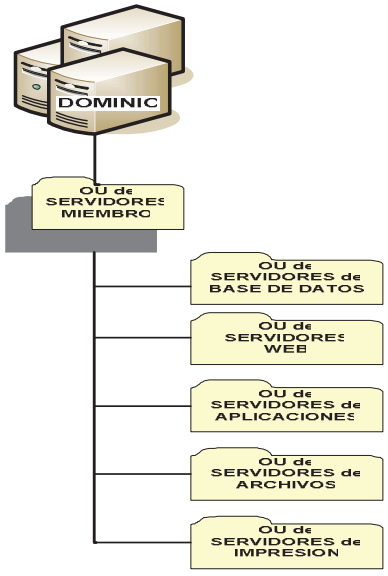

Grafico # 4.
Esquema de arquitectura de OUs para Servidores Miembro en A.D,

6.1.2.1.2 OU de Servidores de Infraestructura

En este contenedor se tienen que concentrar todos los servidores o equipos destinados a dar soporte a la infraestructura u operaciones del dominio y a los recursos del mismo.

En este punto se deben ubicar los siguientes servidores de servicios:

- Servidores WINS
- Servidores de DHCP

A continuación un gráfico que describe la topología de los servidores de infraestructura

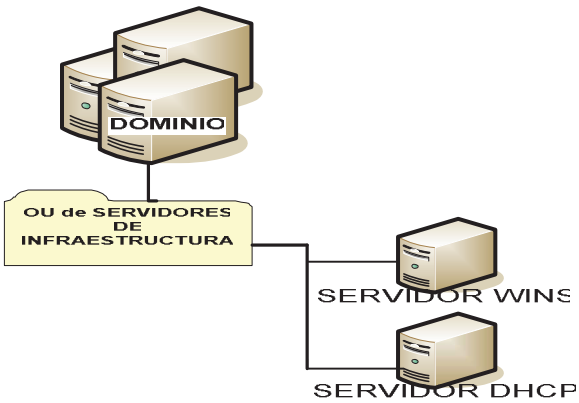

Grafico # 5.
Esquema de arquitectura de OUs para Servidores de Infraestructura en A.D,

6.1.2.1.3 OU de Domain Controllers

En este contenedor se listan todos los controladores de dominio que existan en la infraestructura. Al igual que en el caso de los grupos de servidores anteriores, los controladores de dominio tienen características específicas; por ello, las políticas de grupo deben ser tratadas por separado del resto de los equipos y recursos de red.

A continuación un gráfico que describe la topología de los servidores controladores de dominio:

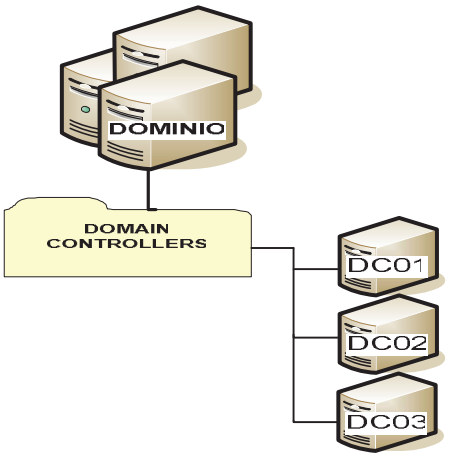

Grafico # 6.
Esquema de arquitectura de OUs para Servidores Controladores de Dominio en A.D,

6.1.2.2 OUs de Administración de Usuarios y Recursos

En una red financiera no sólo se debe pensar en los equipos y servicios que se brindan, ya que esta solamente es una parte diminuta de los recursos que existen en la misma.

Los usuarios internos y recursos compartidos (estaciones de trabajo, impresoras, etc), que existen en la red de computadoras de una institución financiera, son el grueso en la administración de una infraestructura de este tipo, dado el volumen de configuraciones que esto significa.

Para el fin último de facilitar la administración de los recursos de red y usuarios, Ching, Ruben (2005), recomienda separar los recursos por áreas de trabajo, para lo cual, tomando en cuenta la estructura clásica de las instituciones Financieras (Ver **# 13,** Estructuración de Instituciones Financieras), se deberán crear los siguientes OUs en la estructura del AD:

6.1.2.2.1 OU para usuarios y equipos

Dado que la propuesta está enfocada hacia la estructuración que tendría una institución financiera, se recomienda crear los siguientes OUs según las áreas de trabajo clásicas de una organización de esta índole.

Se definirá una estructura individual tomando en cuenta la división estratégica de las instituciones financieras en Agencias, Sucursales y Casa Matriz (Oficinas Principales).

La estructura debe incluir las siguientes áreas, dentro de las cuales se deben definir OUs específicos para identificar usuarios y equipos:

- Casa Matriz
    - Gerencia General
    - Dirección Administrativa
    - Dirección de Contabilidad
    - Dirección de Negocios
    - Dirección de Finanzas
    - Dirección Jurídica
    - Dirección de Créditos
    - Dirección de Tecnología y Operaciones
        - Desarrollo de Sistemas
        - Producción de Sistemas
        - Redes y comunicaciones
        - Seguridad Informática
    - Dirección de Recursos Humanos
    - Auditoria
    - Otras
- Agencias
    - Área Administrativa
    - Área de Contabilidad
    - Servicio al Cliente
        - Cajas
        - Plataforma de Servicios
        - Tarjetas de Crédito
        - Créditos
- Sucursales
    - Área Administrativa
    - Área de Contabilidad

- Área de Tecnología
- Servicio al Cliente
    - Cajas
    - Plataforma de Servicios
    - Tarjetas de Crédito
    - Créditos

Al igual que en los casos anteriores, se deben crear políticas de grupo relacionadas y configuradas según las áreas de trabajo, de manera que las necesidades de los usuarios, respecto de las herramientas que requieren para sus funciones, sean satisfechas al mismo tiempo que se forme una ambiente seguro y controlado de los recursos.

Nota: Para la graficación siguiente se toma como premisa que la institución financiera cuenta con enlaces pobres, por lo cual debe implementar varios dominios enlazados con relaciones de confianza.

6.1.2.2.1.1 Esquema para Casa Matriz

A continuación un gráfico que describe la topología de los OUs para la administración de usuarios y equipos para Casa Matriz:

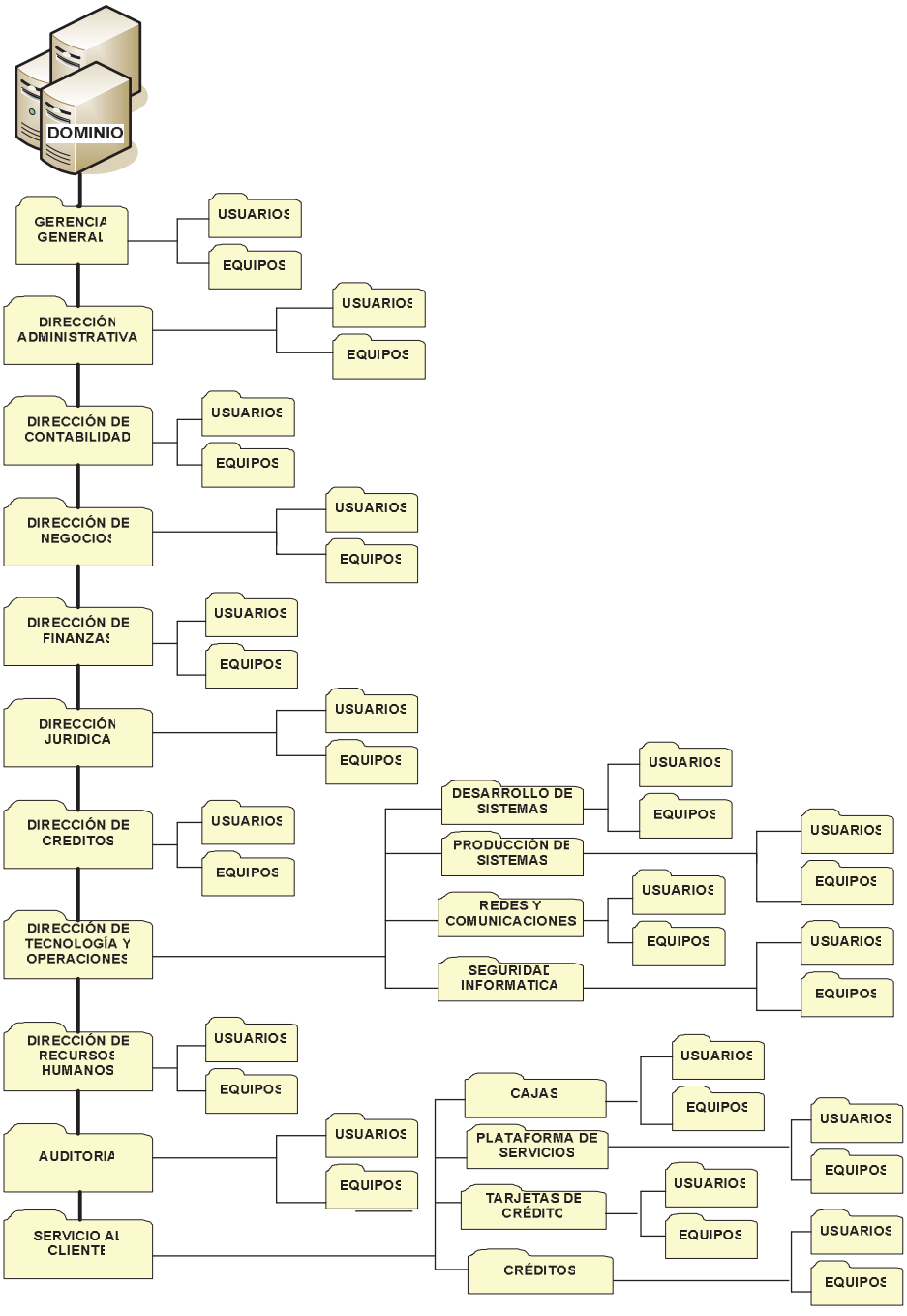

Grafico # 7.
Esquema de arquitectura de OUs en Casa Madriz
para usuarios y equipos según áreas de trabajo en A.D,

6.1.2.2.1.2 Esquema para Sucursales

A continuación un gráfico que describe la topología de los OUs para la administración de usuarios y equipos para Sucursales:

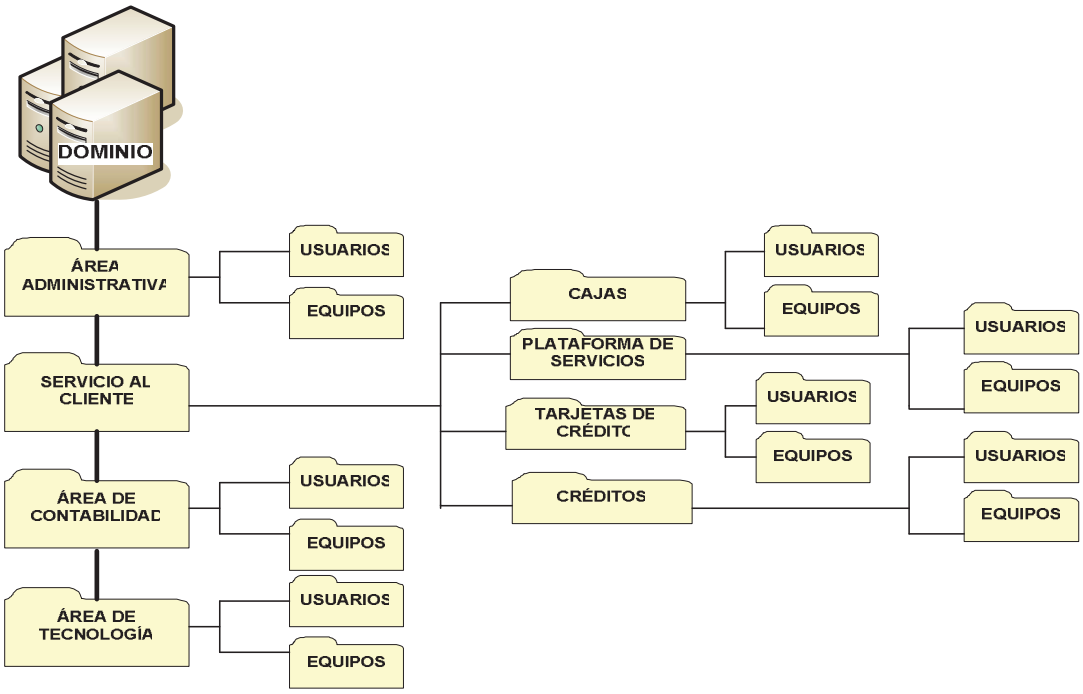

Grafico # 8.
Esquema de arquitectura de OUs en Sucursales
para usuarios y equipos según áreas de trabajo en A.D,

6.1.2.2.1.3 Esquema para Agencias

A continuación un gráfico que describe la topología de los OUs para la administración de usuarios y equipos para Agencias:

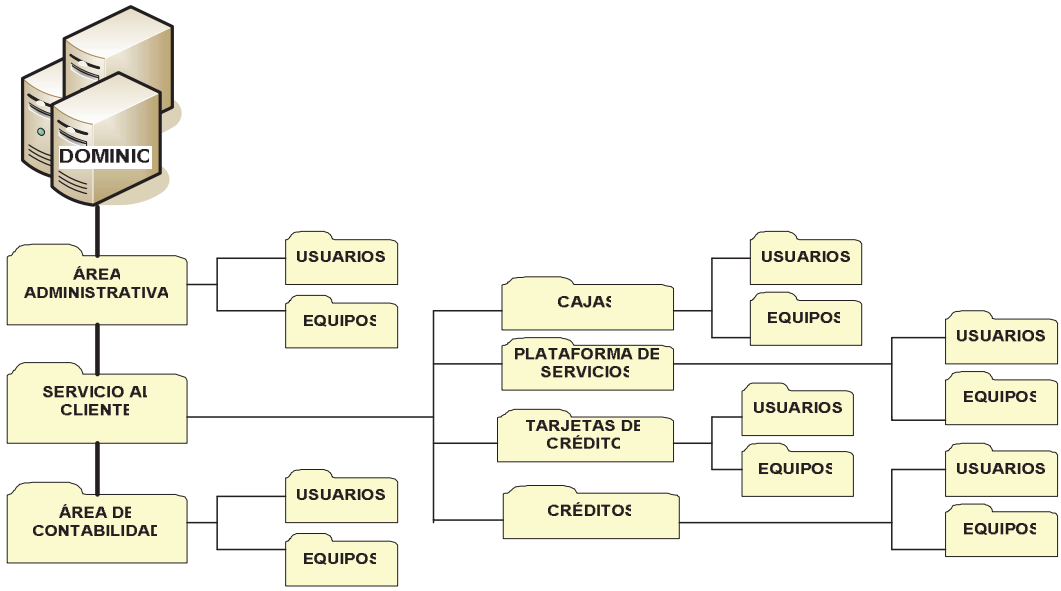

Grafico # 9.
Esquema de arquitectura de OUs en Agencias
para usuarios y equipos según áreas de trabajo en A.D,

A diferencia de las sucursales, las Agencias por lo general no cuentan con un área especializada en tecnología ya que su infraestructura y ámbito de acción son más reducidos que los de una sucursal.

6.1.2.2.2 OU de Usuarios de Administración

Cuando se tenga bien definida la estructuración del Active Directory en cuanto a la distribución de sus objetos según la recomendación anterior, se debe tomar en cuenta la parte administrativa de los mismos.

Según la Guía de Seguridad de Windows Server2003 (2005), se recomienda definir grupos administrativos, los cuales serán los encargados, según su límite de administración; de definir las políticas de grupo correspondientes en cuanto a la seguridad de sus áreas de trabajo. Se recomienda la creación de los siguientes grupos administrativos:

Tabla # 2
OUs para Usuarios de Administración

NOMBRE DEL GRUPO ADMINISTRATIVO	DESCRIPCIÓN
Administradores de Dominio	Responsables de administrar y controlar las políticas de seguridad de los equipos listados en el OU de Domain Controllers. Adicional a esto cuenta con derechos de administración sobre todos los recursos del dominio (Súper – usuarios)
Administradores de Servidores Miembro	Responsables de establecer las políticas de seguridad de la estructuración de los servidores Miembro. Administran y controlan los equipos listados en este OU
Administradores Locales	Administran, controlan y dan mantenimiento a los usuarios y equipos listados dentro del OU correspondiente.
Administradores de Servidores de Infraestructura	Responsables de los servidores listados en este OU; a saber los servidores DHCP y WINS.
Administradores de Datos	Estos usuarios tienen la función de establecer políticas, administrar y controlar los objetos que fueron designados bajo su responsabilidad.

Una vez definidos estos grupos en la estructuración del Active Directory, se deben seleccionar los usuarios que van a formar parte de estos grupos de administración.

Para más referencias ver **Anexo # 5**, Delegación de Permisos para Usuarios y Grupos en Active Directory.

A continuación un gráfico que describe la topología de los OUs para administración:

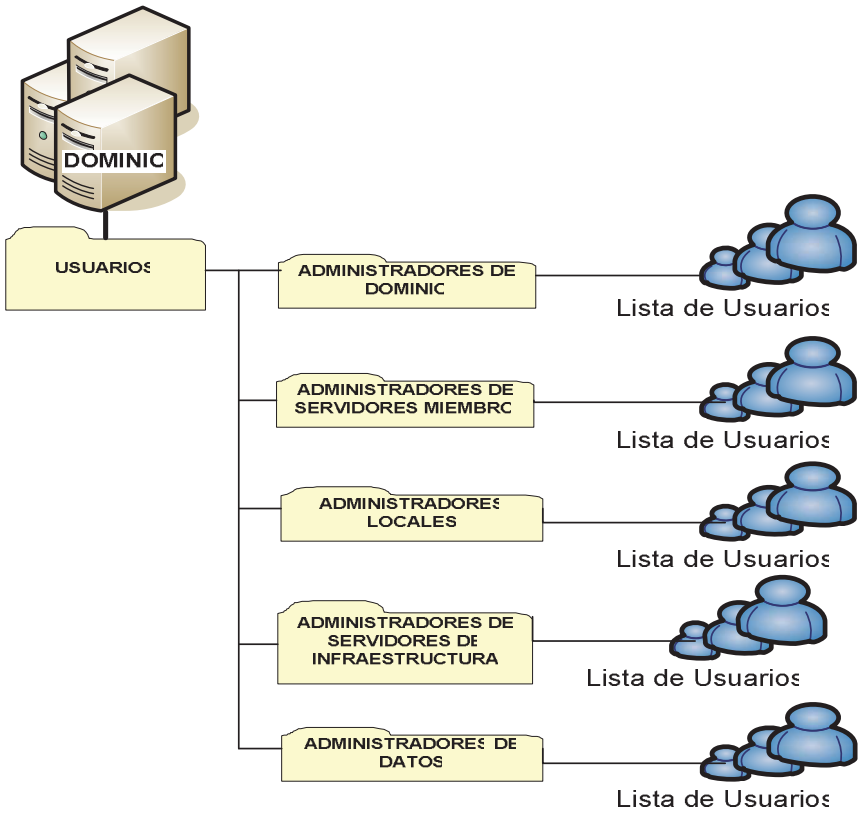

Grafico # 10.
Esquema de arquitectura de OUs para administración en A.D,

6.2 Estrategia para la Implementación de Seguridad

Una adecuada estructuración en el diseño del Active Directory es un complemento vital para asegurar una apropiada distribución de políticas de seguridad y configuraciones en los objetos presentes en la infraestructura de red.

Las políticas de grupo (GPO), son muy útiles para actualizar un gran número de recursos al mismo tiempo, lo cual se logra con el simple hecho de modificar parámetros dentro de la plantilla de seguridad.

Según explicó Quesada, Omar (2005), las políticas de grupo es una herramienta poderosa para la generación y distribución de seguridad en la organización. Según comentó Omar, la eficacia de la GPO va a depender de una adecuada definición de los parámetros configurables en la plantilla.

En este punto es importante conocer a fondo la lógica utilizada para la aplicación de políticas de grupo, esto con la finalidad de poder estructurar las políticas de grupo de igual manera que se hizo anteriormente con los OUs.

6.2.1 Utilización de Políticas de Grupo

Según la Guía de Seguridad de Windows Server2003 (2005), las políticas de grupo se acumulan y aplican en el orden que se muestra en la siguiente gráfica:

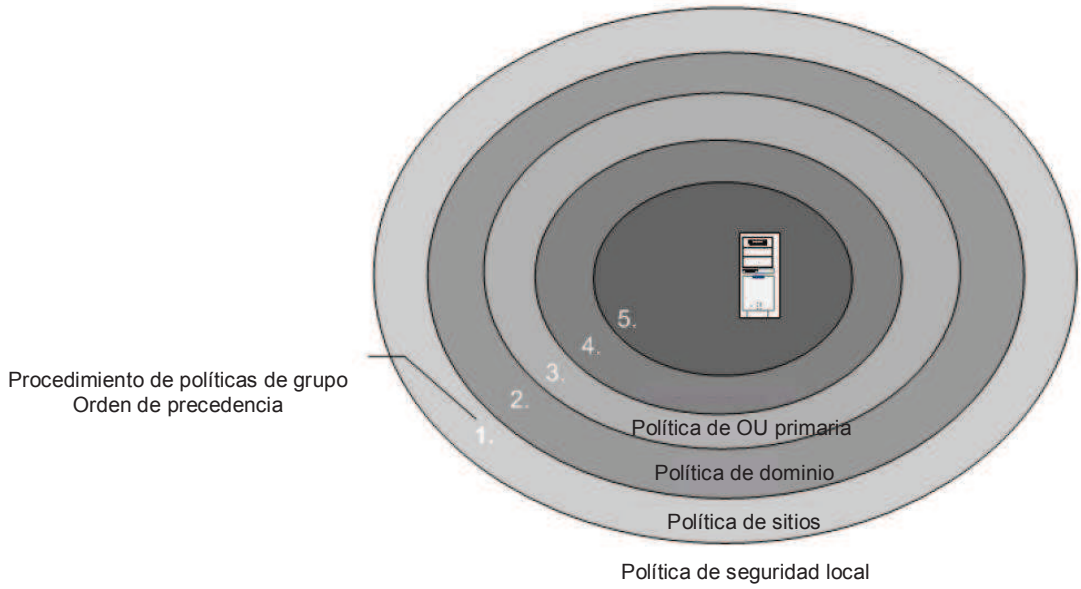

Grafico # 11.
Jerarquía de aplicación de GPOs
Tomado de la Guía de Seguridad de Windows Server2003 (2005)

Como se mencionó en el marco teórico, Active Directory posee una estructura jerárquica, razón por la cual los objetos que son hijos de otros objetos heredan la configuración y políticas aplicadas a los padres.

Las políticas de grupo como se puede observar en el gráfico anterior, se aplican primero en el nivel de políticas de máquina local, después de eso, se aplican los GPOs a nivel del sitio, y después a nivel del dominio.

Si el servidor está anidado en varios OUs, primero se aplican los GPOs que existen en la OU de mayor nivel. El proceso de aplicar GPOs continua hacia abajo en la jerarquía de OUs y se deben tomar en consideración los siguientes puntos:

Se debe establecer el orden de aplicaciones del GPO para niveles de políticas de grupos con varios GPOs. Si varias políticas especifican la misma opción, tendrá prioridad la última que se haya aplicado.

6.2.2 Creación de Políticas de Línea Base y Plantillas de Seguridad

La Guía de Seguridad de Windows Server2003 (2005), recomienda la creación de políticas estándar aplicables a un grupo de objetos específicos. La idea central de la generación de una política de línea base es crear una serie de configuraciones comunes que contengan todos los objetos de la infraestructura de la institución financiera en cuanto a seguridad.

Para esta propuesta se tomará en cuenta la línea base para servidores miembro, dominio, usuarios y estaciones de trabajo según las mejores prácticas recomendadas por Microsoft.

Una política de línea base debe estar estructurada de tal manera que permita la aplicación de configuraciones específicas para ciertos objetos de la organización; por ejemplo, dentro de la configuración básica de todos los servidores se puede establecer la política de que ningún equipo tenga habilitado el Internet Information Service (IIS), sin embargo algunos servidores por cuestiones de funcionalidad van a requerir que se encuentre habilitado, dentro de los cuales se podría mencionar los servidores WEB.

Para estos casos, se deben establecer políticas a nivel de OU o a nivel local para solventar estos requerimientos especiales según el rol del servidor o equipo.

Ver **Anexo # 6**, Creación de Políticas de Grupo importando Plantillas de Seguridad.

6.2.2.1 Política de línea base para el dominio

La línea base para el dominio toma en cuenta requisitos de seguridad comunes, como políticas de cuenta de contraseñas que se deben implementar para todos los servidores en el dominio. Ver **Anexo # 7**, Línea Base para el Dominio.

Según la Guía de Seguridad de Windows Server2003 (2005), los tipos de cambios de seguridad que se recomienda aplicar a nivel de dominio son los siguientes:

- Modificar permisos del sistema de archivos.
- Modificar permisos en objetos del registro.
- Cambiar configuraciones en el registro.
- Configurar los registros de auditoría y eventos.
- Configurar las políticas de cuenta y de contraseñas.

Se debe crear una plantilla de seguridad tomando en cuenta la configuración base mínima según los puntos anteriormente mencionados.

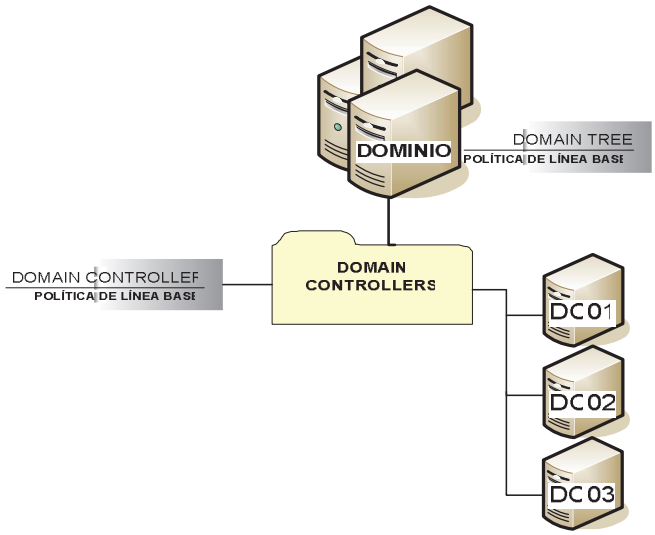

Grafico # 12.
Esquema de arquitectura de OUs para la aplicación de líneas base a nivel de dominio en el A.D,

Para la configuración de seguridad de los Domain Controllers, ver **Anexo # 9**, Línea Base para Domain Controllers.

6.2.2.2 Política de línea base para servidores miembro

Ya creada la estructura en el AD para los servidores miembro, se debe crear una plantilla de seguridad de línea base e importarla en la política de grupo correspondiente.

Una vez creada la plantilla de seguridad, la misma debe ser importada en el OU de servidores miembro.

La política de grupo aplicará las configuraciones de la plantilla de línea base a cualquier servidor en el OU de los servidores miembro, así como a cualquier servidor de las OUs secundarias o hijas.

Según comentó Quesada, Omar (2005), este tipo de plantilla debe ser lo suficientemente confiable para asegurar los diferentes roles de equipos, pero a la vez flexible para permitir configuraciones especiales según los roles. Omar recomienda la utilización de plantillas basadas en los niveles de seguridad 2 y 3 que se definen en la Guía de Seguridad de Windows Server 2003.

A continuación un gráfico que describe la topología de los OUs y la aplicación de líneas base según su funcionalidad:

Ver **Anexo # 8**, Base Line para Servidores Miembro.

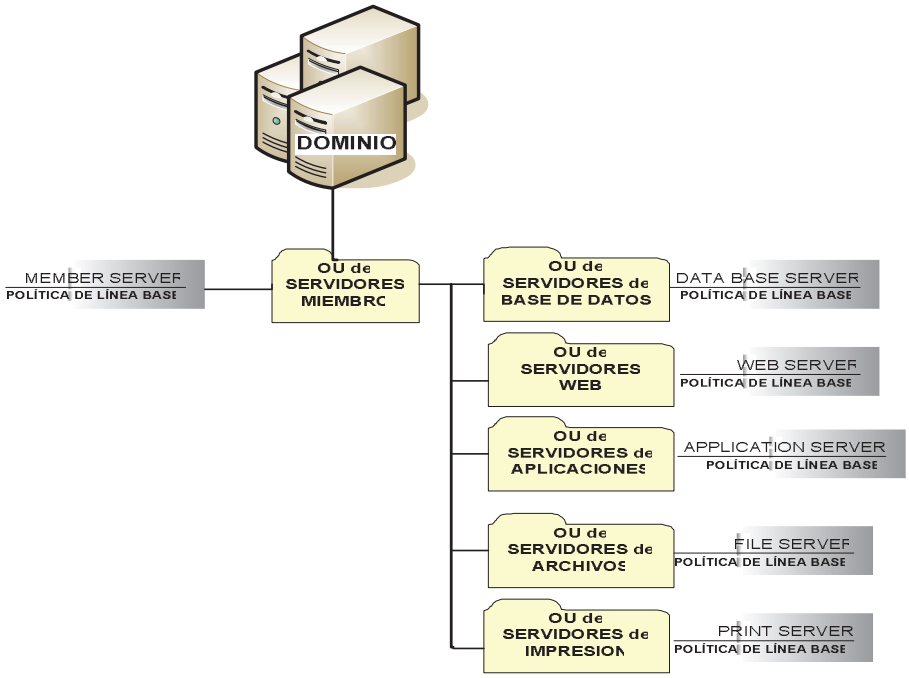

Grafico # 13.
Esquema de arquitectura de OUs para aplicar de líneas base en servidores miembro del A.D,

6.2.2.3 Política de línea base para cuentas de usuarios

Las políticas de cuentas incluye la estandarización en la utilización de configuraciones de seguridad a nivel de contraseñas y bloqueo de las cuentas.

La política de cuentas de usuarios proporciona un mecanismo para establecer la complejidad y la frecuencia de cambios para contraseñas para ambientes altamente seguros. Por lo general esta política se establece a nivel de dominio (Hacer referencia al **Anexo # 7**)

6.2.2.3.1 Política de contraseñas y bloqueo de cuentas

Las políticas de contraseñas ayudan a establecer reglas o restricciones a nivel de usuarios en cuanto al establecimiento de contraseñas complejas, las cuales deben que cambian regularmente con lo cual se reducen la posibilidad de un ataque exitoso a contraseñas. Las configuraciones de las políticas de contraseñas controlan la complejidad y la vida útil de las contraseñas.

Dependiendo de las políticas de seguridad de la información con que cuenta la organización, se debe definir un nivel de seguridad para el establecimiento de las contraseñas de usuarios. La educación de los usuarios, en cuanto a buenas prácticas en la utilización de contraseñas, ha sido un verdadero dolor de cabeza para los administradores de redes. Por esta razón es necesario contar con un mecanismo que obligue al usuario a seguir estos lineamientos.

A continuación aparecen algunas recomendaciones hechas por Ching, Ruben (2005) sobre el tema:

- Evitar la utilización de contraseñas en aumento con un dígito.
- Evitar preceder o anexar un número a contraseñas.
- Evitar el uso de contraseñas que otros puedan adivinar fácilmente viendo su escritorio (como los nombres de sus mascotas, equipos deportivos y familiares).
- Evitar palabras de la cultura popular.
- Evitar pensar en las contraseñas como palabras en sí, se recomienda la utilización de frases en vez de palabras clave.

- Imponer el uso de letras mayúsculas y minúsculas, números y símbolos en todas las contraseñas.
- Imponer el uso de espacios y caracteres que sólo se pueden producir utilizando la tecla Alt.

Estas recomendaciones también deben ser aplicadas en cuentas de dominio utilizadas para el soporte de servicios.

6.2.2.3.2 Bloqueo de cuentas

Otro de los puntos a tratar en relación con las cuentas de usuario es el bloqueo de cuentas. Se recomienda configurar la política de seguridad de cuentas para que el usuario se bloquee después de 3 intentos fallidos de inicio de sesión.

Otro de los parámetros que se debe configurar en este punto son los derechos para desbloquear códigos de usuarios. Dicha responsabilidad debe estar a cargo de los administradores locales según el área de trabajo en el que se encuentre.

Ver **Anexo # 2**, Configuración de la Seguridad de Passwords.

6.2.2.4 Política de línea base para Auditoria del Sistema

Una política de auditoria determina los sucesos de seguridad que reportarán a los administradores de red, de manera que se registre la actividad del usuario o del sistema en las categorías específicas de sucesos.

El administrador puede supervisar la actividad relacionada con la seguridad si un usuario se conecta o desconecta de una PC, o si se realizan cambios a una configuración de política de auditoria.

Si no se configura ninguna auditoria, será difícil o imposible determinar qué sucedió durante un incidente de seguridad.

Como parte de la propuesta se recomienda auditar los siguientes aspectos:

- Auditar sucesos de inicio de sesión de usuarios
- Auditar los accesos al AD

- Auditar accesos a objetos
- Auditar cambio de políticas
- Auditar el uso de privilegios
- Auditar sucesos del sistema

6.2.2.5 Opciones de Seguridad

Las opciones de seguridad de las políticas de grupo se utilizan con el fin de establecer las configuraciones de seguridad para los equipos y servidores que se encuentran dentro de la infraestructura, tales como las firmas digitales de los datos, los nombres de cuenta del administrador y de invitado, las unidades del disco flexible y el acceso a la unidad de CD–ROM, comportamiento de la instalación de controlador e indicadores de inicio de sesión.

Según Quesada, Omar (2005), algunas recomendaciones que se pueden tomar en cuenta en el establecimiento de opciones de seguridad, por medio de plantillas de seguridad, son las siguientes:

- Cambiar el nombre del administrador del equipo
- Cambiar el nombre y bloquear el usuario GUEST
- No utilizar claves de inicio de sesión en blanco
- Limitar y auditar el permiso de apagar el sistema (por lo menos en el caso de servidores)
- Limitar los privilegios para la configuración de impresoras
- Restringir el acceso a medios extraíbles
- No mostrar el nombre del ultimo usuario que inició sesión

6.2.2.6 Incluir Registros en el Regedit

Adicional a todas las configuraciones anteriormente realizadas, se deben agregar varias entradas en el archivo de registro de Windows por medio de las políticas de seguridad para fortaleces el sistema operativo contra posibles ataques como la Negación de Servicio o descubrimiento de nombres NetBIOS.

Ver **Anexo # 10**, Configuraciones adicionales del registro

6.2.3 Pasos a seguir para la distribución de políticas de seguridad

Según todas las descripciones anteriores relacionadas con las posibles configuraciones de seguridad, a continuación se hace un resumen con los pasos por seguir para implementar las políticas de seguridad de grupo en la infraestructura de Active Directory.

1. Cree una estructura de OUs.
2. Mueva las recursos o objetos correspondientes a las OUs apropiadas.
3. Cree los grupos administrativos.
4. Agregue las cuentas de dominios apropiados a los grupos administrativos.
5. Delegue la administración para cada OU a los grupos de dominios apropiados.
6. Cree las políticas de grupos y plantillas de seguridad específicas según los OUs creados
7. Vincule cada Política de grupo a cualquier OU adicional, según se requiera.
8. Importe las plantillas de seguridad creadas a cada GPO según corresponda.
9. Establezca permisos sobre cada GPO para que los grupos de dominios apropiados tengan control sobre éstos.
10. Agregue los grupos de dominios apropiados a los Grupos restringidos para cada GPO.
11. Pruebe y perfeccione las políticas de grupo.

Un tema importante en el tema de las políticas se seguridad es que no existen fórmulas perfectas para la implementación de las misma. Las infraestructuras

tecnológicas varías de una organización a otra, sin embargo se puedes establecer puntos comunes para organizaciones con lógicas de negocio similares.

Una vez establecidas las líneas bases para los objetos presentes en la infraestructura, se debe trabajar en la afinación de los roles específicos de los servidores, creando políticas exclusivas para cada sistema según la configuración que requieran, sin embargo este es un trabajo muy minucioso y depende de las aplicaciones que se encuentren en los mismos.

6.3 Generación de Plantillas y Políticas de Seguridad

Como se mencionó anteriormente en la estrategia de implementación, uno de los factores críticos para el aseguramiento de todos los elementos de la red es la utilización de plantillas de seguridad.

Dichas plantillas de seguridad están estrechamente ligadas a las políticas institucionales creadas para asegurar la confiabilidad, integridad y disponibilidad de la información.

El primer paso para el establecimiento de un adecuado plan de seguridad para cualquier institución financiera, es el establecimiento de estas políticas de seguridad, para lo cual se define lo siguiente:

6.3.1 Generación de Políticas de Seguridad

En el transcurso del diagnóstico se habló de la necesidad de contar con el apoyo gerencial de la organización financiera para poder implementar un proyecto de esta envergadura.

La presencia de políticas institucionales enfocadas en el manejo de la seguridad de la información, es un insumo fundamental para poder generar las configuraciones necesarias para cumplir dichas políticas.

Por lo general las instituciones financieras tienen un área de trabajo especializado en la seguridad informática. Este departamento es el que tiene la responsabilidad de generar las políticas necesarias para asegurar que la información empresarial está protegida.

Las políticas de seguridad establecidas por la organización deberían estar enfocadas en las siguientes áreas de interés:

- Políticas para en el manejo y trasiego de la información
- Políticas para la administración y control de la infraestructura tecnológica
- Políticas de manejo de cuentas de usuario
- Políticas para la utilización de herramientas y aplicaciones
- Políticas de monitoreo y auditoria de los sistemas

Las anteriores son las áreas mínimas que deberían abarcar las políticas para poder contar con un adecuado plan de seguridad.

En la confección de las políticas se deben considerar varios puntos, dentro de los cuales se pueden mencionar las siguientes:

- Propósito de la política
- Alcance de la política
- Descripción general
- Roles y Responsabilidades

Es importante mencionar que una política por si sola no trae ningún beneficio a la organización. Una vez creadas dichas políticas, deben ser divulgadas e implementadas para que realmente agreguen valor.

El control y monitoreo del cumplimiento de las políticas establecidas, van a convertirse en un indicador que nos ayudará a medir el desempeño de nuestro plan de seguridad; y a la vez va a reducir los riesgos presentes en la infraestructura tecnológica ante posibles ataques a los recursos de la organización.

6.3.2 Generación de Plantillas de seguridad de Seguridad

Una vez creadas las políticas institucionales, estas reglas deben ser traducidas a parámetros dentro de la configuración de las plantillas de seguridad. Esta parametrización de variables va a lograr poner en acción las políticas establecidas por medio de su distribución en los diferentes objetos del AD en donde se apliquen.

Para la presente propuesta, se generaron varias plantillas de seguridad de Línea Base para equipos presentes en la infraestructura de Active Directory según la estructuración recomendada en puntos anteriores.

Las plantillas diseñadas para esta propuesta se confeccionaron de acuerdo a las mejores prácticas recomendadas por Microsoft, en relación a configuraciones de seguridad conocidas y ampliamente probadas en el entorno tecnológico; todo esto dependiendo de los roles de los equipos dentro de la infraestructura de la organización.

Las plantillas generadas para la propuesta se describen a continuación:

6.3.2.1 Línea Base para el Dominio

La línea base para el dominio toma en consideración aspectos de configuración de cuentas de usuarios.

Todos los demás parámetros de configuración dentro de la plantilla aparecerán como "No Definidos", esto con la finalidad de que plantillas posteriores puedan realizar las configuraciones respectivas sin que se afecte la jerarquía de las políticas de grupo.

Ver **Anexo # 7**, Línea Base para el Dominio

6.3.2.2 Línea Base para Domain Controllers

La línea base para el domain controllers toma en consideración aspectos de configuración tales como los siguientes:

- Configuración de las bitácoras de Seguridad, Aplicación y Sistema
- Configuración de las Auditorias del Sistema
- Configuración de algunos parámetros de permisos y privilegios
- Valores en el Regedit

Dicha política solamente debe ser aplicada sobre los servidores que tengan el rol de controladores de dominio dentro de la estructura de Active Directory.

Ver **Anexo # 9**, Línea Base para Domain Controllers

6.3.2.3 Línea Base para Servidores Miembro

La línea base para el servidores miembro toca una serie de configuraciones a un nivel más amplio que en las líneas base de los casos anteriores.

En esta plantilla se seguridad se canaliza la configuración de seguridad base para la mayoría de los equipos dentro de la infraestructura tecnológica empresarial.

Modifica configuraciones tales como las siguientes:

- Configuración de las auditorias del sistema
- Configuración de los servicios del sistema
- Configuración de las bitácoras de Seguridad, Aplicación y Sistema
- Configuración de parámetros de permisos y privilegios
- Valores en el Regedit

Es importante señalar que esta línea base desactiva todos los servicios innecesarios para el funcionamiento básico del sistema operativo de los equipos en donde se aplica la plantilla.

De quererse utilizar aplicaciones que requieran que alguno de los servicios de sistema desactivados sean nuevamente habilitados, se debe crear una política específica para dichos equipos.

6.3.3 Gestión y Control

Haciendo un análisis en retrospectiva, se definieron los puntos necesarios para contar con una adecuada estructuración de la plataforma tecnológica y así poder distribuir seguridad según las políticas establecidas por la organización.

Es en este momento cuando se debe definir un rol de trabajo que asegure el cumplimiento de dichas políticas y controle de una manera más adecuada el flujo de este proceso.

Debe existir una persona o grupo de personas que posean la responsabilidad de velar por la disponibilidad, integridad y confidencialidad de la información y sistemas de la organización.

En el caso de las instituciones financieras, por lo general se cuenta con un departamento dedicado a velar por la seguridad informática. Dicho grupo será el responsable de las siguientes acciones:

- Definir y mantener actualizadas las políticas de seguridad de la información
- Gestionar la aplicación de dichas políticas a los objetos correspondientes
- Verificar el cumplimiento de dichas configuraciones.
- Velar por un mejoramiento continuo del proceso.

6.4 Reseña para la Configuración y Administración del Esquema de Seguridad por medio de Active Directory

Anteriormente se describieron todos los pasos necesarios para la generación y una adecuada aplicación de políticas y plantillas de seguridad.

Según lo descrito, debe existir en la organización algún ente responsable de administrar dicha infraestructura de seguridad, con la finalidad de asegurar el cumplimiento y la efectividad de dichas pautas de seguridad; para lo cual deberá realizar una serie de actividades previas a la implementación de este esquema.

6.4.1 Plataforma Tecnológica para soportar el Active Directory

Dado que la propuesta planteada se basa en la aplicación de plantillas de seguridad por medio de Active Directory, la definición de una estructura de directorio es fundamental para poder distribuir seguridad entre los objetos presentes en la infraestructura tecnológica de la institución financiera.

En el caso de que la organización no cuente con una infraestructura de AD, se deben gestionar todos los aspectos necesarios para su implementación. Por lo general esta acción implica la creación de todo un proyecto de implementación que consume muchos recursos, tiempo y esfuerzo, para lo cual se debe tomar en consideración los siguientes puntos en cuanto al desarrollo del proyecto:

- Inicio del Proyecto
    - Definir los objetivos y alcance del proyecto
    - Identificar necesidades de recursos
    - Asignación de roles y responsabilidades
- Planeación y organización del Proyecto
    - Definir los objetivos definitivos
    - Justificación económica apoyada en un **análisis de riesgos**.
    - Justificación técnica y operativa, apoyada en el planteamiento de la estructuración tecnológica.

    - Establecer mecanismos de seguimiento

- Ejecución del Proyecto
    - Confección de un plan de proyecto (definir tareas y entregables en fechas específicas, dar seguimiento a las actividades).

- Finalización
    - Informes finales
    - Comunicación de resultados
    - Seguimiento posterior a la finalización

La creación de un plan de proyecto no está dentro de los alcances de esta propuesta, ya que el establecimiento, dimensión y metodología de cada proyecto de implementación difiere en cuanto a volumen y forma en cada organización.

Los puntos anteriores son requisitos mínimos para el establecimiento de proyectos de índole tecnológica, según mi experiencia en proyectos tecnológicos por medio de la metodología del **PMI** (Proyect Management Institute).

Una vez creadas las bases tecnológicas para soportar la infraestructura de Active Directory, se debe iniciar con la estructuración de la misma para agilizar y ordenar la implementación y distribución de políticas de seguridad.

6.4.2 Creación de la Infraestructura de Active Directory

Según la Guía de Seguridad del Windows2000 (2005), las siguientes son actividades básicas propuestas para la implementación de una infraestructura de Active Directory:

- Crear un dominio
- Crear un nuevo Domain Tree
- Instalar un servidor de DNS
- Crear la base de datos y los Log Files del Active Directory
- Crear el Shared System Vomune (SYSVOL)

Ver **Anexo # 11**, Guía para la instalación de Active Directory.

Una vez instalado el producto, se debe proceder a estructurar los recursos del dominio, creando la distribución de unidades organizacionales que se definió en puntos anteriores de la propuesta.

6.4.3 Administración del esquema de seguridad

La administración y mantenimiento de la infraestructura de seguridad es fundamental para garantizar la integridad, disponibilidad y confidencialidad de la información, usuarios y sistemas de la organización.

Los encargados de la infraestructura de seguridad, tienen la responsabilidad de velar por el cumplimiento de las políticas de seguridad institucionales y por brindar acciones proactivas con el fin último de garantizar el aseguramiento del dominio tecnológico.

La labor de los administradores de la seguridad se enfoca a la creación y aplicación de plantillas de seguridad según las políticas establecidas, el mantenimiento en general de los recursos de red y el monitoreo constante en busca de focos de posibles ataques o comportamientos sospechosos, para así brindar las soluciones oportunas a posibles problemas de seguridad.

Según Quesada, Omar (2005), algunas labores de administración del esquema de seguridad son las siguientes:

- Definición de los alcances de las políticas de seguridad y aplicación de dichas políticas en los OU que corresponda.
- Delegación de responsabilidades y administración de recursos a administradores locales.
- Delegación de permisos a usuarios
- Configuración de la seguridad de la infraestructura (equipos y sistemas)
- Establecimiento de reglas y castigos en cuanto a violaciones a la seguridad.
- Actualización periódica de las políticas de seguridad organizacionales dependiendo de las variaciones que tengan. Pruebas de funcionalidad de las políticas aplicadas y planes proactivos de mejoramiento.
- Auditoria y monitoreo

Las pruebas de funcionalidad de las políticas aplicadas pueden evaluarse tomando en cuenta diversos factores tales como lo que se aprecia en el siguiente gráfico:

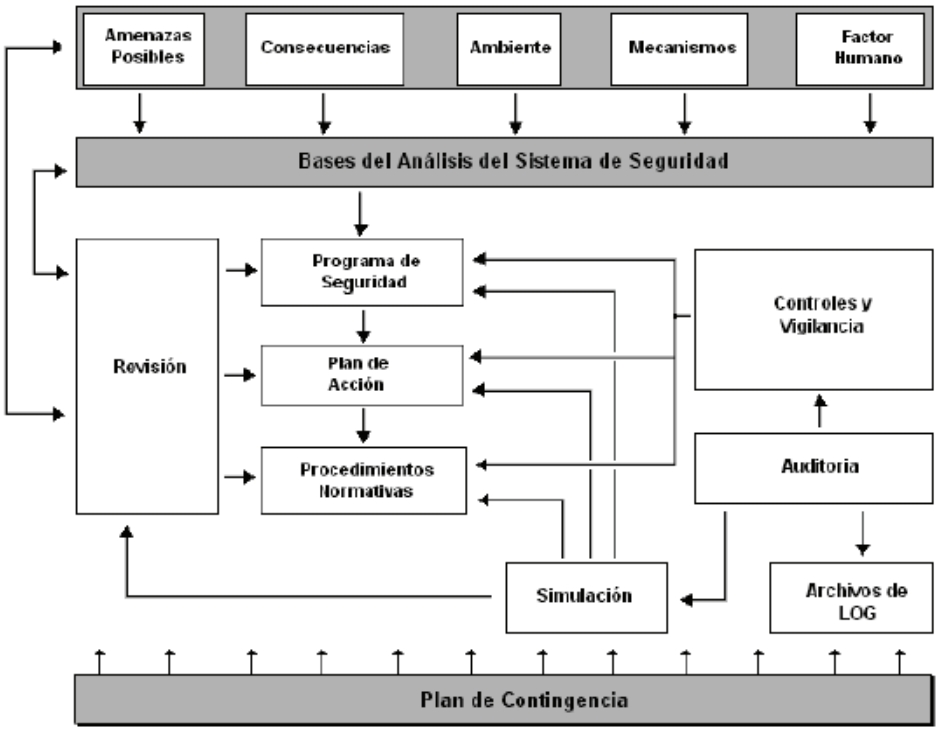

Grafico # 14.
Bases para Analizar un Sistema de Seguridad,
Tomado del Manual de Seguridad en Redes http://www.arcet.gov.ar, 2005

Como se muestra en el gráfico anterior, se empieza por una evaluación de las amenazas presentes en el ambiente tales como vulnerabilidades, factor humano, mecanismo utilizados por los intrusos informáticos para vulnerar los sistemas y, lo más importante, las posibles consecuencias que pueden causar estas amenazas.

Una vez identificadas estas bases, se debe originar el esquema de seguridad o, según el caso, revisar y corregir el esquema actual, estableciendo planes de acción, normas, procedimientos y configuraciones en la infraestructura.

BIBLIOGRAFIA

Paginas WEB Visitadas

http://www.BibliotecaInformatica.net
http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/evaluate/05w2kada.mspx
http://www.canaudit.com/Perspectives/Volume4_Issue9_SpanishVersion.pdf
http://www.securitymanagement.com/library/000775.html
http://www.microsoft.com/spain/technet/recursos/articulos/secmod221.mspx
http://www.monografias.com/trabajos3/firewalls/firewalls.shtml
http://www.nist.gov/
http://www.microsoft.com/spain/seguridad/guidance/prodtech/ActiveDirectory.mspx
http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/Appendix_D.asp
http://www.microsoft.com/spain/technet/seguridad/recursos/glosario/glossary_a_z.asp
http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/evaluate/05w2kada.mspx
http://www.landesk.com/docs/datasheet/ldms8/ds_svrmgr_es.pdf
http://download.microsoft.com/download/8/3/c/83cdeb26-04d0-4331-856d-ef9e47aae4c8/SMS_2003_BDM.ppt
http://www.isoftland.com/info/gfifax/lanet/
http://www.microsoft.com/spain/technet/seguridad/herramientas/sus.asp

Computer Security Institute (http://www.gocsi.com/press/). 2004, CMP Media LLC, USA

Microsoft TechNet Latinoamérica. *Resumen Técnico de Active Directory* (http://www.microsoft.com/latam/technet/articulos/199909/art05/). 2004

Microsoft TechNet España (http://www.microsoft.com/spain/seguridad/guidance/prodtech/ActiveDirectory.mspx). 2004

Microsoft TechNet España (http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/Appendix_D.asp). 2004

Microsoft TechNet España
(http://www.microsoft.com/spain/technet/seguridad/recursos/glosario/glossary_a_z.asp). 2004

Computer Security Institute
(http://www.gocsi.com/press/). 2004

Symantec
(http://www.symantec.com/region/mx/enterprisesecurity/content/risks/LAM_3106.html, http://www.symantec.com/region/mx/enterprisesecurity/threat_report/volIV/, http://www.symantec.com/region/mx/enterprisesecurity/content/risks/LAM_3522.html, http://www.symantec.com/region/mx/enterprisesecurity/content/expert/LAM_4779.html, http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_4141.html). 2004

CERT® Coordination Center (2004)
(http://www.cert.org/archive/ataques.pdf)

Theil, Ricardo (2004). *Cyberterrorismo y Terrorismo*.
(http://cyberterrorism.blogspot.com/2004/02/en-un-principio-la-red-fue-creada-para.html)

Wikipedia (2005). *Definición de Antivirus*
(http://es.wikipedia.org/wiki/Antivirus)

Windows Update (2005)
(http://windowsupdate.microsoft.com/)

US-CERT (2004). *Common Vulnerabilities and Exposures*
(http://www.us-cert.gov/cve/index.html)

Nacional Institute for Standards and Technology (2005)

Charlas, Seminarios y Foros

Wong, William (2004). *Defensa profunda contra código dañino*. Segundo Foro Latinoamericano de Seguridad, 2004, Costa Rica. (http://www.microsoft.com/costarica/technet/).

Alfaro, Elier (2004). *Implementación de la seguridad en el servidor en Windows 2000 y Windows Server 2003.* Segundo Foro Latinoamericano de Seguridad, 2004, Chile. (http://www.microsoft.com/chile/technet/2do_foro_seguridad/).

Serrano, José (2003). *Microsoft Windows 2000 Server Active Directory*. (http://www.rediris.es/jt/jt2000/trans/jt2000-2-2.ppt)

Ardita, Julio (2002). *Ataque a los Sistemas Informáticos, Técnicas de Testing de vulnerabilidades*, Escuela Politécnica del Ejército de Ecuador (ESPE), 22 de Abril del 2002, Quito-Ecuador. (www.cybsec.com/ingles/ataque.pdf)

Libros Consultados

Minasi, Mark, Anderson, Christa, Beveridge, Michele, Callahan, C.A, Justice, Lisa.(2002). *Mastering Windows Server 2003*. Fourth Edition, Sybex Inc, United States of America.

Spealman, Jill., Hudson, Kart., Craft, Melissa(2004), *Windows Server 2003 Active Directory Infraestructure,* Microsoft Press, United States of America.

Documentos en Línea

Grupo Mnemosine (2004). *Cyberterrorismo* (http://www.universidadabierta.edu.mx/Biblio/EdyTec/Cyberterrorismo.doc)

Guía de Seguridad de Windows 2003 (http://www.microsoft.com/latam/technet/seguridad/articulos/ddmmyy_guia_seguridad_windows_server_2003.asp). 2004

Guía de Seguridad de Windows 2000
(http://www.arcert.gov.ar/webs/textos/guide_to_securing_microsoft_windows_2000_act.pdf). 2005

Guía Microsoft de Gestión de Parches de Seguridad
(http://www.microsoft.com/latam/technet/seguridad/herramientas/guia_parches.asp). 2005

M. Minguet Melian (2004). *Introducción a la Seguridad Informática.*
(http://www.uned.es/413042/material/IntroSegInformatica.doc)

Entrevistas a Expertos

Quesada, Omar (2005). *Entrevista a Expertos sobre Infraestructura del Active Directory*. Consultor Biznet S.A. San Jose, Costa Rica.

Ching, Ruben (2005). *Entrevista a Expertos sobre Infraestructura del Active Directory*. Administrador Infraestructura del Active Directory y Exchange, Banco Nacional de Costa Rica. San Jose, Costa Rica.

Tesis en Línea

Borghello, Cristian (2001). *Seguridad Informática: Implicaciones e Implementación*. www.cfbsoft.com.ar

Índice

DEDICATORIA 2
AGRADECIMIENTOS 3
PRESENTACION 4
CAPÍTULO 1 5
PROBLEMA DE INVESTIGACIÓN 5
1.1 Introducción 6
1.2 Justificación 7
1.3 Planteamiento del problema 9
1.4 Problema de investigación 10
1.5 Objetivos 10
1.5.1 Objetivo general de diagnóstico 10
1.5.2 Objetivos específicos de diagnóstico 10
1.5.3 Objetivo general de la propuesta 11
1.5.4 Objetivos específicos de la propuesta: 11
CAPÍTULO 2 12
MARCO TEORICO 12
2.1 Seguridad 13
2.2 Violaciones de Seguridad 14
2.3 Tendencias en el Sector Financiero 16
2.3.1 Análisis de Vulnerabilidades 16
2.3.2 Herramienta para la gestión de Seguridad (Active Directory) 17
2.3.2.1 Definición de Active Directory (AD) 18
2.3.2.2 Funciones de Active Directory 18
2.3.2.3 Estructura de Active Directory 19
2.3.2.3.1 Objeto 19
2.3.2.3.2 Contenedor 20
2.3.2.3.3 Domain 20
2.3.2.3.4 Domain Tree 20
2.3.2.3.5 Domain Forest 22
2.3.2.3.6 Organization Units (OU) 22
2.3.2.3.7 Sitio 22
CAPÍTULO 3 23
MARCO METODOLOGICO 23
3.1 Tipo de investigación 24
3.2 Muestreo 24
3.3 Población 24
3.4 Descripción del instrumento de recolección de datos 24
3.4.1 Entrevistas a expertos: 25
3.5 Alcances 25
3.6 Limitaciones 25
CAPÍTULO 4 26
DIAGNÓSTICO 26
4.1 Riesgos en el Sector Financiero 27
4.1.1 Aumento de Intrusos Informáticos 28
4.1.2 Orígenes de los Crímenes Informáticos 29

4.1.2.1 Delitos informáticos de carácter económicos 29
4.1.2.2 Delitos informáticos en contra de la privacidad de la información 30
4.1.3 Delitos Informáticos en el Ámbito Financiero 30
4.1.3.1 Fraudes cometidos a través de la manipulación de sistemas informáticos 30
4.1.3.2 Copia ilegal de software y espionaje informático 30
4.1.3.3 Sabotaje informático 31
4.1.3.4 Uso ilegitimo de sistemas informáticos ajenos 31
4.1.3.5 Acceso a sistemas informáticos sin autorización: 31
4.1.4 Amenazas e Impactos 32
4.1.4.1 Tipos de Amenazas 32
4.1.4.1.1 Intercepción 32
4.1.4.1.2 Modificación 33
4.1.4.1.3 Interrupción 33
4.1.4.1.4 Generación 33
4.1.4.2 Impactos 33
4.1.4.2.1 Tipificación de las pérdidas 34
4.1.4.2.2 Valoración económica 34
4.2 Políticas de Seguridad y Configuraciones en el AD 36
4.2.1 Configuración del AD 37
4.2.1.1 Límites de seguridad 37
4.2.1.2 Políticas de Seguridad y Configuración de Objetos 38
4.2.1.2.1 Restringir nivel de permisos 38
4.2.1.2.2 Configuración de Seguridad de Objetos 40
4.2.1.2.3 Restringir el acceso 40
4.2.1.2.3.1 Protocolo LDAP (Lightweight Directory Access Protocol) 41
4.2.1.2.3.2 Servicios de Windows para el control de accesos 42
4.2.1.2.4 Filtrar el tráfico de correo electrónico 42
4.2.1.2.5 Minimizar el uso de claves estáticas 43
4.2.1.2.6 Actualizaciones de Seguridad 43
4.2.1.2.7 Limitar y controlar la utilización de dispositivos 44
4.3 Técnicas de Ataque a Equipos y Usuarios 45
4.3.1 Tendencias en el ámbito del delito informático 45
4.3.1.1 Primer Tendencia : Automatización y velocidad de las herramientas de ataque 46
4.3.1.1.1 Escaneo de Víctimas Potenciales: 46
4.3.1.1.2 Sistemas comprometidos o vulnerables: 46
4.3.1.1.3 Propagación del ataque 46
4.3.1.1.4 Manejo coordinado de las herramientas de ataque 47
4.3.1.2 Segunda Tendencia: Incremento de la complejidad de las herramientas de Ataque 47
4.3.1.2.1 Naturaleza oculta 47
4.3.1.2.2 Comportamiento dinámico 48
4.3.1.2.3 Modularidad de las herramientas de ataque 48
4.3.1.3 Tercer Tendencia: Descubrimiento acelerado de vulnerabilidades 48
4.3.1.4 Cuarta Tendencia: Incremento en la permeabilidad de los Firewalls 49
4.3.1.5 Quinta Tendencia: Incremento de la amenaza asimétrica 49
4.3.2 Vulnerabilidades más utilizadas y técnicas de ataque 49

4.3.2.1 Vulnerabilidades físicas 49
4.3.2.1.1 Empleados 50
4.3.2.1.2 Ex – Empleados 51
4.3.2.1.3 Hackers 51
4.3.2.1.4 Crackers 51
4.3.2.2 Vulnerabilidades Lógicas 51
4.3.2.2.1 Virus 52
4.3.2.2.2 Caballos de Troya 52
4.3.2.2.3 Bombas Lógicas 52
4.3.2.2.4 Remailers 52
4.3.2.2.5 Electronic Mail Bombs 53
4.3.2.2.6 Worms 53
4.3.2.2.7 Puertas Traseras (Back Doors) 53
4.3.2.2.8 Sniffers 54
4.3.2.2.9 Software de Mensajería 54
4.4 Hardware y Software especializados en seguridad 55
4.4.1 Software utilizado para la implementación de seguridad 55
4.4.1.1 Software Antivirus 55
4.4.1.2 Parches de Seguridad 56
4.4.1.2.1 System Management Server (SMS) 56
4.4.1.2.2 LANDesk Server Manager 57
4.4.1.2.3 LANguard Network Security Scanner 57
4.4.1.2.4 Microsoft Software Update Services (SUS) 58
4.4.1.3 Services Packs (SP) 59
4.4.1.4 Antispyware 59
4.4.1.5 Certificados Digitales 60
4.4.1.6 IPSec (Internet Protocol Security) 61
4.4.1.7 Detectores de Intrusos 62
4.4.2 Hardware utilizado para la implementación de seguridad 63
4.4.2.1 Firewalls 63
4.4.2.2 Biometría 63
4.4.2.3 Emisión de calor: 64
4.4.2.3.1 Huella digital: 64
4.4.2.3.2 Verificación de la voz: 64
4.4.2.3.3 Verificación de patrones oculares: 64
4.5 Mejores Prácticas y Técnicas de Aseguramiento 65
4.5.1 Mejores prácticas para asegurar el entorno 65
4.5.1.1 Medidas de Seguridad Administrativas 65
4.5.1.2 Defensas Físicas 66
4.5.1.3 Defensas Lógicas 66
4.5.1.3.1 Controles de Acceso 67
4.5.1.3.1.1 Identificación y Autorización: 67
4.5.1.3.1.2 Roles o Perfiles 68
4.5.1.3.1.3 Modalidad de Acceso 68
4.5.1.3.1.4 Ubicación y Horario 69
4.5.1.3.1.5 Palabras Clave: 69
4.5.1.3.2 Herramientas de Seguridad 70
4.5.1.3.2.1 Encriptación 70
4.5.1.3.2.2 Listas de control de acceso (ACL) 70
4.5.1.3.2.3 Utilización de Firewalls 70

4.5.2 Técnicas para el Aseguramiento ... 71
4.5.2.1 Vulnerar para proteger ... 71
4.5.2.2 Administración de la Seguridad ... 72
4.5.2.3 Seguridad en protocolos y servicios ... 72
4.5.2.4 Plantillas de Seguridad ... 73
CAPÍTULO 5 ... 74
CONCLUSIONES Y RECOMENDACIONES ... 74
5.1 CONCLUSIONES ... 75
5.1.1 Amenaza Presente ... 75
5.1.2 Diseño Seguro ... 75
5.1.3 Herramientas para el Aseguramiento ... 76
5.1.4 Metodologías Utilizables ... 76
5.1.5 Utilizar Active Directory ... 76
5.2 RECOMENDACIONES ... 77
5.2.1 Implementar Active Directory ... 77
5.2.2 Complementar Active Directory con otras herramientas ... 77
5.2.3 Mejoramiento Continuo ... 77
CAPÍTULO 6 ... 79
PROPUESTA PARA LA IMPLEMENTACIÓN DE SEGURIDAD CON ACTIVE DIRECTORY ... 79
6.1 Estructura del Active Directory ... 80
6.1.1 Establecer los límites del directorio ... 80
6.1.1.1 Limites de seguridad ... 81
6.1.1.2 Límites administrativos ... 81
6.1.1.2.1 Administradores de servicios ... 82
6.1.1.2.2 Administradores de datos ... 82
6.1.2 Estructura de las Unidades Organizacionales (OUs) ... 83
6.1.2.1 OUs para la Administración de Servidores ... 83
6.1.2.1.1 OU de Servidores Miembro ... 83
6.1.2.1.2 OU de Servidores de Infraestructura ... 85
6.1.2.1.3 OU de Domain Controllers ... 85
6.1.2.2 OUs de Administración de Usuarios y Recursos ... 86
6.1.2.2.1 OU para usuarios y equipos ... 86
6.1.2.2.1.1 Esquema para Casa Matriz ... 89
6.1.2.2.1.2 Esquema para Sucursales ... 90
6.1.2.2.1.3 Esquema para Agencias ... 91
6.1.2.2.2 OU de Usuarios de Administración ... 91
6.2 Estrategia para la Implementación de Seguridad ... 94
6.2.1 Utilización de Políticas de Grupo ... 94
6.2.2 Creación de Políticas de Línea Base y Plantillas de Seguridad ... 95
6.2.2.1 Política de línea base para el dominio ... 96
6.2.2.2 Política de línea base para servidores miembro ... 97
6.2.2.3 Política de línea base para cuentas de usuarios ... 98
6.2.2.3.1 Política de contraseñas y bloqueo de cuentas ... 98
6.2.2.3.2 Bloqueo de cuentas ... 99
6.2.2.4 Política de línea base para Auditoria del Sistema ... 99
6.2.2.5 Opciones de Seguridad ... 100
6.2.2.6 Incluir Registros en el Regedit ... 101
6.2.3 Pasos a seguir para la distribución de políticas de seguridad ... 101
6.3 Generación de Plantillas y Políticas de Seguridad ... 103

6.3.1 Generación de Políticas de Seguridad 103
6.3.2 Generación de Plantillas de seguridad de Seguridad 104
6.3.2.1 Línea Base para el Dominio 105
6.3.2.2 Línea Base para Domain Controllers 105
6.3.2.3 Línea Base para Servidores Miembro 106
6.3.3 Gestión y Control 106
6.4 Reseña para la Configuración y Administración del Esquema de Seguridad por medio de Active Directory 108
6.4.1 Plataforma Tecnológica para soportar el Active Directory 108
6.4.2 Creación de la Infraestructura de Active Directory 109
6.4.3 Administración del esquema de seguridad 110
BIBLIOGRAFIA 112
Paginas WEB Visitadas 113
Charlas, Seminarios y Foros 115
Libros Consultados 115
Documentos en Línea 115
Entrevistas a Expertos 116
Tesis en Línea 116
Índice 117
Índice de Gráficos y Tablas 122
ANEXOS 123

Índice de Gráficos y Tablas

Tabla # 1 15
Violaciones de Seguridad 15
Grafico # 1 21
Esquema de Relaciones de confianza en A.D, ... 21
Grafico # 2 21
Esquema de Espacio de Nombres en A.D, ... 21
Grafico # 3 36
Esquema de arquitectura para la administración de A.D, ... 36
Grafico # 4 84
Esquema de arquitectura de OUs para Servidores Miembro en A.D, ... 84
Grafico # 5 85
Esquema de arquitectura de OUs para Servidores de Infraestructura en A.D, ... 85
Grafico # 6 86
Esquema de arquitectura de OUs para Servidores Controladores de Dominio en A.D, ... 86
Grafico # 7 89
Esquema de arquitectura de OUs en Casa Madriz 89
para usuarios y equipos según áreas de trabajo en A.D, ... 89
Grafico # 8 90
Esquema de arquitectura de OUs en Sucursales 90
para usuarios y equipos según áreas de trabajo en A.D, ... 90
Grafico # 9 91
Esquema de arquitectura de OUs en Agencias 91
para usuarios y equipos según áreas de trabajo en A.D, ... 91
Tabla # 2 92
OUs para Usuarios de Administración 92
Grafico # 10. 93
Esquema de arquitectura de OUs para administración en A.D, ... 93
Grafico # 11. 94
Jerarquía de aplicación de GPOs 94
Grafico # 12. 96
Esquema de arquitectura de OUs para la aplicación de líneas base 96
a nivel de dominio en el A.D, ... 96
Grafico # 13. 97
Esquema de arquitectura de OUs para aplicar de líneas base en servidores miembro del A.D, ... 97
Grafico # 14. 111
Bases para Analizar un Sistema de Seguridad, ... 111

ANEXOS