UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

DESARROLLO DE UNA HERRAMIENTA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA BASADA EN EL "WINDOWS 2000 SECURITY CONFIGURATION GUIDE".

DISEÑO DE UN PROYECTO PARA UNA ORGANIZACIÓN

GONZÁLEZ GALVÁN BRENDA INGRID
VIEYRA QUIROZ EDSON JAVIER

MÉXICO, D.F. **2007**

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

DESARROLLO DE UNA HERRAMIENTA DE AUDITORÍA DE SEGURIDAD INFORMÁTICA BASADA EN EL "WINDOWS 2000 SECURITY CONFIGURATION GUIDE".

DISEÑO DE UN PROYECTO PARA UNA ORGANIZACIÓN
QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

GONZÁLEZ GALVÁN BRENDA INGRID
VIEYRA QUIROZ EDSON JAVIER

ASESOR:
L.I. Y MTRA. RITA AURORA FABREGAT TINAJERO

MÉXICO, D.F. **2007**

DEDICATORIAS
BRENDA

A mi madre y abuelitos:

Las personas que más admiro y los seres más maravillosos que la vida me ha dado la oportunidad de conocer.
Gracias por su apoyo moral, cariño, paciencia y comprensión que desde pequeña me han brindado, gracias por guiar mi camino y estar siempre junto a mí en todo momento y por alentarme a seguir adelante.

Gracias por inculcarme los valores que ahora poseo y por llenar mi vida de tanto amor, dicha y felicidad.

Gracias por ser las luces que iluminan y dan sentido a mi vida.

Quiero que sepan que este triunfo también es suyo y que su amor y apoyo fue lo que me ayudó a conseguirlo.

Los amo.

A Edson:

Por ser tan paciente conmigo mientras desarrollamos el proyecto y por su apoyo incondicional que en todo momento me ha brindado.

A Rita

A nuestra asesora, por el apoyo y tiempo dedicado para la realización de este proyecto.

DEDICATORIAS
EDSON

A mi Madre, Padre y Hermano

A estas tres personitas que significan tanto en mi vida y que sin su cariño, apoyo, paciencia, comprensión y motivación este logro nunca hubiera llegado y sin quienes no podría apreciarlo tanto como lo hago en este momento, es a ustedes a quienes debo lo que soy, los quiero mucho.

A mi Familia

A mis primos, tíos y abuelitos de quienes recibí un apoyo incondicional y enorme y a quienes en esta dedicatoria les expreso mi gratitud.

A Brenda

Por ser una persona tan incondicional en el transcurso de esta etapa tan importante para ambos, por tenerme esa gran cantidad de paciencia que yo sé que no cualquiera tiene, por estar ahí en cada instante en que la necesité, gracias Bren.

A Rita

A nuestra asesora por habernos apoyado y dedicado tanto del tiempo que tan valioso consideramos, y por ser una parte tan importante del proyecto.

Desarrollo de una herramienta de Auditoría de Seguridad Informática basada en el "Windows 2000 Security Configuration Guide".

INTRODUCCIÓN

En la última parte de la historia actual, las computadoras han tenido mayor injerencia en nuestra vida diaria, formando parte sustancial en el desarrollo social y tecnológico a nivel mundial.

En particular la automatización de los procesos que se dan en las organizaciones ha ayudado a optimizar éstos, con la aparición de las computadoras, el manejo de la información se hizo más ágil y sencillo.

El valor más importante de la información es su ventaja competitiva en el mercado. Particularmente en las empresas dedicadas a los servicios con grandes bases de datos de clientes, en las empresas de ingeniería y del sector industrial que resguardan secretos industriales o patentes y en las empresas dedicadas a la computación con códigos fuentes de programas.

La seguridad de la información está basada en tres elementos principales: confidencialidad, integridad y disponibilidad. [1]

Confidencialidad

El objetivo de este elemento es implementar las medidas de seguridad necesarias que garanticen que la información sólo estará disponible para aquellos que se tenga contemplado. Existen casos en los que la confidencialidad juega un papel predominante. Por ejemplo, en los casos en los cuales existen datos que proporcionan una ventaja competitiva a una empresa u organización, como podría ser, algún material o procedimiento especial en la fabricación de un producto.

[1] Con base en Horton Mike, Mugge Clinton. **Claves Hackers**

Los datos en los que la confidencialidad es el objetivo principal suelen encontrarse protegidos mediante la segmentación de la información, es decir, que los datos no se encuentren concentrados en un mismo lugar, y mediante medidas estrictas de control de acceso para impedir los accesos no autorizados.

Integridad

Este segundo elemento intenta implementar medidas de seguridad para garantizar que los datos son fiables y que no han sufrido modificaciones. Este punto resulta especialmente crítico cuando los datos se utilizan para llevar a cabo análisis estadísticos o cálculos matemáticos.

Disponibilidad

La disponibilidad se refiere a implementar las medidas de seguridad necesarias para garantizar que los datos estén accesibles en el momento en el que se requiera.

La disponibilidad puede resultar de importancia crítica en los casos que se tenga que acceder a los datos o a las aplicaciones en tiempo real. En el caso en el que se vea afectada la disponibilidad, el impacto financiero en una empresa puede llegar a ser de magnitudes enormes. La importancia de la disponibilidad radica en que si esta no se garantiza, el acceso a la información se ve interrumpido como resultado de una falla o defecto en la arquitectura de seguridad.

Una organización debe tener en cuenta cada uno de estos elementos y aplicar las medidas adecuadas para proteger esta información, una de tales medidas es la Auditoría Informática.

La auditoría es una actividad necesaria en el ámbito empresarial, principalmente en lo referente a los aspectos contables, administrativos y en tecnologías de información.

En lo concerniente a las tecnologías de información la auditoría es una herramienta proactiva la cual nos ayuda a prevenir futuros inconvenientes que pudieran causar perjuicio a nuestra infraestructura tecnológica y en particular a los sistemas de cómputo.

Auditoría en Seguridad Informática

La Auditoría en Seguridad Informática cobra utilidad al ayudarnos a identificar posibles riesgos, prevenir situaciones no deseadas con respecto a la información y mitigar en la medida de lo posible tales riesgos.

Generalmente la auditoría suele apegarse a alguna norma, puede ser de carácter internacional o simplemente uno definido por la propia organización.

En la actualidad la realización de una auditoría de Seguridad en Informática se ha convertido en una actividad casi indispensable, ya que en la mayoría de las organizaciones la pérdida de información podría resultar catastrófica.

En la mayoría de las organizaciones se hace uso extensivo de servidores y computadoras personales con sistema operativo Windows, y si bien esta aplicación no ha sido ejemplo de sistema operativo seguro, se sigue empleando masivamente, por consiguiente es el sistema operativo más atacado. En este sistema operativo es muy común que una nueva vulnerabilidad sea descubierta o la forma de explotar una vulnerabilidad vieja haya sido dada a conocer por algún código malicioso, por lo cual la realización de una auditoría de seguridad particularmente rigurosa se hace necesaria en el caso de Windows.

La importancia de la prevención

Como se mencionó anteriormente es común oír o leer que en Windows se descubrió un nuevo agujero de seguridad, pero si aún no existe un programa que haga uso mal intencionado de esa falla el problema no es tan grave, del lado del administrador, y se reduce a conseguir el parche que corrija dicha vulnerabilidad. Al contrario de este caso, si nos encontramos en el supuesto de que no actualizamos nuestros sistemas de una forma oportuna, entonces se darán situaciones en que seamos atacados por malware que explota vulnerabilidades para las cuales existía la corrección tiempo atrás. Este tipo de fallas son detectadas en una auditoría en Informática.

Las auditorías en Informática ciertamente abarcan muchos tópicos relevantes como pueden ser prevención de desastres, planes de recuperación, procesos, eficiencia de ejecución de aplicaciones, etc.

Uno de los aspectos importantes en la auditoría de Tecnologías de información es la auditoría a sistemas operativos, puesto que en este tipo de programas es en donde se van a proporcionar los servicios que una organización provee, en este sentido podemos listar otros tipos de auditoría que sería susceptible de aplicar, en este caso la auditoría de seguridad es lo que nos ocupará a lo largo de este documento, contemplando así los 3 tópicos importantes en los cuales se basa la auditoría son la confidencialidad, la integridad y la disponibilidad como se mencionó anteriormente.

Seguridad en sistemas operativos

Existe una amplia gama de sistemas operativos disponibles en el mercado, algunos son de libre distribución, de código abierto, comerciales y de licencia gratuita.

Existen sistemas operativos, cuyo nivel de seguridad es considerado aceptable, sin embargo nos regiremos bajo la premisa de que no hay sistema seguro puesto que la seguridad depende del administrador, y es aquí en donde entra la herramienta a desarrollar ya que ésta servirá como guía de acción para un administrador en sus configuraciones seguras o no seguras.

La importancia de la auditoría

- **La explotación de vulnerabilidades es más costosa que su prevención**

Cuando un sistema de información es comprometido en su seguridad por la explotación de alguna vulnerabilidad el resultado es más costoso en muchos aspectos importantes como:

El sistema probablemente quede fuera de línea por algún tiempo lo que representa pérdidas monetarias para las instituciones.

El desprestigio que representa para una organización, puesto que la empresa pierde credibilidad con respecto a su infraestructura tecnológica. Esta parte cobra mayor importancia en casos en los cuales se provea de implementaciones, por ejemplo, de banca electrónica y comercio electrónico, puesto que los usuarios se sienten amenazados por la pérdida de algún bien monetario o material.

Es necesario destinar recursos para la reparación técnica de los desperfectos que hayan sido causados por la vulnerabilidad.

Teniendo en cuenta los aspectos anteriores podemos ver claramente que estas consecuencias no deseadas pueden verse prevenidas haciendo una revisión con antelación de los controles de seguridad en las organizaciones.

- **Facilidad de implementación**

La realización de una auditoría, así como la aplicación de las medidas correctivas que a partir de ella se propongan, la mayoría de las veces conllevarán mayor facilidad de aplicación que la reparación de un sistema vulnerado.

La auditoría no remedia todo

Existirán casos, quizá con amplia frecuencia, en los que la auditoría nos identifique vulnerabilidades que no nos sea posible minimizar.
Pondremos el ejemplo de un servidor web con IIS. Es sabido que al servicio de Internet Information Service se le han descubierto infinidad de vulnerabilidades, huecos de seguridad y demás fallas que podrían significar importantes riesgos para nuestra infraestructura de red, pero si nuestro servidor está proporcionando el servicio de web entonces difícilmente podríamos eliminar el riesgo por una intrusión a través del IIS, aunque sí podríamos tomar medidas que resulten preventivas y que puedan ayudar a minimizar el riesgo.

Si bien en este caso es difícil remediar el hueco de seguridad que implicaría el tener instalado IIS, sí nos hace conscientes del riesgo y en base a esto tomar medidas preventivas, como lo serían el realizar un buen esquema de permisos para prevenir un mayor daño en caso de alguna posible intrusión y aplicar los parches de seguridad de IIS con la mayor rapidez posible. Otra ventaja es que al hacernos conscientes de los riesgos podemos tomar medidas drásticas como la instalación de un Servidor Web Apache.

Puntos importantes en una auditoría

Una parte fundamental antes de empezar con la realización de una auditoría es la delimitación de los puntos a auditar. Como se comentó anteriormente existen distintos puntos de los cuales es factible hacer una revisión.

En lo que a Auditoría de Seguridad se refiere, existen puntos que se deben considerar como lo son:

- Autenticación
- Servicios
- Permisos y Control de acceso
- Actualización y Parches
- Vulnerabilidades

Autenticación

La autenticación es el conjunto de métodos de los cuales disponemos para verificar que un usuario es quien dice ser. Existen varias formas de autenticación, de las cuales la utilización de contraseñas es la más común. Ésta se refiere a una palabra o frase de uso particular y secreta para cada usuario.

Las características de una contraseña son la longitud y la complejidad. La longitud se refiere al número de caracteres del cual consta y la complejidad se refiere a la diversidad de uso en los caracteres que contiene.

Es recomendable que la longitud de una contraseña sea de un mínimo de 8 caracteres, en cuanto a la complejidad se recomienda el uso de letras mayúsculas y minúsculas, así como el uso de números y caracteres especiales, con el fin de reducir la probabilidad de que dicha contraseña sea vulnerable a ataques de diccionario y de fuerza bruta.

También es recomendable que las contraseñas sean cambiadas periódicamente, porque si el hash de ésta es obtenido, sea menos probable que éste siga siendo el mismo para cuando sea descifrado.

- **Servicios vulnerables**

Algunas versiones de determinados servicios o aplicaciones, presentan ciertas vulnerabilidades que representan un riesgo potencial para el sistema, por lo cual es recomendable deshabilitar estos servicios o desinstalar esas aplicaciones, así como también es recomendable dar de baja los servicios y puertos que no son utilizados, puesto que un atacante podría aprovecharse de ellos.

Actualización de sistemas operativos y Parches

Los sistemas operativos están escritos con una gran cantidad de líneas de código, incluso millones de líneas, motivo por el cual es muy susceptible que existan fallas en él, esto es errores de programación, que pudieran llegar a provocar desbordamientos del buffer *(buffer overflow)*, race condition, entre muchos otros que pudiesen presentarse. Estas fallas en sí mismas pueden provocar inestabilidad en el sistema, resultados inesperados o incluso la caída de la aplicación. Si bien estas fallas representan inconsistencias molestas en el uso, más allá pueden significar vulnerabilidades de las cuales algún intruso pudiera aprovecharse y obtener beneficios como el robo de información, acceso local o incluso acceso remoto. Las actualizaciones y HotFixes se encargan de la corrección de estos problemas, en el caso particular de Microsoft Windows éstas se liberan el segundo martes de cada mes.

Si bien pueden existir vulnerabilidades para las cuales no ha sido liberada una actualización o parche y pudiese existir un exploit que ataque tal vulnerabilidad, las actualizaciones resultan de gran importancia para mantener el sistema lo más protegido posible.

Vulnerabilidades

Este apartado es especialmente importante ya que las vulnerabilidades son fallas o defectos en el desarrollo o en la implementación de un software, en este caso el sistema operativo. Quizá esta parte de la auditoría sea la de mayor dificultad de implementación dada la complicación que conlleva la detección de una vulnerabilidad.

Por lo antes mencionado es que se propone el desarrollo de una herramienta de Auditoría que permita evaluar el grado de cumplimiento de la configuración del equipo analizado contra la sugerida en el documento Windows 2000 Security Configuration Guide publicado por Microsoft en octubre de 2002[2], documento que toma como lineamiento el estándar Common Criteria.

La herramienta verificará si se tiene instalado algún antivirus y firewall, el espacio disponible en disco duro, el número de sistemas operativos instalados, el estado de los controladores de dispositivos, protocolos de transporte habilitados, servicios vulnerables y duplicación de nombre del equipo en la red.

También realizará una verificación sobre los valores del registro y las políticas definidas en el equipo analizado.
Finalmente, la herramienta proveerá un mecanismo de verificación de Hotfixes, Service Pack e Internet Explorer validando que se tengan instaladas las versiones más recientes publicadas por Microsoft.

[2] http://download.microsoft.com/download/8/c/c/8cc94365-13d6-4975-bf69-9d4cd16a01a7/w2kccscg.pdf <3 de agosto 2006>

CAPÍTULO 1 MARCO TEÓRICO

Windows 2000[3]

Las series de Microsoft Windows 2000 son una colección de sistemas operativos que ofrecen la posibilidad de participar en una red, ya sea como servidores o como clientes. Las series de Windows 2000 incluyen características de Windows NT y Windows 98. Ofrecen tecnologías avanzadas e Internet, administración, seguridad y tecnologías de conectividad.

La familia de Windows 2000 incluye:

- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Professional
- Windows 2000 DataCenter

Windows 2000 Server sustituye a Windows NT Server.

Windows 2000 Server es el componente principal dentro de un entorno de red cliente-servidor, permite establecer y mantener un dominio en el que pueden interactuar otros servidores y un gran número de clientes. Integra servicios de directorio fiables preparados para la web, de red y de aplicaciones.

Los objetivos principales de Windows 2000 son: [4]

- Aumentar la fiabilidad.
- Conseguir grandes niveles de disponibilidad del sistema en general.
- Mejorar la escalabilidad.

---

[3] Spencer Kenneth, Goncalves Marcus Guía Avanzada Microsoft Windows 2000 Server Administración y Control, p. 2

[4] Ibidem, p.4-5

Permitiendo así conseguir:

- Servicios de organización por cluster y equilibrios de carga mejorados: Windows 2000 Advanced Server integra compatibilidad con la organización por clusters así como el equilibrio de carga integrado para redes y aplicaciones.
- Una escalabilidad mayor: Windows 2000 Server puede escalar desde pequeños grupos de trabajo hasta grandes instalaciones de centros de datos y también es compatible con sistemas de multiprocesamiento simétrico, soportando hasta 32 procesadores y permitiendo utilizar hasta 64 Gigabytes de memoria física.
- Arquitectura del sistema más fiable: Dos de las mejoras son protección de la memoria avanzada para el núcleo y firma de controladores.
- Número reducido de servicios necesarios: Muchas de las tareas administrativas que requerían reiniciar el equipo en Windows NT Server, ya no lo requieren en Windows 2000 Server.
- Servicios integrales de archivos, impresión y web: Windows 2000 Server incluye compatibilidad para administración de cuotas de discos y administración de volúmenes dinámicos.
- Servicios web: Soporte para la impresión en Internet y para el servicio Web de IIS 5.0.
- Infraestructura de administración global: Windows 2000 Server permite a las compañías configurar servicios a través de la red. El instrumental de administración de Windows *(WMI)*, la consola de Administración de Microsoft *(MMC)*, Windows Scripting Host *(WSH)* y el modelo de objetos componentes *(COM)* permiten una infraestructura de administración global.
- Seguridad flexible a nivel de empresa: Windows 2000 Server permite compatibilidad con Kerberos y con la Infraestructura de llave pública *(PKI)*.
- Servicios integrados de directorio: Active Directory de Windows 2000 Server proporciona un punto de administración

para cuentas de usuario, clientes, servidores y aplicaciones de Windows. Active Directory también se puede sincronizar con directorios existentes para reducir el número de tareas de administración redundantes.

- Integración con sistemas existentes: Windows 2000 Server funciona conjuntamente con las plataformas y tecnologías que posea.
- Multiprocesador: Windows 2000 es compatible con multiprocesamiento real, el estándar para Windows 2000 Professional es de hasta dos procesadores. En sistemas con varios procesadores, cada procesador puede ejecutar un subproceso de forma simultánea, ofreciendo así un rendimiento elevado.
- Almacenamiento: Windows 2000 soporta hasta 4 GB de RAM, y 2 TB de disco duro para volúmenes NTFS, 32 GB para volúmenes FAT 32 y 4GB para volúmenes FAT 16.

Una de las mejoras más importantes en Windows 2000 Server sobre Windows NT 4.0 Server es la introducción de Active Directory. Se trata de un conjunto integrado de servicios de directorio que proporcionan administración centralizada de recursos y de seguridad y mecanismos de control. Combina estructuras organizativas, anteriormente separadas, en una agrupación que incluye usuarios, grupos, seguridad, servicios y recursos de red.

Windows 2000 Professional es la versión cliente de la línea de productos Windows 2000 el cual ofrece un entorno de computación sólido para equipos de escritorio y portátiles.

Sistema de Archivos.[5]

Windows 200 es compatible con 4 sistemas de archivos

- FAT *(File Allocation Table)* es el sistema de archivos utilizado en DOS. Windows 2000 utiliza una implementación de una extensión de FAT virtual (VFAT).
- VFAT incluye compatibilidad para nombres de archivo largo y archivos y volúmenes de 4 GB. FAT de Windows 2000 es también conocida como FAT16.
- FAT32 Es una mejora del sistema operativo FAT16 que era parte del OSR2 de Windows 95 y que posteriormente fue parte de Windows 98. Windows 2000 incluye compatibilidad con FAT32 principalmente para obtener las mejoras en el tamaño de archivo y de volumen de 32GB sobre FAT16.
- NTFS (sistema de archivos de nueva tecnología:*New Tecnology File System*). Es un sistema de archivos de alto rendimiento, seguro y orientado a objetos que apareció por primera vez con Windows NT, NTFS es compatible con el sistema de archivos cifrado (EFS, *Encrypted File System*), característica nueva en Windows 2000.

[5] Ibidem, p. 9

Active Directory de Microsoft [6]

Active Directory es un nuevo mecanismo de control y de administración de Windows 2000. Windows 2000 Server y Advanced Server son compatibles con Active Directory para crear mantener y administrar un dominio.

El Active Directory es un servicio de red que almacena información acerca de los recursos existentes en la red y controla el acceso de los usuarios y las aplicaciones a dichos recursos. De esta forma, se convierte en un medio de organizar, administrar y controlar centralizadamente el acceso a los recursos de la red.

El Active Directory se ha implementado siguiendo una serie de estándares y protocolos existentes, ofreciendo interfaces de programación de aplicaciones que facilitan la comunicación con otros servicios de directorio. Entre ellos, se pueden encontrar los siguientes:

- DHCP (*Dynamic Host Configuration Protocol*, Protocolo de configuración dinámica de computadoras) que permite la administración desatendida de direcciones de red.
- DNS (*Domain Name System,* Servicio de nombres de dominio) que permite la administración de los nombres de computadoras. Este servicio constituye el mecanismo de asignación y resolución de nombres en Internet.
- SNTP (*Simple Network Time Protocol,* Protocolo simple de tiempo de red) que permite disponer de un servicio de tiempo distribuido.
- LDAP (*Lightweight Directory Access Protoco,* Protocolo ligero de acceso a directorio). Este es el protocolo mediante

[6] Ibidem p. 10

el cual las aplicaciones acceden y modifican la información existente en el directorio.

- Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas.
- Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

Active Directory combina diversos aspectos de una red como son usuarios grupos, host, clientes, opciones de seguridad, recursos vínculos de red y transacciones en una estructura organizativa jerárquica, centralizada y que se puede administrar. Este mecanismo simplifica la administración de una red combinando las distintas actividades anteriores en una única interfaz en la que se incluyen seguridad, administración de cuentas y usuarios y acceso a los recursos.

Protocolo Kerberos [7]

Una de las mejoras más importantes del sistema de seguridad de Windows 2000 es incluir el protocolo de autenticación Kerberos v5, el cual autentica a un cliente para un servidor antes de que el sistema permita la comunicación entre ellos.

El protocolo Kerberos proporciona seguridad de red regulando el acceso de usuarios a los servicios de red. En un entorno Kerberos existe como mínimo un servidor que ejecuta el servidor Kerberos. El servidor Kerberos proporciona servicios de autenticación para probar que el usuario solicitante es auténtico. Al servidor Kerberos también se le conoce como centro de distribución de claves (KDC *Key Distribution Center*).

[7] Ibidem, p. 297-298

Además de ofrecer autenticación, Kerberos puede proporcionar otros servicios de seguridad tales como integridad de datos y confidencialidad de datos.

Kerberos utiliza el cifrado de clave privada basado en DES (DES: *Data Encryption Standar*) Cada Cliente y cada Servidor tienen una clave privada DES. El protocolo Kerberos hace referencia a estos clientes y servidores como principales. La contraseña del cliente hace referencia a la clave privada del cliente.

El servidor Kerberos mantiene en la base de datos segura la lista de nombres y claves privadas de todos los clientes y servidores que tienen permiso de utilizar los servicios del servidor Kerberos. Kerberos asume que todos los usuarios mantienen sus contraseñas seguras. El protocolo Kerberos resuelve el problema de cómo puede un servidor asegurar la identidad de un cliente haciendo que tanto el cliente como el servidor confíen en una tercera parte en este caso el servidor Kerberos. El servidor Kerberos comprueba la identidad del cliente.

Descripción del Registro [8]

EL registro es una base de datos jerárquica central utilizada en Microsoft Windows 9x, Windows CE, Windows NT y Windows 2000 con el fin de almacenar información necesaria para configurar el sistema para uno o varios usuarios, aplicaciones y dispositivos de hardware.

El Registro contiene información que Windows utiliza como referencia continuamente, por ejemplo los perfiles de los usuarios, las aplicaciones instaladas en el equipo y los tipos de documentos que cada aplicación puede crear, las configuraciones de las hojas

[8] Con base en García Marín David, Jiménez Pérez Hugo. **Windows 2000 Server Activo.** p.575-580

de propiedades para carpetas y los iconos de aplicaciones, los elementos de hardware que hay en el sistema y los puertos que se están utilizando.

El Registro reemplaza la mayoría de los archivos .ini , archivos de texto que se utilizan en los archivos de configuración de Windows 3.x y MS-DOS.

El área de exploración del Editor del Registro muestra carpetas. Cada carpeta representa una clave predeterminada del equipo local. Cuando se obtiene acceso al Registro de un equipo remoto, sólo aparecen dos claves predefinidas: HKEY_USERS y HKEY_LOCAL_MACHINE. A continuación se enumeran las claves predefinidas que utiliza el sistema. El tamaño máximo del nombre de una clave es de 255 caracteres.

HKEY_CURRENT_USER
Contiene la raíz de la información de configuración del usuario que ha iniciado sesión. Las carpetas del usuario, los colores de la pantalla y la configuración del Panel de control se almacenan aquí. Esta información está asociada al perfil del usuario. Esta clave a veces aparece abreviada como "HKCU".

HKEY_USERS
Contiene todos los perfiles de usuario cargados activamente en el equipo. HKEY_CURRENT_USER es una subclave de HKEY_USERS. HKEY_USERS puede aparecer abreviada como "HKU".

HKEY_LOCAL_MACHINE
Contiene información de configuración específica del equipo (para cualquier usuario). Esta clave a veces aparece abreviada como "HKLM".

HKEY_CLASSES_ROOT

Es una subclave de HKL\Software. La información que se almacena aquí garantiza que cuando abra una carpeta mediante el Explorador de Windows, se abrirá el programa correcto. Esta clave a veces aparece abreviada como "HKCR". En el caso de Windows 2000, esta información se almacena en dos claves: HKEY_LOCAL_MACHINE y HKEY_CURRENT_USER.

La clave HKEY_LOCAL_MACHINE\Software\Classes contiene la configuración predeterminada que se puede aplicar a todos los usuarios del equipo local.

La clave HKEY_CURRENT_USER\Software\Classes contiene la configuración que reemplaza la configuración predeterminada y que se aplica únicamente al usuario interactivo.

La clave HKEY_CLASSES_ROOT proporciona una vista del Registro que combina la información de estos dos orígenes. HKEY_CLASSES_ROOT también proporciona una vista combinada para los programas diseñados para versiones anteriores de Windows. Para cambiar la configuración del usuario interactivo, se deben realizar los cambios en HKEY_CURRENT_USER\Software\Classes en lugar de en HKEY_CLASSES_ROOT. Para cambiar la configuración predeterminada, se deben realizar los cambios en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores en una clave de HKEY_CLASSES_ROOT, el sistema almacena la información en HKEY_LOCAL_MACHINE\Software\Classes. Si escribe valores para una clave en HKEY_CLASSES_ROOT y la clave ya existe en HKEY_CURRENT_USER\Software\Classes, el sistema almacenará la información ahí, en lugar de en HKEY_LOCAL_MACHINE\Software\Classes.

HKEY_CURRENT_CONFIG

Contiene información acerca del perfil de hardware que utiliza el equipo local cuando se inicia el sistema.

La siguiente tabla enumera los tipos de datos definidos actualmente que se usan en Windows. El tamaño máximo del nombre de un valor para Windows 2000 260 caracteres ANSI o 16.383 caracteres Unicode.

Tabla 1. Tipos de datos del registro

Nombre	Tipo de datos	Descripción
Valor binario	REG_BINARY	Datos binarios sin formato. La mayoría de la información sobre componentes de hardware se almacena en forma de datos binarios y se muestra en formato hexadecimal en el Editor del Registro.
Valor DWORD	REG_DWORD	Datos representados por un número de 4 bytes de longitud.Muchos parámetros de controladores de dispositivo y servicios son de este tipo y se muestran en el Editor del Registro en formato binario, hexadecimal o decimal. DWORD_LITTLE_ENDIAN (el byte menos significativo está en la dirección inferior) y REG_DWORD_BIG_ENDIAN (el byte menos significativo está en la dirección superior) son

		valores relacionados.
Valor alfanumérico expandible	REG_EXPAND_SZ	Cadena de datos de longitud variable. Este tipo de datos incluye variables que se resuelven cuando un programa o servicio utiliza los datos.
Valor de cadena múltiple	REG_MULTI_SZ	Cadena múltiple. Valores que contienen listas o valores múltiples; este es el formato cuya lectura resulta más sencilla. Las entradas aparecen separadas por espacios, comas u otros signos de puntuación.
Valor de cadena	REG_SZ	Cadena de texto de longitud fija.
Valor binario	REG_RESOURCE_LIST	Serie de matrices anidadas diseñadas para almacenar una lista de recursos utilizados por el controlador de un dispositivo de hardware o uno de los dispositivos físicos que controla. El sistema detecta y escribe estos datos en el árbol \ResourceMap que se muestra en el Editor del Registro en formato hexadecimal como valor binario.
	REG_RESOURCE_REQUIREMENTS_	Serie de matrices anidadas diseñadas para almacenar

Valor binario	LIST	una lista de controladores de dispositivo de posibles recursos de hardware que el controlador, o uno de los dispositivos físicos que controla, pueden utilizar. El sistema escribe un subconjunto de esta lista en el árbol \ResourceMap. El sistema detecta estos datos y los muestra en el Editor del Registro en formato hexadecimal como un valor binario.
Valor binario	REG_FULL_RESOURCE_DESCRIPTOR	Serie de matrices anidadas diseñada para almacenar una lista de recursos utilizados por un dispositivo físico de hardware. El sistema detecta y escribe estos datos en el árbol \HardwareDescription que se muestra en el Editor del Registro en formato hexadecimal como valor binario.
Ninguna	REG_NONE	Datos que no pertenecen a ningún tipo en particular. El sistema o una aplicación escribe estos datos en el Registro y los muestra en el Editor del Registro en formato hexadecimal como

		un valor binario.
Vínculo	REG_LINK	Cadena Unicode que da nombre a un vínculo simbólico.
Valor QWORD	REG_QWORD	Datos representados por un número entero de 64 bytes. Estos datos se muestran en el Editor del Registro como un valor binario.

Seguridad [9]

Es importante mantener el equipo seguro para proteger no sólo los datos si no también la red. Un buen sistema de seguridad debe confirmar la identidad de aquellos que intentan tener acceso a los recursos del equipo, proteger recursos específicos del acceso no apropiado por parte de usuarios y proporcionar una forma sencilla y eficaz de instalar y mantener la seguridad.
Para poder conseguir estos objetivos Windows 2000 profesional ofrece características de seguridad:

- Cuentas de usuario
- Cifrado(unidades NTFS)
- Permisos y control de acceso
- Derechos de usuario
- Directivas de grupo

Cuentas de usuario

Para poder utilizar un equipo que ejecute Windows 2000 debe tener una cuenta de usuario que conste de un nombre de usuario único y una contraseña, si la cuenta de usuario ha sido desactivada

[9] Ibidem, p.283-297

o no existe Windows 2000 le impide tener acceso al equipo asegurando que solo los usuarios válidos tienen acceso al equipo.

Cifrado para unidades NTFS

El sistema de archivos cifrado (EFS, *Encrypted File System*) es la principal tecnología de cifrado de archivos y directorios de NTFS en Windows. Basado en criptografía de clave pública.
EFS funciona como un servicio de sistema integrado dificultando ataques.

EFS soluciona principalmente problemas de seguridad provocados por herramientas disponibles en otros sistemas operativos que permiten a usuarios tener acceso a archivos de un volumen NTFS sin una comprobación de acceso.

El cifrado de archivos y carpetas los mantiene a salvo de usuarios sin autorización para leer estos archivos. Si un usuario intenta tener acceso a un archivo cifrado y posee la clave privada, podrá abrir el archivo y trabajar con él de forma transparente y por otro lado niega el acceso a un usuario que no posea la llave privada.

Permisos y control de acceso [10]

Cuando se establecen permisos en un archivo o carpeta se debe especificar los grupos y usuarios cuyo acceso se desea permitir o denegar. Una vez hecho esto debe especificarse el tipo acceso. Para esta tarea resulta más sencillo y práctico especificar cuentas de

[10] http://fferrer.dsic.upv.es/cursos/Windows/basico/ch05s07.html#sec:prot:permisos <30 de octubre 2006>

grupo cuando se asignan permisos a objetos para poder simplemente agregar usuarios al grupo adecuado cuando se haga necesario permitir o restringir acceso a tales usuarios.

La parte de permisos en un sistema operativo se refiere al nivel de acceso y privilegios en el manejo de los archivos características y configuraciones.

La Tabla 2muestra los permisos estándar de carpetas y archivos junto con su descripción. La descripción de las tablas hacen referencia a las acciones que cada permiso concede. Es importante recordar que en Windows 2000 cada permiso puede ser positivo o negativo, es decir, que realmente cada permiso permite o deniega la acción correspondiente. Como puede verse en ambas tablas, muchos de los permisos estándar se definen de forma incremental, de forma que unos incluyen y ofrece un nivel de acceso superior que los anteriores. La herencia de permisos se establece de forma natural: las carpetas heredan directamente los permisos estándar establecidos en la carpeta padre, mientras que los archivos heredan cualquier permiso excepto el de `Listar` (sólo definido para carpetas).

Tabla 2. Permisos estándar en Windows 2000

CARPETAS

Nombre	**Significado**
Listar	Permite ver los archivos y subcarpetas que contiene la carpeta.
Leer	Permite ver el contenido de los archivos y subcarpetas, así como su propietario, permisos y atributos
Escribir	Permite crear nuevos archivos y subcarpetas. Permite modificar los atributos de la propia carpeta, así como ver su propietario, permisos

	y atributos.
Leer y ejecutar	Permite moverse por la jerarquía de subcarpetas a partir de la carpeta, incluso si no se tienen permisos sobre ellas. Además, incluye todos los permisos de Leer y de listar.
Modificar	Permite eliminar la carpeta más todos los permisos de Escribir y de Leer y ejecutar.
Control total	Permite cambiar permisos, tomar posesión y eliminar subcarpetas y archivos (aún sin tener permisos sobre ellos), así como todos los permisos anteriores.

ARCHIVOS

Nombre	**Significado**
Leer	Permite ver el contenido del archivo, así como su propietario, permisos y atributos.
Escribir	Permite sobrescribir el archivo, modificar sus atributos y ver su propietario, permisos y atributos.
Leer y ejecutar	Permite ejecutar el archivo más todos los permisos de Leer.
Modificar	Permite modificar y eliminar el archivo más todos los permisos de Escribir y de Leer y Ejecutar
Control total	Permite cambiar permisos y tomar posesión del archivo, más todos los permisos anteriores.

Cuando la asignación de permisos que se quiere realizar no se ajusta al comportamiento de ninguno de los permisos estándar, entonces se deben asignar permisos individuales.

La Tabla 3 muestra cuáles son los permisos individuales en Windows 2000, junto con su significado concreto. También en este

caso debe entenderse que cada permiso puede ser concedido de forma positiva o negativa.

Tabla 3. Permisos individuales en Windows 2000

Nombre	**Significado**
`Atravesar carpeta/ejecutar archivo`	Aplicado a una carpeta, permite moverse por subcarpetas en las que puede que no se tenga permiso de acceso. Aplicado a un archivo, permite su ejecución.
Leer carpeta/Leer datos	Aplicado a una carpeta, permite ver los nombres de sus archivos y subcarpetas. Aplicado a un archivo, permite leer su contenido.
Leer atributos	Permite ver los atributos del archivo/carpeta.
Leer atributos extendidos	Permite ver los atributos extendidos del archivo o carpeta. (Estos atributos están definidos por los programas y pueden variar).
Crear archivos/escribir datos	Aplicado a una carpeta, permite crear archivo en ella. Aplicado a un archivo, permite modificar y sobrescribir su contenido.
Crear carpetas/anexar datos	Aplicado a una carpeta, permite crear subcarpetas en ella. Aplicado a un archivo, permite añadir datos al mismo.
Escribir atributos	Permite modificar los atributos de un archivo o carpeta.
Escribir atributos extendidos	Permite modificar los atributos extendidos de un archivo o carpeta.
Borrar subcarpetas y	Sólo se puede aplicar a una carpeta, y

archivos	permite borrar archivos o subcarpetas de la misma, aún no teniendo permiso de borrado en dichos objetos.
Borrar	Permite eliminar la carpeta o archivo.
Leer permisos	Permite leer los permisos de la carpeta o archivo.
Cambiar permisos	Permite modificar los permisos de la carpeta o archivo.
Tomar posesión	Permite tomar posesión de la carpeta o archivo.

La siguiente tabla explica el subconjunto de los permisos individuales que forman cada uno de los permisos estándar mencionados anteriormente.

Tabla 4. Subconjunto de permisos individuales

Permiso	**C. Total**	**Modificar**	**Leer y Ej.**	**Listar**	**Leer**	**Escribir**
Atravesar carpeta/ejecutar archivo	√	√	√	√		
Leer carpeta/Leer datos	√	√	√	√	√	
Leer atributos	√	√	√	√	√	
Leer atributos extendidos	√	√	√	√	√	
Crear archivo/escribir datos	√	√				√
Crear carpetas/anexar datos	√	√				√

Permiso	C. Total	Modificar	Leer y Ej.	Listar	Leer	Escribir
Escribir atributos	√	√				√
Escribir atributos extendidos	√	√				√
Borrar subcarpetas y archivos	√					
Borrar	√	√				
Leer permisos	√	√	√	√	√	√
Cambiar permisos	√					
Tomar posesión	√					

Derechos de usuario

Los derechos de usuario son reglas que determinan las acciones que puede realizar un usuario en un equipo. Además, los derechos de usuario controlan si un usuario puede iniciar una sesión en un equipo de manera local o en red, agregar a usuarios locales a grupos locales, eliminar usuarios etc. Windows 2000 tiene asignados grupos de derechos de usuarios a grupos integrados.

Los administradores suelen asignar derechos de usuario agregando una cuenta de usuario a uno de los grupos integrados o creando un nuevo grupo y asignando derechos de usuario específicos, en consecuencia los usuarios incluidos en tal grupo heredan automáticamente todos los derechos de usuario asignados a las cuentas del grupo los derechos de grupo se administran mediante directivas de grupo.

Directivas de grupo

La directiva de grupo es utilizada para definir y controlar el funcionamiento de los programas y los recursos los recursos de red y el sistema operativo para los usuarios y recursos de una organización.

En un entorno de Active Directory, Windows 2000 aplica la directiva de grupo a usuarios en función de su pertenencia a sitios, Dominios o unidades organizativas.

Windows 2000 incorpora varias características de seguridad mediante un sistema de inicio de sesión de usuario seguro y obligatorio. Las características de seguridad promueven el uso de controles de acceso eficaces y fiables a todos los recursos y activos de una red. Las características de seguridad de Windows 2000 incluyen:

- Protección de memoria.
- Auditoría de sistemas en todos los niveles de sucesos y actividades.
- Controles precisos sobre el acceso a archivos y carpetas.
- Controles precisos en todos los niveles de limitaciones de acceso a red.

Modelo de seguridad[11]

Lo fundamental del modelo de seguridad de Windows 2000 radica en los descriptores de Seguridad (*Security Descriptors*, SD) y las listas de Control de Acceso (*Access Control Lists*, ACL). Todos los objetos asegurables, como archivos, unidades, procesos,

[11] Schmidt Jeff, **Guía Avanzada Seguridad en Microsoft Windows 2000,** 46-57 p.

impresoras tienen un descriptor de seguridad adjunto. Un descriptor de seguridad tiene lo siguientes datos:

- El SID del objeto propietario.
- El SID del grupo propietario principal.
- La lista de control de acceso discrecional (*Discretionary Access Control List*, DACL).
- La lista de control de acceso del sistema (*System Access Control List*, SACL).

Los SID son identificadores numéricos de longitud variable con los que Windows 2000 representa a cada cuenta, grupo, máquina y dominio, este número es independiente al número de cuenta.

Las ACL *(Access Control Lists)* contienen los permisos actuales asignados a un objeto, además de instrucciones de auditoría para el núcleo. Una ACL consiste en un encabezado seguido por cero o más ACE (*Access Control Entries*, Entradas de Control de Acceso). Una ACL con ninguna ACE se llama ACL nula.

Hay dos tipos de ACL: ACL discrecionales (DACL) y ACL de sistema (SACL). Las DACL definen permisos de acceso al objeto que protegen, mientras que las SCAL contienen instrucciones de auditoría para el sistema.

Servicios [12]

Un servicio de Windows 2000 es una imagen que se ejecuta como una tarea en segundo plano.
El control de los servicios está a cargo del Administrador de Control de Servicios (*Service Control Manager*, SCM). Los servicios pueden comenzar automáticamente en el arranque del

[12] Ibidem, p. 93-95

sistema, un usuario puede iniciarlos manualmente o puede hacerlo algún otro programa.

El SCM controla completamente el tiempo de vida de un servicio. EL SCM es quien inicia los servicios. Su proceso, el services.exe, posee los procesos de todos los servicios que se están ejecutando.

Los servicios normalmente entran en una de estas categorías:

- Proporcionan algún tipo de recurso a otros usuarios o máquinas de la red. Es la utilización más normal.
- Tareas que no podrían o no deberían involucrar al usuario de consola. Esto también podría ocurrir porque las tareas son de procesamiento en segundo plano o porque necesitan más privilegios de seguridad de los que tiene el usuario de consola.
- Revisión de otros servicios, proceso o alguna otra función del sistema.

Cumple principalmente con estas tareas:

- Mantener una base de datos de servicios instalados.
- Procesar solicitudes de instalación y eliminación de servicios.
- Iniciar servicios especificados como de inicio automático en el arranque.
- Mantener una base de datos de todos los servicios en ejecución y su estado.
- Aceptar y dar salida a mensajes de usuarios y otros procesos al servicio adecuado, lo que incluye iniciar o detener solicitudes.

La base de datos de servicios aparece en el registro, en HKLM\System\CurrentControlSet\Services, bajo esta clave hay subclaves para todos y cada uno de los servicios instalados.[13]

Un valor DWORD hexadecimal o decimal determina el tipo de inicio del servicio. Los valores posibles de esta clave son:

1. Un valor **2** significa un tipo de inicio *Automatic,* es decir, el servicio se inicia automáticamente mientras se carga el sistema operativo. Esta opción puede incrementar el tiempo de inicio del sistema, así como el consumo de recursos, mientras que el servicio igual no es necesario.
2. Un valor **3** significa un tipo de inicio *Manual*, es decir, que el servicio no se inicia de forma predeterminada tras la carga del sistema operativo, en cambio puede ser iniciado manualmente en cualquier instante.
3. Un valor **4** significa que el servicio está *deshabilitado*, es decir, obliga al administrador a tener que habilitarlo antes de poder ejecutarlo.

Common Criteria[14]

Antecedentes

Common Criteria es el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos de tecnologías de información y es ampliamente aceptado por la comunidad internacional.

---

[13] http://fferrer.dsic.upv.es/cursos/Windows/basico/ch04s02.html <4 de noviembre 2006>

[14] Con base en información de la página electrónica http://www.microsoft.com/spain/enterprise/perspectivas/numero_6/seguridad.mspx/202003 <12 de noviembre de 2006>

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (Trusted Computer System Evaluation Criteria) y publicados en *The Orange Book* (El Libro Naranja). En las décadas posteriores, varias organizaciones de diferentes países como CSE (Canadá), SCSI (Francia), BSI (Alemania), NLNCSA (Holanda), CESG (Reino Unido), NIST y NSA(USA) tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas más flexibles y adaptables a la constante evolución de los sistemas de TI.

De ahí la comisión europea, en el año 1991 publicó el ITSEC (Information Technology Security Evaluation Criteria), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canadá, igualmente se desarrollaron en 1993 los criterios CTCPEC (Canadian Trusted Computer Product Evaluation) uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publicó los Federal Criteria como una aproximación a unificar los criterios europeos y americanos. En 1996 se publica la versión 1.0 y en 1998 la versión 2.0 del Common Criteria.

Tal escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general, y en esa labor la *Internacional Organisation for Standard* (ISO) comienza a trabajar a principios de los años 90 dando como resultado la certificación Common Criteria (o ISO-IEC 15408)

Common Criteria es un estándar mundial de seguridad que permite medir la fiabilidad de los productos de tecnologías de la información, permitiendo aumentar la confianza de los usuarios en las tecnologías de la información y habilitarlos para tomar decisiones con información y criterio, por encima de otras consideraciones subjetivas.

Niveles de evaluación de la seguridad [15]

La estructura del CC también nos provee de una gran flexibilidad en la especificación de productos seguros. El consumidor y las demás partes pueden especificar la funcionalidad de seguridad en un producto en términos de perfiles de protección estándar e independientemente seleccionar el nivel de seguridad para la evaluación de un conjunto definido de 7 niveles incrementales de evaluación de seguridad, desde EAL1 hasta EAL 7.

Los 7 EAL's son los siguientes:

EAL1 - functionally tested
EAL2 - structurally tested
EAL3 - methodically tested and checked
EAL4 - methodically designed, tested and reviewed
EAL5 - semiformally designed and tested
EAL6 - semiformally verified design and tested
EAL7 - formally verified design and tested

Arriba del EAL 4, se requiere la aplicación de técnicas incrementales de ingeniería en seguridad especializada. Los objetivos de evaluación que cumplan con los requerimientos de este nivel de seguridad estarán diseñados y desarrollados con el propósito de cumplir con esos requerimientos, En el nivel más alto (EAL7) existen limitantes significativas a la hora de cumplir con los requerimientos, esto en parte se debe al impacto substancial del costo en las actividades tanto del desarrollador como del evaluador y también se deben a que al más simple de los productos se le

[15] Con base en la información de la página electrónica del Common Criteria http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf <15 de noviembre de 2006>

complique la aplicación de técnicas de análisis formal que estén a la vanguardia.

EAL1 prueba funcional: se aplica cuando algún nivel de confianza en la operación se requiere, pero las amenazas a la seguridad no son tomadas como algo serio.
Una evaluación en este nivel debe proveer evidencia de que las funciones del objeto a evaluar son consistentes con su documentación.

EAL2 prueba estructural: requiere la cooperación del desarrollador en términos de la entrega de información de diseño y resultados de las pruebas pero no debe demandar mayor esfuerzo en la parte del desarrollador.
Se aplica en circunstancias donde desarrolladores o usuarios requieren de un bajo a moderado nivel de seguridad. Una evaluación como esta puede surgir cuando se busque asegurar sistemas legados o donde el acceso al desarrollo pudiera ser limitado.

EAL3 metódicamente probado y verificado: permite a un desarrollador obtener un alto nivel de seguridad en la fase de diseño sin la alteración substancial de las buenas prácticas de desarrollo existentes. Puede aplicarse donde el requerimiento de seguridad es moderado.

EAL4 metódicamente desarrollado, probado y revisado: permite a un desarrollador maximizar el aseguramiento que se obtuvo de una ingeniería en seguridad basada en buenas prácticas comerciales de desarrollo. A pesar de ser rigurosas estas prácticas no requieren habilidades especiales u otros recursos.
Es aplicable en circunstancias donde los desarrolladores o usuarios requieren de un moderado a alto nivel de seguridad

EAL5 semiformalmente diseñado y probado: permite al desarrollador obtener un máximo nivel de seguridad basado en prácticas de desarrollo comercial rigurosas que son soportadas por la aplicación moderada de técnicas especializadas de ingeniería en seguridad.

EAL 5 puede aplicarse donde el requerimiento que se busca es un alto nivel de seguridad
EAL 5 provee de un análisis que incluye toda la implementación, la búsqueda de vulnerabilidades debe asegurar la resistencia a la penetración de atacantes con un potencial de ataque moderado.

EAL 6 diseño semiformalmente verificado y probado: permite al desarrollador ganar un alto aseguramiento con la aplicación de técnicas de ingeniera de seguridad especializadas en un riguroso ambiente de desarrollo para producir un objetivo de evaluación de máxima calidad que proteja los activos de alto valor en contra de riesgos significativos. EAL 6 se aplica al desarrollo de objetivos de evaluación de seguridad especializada en situaciones de alto riesgo donde el valor de los activos protegidos justifica los costos adicionales.

Esta EAL implica la búsqueda de vulnerabilidades que aseguren la resistencia a la penetración de atacantes con un alto potencial de ataque.

EAL 7 diseño formalmente verificado y probado: se aplica al desarrollo de objetivos de evaluación de seguridad para aplicación en situaciones de extremo alto riesgo y/o donde el alto valor de los activos justifica los altos costos. La aplicación práctica de EAL7 se limita actualmente a objetivos de evaluación enfocados estrictamente en funcionalidad de seguridad que está sujeta a un análisis formal extensivo.

Windows 2000 y Common Criteria

El 29 de Octubre de 2002 Microsoft Windows 2000 obtiene la certificación EAL4 + Flaw Remediation, es decir, la máxima certificación de seguridad para un sistema operativo comercial.

"Se trata de una única vara de medir, una norma que especifica, mide y garantiza la seguridad de un producto y que, además, está reconocida en catorce países de Europa, América, África y el continente australiano", afirma Héctor Sánchez, responsable de Seguridad en Microsoft Ibérica

Una de las mayores ventajas de este conjunto de criterios es que permite a los usuarios comparar sus requerimientos específicos frente a los estándares de Common Criteria, para determinar el nivel de seguridad que necesitan.
También pueden saber más fácilmente cuándo un producto cumple con una serie de especificaciones. Otro de los beneficios de la Certificación Common Criteria es que proporciona a los usuarios guías que simplifican el despliegue y la operación de Microsoft Windows 2000 en un entorno de red seguro.

Administrador de Sistemas

El Administrador de Sistemas es la persona responsable de configurar, mantener y actualizar el sistema o conjunto de sistemas que forman una red, cuidando el funcionamiento del software, hardware y periféricos de forma que estén disponibles para ser utilizados por los usuarios.[16]

Las responsabilidades generalmente incluyen:

[16] http://www.super.unam.mx/admon/ <23 de noviembre de 2006>

- Realizar copias de seguridad.
- Actualizar el sistema operativo, y configurar los cambios.
- Instalar y configurar el nuevo hardware y software.
- Agregar, borrar y modificar información de las cuentas de usuarios, reestablecer contraseñas.
- Responder consultas técnicas.
- Responsable de la seguridad.
- Responsable de documentar la configuración del sistema.
- Resolución de problemas.
- Configuración óptima del sistema.
- Implantación de DRP's *(Disaster Recovery Plan)*.

En grandes organizaciones, algunas de las tareas listadas arriba se dividen entre diferentes administradores de sistema. Por ejemplo, debe haber un individuo o un grupo responsable de probar e instalar las nuevas actualizaciones.

En organizaciones más pequeñas, un administrador también puede tener responsabilidades asociadas a otros campos, como pueden ser:

- Soporte técnico.
- Administrador de base de datos.
- Administrador de red.
- Analista de sistemas.
- Administrador de seguridad.
- Programador.

Los administradores de sistema, en grandes organizaciones, tienden a no ser arquitectos de sistemas, ingenieros de sistemas ni diseñadores de sistemas. Como sucede con muchos roles de este campo, en las pequeñas organizaciones las diferencias de roles no están muy delimitadas. Los administradores de sistema Senior,

tienen conocimiento en varias de estas otras áreas, como resultado de su amplia experiencia laboral.[17]

Auditoría

Es un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.[18]

La auditoría incluye la planeación de ésta, el examen y la evaluación de la información, la comunicación de los resultados y la toma de decisiones. [19]

La auditoría se apega a que las tareas desempeñen las normas, políticas, procedimientos y técnicas generalmente establecidas por los organismos aceptados a nivel nacional e internacional.

Auditoría interna

La auditoría interna es aquella que es realizada con recursos materiales y humanos propios de la empresa. Existe por expresa decisión de la empresa.

Ventajas:

- Periódicamente se pueden realizar revisiones globales.
- Forma parte de las actividades normales de la empresa.

[17] http://es.wikipedia.org/wiki/Administrador_de_sistemas <23 de octubre 2006>

[18] Echenique García, José Antonio. **Auditoría en informática,** p 2

[19] Ibidem, p. 31

- El personal se habitúa a las auditorías y las recomendaciones que son ofrecidas como resultado de éstas benefician el trabajo del personal involucrado.

Desventajas:
- Solamente las empresas grandes pueden poseer esta área como parte de su organización.

Auditoría externa

La auditoría externa es aquella que es realizada por personas ajenas a la empresa, se presupone una mayor objetividad en los resultados de la misma.

Ventajas:
- Se pueden contrastar los informes internos y externos.
- Se tiene una visión más objetiva del estado actual de la empresa.

Desventajas:
- Puede ser muy costosa.
- El personal interno puede entorpecer las labores del auditor y de su grupo de trabajo.

Auditor

El auditor es el especialista encargado de evaluar la eficiencia y eficacia de un área u organismo en particular, y mediante el señalamiento de cursos alternos de acción para la toma de decisiones que permitan corregir los errores, en caso que existan, o mejorar algún procedimiento.

Características de un auditor
- Conocimientos técnicos actualizados.

- Debe ser objetivo, para no tomar decisiones basadas en preferencias personales, es decir, capaz de emitir juicios imparciales.
- Capacidad para comunicarse tanto de manera oral como escrita.
- Facilidad para tratar con personas.[20]

Auditoría en Informática

"La auditoría en informática es la revisión y evaluación de los controles, procedimientos, técnicas y estándares de informática, así como de los equipos de computo, su utilización, eficiencia, eficacia y seguridad de la organización que participan en el procesamiento de la información a fin de que por medio del señalamiento de los cursos alternativos se logre una utilización mas productiva y segura que servirá para una adecuada toma de decisiones." Álvarez Anguiano[21]

La auditoría en Informática es el proceso de recolección y evaluación de evidencias para determinar cuándo son salvaguardados los activos de los sistemas computarizados, de qué manera se mantiene la integridad de los datos y cómo se logran los objetivos de la organización eficazmente y se usan los recursos eficientemente. [22]

La auditoría en Informática deberá evaluar los sistemas de información, desde sus entradas, procedimientos, comunicación, controles, integridad de archivos, seguridad física y lógica, personal y obtención de información.[23]

---

[20] Ibidem, p. 28
[21] Lic. Eduardo Estrada Martínez, Apuntes de Auditoría en informática
[22] Echenique García, José Antonio. **Auditoría en informática,** p. 26
[23] Ibidem, p.19

Campo de acción de la Auditoría en Informática

- La evaluación administrativa del área de Informática.
- La evaluación de los sistemas y procedimientos para conocer su eficiencia y eficacia
- La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes y bases de datos).
- Seguridad de la información.
- Aspectos legales de los sistemas y de la información.

Objetivos de la Auditoría en Informática [24]

- Incrementar la satisfacción de los usuarios de sistemas computarizados.
- Asegurar mayor integridad, confidencialidad y disponibilidad de la información mediante la recomendación de configuraciones y controles específicos.
- Conocer la situación actual del área informática y las actividades y esfuerzos para lograr los objetivos propuestos.
- Minimizar riesgos en el uso de la tecnología de la información.
- Ayudar a la toma de decisiones sobre inversión para evitar gastos innecesarios.
- Capacitar sobre controles en sistemas de información.
- Salvaguardar los activos de la empresa, es decir, software, hardware y recursos humanos.

[24] Lic. Eduardo Estrada Martínez, Apuntes de Auditoría en informática.

CAPÍTULO 2. ANÁLISIS

1. MOTIVACIÓN DEL PROYECTO

Propósito

Desarrollar una herramienta que sirva de ayuda al administrador de equipos con sistema operativo Windows 2000 Professional, Windows 2000 Server y Windows 2000 Advanced Server a realizar una auditoría de las configuraciones de seguridad definidas en el Windows 2000 Security Configuration Guide, generando reportes en formatos html y txt para su mayor entendimiento y análisis posterior.

Situación óptima

Contar con un sistema operativo Windows 2000 que se encuentre siempre actualizado, libre de virus y resistente a ataques, mediante actualizaciones de seguridad, el uso de programas antivirus y firewalls actualizados, y configuraciones robustas que reduzcan las amenazas a los sistemas para evitar así ataques que perjudiquen considerablemente a la organización, ya sea a sus activos o al funcionamiento de la misma.

Problemas

- Que los administradores no apliquen a tiempo actualizaciones de seguridad que puedan eliminar algunos riesgos.
- Que el administrador no se encargue de la actualización de programas antivirus.
- Que se tengan configuraciones débiles que puedan facilitar el éxito de un ataque.
- Tener habilitados servicios innecesarios.
- Que no se apliquen políticas correctas a los usuarios.

Implicación

Al no seguir las recomendaciones resultantes de una auditoría, la administración de los equipos resultará más complicada, además que los sistemas se vuelven más vulnerables, siendo blanco fácil de ataques por códigos maliciosos, usuarios malintencionados o intrusos .

Necesidad

En el contexto de una empresa se ha determinado que el eslabón más débil en la Seguridad Informática suelen ser los usuarios finales, dado que no es muy común que se suela poseer contraseñas fuertes o que se actualicen los sistemas operativos, aplicaciones o antivirus, incluso en muchas organizaciones se carece de software antivirus, motivo por el cual se hace necesaria una herramienta que pueda verificar estos controles y así incrementar el nivel de seguridad en una organización que haga uso de Windows 2000 Professional, Windows 2000 Server y Windows 2000 Advanced Server.

2. DECLARACIÓN DEL PROYECTO

Objetivo del sistema:

Automatizar la realización de auditorías de las configuraciones de seguridad definidas en el Windows 2000 Security Configuration Guide para equipos con sistema operativo Windows 2000.

Se pretende que la herramienta sea adoptada como una utilería de uso frecuente por los administradores de equipos con sistema operativo Windows 2000.

Alcance:

- Generar reportes que le permitan al administrador del sistema Windows 2000 conocer el nivel de cumplimiento de las configuraciones de seguridad definidas en el Windows 2000 Security Configuration Guide para el equipo en el cual fue ejecutada la herramienta.
- Generar información acerca de las actualizaciones de seguridad aplicadas a cada equipo (Service Pack y HotFixes).
- Dar a conocer configuraciones débiles que se encuentren en el equipo analizado.
- Obtener información sobre si se tiene instalado algún antivirus y firewall.
- Obtener información relevante acerca de la plataforma de hardware del sistema, como lo es el espacio disponible en disco duro, sistema de archivos, contraseña en el BIOS, compatibilidad de hardware, utilizando tecnologías de scripts y no una aplicación de escritorio, dotando a la herramienta de portabilidad para cualquier sistema bajo plataforma NTFS.

Exclusiones:

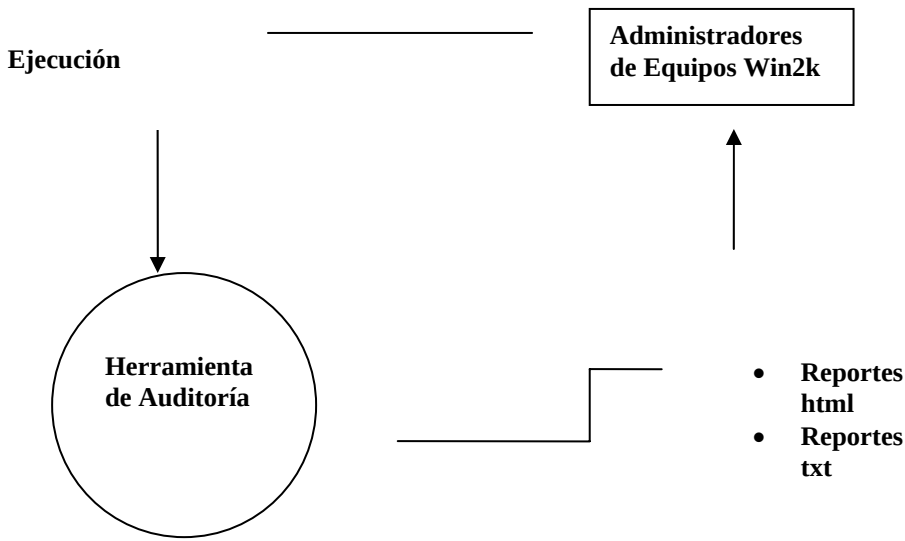
- La herramienta no realizará auditaría a equipos que no cuenten con sistema operativo Windows 2000 Professional, Windows 2000 Server o Windows 2000 Advanced Server,
- La ejecución de la herramienta no se llevará a cabo en un ambiente de red, es decir, su ejecución será de manera local.
- La herramienta no tiene la capacidad de modificar o corregir las malas configuraciones que llegaran a detectarse, simplemente servirá como guía de acción para la toma de decisiones en cuanto a la Administración del Sistema de Cómputo analizado.

3. PERFIL DEL USUARIO

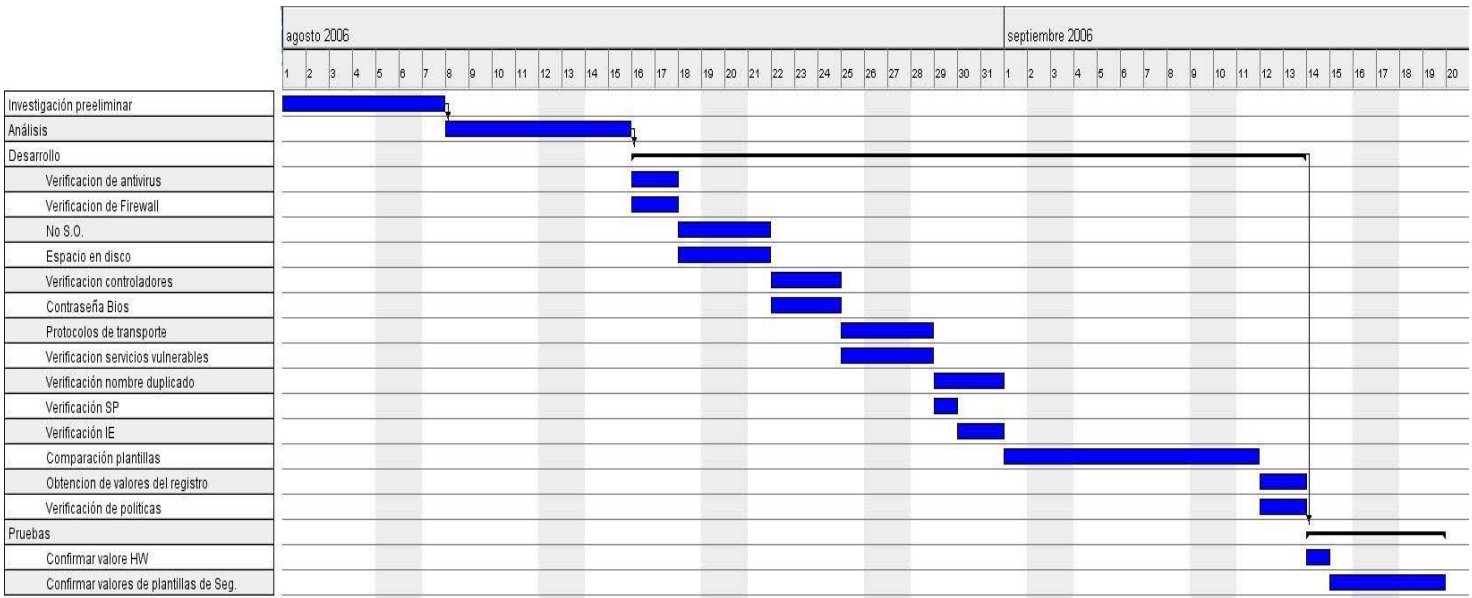
Para la herramienta se tiene contemplado que el usuario final sea un administrador de equipos Windows 2000, en tal caso puede ser un administrador de servidores o un usuario final.

Se pretende con el uso de la herramienta, facilitar la tarea de auditoría al administrador de los equipos Windows 2000, llevándole así a una mejor toma de decisiones en materia de seguridad informática.

4. DIAGRAMA DE CONTEXTO



5. PLANEACIÓN DEL PROYECTO



Comparativa de herramientas de auditoría en plataforma Windows

En la actualidad existen pocas herramientas que tengan la utilidad de realizar auditorías confiables y completas a los sistemas Windows 2000, por lo cual se propone el desarrollo de una aplicación de auditoría que sirva como una guía de *hardening* para dichos sistemas.

Se llevó a cabo el análisis de tres herramientas de auditoría disponibles en el mercado; *WindAudit, Belarc Advisor y Microsoft Baseline Security Analyzer***,** con el objeto de conocer fortalezas y debilidades de cada una de ellas y ofrecer así una ventaja con el desarrollo de la herramienta propuesta.

WinAudit.
Esta herramienta de auditoría está orientada a realizar un inventario de los activos de la máquina, como lo son dispositivos periféricos y hardware en general del equipo analizado. Si bien la auditoría que realiza no es totalmente orientada a hacer una auditoría de seguridad, sí contempla varios puntos relativos a ésta e inclusive hay una sección dedicada a la seguridad.

Los principales puntos abordados en la parte de seguridad en los que Winaudit realiza reportes son los siguientes:

- Puertos abiertos

Este programa determina los puertos lógicos de comunicación que actualmente están a la escucha y de los que se tiene comunicación establecida. Esta salida es muy similar a lo que podemos obtener como resultado de la ejecución de la herramienta del sistema netstat utilizando las opciones "–na", siendo de utilidad para verificar el tipo de conexiones actualmente establecidas desde y

hacia nuestro equipo, proporcionando información valiosa en materia de seguridad ya que algunas aplicaciones maliciosas abren puertos para establecer comunicación con algún equipo remoto desde el cual podrá recibir comandos a ser ejecutados en nuestro equipo con diferentes fines como podrían ser el robo de información o la utilización de los recursos para redirección de ataque u otros diferentes fines.

- Privilegios

Esta herramienta hace una auditoría de los usuarios que se tienen registrados en el sistema y cuáles son los permisos que tienen asignados, los cuales son básicamente permisos de administrador o de usuarios.

- Bitácoras del sistema

En cuanto a las bitácoras se refiere, esta herramienta sólo extrae los registros de tipo erróneo de las bitácoras del equipo, reportando dicha información en un formato más legible que el *eventviewer*, pero siendo en esencia la misma información.

- Características de seguridad

En esta sección se listan algunas configuraciones del sistema relacionadas con la seguridad del mismo, como por ejemplo.

AutoLogon: detecta si está habilitada la característica de autologon, la cual permite que un usuario inicie sesión en el sistema sin necesidad de utilizar sus credenciales, puesto que éstas son almacenadas en el registro.

Screen Saver: esta característica, que aplica al usuario actual, sirve para determinar si el protector de pantalla se encuentra protegido por un password y además identifica el tiempo de espera para que éste entre en función.

User account: muestra las principales características en cuanto a políticas aplicadas a la cuenta del usuario actual se refiere, como serían el tiempo que el password tiene sin modificaciones o si el usuario tiene privilegios de administrador.

All Accounts: muestra importantes características de seguridad que son aplicadas a todas las cuentas de usuario.

Automatic Updates: muestra si el sistema operativo está configurado para llevar a cabo la descarga de actualizaciones, así como también muestra la periodicidad con que ésta se llevará a cabo.

Internet Explorer: muestra las características de seguridad del Internet Explorer, como lo son descarga de archivos, si tiene habilitado Active X, Java o JavaScript.

- Firewall

Muestra las aplicaciones, los Servicios y los puertos autorizados por el firewall del Sistema.

- Actualizaciones del sistema.

Muestra Service Packs, Hotfixes y actualizaciones del Internet Explorer instaladas en el equipo auditado

- Network Files

Muestra aquellos archivos que son accedidos por usuarios remotos.

- Network Sessions

Muestra una lista de usuarios y computadoras que están conectados en el equipo analizado.

- Network Shares

Muestra información sobre los recursos compartidos en el equipo, como lo son el nombre, tipo y ruta del recurso compartido.

- Update agent

Muestra una bitácora histórica de las actualizaciones de seguridad (Hotfixes y Service Packs) hechas en el sistema.

- Programas de arranque

Muestra una lista de los programas que se inician automáticamente al arrancar el equipo.

- Servicios

Muestra una lista de los servicios que el equipo se encuentra ejecutando, los clasifica en drivers y procesos.

Belarc Advisor

Esta herramienta muestra una descripción general del hardware del sistema, como lo son número de discos duros, tarjeta madre del equipo, procesador, memoria física, impresoras, dispositivos de red, entre otros.
Identifica si alguno de los antivirus que se encuentra en su base de datos está activo en el sistema.
Verifica que las actualizaciones de seguridad estén al día y lista los Hotfixes instalados y faltantes.
Hace una valoración de la seguridad del equipo llamada CIS Benchmark basada en la organización *Center of Internet Security*.
Esta auditoría contempla las siguientes características:

- Current Service Pack

Verifica si está instalado el último Service Pack liberado por Microsoft.

- Critical and Security Hotfixes

Verifica si están instalados los últimos Hotfixes que se encuentran disponibles en Microsoft Update.

- Password Policies

Verifica que estén aplicadas las políticas de seguridad en las contraseñas, en lo que respecta a que estas no tengan una duración de 90 días y estén compuestas por al menos 8 caracteres.

- Audit and Account Policies

Verifica que se registren los eventos del sistema, como lo son inicio de sesión, acceso a objetos y de igual manera hace una verificación de la seguridad en cuentas de usuario.

- Anonymous Account Restrictions

Verifica que en los accesos anónimos a través de la red esté limitado el acceso al archivo SAM, previniendo así una enumeración de los usuarios

- Security Options

Verifica que un conjunto de configuraciones avanzadas de seguridad de Windows 2000 estén habilitadas tales como el nivel de autenticación de LAN Manager y que se hayan renombrado las cuentas de los usuarios Administrador e invitado

- Available Services

En esta sección se hace un desplegado de los servicios actualmente en funcionamiento en el sistema.

Esta herramienta también muestra versiones de software, ruta donde se encuentran instalados, así como las licencias de software.

Microsoft Baseline Security Analyzer

Esta herramienta de seguridad, propietaria de Microsoft realiza una revisión de las características de seguridad de la computadora local, en red o en un dominio particular, especificando el rango de direcciones ip's o el nombre del dominio.

- Security Update Scan Results

Verifica si las actualizaciones de seguridad de Windows, Office, MDAC y MSXML se encuentran al día, indicando la cantidad de actualizaciones faltantes.

- Vulnerabilities

* Local Account Password Test: esta prueba verifica, de las cuentas de usuarios, que los passwords no sean débiles o estén en blanco.

***** Administrators: verifica que el número de cuentas de administrador no sea mayor a uno.

* Windows Firewall: verifica si el equipo tiene instalado y configurado el firewall de Windows.

* Automatic Updates: verifica el estado de las actualizaciones automáticas del equipo.

* File System: verifica que las unidades de disco tengan NTFS como sistema de archivos.

* Guest Account: verifica el estado de la cuenta de usuario "Guest".

* Restrict Anonymous: verifica si está restringido las conexiones anónimas al equipo escaneado.

* Autologon: determina si la característica de AutoLogon está habilitada en el equipo, o si la contraseña está cifrada en el registro o almacenada en texto plano.

* Password Expiration: Verifica si alguna cuenta local tiene contraseña que no expira.

- Additional System Information

* Auditing: Determina si la opción de auditoría está habilitada en el equipo escaneado, para el registro de eventos específicos en el sistema, tales como intentos de conexión fallidos y exitosos.

* Services: Determina si los servicios contenidos en el archivo Services.txt están instalados en el equipo analizado, así como su estado actual. Por defecto la lista de servicios contenidos en el archivo es:

MSFTPSVC (FTP)

TlntSvr (Telnet)

W3SVC (WWW)

SMTPSVC (SMTP)

* Shares: Determina si el equipo analizado tiene alguna carpeta compartida. En caso de ser así, se reporta una lista con las carpetas compartidas y sus respectivos permisos NTFS.

* Windows Version: Determina la versión de Sistema Operativo que tiene el equipo analizado.

- Internet Information Services Scan Results

* IIS Status: Verifica el estado del Internet Information Service

- SQL Server Scan Results

***** SQL Server/MSDE Status: Verifica si SQL Server/MSDE está instalado en el equipo analizado.

- Desktop Application Scan Results

* IE Zone: Verifica el nivel de seguridad con el cual está configuradas las zonas de Internet Explorer.

* Macro security: Determina el nivel de seguridad de Microsoft Office 2003, Office XP, Office 2000 y Office 97 con respecto a las macros , en particular PowerPoint, Word, Excel y Outlook. Las macros son tareas automatizadas repetitivas que pueden transmitir virus cuando un usuario abre un documento infectado.

Entorno de desarrollo

Hardware

- 2 Computadoras con las siguientes características
- procesador 2.5 GHz
- 60 GB de espacio en HD.
- 256 MB en memoria RAM.
- Impresora.

Software de Aplicación

- Sistema Operativo Windows 2000 Professional
- Navegador de Internet Mozilla Firefox

Software de Desarrollo

- WMI (*Windows Management Instrumentation*)
- WSH (*Windows Script Host*)
- VBScript (*Visual Basic Script Edition*)

WMI (*Windows Management Instrumentation*)[25]

Al ser Administrador se puede ver a Windows como caja negra, la cual se centra en proveer diferentes funcionalidades, la parte central o core del sistema operativo es quien nos provee de funciones básicas, manejo de protocolos y servicios. En el trabajo como administrador esta visión nos limita a ver al sistema operativo como una entidad configurable pero no manipulable del todo.

[25] Honeyman, Jeffrey **Windows 2000: scripting Windows 2000** p.252-253

Los programadores ven al sistema operativo más como una caja de herramientas que como una caja negra. Windows, desde la perspectiva de Programación, no es más que un conjunto de instrucciones que los programadores invocan para construir aplicaciones y que no necesariamente tiene que escribirse código para manipular directamente el sistema operativo, puesto que Windows provee un conjunto de herramientas para simplificar las tareas de programación.
Combinando estas 2 perspectivas se puede visualizar a Windows como un sistema operativo que puede manipular, crear configuraciones y utilizar instrucciones para satisfacer necesidades particulares.

La herramienta para manipular el sistema operativo en un nivel más bajo es conocida como API interfaz de programación de aplicaciones (*Aplication Program Interface* por sus siglas en inglés), la API nos permite adentrarnos en el sistema operativo para obtener las características que nuestras herramientas pueden configurar.

En Windows el API principal es el API de Win32. La mayoría de las actividades que se realizan en un entorno Windows tiene que ver con el API de Win32.

Otra API que es de gran utilidad es la de *Windows Management Instrumentation* (WMI) el cual permite realizar configuraciones del sistema operativo y hardware además de que algunas funcionalidades de la línea de comandos tienen su equivalente en WMI.

Para la manipulación de las APIs es necesaria la utilización de código en un lenguaje de programación que permita acceder a ellas, en este caso se utiliza vbscript que permite el acceso a la mayoría de las APIs de Windows.

WSH (*Windows Script Host*)[26]

Como anteriormente se vio, para acceder a configuraciones del sistema operativo y realizar actividades que requieren trabajo en un nivel más bajo se hace uso de WMI, en los casos en los cuales se realicen tareas en las que no se requiera manipular el sistema operativo hacemos uso de Windows Script Host ya que este lenguaje de script provee otro tipo de funcionalidad tales como salidas a pantalla o manipulación de archivos las cuales son también necesarias en la realización de la herramienta

VBScript (*Visual Basic Script Edition*)

VBScript es un lenguaje interpretado que surge como variación del lenguaje de programación Visual Basic for Aplications. VBScript es una versión reducida en funcionalidad de Visual Basic for Aplications ya que se eliminaron varias características, algunas de ellas por ser consideradas inseguras, aunque VBScript también posee características propias.

En particular en el desarrollo de esta herramienta este lenguaje es utilizado como plataforma de programación para la utilización de WMI y WSH.

Requerimientos de la aplicación

- Computadora que cuente con la plataforma Windows 2000 Professional, Windows 2000 Server o Windows 2000 Advanced Server.

[26] Ibidem, p.134-136

CAPITULO 3. DESARROLLO

El siguiente código escrito en el lenguaje de programación vbscript, en combinación con WSH y WMI, es el que ejecuta la auditoría y genera el reporte resultante de ésta.
En la siguiente parte de código se definen los objetos de tipo texto en los cuales se escribirá el resultado de la auditoría en código HTML y en texto plano para los reportes.

```
Set escritura = WScript.CreateObject("Scripting.FileSystemObject")
Set texto = escritura.CreateTextFile("reporte.html")
Set file = escritura.CreateTextFile("reporte.txt")
```

Se crea la estructura del archivo HTML y en él se escriben los encabezados de los reportes.

```
texto.Writeline "<HTML>"
texto.Writeline "<title> auditoría </title>"
texto.Writeline "<BODY Bgcolor=FFFFFF>"
texto.writeline "<IMG Src=" & Chr(39)& "./unam_logo.gif" &Chr(39)&
"Heigth=120 Width=120 Align=Left> <IMG Src="& Chr(39)& "./fca.gif"
&Chr(39)& "Heigth=120 Width=120 Align=Right>"
texto.Writeline "<Head><bold><H2><Center> Universidad Nacional
Autónoma De México <BR>"
texto.Writeline "Facultad de Contaduría y Administración <BR>"
texto.Writeline "Herramienta de Auditoría: Windows 2000 Common Criteria
<BR>"
texto.WriteLine"<BR>"
texto.WriteLine "<div align" & "="& "left" & ">"& "<font color="&
"#003399"& " size="& "2" &" face="& "Verdana, Arial, Helvetica, sans-
serif"& ">" & "Fecha: " & Date & "<BR>" & "<BR>
"&"</font></center></div>"
texto.WriteLine "<div align" & "="& "left" & ">"&"<font color="&
"#003399"& " size="& "3" &" face="& "Verdana, Arial, Helvetica, sans-
serif"& ">"& "Reporte de Auditoría" & "<BR>" & "<BR>" & "</font>"
texto.WriteLine"<BR>"
texto.Writeline "<Body>"
```

Se crea el encabezado para el reporte en texto plano

```
file.WriteLine "          Universidad Nacional Autónoma de México"
file.WriteLine "            Facultad de Contaduría y Administración"
file.WriteLine "   Herramienta de Auditoría: Windows 2000 Common Criteria "
file.WriteLine "Fecha: " & Date
file.WriteLine "Reporte de Auditoría"
```

Se crea una tabla para desplegar posteriormente los resultados del análisis de la búsqueda de antivirus

```
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><font
color=#FFFFFF>Antivirus</font></center></font></td</tr>"
texto.WriteLine "</table>"
'-----------------------------------------
file.WriteLine "Antivirus"
file.WriteLine ""
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center>Antivirus</td</tr><td>Resultado</center></td
></tr>"
texto.WriteLine "</table>"
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
```

De una lista de los antivirus más comunes, se busca en los procesos en ejecución si hay coincidencias con dicha lista
Esta lista de procesos se obtiene a través de la clase Win32_Process implementando una consulta, una vez hecha la consulta y si encuentra algún antivirus es mandado a imprimir a la tabla y en el caso de que no se encuentre ningún antivirus igualmente reporta este resultado negativo a la tabla

```
On Error Resume Next
strComputer = "."
Set objWMIProceso = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2")
Set procesos = objWMIProceso.ExecQuery("Select * from Win32_Process",,48)
for Each proceso in procesos
If Proceso.Name =  "avpcc.exe"  Then
        texto.writeline"<tr><td>El antivirus instalado es Kaspersky Labs
Antivirus</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>" file.WriteLine "El antivirus instalado es Kaspersky
Labs Antivirus"
cuentaant =cuentaant +1
End If

If Proceso.Name = "avxinit.exe" Then
                texto.writeline"<tr><td>El antivirus instalado es bit-
Defender antivirus</td><td><img src='./paloma.jpg' width='24'
height='25'></td></trfile.WriteLine "El antivirus instalado es bit-Defender
antivirus"
cuentaant =cuentaant +1
End if

If Proceso.Name =  "Dvp95.exe" Then
                texto.writeline"<tr><td>El antivirus instalado es F-Secure
antivirus</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"  file.WriteLine "El antivirus instalado es F-Secure
antivirus"
cuentaant =cuentaant +1
End if

If Proceso.Name =  "Mcshield.exe" Then
                texto.writeline"<tr><td>El antivirus instalado es McAfee
VirusScan</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"  file.WriteLine "El antivirus instalado es McAfee
VirusScan"
                cuentaant =cuentaant +1
End if

Next
if cuentaant = 0 then
```

```
texto.writeline"<tr><td>No esta instalado ningun antivirus</td><td><img
src='./tache.jpg' width='24' height='25'></td></tr>"
file.WriteLine "No esta instalado ningun antivirus"
End If

texto.WriteLine "</table>"
```

Se crea una tabla para desplegar posteriormente los resultados del análisis de la búsqueda de Firewall

```
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><font
color=#FFFFFF>Firewall</font></center></font></td</tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Firewall"
file.WriteLine ""
'-------------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center>Firewall</td</tr><td>Resultado</center></td>
</tr>"
texto.WriteLine "</table>"

texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
```

De una lista de los firewalls de host más comunes, se busca en los procesos en ejecución si hay coincidencias con dicha lista.
Esta lista de procesos se obtiene a través de la clase Win32_Process implementando una consulta, una vez hecha la consulta y si encuentra algún firewall es mandado a imprimir a la tabla y en el caso de que no se encuentre ninguno igualmente reporta este resultado negativo a la tabla

```
On Error Resume Next
strComputer = "."
Set objWMIProceso = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set procesos = objWMIProceso.ExecQuery("Select * from Win32_Process",,48)
for Each proceso in procesos
If Proceso.Name = "zapro.exe" Then
                    texto.writeline "<tr><td>El Firewall instalado es ZoneAlarm Pro</td><td><img src='./paloma.jpg' width='24' height='25'></td></tr>"
file.WriteLine "El Firewall instalado es ZoneAlarm Pro"
cuentafire =cuentafire +1
End If

If Proceso.Name = "winroute.exe" Then
                    texto.writeline"<tr><td>El Firewall instalado es WinRoute</td><td><img src='./paloma.jpg' width='24' height='25'></td></tr>"
file.WriteLine "El Firewall instalado es WinRoute"
cuentafire =cuentafire +1
End if

If Proceso.Name = "umxagent.exe" Then
                    texto.writeline"<tr><td>El Firewall instalado es Tiny Personal Firewall</td><td><img src='./paloma.jpg' width='24' height='25'></td></tr>"
file.WriteLine "El Firewall instalado es Tiny Personal Firewall"
cuentafire =cuentafire +1
End if

Next
if cuentafire = 0 then
texto.writeline "<tr><td> No esta instalado ningun Firewall</td><td><img src='./tache.jpg' width='24' height='25'></td></tr>"
file.WriteLine "No esta instalado ningun Firewall"
End If
texto.WriteLine "</table>"
```

En la siguiente sección en una primera instancia se declara una variable que después será utilizada para la conversión de bytes a megas y posteriormente en gigas

A través de la clase Win32_OperatingSystem hacemos una numeración de los sistemas operativos instalados en la computadora, ya que esta clase nos proporciona la funcionalidad de listar los sistemas operativos instalados en el equipo. Una vez sumados cada uno de los sistemas operativos son reportados a la tabla

```
On Error Resume Next
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2")
```

Se creó la variable de conexión para WMI

```
Const megas = 1048576
```

Se declara la variable megas para posteriormente usarla en la conversión a megabytes

```
Set instOpSis = objWMIService.InstancesOf("Win32_OperatingSystem")
```

Se hace una colección de sistema operativo para sacar el número de los mismos

```
For Each os In instOpSis
        ruta = os.WindowsDirectory
        nosis = nosis + 1                                   Next
'------------------ Sistema operativo ------------------
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Número de
Sistemas operativos</font></center></strong></font></td</tr>"
texto.WriteLine "</table>"
'-------------------------------------------
file.WriteLine "Número de Sistemas operativos"
```

Se crea una tabla para poner los valores de número de sistema operativo

```
'Numero de Sistemas operativos
texto.Writeline "<table width=100% border=1  bordercolor=#0099CC>"
'texto.writeline"<tr>"
texto.Writeline"<tr><td> Sistema local</td><td>Common
Criteria</td><td>Resultado</td></tr>"
texto.Writeline"<tr><td>" & nosis & "Sistemas operativos</td><td>1 Sistema
operativo</td>"
'----------------------------------------
file.WriteLine "Sistema local"
file.WriteLine nosis & "Sistemas operativos"
file.WriteLine  "Common Criteria"
file.WriteLine  "1 Sistema operativo"
'-----------------------------------
```

Se manda a la tabla el valor real aplicado y el valor recomendado Common Criteria

```
if nosis =1 then
texto.Writeline "<td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
```

Si el valor coincide se manda como resultado la imagen paloma.jpg que es una palomita

```
'----------------------------------------
file.WriteLine "Correcto"
'-----------------------------------
else
texto.Writeline "<td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
```

Si el valor no coincide manda como resultado la imagen tache.jpg

```
'----------------------------------------
file.WriteLine "Incorrecto"
'-----------------------------------
End if
```

En la siguiente sección de código se obtiene la unidad en la cual está instalado el sistema operativo y una vez hecho esto se obtiene el sistema de archivos utilizado en dicha unidad a través de la clase objLogicalDisk.FileSystem la cual es la encargada de identificar el sistema de archivos una unidad de disco dada.

```
unidadsisop = Mid (ruta,1, 2)
```

Se obtiene el system drive o unidad de sistema en la mayoría de los casos C:

```
Set objLogicalDisk = objWMIService.Get ("Win32_LogicalDisk.DeviceId='" & unidadsisop &"')
texto.WriteLine "</table>"
texto.WriteLine "<br>"
texto.WriteLine "<br>"
'-----------------------------------
file.WriteLine ""
'------------------ Sistema de archivos ------------------
```

Se declara la tabla para poner el sistema de archivos

```
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Sistema de archivos </font> </center> </strong> </font></td</tr>"
texto.WriteLine "</table>"
'-----------------------------------------
file.WriteLine "Sistema de archivos"
file.WriteLine ""
'-------------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" & Chr(34) & "bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
texto.Writeline"<tr><td> Sistema local</td><td>Common Criteria</td><td>Resultado</td></tr>"
texto.Writeline"<tr><td>"& objLogicalDisk.FileSystem & " </td><td>NTFS</td>"
```

Imprime el sistema de archivos

```
'-----------------------------------------
file.WriteLine "Sistema local"
file.WriteLine  objLogicalDisk.FileSystem
```

```
file.WriteLine  "Common Criteria"
file.WriteLine  "NTFS"
'-----------------------------------
If objLogicalDisk.FileSystem = "NTFS" Then
texto.Writeline "<td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
```
Si es NTFS manda paloma.jpg
```
'-----------------------------------------
file.WriteLine "Correcto"
'-----------------------------------
else
texto.Writeline "<td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
```
Si no es NTFS manda tache.jpg
```
'-----------------------------------------
file.WriteLine "Incorrecto"
'-----------------------------------
End If
texto.WriteLine "</table>"
texto.WriteLine "<br>"
'-------------------------------
file.WriteLine ""
```

En la siguiente sección de código obtenemos el espacio libre en disco duro a partir de la clase objLogicalDisk.size la cual nos arroja un resultado en bytes una vez hecho esto se hace la conversión a Gigabytes para hacer la comparación con el valor definido por el Common Criteria.

```
'------------------espacio en disco mínimo ------------------
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Espacio en
disco <font> </center> </strong> </font></td</tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Espacio en disco"
file.WriteLine ""
```

```
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) &" bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
texto.Writeline"<tr><td> Sistema local</td><td>Common Criteria
</td><td>Resultado</td></tr>"
texto.Writeline"<tr><td>"& Int ((objLogicalDisk.size / megas)/1024)  & "GB"
& " </td><td>2GB</td>"
'-----------------------------------------
file.WriteLine "Sistema local"
file.WriteLine   Int ((objLogicalDisk.size / megas)/1024)  & "GB"
file.WriteLine  "Common Criteria"
file.WriteLine  "2GB"
'-----------------------------------
```

Se imprime la cantidad en GB de disco duro en el sistema y en Common Criteria

```
Tamano = objLogicalDisk.size / megas
If Tamano >= 2048 Then
texto.Writeline "<td> <img src='./paloma.jpg' width='24'
height='25'></td></tr>"
```

Si es superior a los 2GB manda paloma

```
'-----------------------------------------
file.WriteLine "Correcto"
'-----------------------------------
Else
texto.Writeline "<td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
```

Si es inferior manda tache

```
'-----------------------------------------
file.WriteLine "Incorrecto"
'-----------------------------------
End If
texto.WriteLine "</table>"
'------------------------------
```

En esta sección se evalúa el correcto funcionamiento del hardware, verificando el estado de los controladores del sistema, obteniendo en un inicio una colección de todos los controladores de dispositivo a través de una consulta a la clase

Win32_SystemDriver.Una vez obtenida dicha lista verificamos el estado de cada controlador a través de la propiedad objdriver.Status, el cual para ser verificado como correcto debe tener el valor OK. En caso de que algún controlador no tenga dicho estado se reportará con resultado negativo.

```
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font
color=#FFFFFF>Compatibilidad de hardware</td></tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Compatibilidad de hardware"
file.WriteLine ""
'-----------------------------------
Set coldrivers = objWMIService.ExecQuery("Select * from
Win32_SystemDriver",,48)
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) &"bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
For Each objdriver in coldrivers
if objdriver.Status <> "OK" Then
```

Si el driver tiene un estado diferente a ok

```
texto.writeline"<tr><td>Existe un problema de compatibilidad
referente al driver "& objDriver.Name &" </td><td><img src='./tache.jpg'
width='24' height='25'></td></tr>"
```

Manda un tache al reporte

```
'----------------------------------------
file.WriteLine "Existe un problema de compatibilidad referente al driver " &
objDriver.Name
'-----------------------------------
error= error + 1
end if
Next
if error = 0 then
```

```
                texto.writeline"<tr><td>No existe ningún problema con los
controladores</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
```

En el caso contrario manda paloma

```
'----------------------------------------
file.WriteLine "Correcto"
'-------------------------------------
else
        texto.writeline"<tr><td>Es posible que el desperfecto se corrija con la
reinstalación del controlador asociado</td></tr>"
'----------------------------------------
file.WriteLine "Incorrecto"
'-------------------------------------
end if

texto.WriteLine "</table>"
texto.WriteLine "<br>"
texto.WriteLine "<br>"
'----------------------------------------
```

La siguiente sección evalúa si el equipo analizado cuenta con una contraseña a nivel de hardware, es decir, la contraseña en el BIOS, verificando que el valor de la propiedad objItem.PowerOnPasswordStatus sea 1.

```
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Contraseña de
BIOS </center> </strong> </font> </td></tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Contraseña de BIOS"
file.WriteLine ""
'-------------------------------------
Set objWMIService = GetObject("winmgmts:\\" & strComputer &
"\root\cimv2")
Set colItems = objWMIService.ExecQuery("Select * from
Win32_ComputerSystem",,48)
```

texto.Writeline"<tablewidth="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & " bordercolor="&"#0099CC>"
texto.Writeline"<tr><td> Sistema local</td><td>Common
Criteria</td><td>Resultado</td></tr>"
'texto.Writeline"<tr><td>" & objItem.PowerOnPasswordStatus & "
</td><td>Habilitada</td></tr>"
For Each objItem in colItems

If objItem.PowerOnPasswordStatus =0 Then

0 significa contraseña deshabilitada

texto.writeline"<tr><td>Contraseña
deshabilitada</td><td>Contraseña Habilitada</td><td><img
src='./tache.jpg' width='24' height='25'></td></tr>"

Y si se cumple manda tache al reporte

Else
If objItem.PowerOnPasswordStatus =1 Then

1 significa contraseña habilitada

texto.writeline"<tr><td>Contraseña habilitada</td><td>Contraseña
Habilitada</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"

Y si se cumple manda paloma al reporte

'--
file.WriteLine "Contraseña habilitada"
'-----------------------------------

Else
If objItem.PowerOnPasswordStatus =2 Then

2 significa contraseña deshabilitada

texto.writeline"<tr><td>Contraseña no
implementada</td><td>Contraseña Habilitada</td><td><img
src='./tache.jpg' width='24' height='25'></td></tr>"

Y si se cumple manda tache al reporte

'--
file.WriteLine "Contraseña no implementada"
'-----------------------------------

Else

```
If objItem.PowerOnPasswordStatus =3 Then
```

3 significa desconocido

```
texto.writeline"<tr><td>Estado de contraseña desconocido</td><td>Contraseña Habilitada</td><td><img src='./tache.jpg' width='24' height='25'></td></tr>"
```

Si se cumple manda tache al reporte

```
'----------------------------------------
file.WriteLine "Estado de contraseña desconocido"
'---------------------------------
            End If
          End If
        End if
      End if

Next
texto.WriteLine "</table>"
'----------------------------------------
```

Se hace una conexión a la clase Win32_Network_protocol para saber los protocolos instalados en el sistema, si alguno de ellos es diferente al de Tcpip entonces la configuración es incorrecta, por lo que se muestra la imagen tache, de lo contrario muestra la imagen paloma

```
Set colItems = objWMIService.ExecQuery("Select * from Win32_NetworkProtocol",,48)
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Protocolos de transporte </center> </strong> </font></td</tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Protocolos de transporte"
file.WriteLine ""
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" & Chr(34) & "bordercolor="&"#0099CC>"
```

```
texto.Writeline"<tr><td>  Sistema  local</td><td>Common
Criteria</td><td>Resultado</td></tr>"
vari=""
For Each objItem in colItems
                                                    if  vari<>  objItem.Caption
then
                if objItem.Caption<>"Tcpip" then
                                                                'var=var
                        texto.writeline"<tr><td>"& objItem.Caption &
"</td><td>Tcp/IP</td><td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
'----------------------------------------
file.WriteLine "Protocolos de transporte" & objItem.Caption
file.WriteLine "Incorrecto"
'-------------------------------------
                        Else
                        'var=var &
                        texto.writeline"<tr><td>"& objItem.Caption &
"</td><td>Tcp/IP</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
'----------------------------------------
file.WriteLine "Protocolos de transporte" & objItem.Caption
file.WriteLine "Correcto"
'-------------------------------------
                end if
        end if
        vari=objItem.Caption
Next
'var=var &
texto.WriteLine "</table>"
'----------------------------------------
```

Se hace una conexión a la clase Win32_service para saber los servicios instalados en el sistema, si alguno de ellos es IISADMIN o Index Server entonces la configuración es incorrecta, por lo que se muestra la imagen tache, de lo contrario muestra la imagen paloma

```
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Servicios con
vulnerabilidades</font></td></tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Servicios con vulnerabilidades"
file.WriteLine ""
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
'texto.writeline"<tr>"
Set colServ = objWMIService.ExecQuery("Select * from Win32_Service",,48)

cuentaiis = 0
cuentainser = 0
For each servicio in colServ
If servicio.Name = "IISADMIN" Then
                        cuentaiis = cuentaiis + 1
End if
if  servicio.Name = "Cisvc"  Then
cuentainser = cuentainser + 1
end if
next
if cuentaiis >= 1 then
texto.writeline"<tr><td>El servicio IIS no debería estar
habilitado</td><td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
'----------------------------------------
file.WriteLine "El servicio IIS no debería estar habilitado"
'-----------------------------------
Else
```

```
        texto.writeline"<tr><td>Configuracion correcta,no hay
IIS</td><td><img src='./paloma.jpg' width='24' height='25'></td></tr>"
'-----------------------------------------
file.WriteLine "Configuracion correcta,no hay IIS"
'-----------------------------------
End If

If cuentainser >= 1  Then
        texto.writeline"<tr><td>El Servicio de Index Server no debería estar
habilitado</td><td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
'-----------------------------------------
file.WriteLine "El Servicio de Index Server no debería estar habilitado"
'-----------------------------------
Else
        texto.writeline"<tr><td>Configuracion correcta,no hay Servicio de
Index Server</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
'-----------------------------------------
file.WriteLine "Configuracion correcta,no hay Servicio de Index Server"
'-----------------------------------
End If
texto.writeline "</table>"
'-----------------------------------------
```

Se hace una conexión a la clase Win32_NetworkConnection para obtener los nombres de todos los equipos de la red y determinar así si hay algún nombre duplicado.

```
cuenteq = 0

For Each objItem in colItems
        comparar = objItem.CSName
Next

Set colItems = objWMIService.ExecQuery("Select * from
Win32_NetworkConnection",,48)

For Each objItem in colItems
```

```
        eqred = objItem.LocalName
        matriz = split(eqred,"\",-1,1)
        cort1 = matriz(0)
        if comparar = cort1 Then
        cuenteq = cuenteq + 1
        End If
Next
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Equipos con el
mismo nombre que el de la maquina local
</center></strong></font></td</tr>"
texto.WriteLine "</table>"
'----------------------------------------
file.WriteLine "Equipos con el mismo nombre que el de la maquina local"
file.WriteLine ""
'-------------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
texto.Writeline"<tr><td> Sistema local</td><td>Common
Criteria</td><td>Resultado</td></tr>"

if cuenteq = 1 Then
texto.Writeline"<tr><td>" & cuenteq & "</td><td>1</td><td><img
src='./paloma.jpg' width='24' height='25'></td></tr>"
'----------------------------------------
file.WriteLine cuenteq
file.WriteLine "Correcto"
'-------------------------------------
Else
texto.Writeline"<tr><td>" & cuenteq & "</td><td>1</td><td><img
src='./tache.jpg' width='24' height='25'></td></tr>"
'----------------------------------------
file.WriteLine cuenteq
file.WriteLine "InCorrecto"
'-------------------------------------
End if
texto.WriteLine "</table>"
'----------------------------------------
```

Se hace una conexión a la clase Win32_OperatingSystem para saber si se tiene instalada la última versión de Service Pack, es decir, la 4.

```
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font color=#FFFFFF>Service
Pack</font></td</tr></tr>"
texto.WriteLine "</table>"
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"
'----------------------------------------
file.WriteLine "Service Pack"
file.WriteLine ""
'-----------------------------------
strComputer = "."
        Set objWMIService = GetObject("winmgmts:" _
                & "{impersonationLevel=impersonate}!\\" & strComputer &
"\root\cimv2")

                Set colOperatingSystems = objWMIService.ExecQuery _
                        ("Select * from Win32_OperatingSystem")

                        For Each objOperatingSystem in
colOperatingSystems

                                versionInstalada =
objOperatingSystem.ServicePackMajorVersion _
                                        & "." &
objOperatingSystem.ServicePackMinorVersion

                const versionResiste = "4.0"

                                if versionInstalada = versionResiste Then

                                        texto.writeline"<tr><td>Se tiene el
último Service Pack</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"
'----------------------------------------
file.WriteLine "Se tiene el último Service Pack"
```

```
file.WriteLine "Correcto"
'-----------------------------------
                                    else
                                    texto.Writeline"<tr><td>No se tiene el
ultimo Service Pack</td><td><img src='./tache.jpg' width='24'
height='25'></td></tr>"
'-----------------------------------------
file.WriteLine "No se tiene el ultimo Service Pack"
file.WriteLine "Incorrecto"
'-----------------------------------
                    end if
Next
texto.WriteLine "</table>"
'-----------------------------------------
```

Se hace una conexión a la clase MicrosoftIE_FileVersion para determinar si se encuentra instalada la última versión de Internet Explorer.

```
texto.Writeline "<table width=100% border=1  bgcolor=#0099CC
bordercolor=#0099CC>"
texto.writeline"<tr>"
texto.writeline"<td><center><strong><font          color=#FFFFFF>Internet
Explorer</font></td</tr></tr>"
texto.WriteLine "</table>"
'-----------------------------------------
file.WriteLine "Internet Explorer"
file.WriteLine ""
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" &
Chr(34) & "bordercolor="&"#0099CC>"

strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
   & "{impersonationLevel=impersonate}!\\" & strComputer & _
      "\root\cimv2\Applications\MicrosoftIE")

Set colIESettings = objWMIService.ExecQuery _
   ("Select * from MicrosoftIE_FileVersion")
```

```
texto.writeline "<tr><td>Version de IE: </td><td>" & strIESetting.Version &
"</td>"
'-----------------------------------------
file.WriteLine "Version de IE: "
file.WriteLine  strIESetting.Version
'-------------------------------------

        var15 = strIESetting.Version
                const var10 = "6.0.2900.2180"

    if var15 = var10 Then

        texto.writeline"<tr><td>Se tiene la última versión de Internet
Explorer</td><td><img src='./paloma.jpg' width='24'
height='25'></td></tr>"

'-----------------------------------------
file.WriteLine "Se tiene la última versión de Internet Explorer"
file.WriteLine  "Correcto"
'-------------------------------------
    else
        texto.Writeline"<tr><td>No se tiene  la ultima versión hay que
actualizarlo en_
http://www.microsoft.com/windows/ie/default.mspx</td><td><img
src='./tache.jpg' width='24' height='25'></td></tr>"

'-----------------------------------------
file.WriteLine "No se tiene  la ultima version hay que actualizarlo en
http://www.microsoft.com/windows/ie/default.mspx"
file.WriteLine  "Incorrecto"
'-------------------------------------
    end if
texto.WriteLine "</table>"
'-----------------------------------------
```

Esta función se utiliza para determinar si los valores de las llaves de registro del equipo analizado coinciden con los definidos en el Windows 2000 Security Configuration Guide, que son mostrados a continuación:

Bajo la siguiente ruta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ las llaves siguientes deben tener los valores que se mencionan a continuación:

audstub valor start 4
mnmdd valor start 4
ndistapi valor start 4
ndiswan valor start 4
ndproxy valor start 4
parvdm valor start 4
pptpminiport valor start 4
ptilink valor start 4
rasacd valor start 4
rasl2tp valor start 4
raspti valor start 4
wanarp valor start 4

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ valor EnhancedSecurityLevel 1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\parameters valor RestrictNullSessAccess 1

HKEY_CURRENT_USERS\SOFTWARE\policies\Microsoft\Windows\ControlPanel\Desktop valor BlockSendinputResets 1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security valor WarningLevel 90

Bajo la siguiente ruta: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ las llaves siguientes deben tener los valores que se mencionan a continuación:

DisableIpSourceRouting valor 2
EnableDeadGWdetect valor 0
EnableICMPRedirect valor 0
EnablePMTUDiscovery valor 0
EnableSecurityFilters valor 1
KeepAliveTime valor 300,000
SynAttackProject valor 2
TcpMaxConnectResponseRetransmissions valor 2
TcpMaxConnectRetransmissions valor 3
TcpMaxPortsExhaused valor 5

HKEY_LOCAL_MACHINE\System\CurentControlSet\Services\NetBt\Parameters valor start 1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon valor start 5

```
texto.Writeline "<table width=100% border=1 bgcolor=#0099CC bordercolor=#0099CC>"
texto.Writeline "<tr><td><center><strong><font color=#FFFFFF>Valores de las Llaves de Registro definidas por el Comon Criteria comparadas con las del equipo </strong> </font> </td></tr>"
texto.writeline "</table>"
'--------------------------
file.WriteLine "Valores de las Llaves de Registro definidas por el Common Criteria comparadas con las del equipo"
file.WriteLine ""
'----------------------------------
Const HKEY_LOCAL_MACHINE = &H80000002
const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set StdOut = WScript.StdOut
 Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" &_
 strComputer & "\root\default:StdRegProv")

texto.Writeline "<table width=100% border=1 bgcolor=#0099CC
bordercolor=#0099CC>"
```

texto.Writeline "<tr><td> Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\YSTEM\CurrentControlSet\Services\audstub </td></tr>"
texto.writeline "</table>"
'-------------------------
file.WriteLine "Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\audstub"
file.WriteLine ""
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" & Chr(34) &"bordercolor="&"#0099CC>"
texto.Writeline "<tr><td>Valor local</td>"
texto.Writeline "<td>Valor de Common Criteria</td>"
texto.Writeline "<td>Resultado</td></tr>"

strKeyPath = "SYSTEM\CurrentControlSet\Services\audstub"
Se declara una cadena con la ruta del registro en la cual se encuentra el valor a ser auditado

strValueName = "start"
Se declara una variable que contiene el nombre del valor a ser obtenido

oReg.GetDWORDValue HKEY_LOCAL_MACHINE,strKeyPath,strValueName,dwValue
Se obtiene el valor DWORD antes mencionado de la llave que fue declarada anteriormente

texto.writeline "<tr><td>" & dwValue & "</td><td> 4 </td>"
'-------------------------
file.WriteLine "Valor Local " & dwValue & " Valor Comon Criteria 4"
'-----------------------------------
if dwValue <> "" Then
En el caso de que el valor exista se ejecuta lo siguiente

if dwValue <> 4 Then
Se compara el valor obtenido con el valor common criteria

texto.Writeline "<td><img src='./tache.jpg' ><td></tr>"

Si es diferente manda tache al resultado del reporte

'-------------------------

file.WriteLine "Incorrecto"

'----------------------------------

Else

texto.Writeline "<td><img src='./paloma.jpg' width='24' height='25'><td></tr>"

Si es igual manda paloma

'-------------------------

file.WriteLine "Correcto"

'----------------------------------

End if

Else

texto.Writeline "<td><img src='./tache.jpg' width='24' height='25'><td></tr>"

En el caso de que el primer if falle muestra la imagen de tache

'-------------------------

file.WriteLine "Valor inexistente"

'----------------------------------

End if

texto.writeline "</table>"

La siguiente sección tiene que ver con la plantilla de seguridad aplicada al equipo auditado en comparación con las configuraciones de seguridad definidas en el Windows 2000 Security Configuration Guide. Para la obtención de la plantilla de seguridad aplicada actualmente en el equipo se utiliza la ejecución del siguiente comando en la shell de Windows *secedit /export /cfg*. La plantilla basada en el Windows 2000 Security Configuration Guide simplemente se tiene almacenada para su uso.

'-------------------------------Reporte de Plantillas ------------------------------

texto.Writeline "<table width=100% border=1 bgcolor=#0099CC bordercolor=#0099CC>"

texto.Writeline "<tr><td> Reporte de la Plantilla de Seguridad Aplicada Comparada Con la Common Criteria   </td></tr>"

```
texto.writeline "</table>"
'----------------------------------------
file.WriteLine "Reporte de la Plantilla de Seguridad Aplicada Comparada Con la Common Criteria"
'-----------------------------------
texto.Writeline "<table width="&"100%"&" border="& Chr(34)& "1" & Chr(34) & "bordercolor="&"#0099CC>"
texto.Writeline"<tr><td>Common Criteria</td><td>Sistema local</td><td>Resultado</td></tr>"

Const ParaLectura = 1, ParaEscritura = 2, ParaAnexar = 8
```
El modo en que se abrirán los archivos que se requieran

```
    Set objShell = WScript.CreateObject("WScript.Shell")
```
Crea el objeto de shell

```
     Set oShell= WScript.CreateObject("WScript.Shell")
```
Crea el objeto de shell

```
secedit="cmd.exe /c secedit /export /cfg c:\CommonC\plantillaactual.info"
```
Con este Comando sacamos la plantilla actual aplicada al SO

```
oShell.Run secedit
```
Ejecutamos la línea de secedit

```
                    Wscript.sleep 1000
    strComputer = "."

    Set objWMIService = GetObject("winmgmts:" &_
   "{impersonationLevel=impersonate}!\\" &strComputer & "\root\cimv2")

  Dim fso, f, f2so, f2, i  'Declaración de variables
  Set fso = CreateObject("Scripting.FileSystemObject") 'se crea un objeto con la clase Scripting.FileSystemObject
  Set f = fso.OpenTextFile(".\plantilla_CC.txt", ParaLectura, True)
```
Se abre la plantilla en modo de lectura

```
  Set fi= fso.OpenTextFile(".\plantilla_traduccion.txt", ParaLectura, True)
```
Se abre la plantilla en modo de lectura

Do Until f.AtEndOfStream
Ciclo Until donde se cumple hasta la última línea

campo1 = f.ReadLine()
Lee línea por línea y el valor lo guarda en una variable

descripcion=fi.ReadLine()
Set fauxi = fso.OpenTextFile(".\tr.txt",2,True)
Se abre el archivo tr para poder escribir en el la línea que se captura en campo1

fauxi.writeLine(campo1)
Se escribe en el archivo la línea que se captura en campo1

fauxi.close()
Se cierra el archivo
Se aplica el comando sed al archivo, ya que como muestra caracteres extraños no se podía leer para comparar un archivo con otro, por lo que se cambian \ por doble\\por \\% y otros para poder hacer del archivo un formato uniforme para todas la líneas y así poder ser comparado

strCommandi ="C:\unix\bin\sed.exe -e s/\\/\\\\/g -e s/\" & chr(34) & "/\\\\\" & chr(34) & "/g -e s/\%/\\\%/g -e s//*/g .\tr.txt"*

Set objExecObject = objShell.Exec(strCommandi)
Se ejecuta el comando anterior del sed

var2= objExecObject.StdOut.ReadLine()
El resultado lo guarda en la variable
Se aplica el comando Grep, que es una herramienta de terceros, para poder buscar la expresión regular, que en este caso es la de var2 que es la línea que anteriormente fue formateada dentro de actual.info sin importar si son mayúsculas o minúsculas

strCommand = "C:\grep.exe -i " & chr(34) & var2 & chr(34) & " .\plantillaactual.info"

Set objExecObject = objShell.Exec(strCommand)

var1= objExecObject.StdOut.ReadAll()

Set faux = fso.OpenTextFile(".\tr1.txt",2,True)

Se abre el archivo tr1

faux.writeLine(var1)

Se agrega la línea que contiene la variable var1

faux.close()

Se cierra el archivo

Se aplica otro sed para nuevamente dejar uniforme la plantilla cambiando algunos caracteres dentro de tr1 para poder llevar cabo la comparación

strCommand ="C:\unix\bin\sed.exe -e s/\" & chr(34) & "/\&/g .\tr1.txt"

Set objExecObject = objShell.Exec(strCommand)

var2= objExecObject.StdOut.ReadLine()

Set fauxi = fso.OpenTextFile(".\tr.txt",2,True)

fauxi.writeLine(campo1)

fauxi.close()

Se aplica otro sed para nuevamente dejar uniforme la plantilla cambiando algunos caracteres como"" por & dentro de tr que es la variable campo1 para poder llevar cabo la comparación entre cadenas de cada plantilla

strCommandi ="C:\unix\bin\sed.exe -e s/\" & chr(34) & "/\&/g .\tr.txt"

Set objExecObject = objShell.Exec(strCommandi)

varx= objExecObject.StdOut.ReadLine()

Set fauxi = fso.OpenTextFile(".\tr.txt",2,True)

fauxi.writeLine(varx)

fauxi.close()

Se aplica otro sed para nuevamente dejar uniforme la plantilla cambiado algunos caracteres como "" por & dentro de tr que es la variable campo1 para poder llevar cabo la comparación entre cadenas de cada plantilla

strCommandi ="C:\unix\bin\sed.exe -e s/\" & chr(34) & "/\&/g .\tr.txt"
Set objExecObject = objShell.Exec(strCommandi)

varx= objExecObject.StdOut.ReadLine()

Ya que los dos archivos están de manera uniforme se procede a hacer la comparación de la cadena

if Ucase(varx)<>Ucase(var2) then

En el caso de que las variables no sean iguales se aplica el if

if var2<>"" then

Si var2 diferente de nada entonces

texto.Writeline"<tr><td bgcolor=#0099CC><img src='./TSTAPP.ICO'>" & descripcion & "</td></tr>"

'Imprime la descripción(traducción)

'--
file.WriteLine descripcion
'-------------------------------------

texto.writeline "<tr><td><textarea name=textarea cols=50>" & varx & "</textarea></td><td><textarea name=textarea cols=50>" & var2 & "</textarea></td><td><img src='./tache.jpg'></td></tr>" & vbCrlf

Imprime las cadenas no son iguales e imprime las cadenas

'--
file.WriteLine varx

```
file.WriteLine var2
file.WriteLine "No Coincide"
'-------------------------------------
                                else
            texto.writeline "<tr><td bgcolor=#0099CC><font
color=#FFFFFF>" & descripcion & "</font></td></tr>"
'-----------------------------------------
file.WriteLine descripcion
'-------------------------------------
                                texto.writeline "<tr><td><textarea name=textarea
cols=50>" & varx & "</textarea></td><td>No esta definida</td><td><img
src='./tache.jpg'></td></tr>" & vbCrlf
```

Imprime que no está definido

```
'-----------------------------------------
file.WriteLine varx
file.WriteLine "No definido"
file.WriteLine "No Coincide"
'-------------------------------------
                                end if
                        Else
                        texto.writeline "<tr><td bgcolor=#0099CC><font
color=#FFFFFF>" & descripcion & "</font></td></tr>"
'-----------------------------------------
file.WriteLine descripcion
'-------------------------------------
                        texto.writeline "<tr><td><textarea name=textarea
cols=50>" & varx & "</textarea></td><td><textarea name=textarea
cols=50>" & var2 & "</textarea></td><td><img
src='./paloma.jpg'></td></tr>" & vbCrlf
```

Imprime las cadenas son iguales e imprime las cadena

```
'-----------------------------------------
file.WriteLine varx
file.WriteLine var2
file.WriteLine "Si Coincide"
file.WriteLine ""
file.WriteLine ""
```

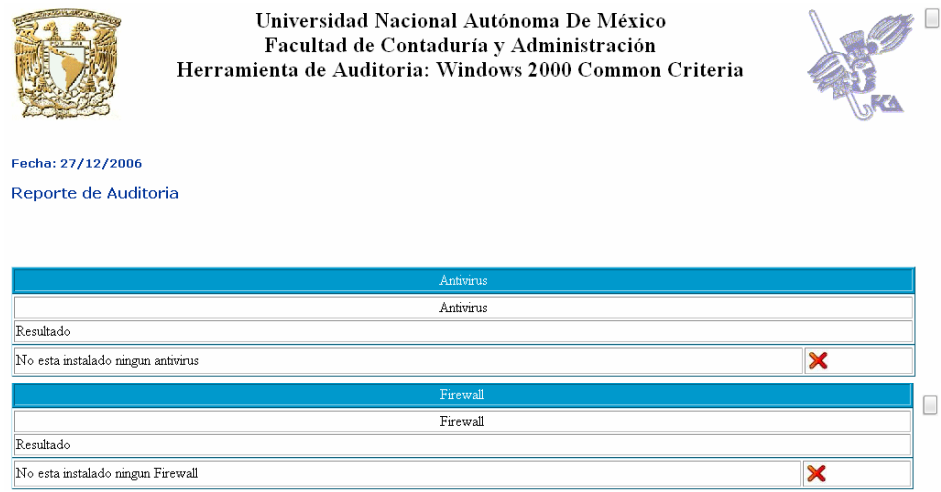
```
'-----------------------------------
                    end if  ' Fin del if
            loop 'Fin del ciclo Do until

texto.WriteLine "</table>"
  f.close  'Se cierra el archivo de traducción
  fi.close ' Se cierra la plantilla  de Common Criteria

wscript.echo "Reporte generado con éxito"
texto  a pantalla
texto.writeline "</table>"
texto.writeline"</body>"
texto.writeline"</html>
```

Si el reporte se realizó de manera exitosa, se envía a pantalla el siguiente mensaje “Reporte generado con éxito”

CAPITULO 4. IMPLEMENTACION

La herramienta desarrollada es una aplicación que realiza un conjunto de verificaciones de las configuraciones de seguridad definidas en el Windows 2000 Security Configuration Guide.

En la primera parte se efectúa una verificación del antivirus, ésta realiza una búsqueda cotejando con una lista de los antivirus más conocidos dando como resultado aprobatorio si es que existe un antivirus instalado en el sistema. Así mismo la segunda sección verifica que esté instalado un firewall de host.



Universidad Nacional Autónoma De México
Facultad de Contaduría y Administración
Herramienta de Auditoria: Windows 2000 Common Criteria

Fecha: 27/12/2006

Reporte de Auditoria

Antivirus	
Antivirus	
Resultado	
No esta instalado ningun antivirus	✗

Firewall	
Firewall	
Resultado	
No esta instalado ningun Firewall	✗

La recomendación de Windows en relación los sistemas operativos instalados en el equipo es que sólo esté instalado Windows esto porque en otros sistemas operativos, principalmente en sistemas operativos tipo UNIX, ocasionalmente se incluyen herramientas para tener acceso a los archivos de Windows.

Número de Sistemas operativos		
Sistema local	Common Criteria	Resultado
1Sistemas operativos	1 Sistema operativo	✔

En cuanto al sistema de archivos que deberá utilizarse es NTFS, principalmente por las nuevas características de seguridad que se implementan en él.

Sistema de archivos		
Sistema local	Common Criteria	Resultado
NTFS	NTFS	✔

El espacio libre con el que deberá contar como mínimo un equipo con sistema operativo Windows 2000 es de 2 GB, con el fin de evitar posibles problemas en el uso del Disco Duro y garantizar la disponibilidad del equipo.

Espacio en disco		
Sistema local	Common Criteria	Resultado
7GB	2GB	✔

En cuanto a la compatibilidad del hardware no deberá existir ningún problema con los controladores de dispositivos que se encuentren en el sistema para problemas de disponibilidad del sistema.

Compatibilidad de hardware	
No existe ningún problema con los controladores	✔

El sistema deberá contar con una contraseña a nivel de hardware, es decir en la BIOS para dificultar el acceso no autorizado.

Contraseña de BIOS		
Sistema local	Common Criteria	Resultado
Contraseña deshabilitada	Contraseña Habilitada	✗

Dentro de los protocolos de red es recomendable que sólo se tenga habilitado TCP/IP, debido a las múltiples vulnerabilidades detectadas en los demás protocolos de transporte disponibles.

Protocolos de transporte		
Sistema local	Common Criteria	Resultado
Tcpip	Tcp/IP	✓
RSVP	Tcp/IP	✗
NetBIOS	Tcp/IP	✗

Existen servicios que han comprobado ser más propensos a vulnerarse que otros, en el caso de Windows, IIS ha resultado tener severos problemas de seguridad y por lo tanto si no está destinado a ser un equipo que provea el servicio de Web el servicio de IIS deberá ser deshabilitado al igual que el servicio de Index Server.

Servicios con vulnerabilidades	
El servicio IIS no debería estar habilitado	✗
Configuracion correcta,no hay Servicio de Index Server	✓

En el entorno de trabajo en una red es necesario tomar la precaución de evitar la duplicidad de nombres en la red.

Equipos con el mismo nombre que el de la maquina local		
Sistema local	Common Criteria	Resultado
1	1	✓

Esta herramienta verifica que se tenga instalado el último Service Pack liberado por Microsoft, puesto que en estos paquetes se contiene las actualizaciones de seguridad más actuales siendo estos Service Pack incrementales, es decir, el último Service Pack contendrá también las actualizaciones de los anteriores.

Service Pack	
No se tiene el ultimo Service Pack	✗

Internet Explorer ha comprobado ser una aplicación muy susceptible a errores de seguridad por lo tanto la herramienta verificará que se tenga instalada la versión más reciente.

Internet Explorer	
No se tiene la ultima version hay que actualizarlo en_ http://www.microsoft.com/windows/ie/default.mspx	✗

Es necesario deshabilitar todos los dispositivos innecesarios, por ello, la herramienta desarrollada comprueba que en el registro el valor start sea 4 en las llaves correspondientes al dispositivo.

Valores de las Llaves de Registro definidas por el Comon Criteria comparadas con las del equipo		
Comprobación del valor start de la llave SHKEY_LOCAL_MACHINE\YSTEM\CurrentControlSet\Services\audstub		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mnmdd		
Valor local	Valor de Common Criteria	Resultado
1	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ndistapi		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ndiswan		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ndproxy		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\parvdm		
Valor local	Valor de Common Criteria	Resultado
2	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pptpminiport		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ptilink		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rasacd		
Valor local	Valor de Common Criteria	Resultado
1	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rasl2tp		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\raspti		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wanarp		
Valor local	Valor de Common Criteria	Resultado
3	4	✗

El valor EnhancedSecurityLevel de la llave de registro HKeyLocalMachine\SYSTEM\CurrentControlSet\Control\Session Manager puesta en 1 habilita la Protección de los objetos del kernel.

Comprobación del valor EnhancedSecurityLevel de la llave SYSTEM\CurrentControlSet\Control\Session Manager		
Valor local	Valor de Common Criteria	Resultado
	1	

Esta modificación en el registro previene que usuarios con sesiones nulas, es decir, sin autenticarse, tengan acceso a recursos compartidos en el equipo.

Comprobación del valor RestrictNullSessAcces de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\parameters		
Valor local	Valor de Common Criteria	Resultado
	1	

Establecer el valor BlockSendInputResets de la llave del registro HKeyLocalMachine\SYSTEM\CurrentControlSet\ControlPanel\Desktop habilita el bloqueo de pantalla protegido con la contraseña del usuario toda vez que se ejecute el protector de pantalla.

Comprobación del valor BlockSendinputResets de la llave HKEY_CURRENT_USERS\SOFTWARE\policies\microsoft\windows\ControlPanel\Desktop		
Valor local	Valor de Common Criteria	Resultado
	1	

El valor de esta llave se refiere al porcentaje de llenado de las bitácoras en el cual se alertará al usuario Administrador.

Comprobación del valor WarningLevel de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security		
Valor local	Valor de Common Criteria	Resultado
	90	

Los valores definidos en el Windows 2000 Security Configuration Guide con respecto al protocolo TCP/IP ayudan a incrementar la resistencia de la pila TCP/IP Windows 2000 en contra de ataques de negación de servicios.

Comprobación del valor DisableIpSourceRouting de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	2	✗

Comprobación del valor EnableDeadGWdetect de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	0	✗

Comprobación del valor EnableICMPRedirect de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
1	0	✗

Comprobación del valor EnablePMTUDiscovery de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	0	✗

Comprobación del valor EnableSecurityFilters de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
0	1	✗

Comprobación del valor KeepAliveTime de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	300000	✗

Comprobación del valor SynAttackProject de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	2	✗

Comprobación del valor TcpMaxConnectResponseRetransmissions de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	2	✗

Comprobación del valor TcpMaxConnectRetransmissions HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	3	✗

Comprobación del valor TcpMaxPortsExhaused de la llave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters		
Valor local	Valor de Common Criteria	Resultado
	5	✗

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\System\CurentControlSet\Services\NetBt\Parameters		
Valor local	Valor de Common Criteria	Resultado
	1	✗

Existe un periodo de gracia permitido para hacer un movimiento antes de que el screen saver sea bloqueado, siendo el default de 5 segundos, pero es recomendable poner este valor en 0.

Comprobación del valor start de la llave HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon		
Valor local	Valor de Common Criteria	Resultado
	0	✗

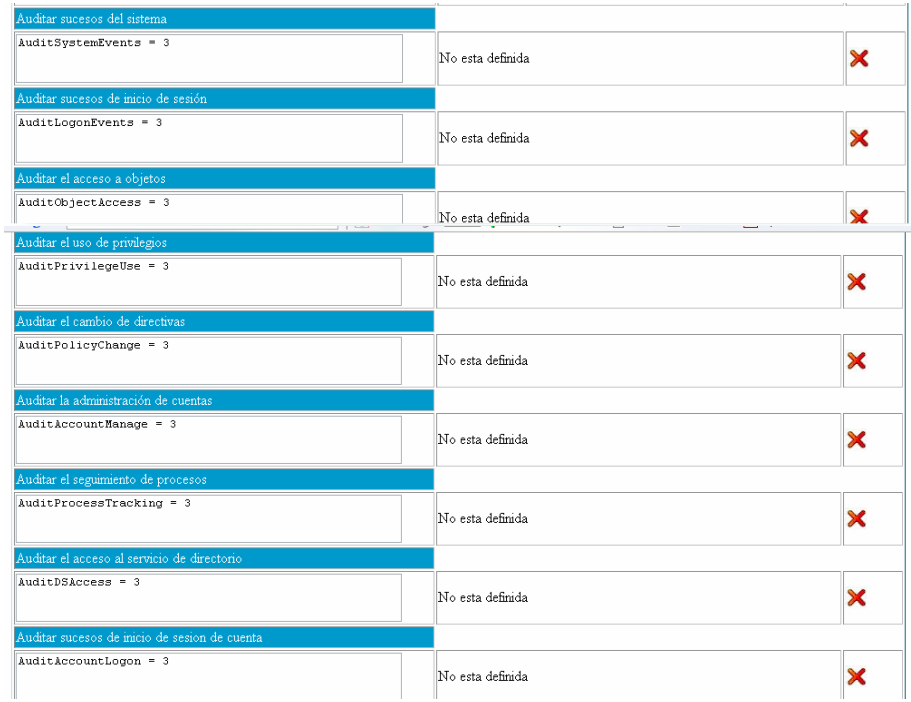
Configuraciones de seguridad de las contraseñas:
Se verifican las características de las contraseñas de usuario definiendo su longitud, complejidad entre otras características.

Reporte de la Plantilla de Seguridad Aplicada Comparada Con la Common Criteria		
Common Criteria	Sistema local	Resultado
Duración mínima de la contraseña		
MinimumPasswordAge = 2	No esta definida	✗
Duración máxima de la contraseña		
MaximumPasswordAge = 42	MaximumPasswordAge = 42	✓
Longitud mínima de la contraseña		
MinimumPasswordLength = 8	No esta definida	✗
Complejidad de la contraseña		
PasswordComplexity = 1	No esta definida	✗
Forzar el historial de contraseñas		
PasswordHistorySize = 24	No esta definida	✗

Configuraciones de bloqueo de cuentas:
Se definen características de inicio de sesión referentes al bloqueo del mismo, en cuanto a los intentos de introducción de credenciales y el tiempo que éste permanecerá bloqueado.

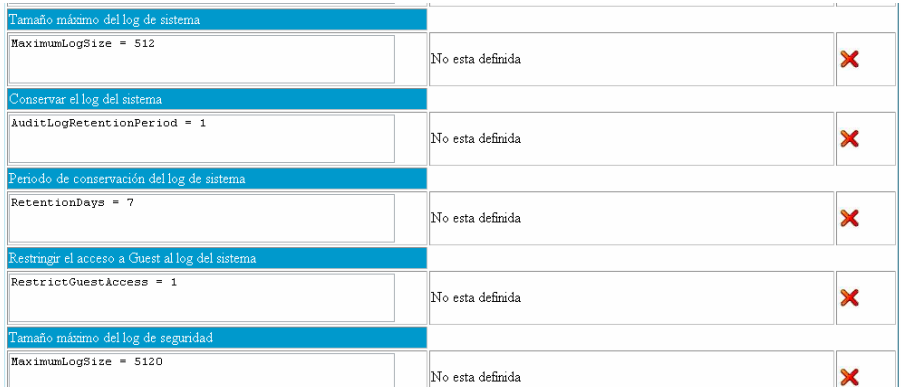
Umbral de bloqueos de cuenta		
LockoutBadCount = 5	No esta definida	✗
Restablecer el bloqueo de cuentas		
ResetLockoutCount = 30	No esta definida	✗
Duración del bloqueo de cuenta		
LockoutDuration = -1	No esta definida	✗
Forzar la salida de sesión cuando el tiempo haya expirado		
ForceLogoffWhenHourExpire = 1	No esta definida	✗

Configuraciones de Auditoría:
Determina cuáles eventos de seguridad son registrados en las bitácoras del equipo, por ejemplo intentos exitosos, fallidos o ambos

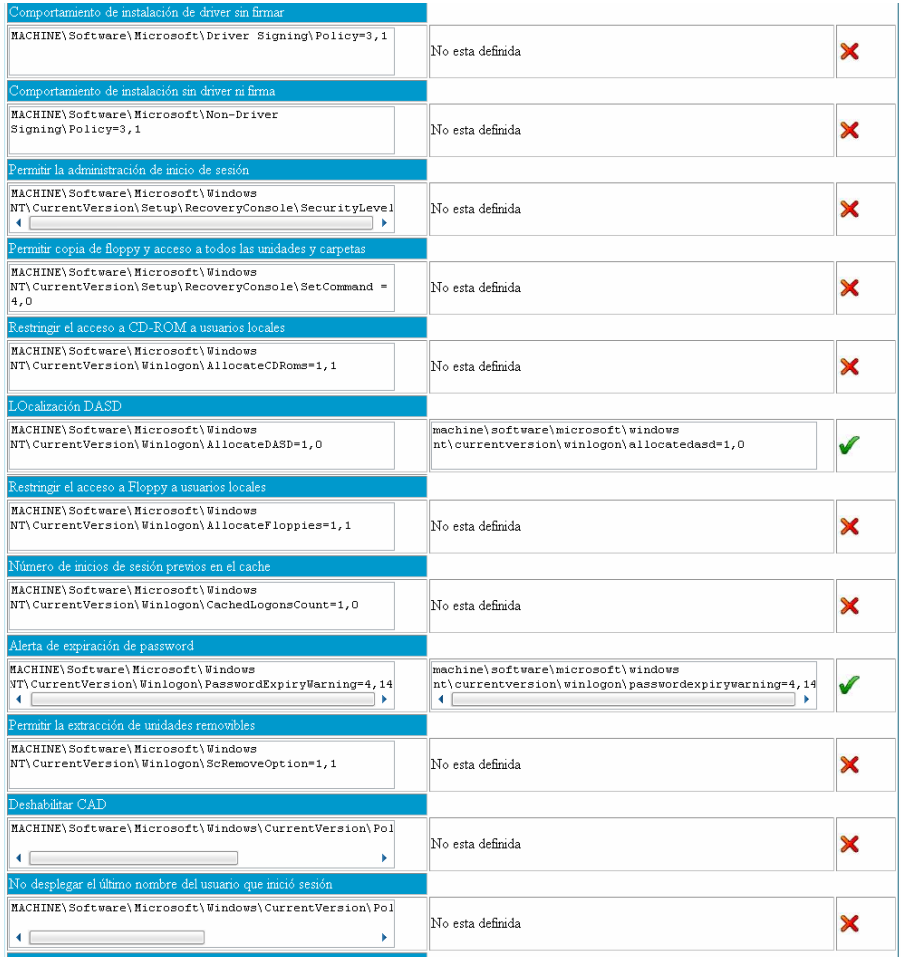


Configuraciones de Kerberos:
Se configuran las características de Kerberos que es el principal método de autenticación en un Dominio con Active Directory.

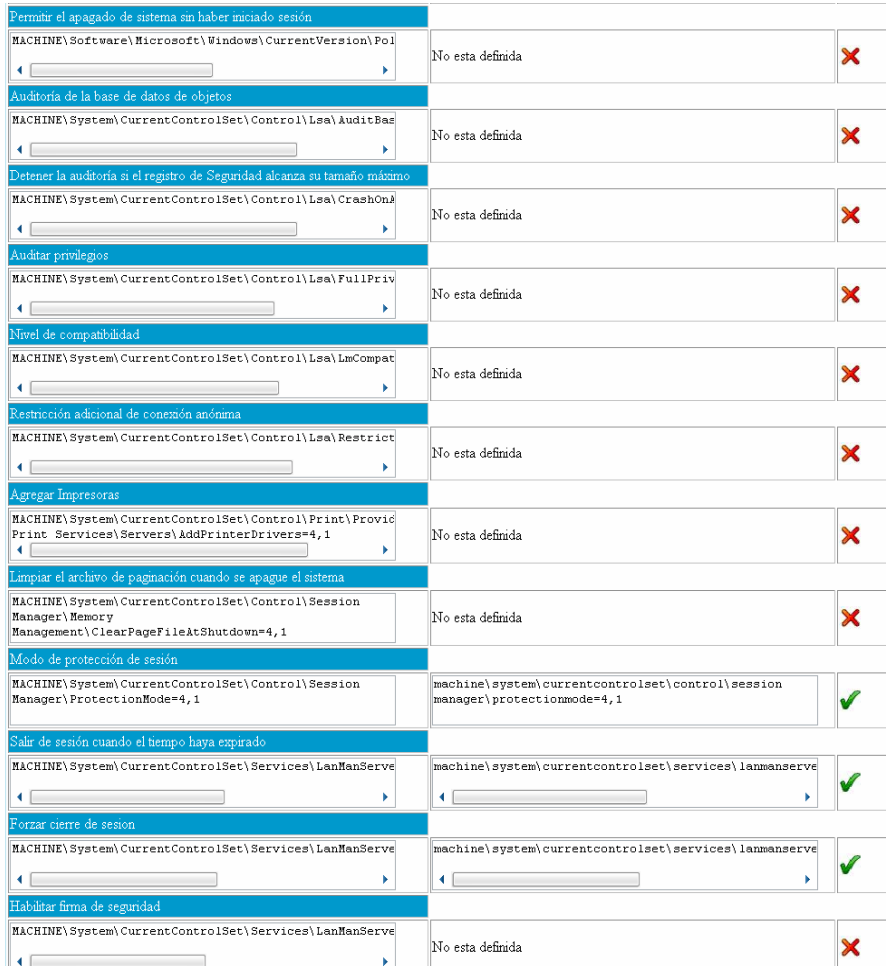
Características de la administración de bitácoras:
En esta se sección se configuran las características del manejo de las bitácoras de seguridad del sistema manipulando tamaños y control de acceso.



Opciones de seguridad:
En esta sección es donde se auditan las principales características de seguridad del equipo tales como firma digital de los datos, nombres de cuentas de administrador e invitado, acceso a dispositivos de almacenamiento extraíbles e instalación de drivers.



Comportamiento de instalación de driver sin firmar		
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1	No esta definida	✗
Comportamiento de instalación sin driver ni firma		
MACHINE\Software\Microsoft\Non-Driver Signing\Policy=3,1	No esta definida	✗
Permitir la administración de inicio de sesión		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel	No esta definida	✗
Permitir copia de floppy y acceso a todos las unidades y carpetas		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand = 4,0	No esta definida	✗
Restringir el acceso a CD-ROM a usuarios locales		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,1	No esta definida	✗
LOcalización DASD		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,0	machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0	✓
Restringir el acceso a Floppy a usuarios locales		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,1	No esta definida	✗
Número de inicios de sesión previos en el cache		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,0	No esta definida	✗
Alerta de expiración de password		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14	machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14	✓
Permitir la extracción de unidades removibles		
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,1	No esta definida	✗
Deshabilitar CAD		
MACHINE\Software\Microsoft\Windows\CurrentVersion\Pol	No esta definida	✗
No desplegar el último nombre del usuario que inició sesión		
MACHINE\Software\Microsoft\Windows\CurrentVersion\Pol	No esta definida	✗



Permitir el apagado de sistema sin haber iniciado sesión		
MACHINE\Software\Microsoft\Windows\CurrentVersion\Pol	No esta definida	✗
Auditoría de la base de datos de objetos		
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBas	No esta definida	✗
Detener la auditoría si el registro de Seguridad alcanza su tamaño máximo		
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnA	No esta definida	✗
Auditar privilegios		
MACHINE\System\CurrentControlSet\Control\Lsa\FullPriv	No esta definida	✗
Nivel de compatibilidad		
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompat	No esta definida	✗
Restricción adicional de conexión anónima		
MACHINE\System\CurrentControlSet\Control\Lsa\Restrict	No esta definida	✗
Agregar Impresoras		
MACHINE\System\CurrentControlSet\Control\Print\Provid Print Services\Servers\AddPrinterDrivers=4,1	No esta definida	✗
Limpiar el archivo de paginación cuando se apague el sistema		
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1	No esta definida	✗
Modo de protección de sesión		
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode=4,1	machine\system\currentcontrolset\control\session manager\protectionmode=4,1	✓
Salir de sesión cuando el tiempo haya expirado		
MACHINE\System\CurrentControlSet\Services\LanManServe	machine\system\currentcontrolset\services\lanmanserve	✓
Forzar cierre de sesion		
MACHINE\System\CurrentControlSet\Services\LanManServe	machine\system\currentcontrolset\services\lanmanserve	✓
Habilitar firma de seguridad		
MACHINE\System\CurrentControlSet\Services\LanManServe	No esta definida	✗

Requerir firma de seguridad		
\LanManServer\Parameters\RequireSecuritySignature=4,0	\lanmanserver\parameters\requiresecuritysignature=4,0	✔
Habilitar contraseña en texto plano		
manWorkstation\Parameters\EnablePlainTextPassword=4,0	manworkstation\parameters\enableplaintextpassword=4,0	✔
Requerir firma de seguridad		
manWorkstation\Parameters\EnableSecuritySignature=4,1	manworkstation\parameters\enablesecuritysignature=4,1	✔
Requerir firma de seguridad en estacion de trabajo		
anWorkstation\Parameters\RequireSecuritySignature=4,0	anworkstation\parameters\requiresecuritysignature=4,0	✔
Deshabilitar el cambio de password		
ervices\Netlogon\Parameters\DisablePasswordChange=4,0	ervices\netlogon\parameters\disablepasswordchange=4,0	✔
Canal seguro encriptar digitalmente o firmar datos de canal seguro		
et\Services\Netlogon\Parameters\RequireSignOrSeal=4,0	et\services\netlogon\parameters\requiresignorseal=4,0	✔
Canal seguro encriptar digitalmente o firmar datos de canal seguro		
et\Services\Netlogon\Parameters\RequireSignOrSeal=4,0	et\services\netlogon\parameters\requiresignorseal=4,0	✔
Canal seguro requiere llave de sesión fuerte		
Set\Services\Netlogon\Parameters\RequireStrongKey=4,0	set\services\netlogon\parameters\requirestrongkey=4,0	✔
Canal seguro firmar digitalmente datos de canal seguro		
et\Services\Netlogon\Parameters\SignSecureChannel=4,0	No esta definida	✘

CONCLUSIONES.

Con base en los resultados de la investigación y realización de este proyecto se concluye lo siguiente:

La auditoría en Informática es una parte esencial para la correcta operación y funcionamiento de los sistemas de información de una organización, en el particular caso de estudio de este proyecto se tomó en consideración la parte correspondiente a la seguridad del Sistema Operativo Windows 2000, tomando como base el documento Windows 2000 Security Configuration Guide para la elaboración de esta herramienta, la cual audita los controles especificados en dicho documento.

La realización del proyecto se concluyó con los siguientes resultados:

Se logró la realización de una herramienta de auditoría que auxiliará al administrador de sistemas operativos Windows 2000 en sus diferentes versiones a realizar una comprobación de los valores definidos por el Windows 2000 Security Configuration Guide, generando reportes en formatos html y txt para su mayor entendimiento y análisis posterior y si así se decide hacer las correcciones de las deficiencias detectadas en los mencionados reportes.

La herramienta realizada permite generar información acerca de las actualizaciones de seguridad aplicadas a cada equipo (Service Pack y HotFixes), obteniene información sobre si se tiene instalado algún antivirus y firewall y finalmente obtiene información relevante acerca de la plataforma de hardware del sistema, como lo es el espacio disponible en disco duro, sistema de archivos, contraseña en el BIOS, compatibilidad de hardware, utilizando tecnologías de scripts y no una aplicación de escritorio, dotando a

la herramienta de portabilidad para cualquier sistema bajo plataforma NTFS.

Por lo tanto, los objetivos planteados al inicio de este proyecto fueron cubiertos y satisfacen las necesidades actuales de Auditoría para los equipos con sistema operativo Windows 2000 Professional, Windows 2000 Server y Windows 2000 Advanced Server dejando las puertas abiertas para su futuro desarrollo y brindar un mayor alcance a la herramienta.

-

GLOSARIO

Activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Ataque de denegación de Servicio: Tipo de ataque informático consistente en conseguir que un equipo o servicio no pueda ser utilizado de forma normal, quedando bloqueado total o parcialmente.

Ataque de diccionario: Un ataque del diccionario consiste en intentar cada palabra en el diccionario como contraseña.

Ataque de fuerza bruta: Forma de recuperar un password probando todas las combinaciones posibles de caracteres hasta encontrar aquella que permite el acceso.

Antivirus: Conjunto de programas de utilería que buscan y erradican un amplio aspecto de problemas, como virus, caballos de Troya y gusanos.

Bit: Es la unidad más pequeña de información. Puede tomar el valor de 0 o 1.

Bitácoras: Archivos generados por diversas aplicaciones para almacenar la actividad de los mismos.

Buffer overflow: Un desbordamiento de buffer ocurre cuando los datos que se escriben en un buffer corrompen aquellos datos en direcciones de memoria adyacentes a los destinados para el buffer, debido a una falta de validación de los datos de entrada. Esto se da comúnmente al copiar cadenas de caracteres de un buffer a otro.

Caballo de Troya: Programa de cómputo que aparenta realizar una función mientras que en realidad hace algo más. Técnicamente, no es lo mismo que un virus, porque a diferencia de éste, no está diseñado para copiarse.

Cifrado: El proceso de codificar datos para prevenir un acceso no autorizado especialmente durante la transmisión, el cifrado se basa usualmente en una clave que es esencial para decodificar

Criptografía: Uso de códigos para convertir datos de modo que sólo un receptor específico será capaz de leerlos, utilizando una clave.

Cliente-servidor: Sistema mediante el cual las aplicaciones quedan divididas en dos partes: la parte residente en la computadora del usuario (el cliente); y la parte residente en una computadora central compartida (el servidor). El cliente se encarga de hacer la interfaz con el usuario. El servidor se encarga de gestionar las aplicaciones, información y periféricos entre los distintos clientes.

Controlador: Un dispositivo hardware o programa que controla o regula otro dispositivo.

Dirección IP: Una dirección IP identifica a una computadora en una red TCP/IP. Está compuesta por una serie de números separada en cuatro secciones por puntos. El número de una

sección no debe exceder a 255. En representación binaria cada sección de una dirección IP requiere 8 bits, de modo que toda la dirección requiere 32 bits.

Dominio: Una colección de computadoras que comparten una base de datos de dominio común y políticas de seguridad. Cada dominio tiene un nombre único**.**

Exploit: Programa informático malicioso que es usado normalmente para explotar una vulnerabilidad en un sistema y acceder a él.

Firewall: Dispositivo de seguridad, que puede ser hardware o software, que controla los accesos a una red local o computadora individual desde el exterior. Mediante el proceso de filtrado examina los paquetes de datos y determina si le permite o no el acceso.

Gusano: A diferencia de un virus, un gusano está diseñado para pasar de una computadora a otra, casi todos los gusanos aprovechan las redes de comunicación (sobre todo Internet), para viajar en los paquetes de correo electrónico y TCP/IP, pasando de una computadora a otra.

Hardening: Proceso mediante el cual se revisa toda la configuración de un equipo para aumentar el nivel de seguridad y hacer más difícil para un atacante poder ganar acceso al sistema.

Hash: Funciòn o método para generar llaves que representen de manera casi unívoca a un documento, registro, archivo, etc.

Host: Servidor que proporciona acceso y servicios a otras computadoras de la red.

Hotfix: Paquete que puede incluir varios archivos y que sirve para resolver un bug específico dentro de una aplicación.

Index Server: Servicio encargado de indizar contenidos y propiedades de archivos localos y/o remotos. Se encarga de mantenerlos en un índice (un catálogo) para que puedan ser accedidos más rápidamente.

Informática: Campo que se encarga del estudio y aplicación práctica de la tecnología, métodos y técnicas relacionados con las computadoras y el manejo de la información por medio electrónicos, orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones fluya de manera oportuna, veraz y confiable.

Intruso: Usuario o programa no autorizado, generalmente con intenciones negativas, en una computadora o red de computadoras.

Inundación SYN (SYN flood): Método de abrumar a un equipo host en una red, mediante el envío de un gran volumen de paquetes de sincronización (SYN), solicitando una conexión, pero nunca respondiendo los paquetes de confirmación devueltos por el host.

MAC: Acrónimo de Media Access Control. En las especificaciones de la IEEE 802.x la capa más baja de las dos subcapas que forman la capa de enlace de datos del modelo OSI. La subcapa MAC gestiona el acceso a la red física, delimita las tramas y se encarga del control de errores.

Malware: Cualquier programa o documento informático que puede causar, directa o indirectamente, un perjuicio al uso normal de una computadora.

Netbios: (Netwok Basic Input/Output System): Es una especificación para enlazar el sistema operativo de red con hardware específico.

PKI (Public Key Infrastructure): Una infraestructura de clave pública (PKI) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.El término PKI se utiliza para referirse a la autoridad certificadora y al resto de componentes.

Proceso: Instancia de un programa en memoria principal.

Protocolo: Conjunto de reglas estándares diseñados para permitir a las computadoras comunicarse con otras e intercambiar información con el mínimo error posible.

Puerto: Es una interfaz para comunicarse con un programa a través de una red. Los puertos de red suelen ser numerados.

Race condition: Error que se produce en programas que no han sido diseñados adecuadamente para su ejecución simultánea con otros. Un ejemplo típico es el interbloqueo que se produce cuando dos procesos están esperando a que el otro realice una acción. Como los dos están esperando, ninguno llega a realizar la acción que el otro espera.

Seguridad en Informática: Rama de la computación la cual consiste de un conjunto de prácticas destinadas a mantener la integridad, confidencialidad y disponibilidad de los datos en un sistema de información así como mitigar los riesgos de seguridad

asociados a la utilización cotidiana de infraestructura de cómputo y telecomunicaciones.
En un sistema se evalúa el nivel de seguridad por la dificultad que éste presente para afectar alguno de los tres puntos anteriores.

Sistema de archivos: Sistema de organización de directorios y archivos, especialmente en lo referente a su integración en el sistema operativo del disco.

The Orange Book: Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD. Un estándar publicado por el gobierno de los Estados Unidos para clasificar la seguridad de los sistemas de Cómputo en cuatro divisiones jerárquicas (A, B, C y D) para satisfacer el nivel de confianza requerido por dicho gobierno para una aplicación particular.

Unicode: Un estándar de carácter de codificación de caracteres de 16 bits desarrollado por el Consorcio Unicode entre 1988 y 1991 utilizando dos bytes para representar cada carácter, Unicode permite que casi todos los lenguajes escritos y alfabetos del mundo se representen utilizando un único conjunto de caracteres.

Virus: Un virus de computadora es un conjunto de instrucciones de programa que se adjuntan a un archivo, se reproducen por sí solos y se dispersan a otros archivos. Tienen la capacidad de corromper archivos, destruir datos o modificar de otra manera la operación de una computadora.

REFERENCIAS

Bibliográfica

Willis Hill, Watts David, Straham Tillman **Windows 2000 System Administration Handbook.** Prentice Hall, Estados Unidos de América, 2000.

García Marín David, Jiménez Pérez Hugo. **Windows 2000 Server Activo.** Prentice Hall Hispanoamericana, México, 2000, 710 p.

Pérez López César **Domine Microsoft Windows 2000 Professional.** AlfaOmega, México, 2001, 666 p.

Schmidt Jeff **Guía Avanzada Seguridad en Microsoft Windows 2000.** Prentice Hall, Madrid, 2001, 802 p.

Spencer Kenneth, Goncalves Marcus **Guía Avanzada Microsoft Windows 2000 Server Administración y Control.** Prentice Hall, Madrid, 2000, 364 p. trad. José Ignacio Sánchez García.

Echenique García, José Antonio. **Auditoría en informática.** McGraw-Hill, 2da. Edición, México, 2001, 300 p.
Thomas A.J., Douglas I.J. **Auditoría Informática.** Parainfo, 2da Edición, Madrid, 1988, 214 p.

Hernández Hernández Enrique. **Auditoría en Informática: Un enfoque metodológico y práctico.** Compañía Editorial Continental, México, 1996, 315 p.

Honeyman, Jeffrey **Windows 2000: scripting Windows 2000** Berkeley, California, McGraw-Hill, 2000, 444 p.

Lissoir, Alain **Leveraging WMI scripting : using Windows Management Instrumentation to solve Windows management problems** Boston : Digital, 2003, 918 p.

Horton Mike, Mugge Clinton. **Claves Hackers** Mc Graw Hill, España 2004, 288p. trad. Rodríguez Vega Jorge.

Profesor Eduardo Estrada Martínez, **Apuntes de Auditoría en informática**, Facultad de Contaduría y Administración, Febrero del 2005.

Electrónica

Windows 2000 Security Configuration Guide
http://download.microsoft.com/download/8/c/c/8cc94365-13d6-4975-bf69-9d4cd16a01a7/w2kccscg.pdf

Windows 2000 y Common Criteria
http://www.microsoft.com/spain/enterprise/perspectivas/numero_6/seguridad.mspx/202003

http://www.microsoft.com/spain/technet/seguridad/recursos/masinfo/criteria.mspx

Common Criteria
http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

Edit Plus
www.editplus.com

Belarc
http://www.belarc.com/

WinAudit
http://www.pxserver.com/WinAudit.htm

Microsoft Baseline Security Analyzer
http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx

Tablas de permisos en Windows 2000
http://fferrer.dsic.upv.es/cursos/Windows/basico/ch05s07.html#sec:prot:permisos

Administrador de sistemas
http://www.super.unam.mx/admon/
http://es.wikipedia.org/wiki/Administrador_de_sistemas