CIB-ESPOL
T
005.80
LEO

Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

"Análisis de las Vulnerabilidades de Windows 2000 Server y Su Servidor Internet Information Server"

TESIS DE GRADO

Previo a la obtención del título de:

Licenciado en Sistemas de Información

Presentada por:

Fernando Jacobo León Gavilanes
Hugo Hernán Melendres Cajamarca
Paúl Angelo Beltrán Bajaña

CIB-ESPOL

GUAYAQUIL–ECUADOR

Año
2005

CIB-ESPOL

AGRADECIMIENTO

A Dios por ser mi guía y por darme la dicha de vivir cada día.

A mis padres que me han apoyado durante toda mi vida estudiantil para formarme como un hombre de bien.

A mis verdaderos amigos, por que en ellos he hallado un gran tesoro.

Hugo Melendres C.

CIB-ESPOL

AGRADECIMIENTO

A Dios por haberme dado la vida, a mis padres por darme su apoyo constante a lo largo de mis años de estudio y a todos los que de una u otra forma han contribuido en mi formación profesional.

Fernando León G.



CIB-ESPOL

AGRADECIMIENTO

A todos mis profesores, compañeros de estudios y amigos, todos ellos conocidos y forjados dentro de este templo del saber, que han intervenido de una u otra forma a través de sus útiles y acertados consejos a lograr culminar esta gran meta que es un objetivo más en mi vida.

Paúl Beltrán B.

DEDICATORIA

A Dios, a mis padres: Aida y Hugo, a mis amigos y para todas aquellas personas que tienen metas y anhelan alcanzarlas. Este trabajo es para todos ustedes.

Hugo Melendres C.

CIB-ESPOL

DEDICATORIA

A mis padres por su constante dedicación y esmero durante toda mi vida estudiantil, a mi esposa por su apoyo incondicional durante el desarrollo de este documento.

Fernando León G.

DEDICATORIA

A Dios como parte principal en mi vida, a mi Abuela por ser lo único y mas grande que tengo, a mi hermano por darme el ejemplo de superación y a mi madre que desde el cielo siempre me ha guiado por el camino correcto.

Paúl Beltrán B.

TRIBUNAL DE GRADUACIÓN



Ing. Mónica Villavicencio

COORDINADORA DE LA LSI

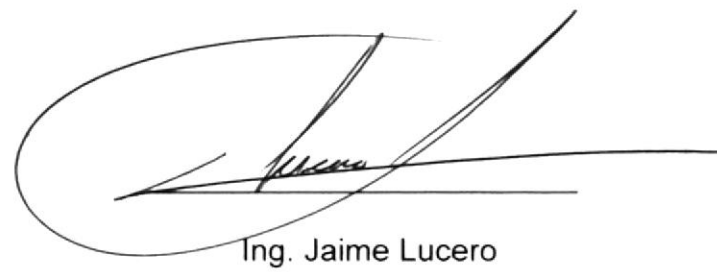
Ing. Albert Espinal S.

DIRECTOR DE TESIS



Ing. Lorena Carló

VOCAL



Ing. Jaime Lucero

VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

Fernando Jacobo León Gavilánez

Hugo Hernán Melendres Cajamarca

CIB-ESPOL

Paúl Ángelo Beltrán Bajaña

RESUMEN

El presente trabajo esta orientado a descubrir las principales vulnerabilidades del Windows 2000 Server y su servidor IIS. Dentro de nuestro estudio hemos considerado las principales falencias de este Sistema Operativo y las posibles soluciones que dentro de este contexto llamaríamos Parches de Seguridad a fin de tratar de satisfacer las necesidades de seguridad más importantes y básicas para usuarios del sistema antes mencionado.

ÍNDICE GENERAL

AGRADECIMIENTO ii

AGRADECIMIENTO iii

AGRADECIMIENTO iv

DEDICATORIA v

DEDICATORIA vi

DEDICATORIA vii

TRIBUNAL DE GRADUACIÓN viii

DECLARACIÓN EXPRESA ix

RESUMEN x

ÍNDICE GENERAL xi

ÍNDICE DE ANEXOS xviii

ÍNDICE DE FIGURAS xx

ÍNDICE DE TABLAS xxii

INTRODUCCIÓN xxiv

CAPÍTULO 1 ***1***

1. INTRODUCCIÓN A LA SEGURIDAD ORIENTADA A SERVIDORES WINDOWS 2000 SERVER **1**

1.1. Seguridad de la Información 1

1.2. Las tecnologías de la información en la actualidad. 6

CIB-ESPOL

1.2.1. Tecnologías y Servicios 9

1.2.2. Información y Tecnologías de la información 10

1.3. Vulnerabilidad de los sistemas informáticos 14

1.3.1. Amenazas a la seguridad de la Información 16

1.3.1.1. Ataques pasivos 17

1.3.1.2. Ataques activos 18

CAPÍTULO 2 ***20***

2. INFRAESTRUCTURA DE WINDOWS 2000 SERVER 20

2.1. Descripción de la Arquitectura del Internet Information Server 5.0 20

2.1.1. La importancia estratégica de los servicios web 21

2.1.2. Windows 2000 como un Servidor de Internet 24

2.1.3. Servicios web 25

2.1.3.1. Servidores virtuales 25

2.1.3.2. Soporte para WebDAV 34

2.1.3.3. Compresión del protocolo HTTP 35

2.1.3.4. Aislamiento de Web Sites, aplicaciones y servicios 35

2.1.3.5. Servidor FTP 36

2.1.3.6. Servicio SMTP 38

2.1.3.7. Servicio de Noticias TNP 47

2.1.3.8. Active Server Pages 52

2.1.3.9. Administración mediante Web y administración delegada 53

2.1.3.10. Seguridad 53

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ESPOL CIB-ESPOL

2.1.4. Comparación con Internet Information Server 4.0 ____ 54

2.1.4.1. Internet Information Server 4.0 ____ 55

2.1.4.2. Servidor Internet Information Server 5.0 Incorporado ____ 55

2.1.4.3. Rendimiento ____ 56

2.1.4.4. Seguridad Digest Authentication ____ 56

2.1.4.5. Servidor de aplicaciones ____ 57

2.1.5. Seguridad en IIS 5 ____ 62

2.2. Seguridad en Windows 2000 Server ____ 71

2.2.1. Introducción ____ 71

2.2.1.1. Microsoft Operations Framework (MOF) ____ 73

2.2.1.2. Definición de riesgo de seguridad ____ 76

2.2.1.3. Administrar la seguridad con la Directiva de Grupo de Windows 2000 ____ 78

2.2.1.4. Asegurar servidores basándose en su función ____ 79

2.2.1.5. Administrar revisiones ____ 80

CAPÍTULO 3 ____ ***81***

3. COMPONENTES DE SEGURIDAD NECESARIOS PARA REALIZAR UN ANÁLISIS DE UNA ORGANIZACIÓN ORIENTADA A LA IMPLEMENTACIÓN DE WINDOWS 2000 SERVER ____ **81**

3.1. Políticas básicas de Windows 2000 Server ____ 82

3.1.1. Políticas Básicas ____ 83

3.1.1.1. Auditoría y Configuración de Eventos Log ____ 83

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ESPOL
CIB-ESPOL

3.1.1.2. Fortaleciendo los procedimientos adicionales de los Servidores Miembros ____ 85

3.1.1.2.1. Fortaleciendo Procedimientos Manuales ____ 86

3.2. Componentes administrativos de la seguridad de riesgo. ____ 89

3.2.1. La necesidad de un programa estratégico de seguridad. ____ 89

3.2.2. Recursos ____ 95

3.2.3. Relación entre las Amenazas, Exposiciones, Vulnerabilidades y Medidas de prevención. ____ 97

3.2.3.1. Tipos de Amenazas ____ 104

3.2.3.1.1. Incidentes catastróficos ____ 105

3.2.3.1.2. Fracasos Mecánicos ____ 106

3.2.3.1.3. Amenazas Humanas ____ 107

3.2.3.2. Clasificación de las amenazas ____ 110

3.2.3.2.1. Identidad de Spoofing. ____ 111

3.2.3.2.2. Manipulación de datos ____ 111

3.2.3.2.3. Repudiación ____ 111

3.2.3.2.4. No Repudio ____ 112

3.2.3.2.5. La divulgación de la información ____ 112

3.2.3.2.6. Rechazo de Servicio ____ 112

3.2.3.2.7. Elevación de Privilegio ____ 113

3.2.3.2.8. Exploits ____ 113

3.2.3.2.9. Eliminación y Alteración de la Información. ____ 114

3.2.3.2.10. Fraude común y robo de información. 114

3.2.3.2.11. Destrucción de las operaciones normales del negocio 115

3.2.3.3. Métodos de Ataques 115

3.2.3.4. Vulnerabilidades 116

3.2.3.5. Riesgos 117

3.2.3.6. Medidas de Prevención 118

3.3. Gestión de Parches 121

3.3.1. Service Packs 122

3.3.2. Hotfixes o QFEs 123

3.3.3. Parches de seguridad 124

3.3.4. Manejo de parches en las organizaciones 124

3.3.4.1. Evaluar el ambiente actual 126

3.3.4.2. Servicio de actualización de software 126

3.3.4.3. Actualizar los servicios de seguridad 127

3.3.4.4. Comunicación 128

3.3.5. Proceso de Gestión de Parches 128

3.3.5.1. Mejorar el Proceso de Gestión 129

3.3.6. El Analizador Básico de Seguridad de Microsoft (MBSA) 130

3.3.7. Plan de parches 130

3.3.7.1. Clasificando los parches 131

3.3.7.2. Probando los Parches 132

CIB-ESPOL

3.3.7.3. Evaluando el Parche 133

3.3.7.4. Instalando los parches 134

3.3.7.5. Funcionamientos del servidor 134

3.3.7.6. Funcionamientos de la aplicación 135

3.3.7.7. Desinstalar el parche 135

3.3.7.8. Crear un Plan de Reversión 136

3.3.7.9. Implementar Parches 136

3.3.7.10. Supervisar los parches 136

CAPÍTULO 4 ***138***

4. ANÁLISIS DE LAS VULNERABILIDADES DE WINDOWS 2000 SERVER Y EL SERVICIO IIS 5.0 **138**

4.1. Estudio General de las Vulnerabilidades 138

4.1.1. Estadísticas de Ataques a las Vulnerabilidades 138

4.1.2. Percepción de seguridad en las organizaciones 144

4.1.3. Estadísticas de Ataques de Vulnerabilidades de Windows 2000 Server y del IIS 5.0 152

4.2. Vulnerabilidades del Windows 2000 Server 155

4.2.1. Vulnerabilidades en los Servicios 156

4.2.2. Vulnerabilidades en los protocolos 164

4.2.3. Vulnerabilidades del Sistema Operativo 167

4.3. Vulnerabilidades del Internet Information Server 5.0 170

4.3.1. Vulnerabilidades en los Servicios 171

4.3.2. Vulnerabilidades en los protocolos 185

4.4. Casos de estudio orientados al Análisis de las Vulnerabilidades más críticas del Windows 2000 Server y el IIS 5.0. 189

CAPÍTULO 5 ***207***

5. CONCLUSIONES Y RECOMENDACIONES **207**

ANEXOS ***210***

ABREVIATURAS ***242***

BIBLIOGRAFÍA ***246***

CIB-ESPOL

ÍNDICE DE ANEXOS

ANEXO A ____ 211

PLAN DE CONTINGENCIA ORIENTADO AL MANEJO Y FORTALECIMIENTO DE LA SEGURIDAD DEL WINDOWS 2000 SERVER Y EL SERVICIO IIS ____ 211

ANEXO B ____ 220

HERRAMIENTAS DE PROTECCIÓN DE LA SEGURIDAD DENTRO DE WINDOWS 2000 SERVER ____ 220

ANEXO C ____ 226

CASO DE ESTUDIO ____ 226

"PENETRACIÓN DE VIRUS NIMDA A TRAVES DE VULNERABILIDAD DE WINDOWS 2000" ____ 226

ANEXO D ____ 231

Tabla 3.1. Privilegios de Diferentes Tipos de Cuentas en Ambientes Windows 2000 ____ 231

ANEXO F ____ 232

Tabla 3.2. Componentes Importantes de Seguridad ____ 232

ANEXO G ____ 233

Tabla 3.4. Componentes Importantes de Seguridad ____ 233

ANEXO H ____ 234

Listado de las Vulnerabilidades más comunes en el Windows 2000 Server 234

ANEXO I 240

Listado de las Vulnerabilidades más comunes en el Internet Information Server 5.0. 240



CIB-ESPOL

ÍNDICE DE FIGURAS

Figura 2.1. El Modelo de Procesos MOF _____ 74

Figura 3.1. La Matriz de la Administración de Riesgo _____ 100

Figura 3.2. El camino para comprometer los recursos _____ 102

Figura 3.3. Relaciones entre los componentes de seguridad _____ 120

Figura 4.1. Cuadro Estadístico de casos reportados de vulnerabilidades en los últimos cinco años. _____ 140

Figura 4.2. Cuadro estadístico de los casos reportados de vulnerabilidades por aplicaciones en los últimos cinco años. _____ 143

Figura 4.3. Cuadro estadístico de la percepción del valor de la seguridad en las organizaciones _____ 145

Figura 4.4. Gráfico estadístico de los criterios de medidas de seguridad en las empresas _____ 147

Figura 4.5. Cuadro estadístico de la percepción de las empresas sobre la inversión en seguridad informática _____ 149

Figura 4.6. Gráfico de los Niveles de información comprometida por tipo de ataques _____ 151

Figura 4.7. Gráfico de los porcentajes de ataque de las vulnerabilidades más críticas del Windows 2000 Server y el IIS 5.0. según el CERT _ 155

CIB-ESPOL

Figura 4.8. Cuadro estadístico del tiempo no productivo por cada nivel de incidencia de una vulnerabilidad para Burger King Co. Ecuador____ 195

Figura 4.9. Gráfico estadístico de pérdidas estimadas por nivel de incidencia de una vulnerabilidad en Burger King Co. _____ 196

Figura 4.10. Cuadro estadístico del tiempo no productivo por cada nivel de incidencia de una vulnerabilidad para Ecuacotton_____ 204

Figura 4.11. Gráfico estadístico de pérdidas estimadas por nivel de incidencia de una vulnerablilidad para Ecuacotton _____ 204

CIB-ESPOL

ÍNDICE DE TABLAS

Tabla 3.1. Privilegios de Diferentes Tipos de Cuentas en Ambientes Windows 2000 _____ 231

Tabla 3.2. Componentes Importantes de Seguridad _____ 232

Tabla 3.3. Los tipos de Amenazas _____ 104

Tabla 3.4. Componentes Importantes de Seguridad _____ 233

Tabla 3.5. Tipos de Vulnerabilidades _____ 117

Tabla 4.1. Casos reportados de vulnerabilidades en los últimos cinco años. _____ 139

Tabla 4.2. Casos reportados de vulnerabilidades por aplicaciones en los últimos cinco años. _____ 142

Tabla 4.3. Percepción del valor de la seguridad en las organizaciones __ 145

Tabla 4.4. Criterios de medidas de seguridad en las empresas _____ 147

Tabla 4.5. Percepción de las empresas sobre la inversión en seguridad informática _____ 149

Tabla 4.6. Niveles de información comprometida por tipo de ataques ___ 150

Tabla 4.7. Los porcentajes de ataques de las vulnerabilidades más críticas del Windows 2000 Server y del IIS 5.0. según el CERT _____ 154

Tabla 4.8. Ingresos estimados por ventas de Burger King Co. Ecuador _ 194

Tabla 4.9. Riesgos vs. Costos Estimados de Burger King Co. Ecuador _ 195

Tabla 4.10. Ingresos estimados por pedidos de Ecuacotton S.A. _____ 202

Tabla 4.11. Riesgos vs. Costos estimados de Ecuacotton S.A._____ 203

INTRODUCCIÓN

CIB-ESPOL

Este trabajo se ha preparado con la finalidad de servir de apoyo a cualquier persona o instancia interesada en tener una guía de consulta ante posibles problemas que se puedan suscitar dentro de un ambiente con Windows 2000 Server.

El concepto de la seguridad de la información es amplio, debido a la gran cantidad de factores que intervienen, sin embargo es posible dar una aproximación a la definición y se puede decir que la seguridad es el conjunto de metodologías, documentos, programas y dispositivos físicos encaminados a lograr que la información disponible en un ambiente dado, sea accedida única y exclusivamente por quienes tengan la autorización para hacerlo.

En la actualidad las empresas utilizan con más frecuencia las computadoras para manejar y almacenar su información vital que constituye el activo más valioso, esto les proporciona muchos beneficios, pero también los hace vulnerables a los diferentes delitos informáticos si no se cuenta con un sistema de seguridad. Entre ellos, se pueden mencionar el robo, destrucción o modificación de información, fraude, etc., que son realizados por personas con algún conocimiento de computación ya sea dentro o fuera de la empresa.

Este documento tiene como objetivo ser una herramienta de consulta para la prevención o solución de problemas relacionados con la seguridad de este sistema operativo y el servicio antes mencionado, así como también presentar un análisis de las vulnerabilidades más importantes, para una mejor comprensión de lo que puede suceder de presentarse estas eventualidades.

El alcance de este trabajo abarca desde una introducción sobre la seguridad en el Windows 2000 Server así como un detalle de la infraestructura de este sistema operativo y de su servicio Internet Information Server 5.0, además de las normas necesarias para su buen funcionamiento. También se presenta un análisis de las vulnerabilidades más comunes en estas plataformas. Este trabajo no incluye un análisis de todas las vulnerabilidades existentes dentro de estas aplicaciones ya que resultaría inalcanzable dentro del marco teórico de este documento, así como también se excluyen manuales de instalación y operación de los mismos.

En el capítulo 1 se ofrece una introducción a la seguridad de la información en los servidores Windows 2000 Server, para poder entender su importancia.

En el capítulo 2 se detalla la infraestructura del Windows 2000 Server y su servicio Internet Information Server 5.0. de tal manera que sirva como una referencia para conocer el funcionamiento de ambas plataformas.

En el capítulo 3 se presentan los componentes de seguridad necesarios para la implementación del Windows 2000 Server, lo cual permite optimizar las seguridades dentro del sistema operativo, logrando minimizar la posibilidad de que se presenten problemas en el mismo.

En el capítulo 4 se realiza un detalle de las vulnerabilidades más comunes que se presentan en estas dos aplicaciones, analizando cuales son las mas críticas que afectan a estos sistemas y determinando soluciones a dichas vulnerabilidades con el fin de proteger nuestro servidor Windows 2000.

En el capítulo 5 se presentan la conclusiones acerca del presente documento.

CAPÍTULO 1

1. INTRODUCCIÓN A LA SEGURIDAD ORIENTADA A SERVIDORES WINDOWS 2000 SERVER

1.1. Seguridad de la Información

Definir la seguridad de la información es complejo, debido a la gran cantidad de factores que intervienen. Sin embargo es posible dar una aproximación a la definición y se puede decir que la seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, tengan acceso única y exclusivamente quienes tengan la autorización para hacerlo. Existe una medida cualitativa para la seguridad que dice: "Un sistema es seguro, si se comporta como los usuarios esperan que lo haga".

La computadora es un instrumento que maneja grandes volúmenes de información, los cuales pueden ser mal utilizados por personas intrusas o no autorizadas. La complejidad creciente y el alcance del uso de las computadoras en una organización ha propiciado que los sistemas de

CIB-ESPOL

almacenamiento y divulgación de información se encuentren en manos de unas cuantas personas, las cuales al efectuar su trabajo y concentrarse más que nada en ello, no realizan controles adecuados en el uso de los mismos, es decir, en estos sistemas.

El punto de vista tradicional sobre seguridad otorga mayor atención a los aspectos de seguridad clásicos, como son: el acceso físico, y la seguridad de los datos. Ahora bien, este enfoque parecía funcionar cuando las operaciones de cómputo de una entidad estaban centralizadas, hoy en día esta situación ha cambiado.

Estamos en la era del procesamiento distribuido o ínter conectividad informática. La actualidad exige nuevas técnicas del manejo de información que agilice el intercambio de datos, puesto que cada sector que necesita información al instante debe contar con un terminal eficiente, y no solicitar los datos al centro de cómputo y esperar que el personal a cargo se la otorgue.

Actualmente el concepto de centralización de la información puede considerarse antiguo. Para que una organización logre una inmersión exitosa, salvo algunos casos excepcionales, debe estar acorde a la globalización de la información, dándose a conocer al mundo y estableciendo una comunicación integral entre clientes actuales y potenciales.

Por lo tanto, se requiere un enfoque amplio que abarque cierto número de aspectos relacionados entre sí de manera metódica, agrupándolos convenientemente. El escrutinio cuidadoso de estas áreas revelará que ninguna de ellas es, por sí sola, de importancia exclusiva. Pero puede darse el caso que en una instalación específica, pueda tener mayor relevancia y, consecuentemente, requerir mayor atención.

Sin embargo si se incurre en el error de excluir una de estas áreas se dejaran vacíos o poros en las estructuras referentes a administración y control de la seguridad. El enfoque propuesto, el cual abarca metódicamente todas estas áreas se denomina Seguridad Total.

Esto indica que en toda organización debe existir un sistema de Seguridad de Información y un personal responsable que este a cargo de la dirección para la aplicación adecuada, metódica, organizada y controlada de las políticas y procedimientos de seguridad física y lógica de la organización como así también de los recursos involucrados para la consecución de los objetivos de la compañía. La seguridad debe ser tratada como una línea y como una función personal de la organización. Debe haber consenso de que la misma involucre a toda la compañía nivel por nivel.

La función básica del director de seguridad de la información es ayudar a la gerencia a hacer que su propia seguridad sea fácil de llevar. Se tendrá cuidado de no asignar responsabilidades al administrador que son propiamente de la gerencia. A continuación se presenta una lista de principales funciones para el responsable de la seguridad de la información:

- Proveer un apoyo administrativo directo para la instalación de los sistemas de seguridad que aseguren el uso de todos los sistemas en línea.
- Establecer objetivos para el desarrollo futuro de los sistemas de seguridad a medida que vayan evolucionando los sistemas en línea.
- Determinar los requisitos de recursos especiales, tales como recursos humanos, capacitación, equipamiento y planes de desarrollo, programas de seguridad y los presupuestos relacionados a la seguridad.
- Negociar con niveles múltiples de programación de apoyo de la gerencia para asegurar la integración de los objetivos de seguridad asignados, con la estrategia de procesamiento de datos a largo alcance.
- Analizar continuamente y evaluar las alternativas de seguridad para determinar que línea de acción debe seguir basada en las implicaciones técnicas, conocimiento de los objetivos del negocio y la

política de protección de activos corporativos, procedimientos y requerimientos.

- Asegurar que los proyectos asignados estén alineados con los objetivos de seguridad corporativa y sean completados de acuerdo con el programa dentro de los gastos consignados; informar a la gerencia tan pronto como sea posible de los problemas que podría materialmente afectar los objetivos, programas y gastos; sugerir soluciones alternativas.
- Supervisar el uso de todos los sistemas en línea para descubrir y actuar sobre los accesos desautorizados, y uso de los datos del propietario del negocio.
- Dirigir auditorias de seguridad, participar en evaluaciones de seguridad y proveer guía asistencia, como es debido, para facilitar la realización de los programas de protección del patrimonio de la institución.
- Revisar los esfuerzos de documentación asociados con diversos sistemas de seguridad.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

1.2. Las tecnologías de la información en la actualidad.

La situación actual de las "Tecnologías de la Información[1]"; informática, electrónica y telecomunicaciones, muestran que es posible capturar, almacenar, procesar y transmitir información con muy pocas limitaciones en cuanto a volumen, tipo, velocidad, distancia y costo.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

Esto ha sido durante mucho tiempo difícil y costoso, porque era necesario un transporte del soporte material de la información, sólo aliviado para las situaciones de proximidad física.

Compárese, por ejemplo, el intervalo de un mes necesario hace cien años para enviar un mensaje de Europa a América, con los pocos segundos que bastan hoy empleando correo electrónico o fax.

Como sabemos, la relación social se apoya en la comunicación, la consecuencia va a ser la alteración de muchos aspectos fundamentales de la estructura y las funciones de la sociedad, incidiendo directamente en el modo de entender de los grupos sociales, los símbolos, la propiedad, la enseñanza, el trabajo y el ocio. Se está pasando de una situación en que la información

---

[1] Tomado de http://www.abcdatos.com

era difícil de obtener y de manejar, a otra totalmente opuesta; habrá que pasar igualmente de una cultura de escasez a otra de abundancia de información.

Ahora se puede notar que los cambios están ocurriendo a un ritmo especialmente rápido, porque las distintas tecnologías han llegado a un punto de convergencia en el cual se aplican sinérgicamente[2] y de forma generalizada. Aunque es difícil predecir en detalle las consecuencias, sí es posible identificar qué aspectos sociales se van a ver afectados.

Si hacemos un análisis previo, la Electrónica, la Informática y las Telecomunicaciones no son nuevas tecnologías, estas se han ido desarrollando progresivamente en el último siglo y medio[3]. El telégrafo tiene 150 años, el teléfono y la informática más de cien, la televisión y los circuitos integrados unos cincuenta. En este tiempo, la Electrónica ha conseguido enormes capacidades de cálculo, de proceso y de almacenamiento de datos, y poniéndolas en el mercado a precios reducidos; la Informática permite ofrecer programas eficaces para aplicaciones personales, administrativas e industriales, técnicas eficientes de codificación y compresión de datos; y las

---

[2] Sinergia: Acción concertada de varios órganos para realizar una función.

[3] Tomado de http://www.abcdatos.com

Telecomunicaciones llegan a todas partes y permiten la transmisión de grandes cantidades de información, gracias a la extensión de las redes por cable y por ondas. La influencia de todas ellas en la actividad social resulta evidente.

Tras ese período de desarrollo paralelo, en este último lustro han llegado a un punto de convergencia en el cual, por primera vez, las tres tecnologías se pueden utilizar en coordinación, de tal forma que los límites entre una y otra empiezan a resultar difusos: televisión por cable, teléfono por computadora, teletexto, Internet. La clave de esta sinergia está en la digitalización de las telecomunicaciones, que permite su tratamiento informático.

Un ejemplo[4] que ilustra adecuadamente las diferencias en los elementos de comunicación es el siguiente: El sistema hormonal, basado en sustancias que viajan de una parte del organismo a otra por distintas vías, es limitado en cuanto a velocidad y capacidad. El sistema nervioso, por el que sólo circula la información, supera esas limitaciones, resulta mucho más ágil y permite funciones mucho más complejas.

---

[4] Tomado de http://www.conocimientosweb.net

1.2.1. Tecnologías y Servicios

Si hacemos un resumen de lo expuesto anteriormente podemos decir que las tecnologías de información y comunicación siguen evolucionando rápidamente, a pesar de la falta de consenso sobre los productos o servicios específicos que tendrán éxito y por cuánto tiempo. Estamos experimentando una avalancha de innovación caracterizada no tanto por una tecnología o ciencia única, sino más bien por el conjunto de varias tecnologías y servicios que se complementan.

Producto de este desarrollo hoy contamos con programas más accesibles y de fácil utilización, pantallas de contacto, teclados y lenguajes sencillos que han hecho posible la diversidad, el manejo y acceso cada vez masivo y menos especializado. En el centro de esta innovación tecnológica se encuentra el microprocesador, que provee control y memoria. Los microprocesadores se pueden hallar en cada dispositivo mecánico y electrónico, desde las unidades de control (por ejemplo: señales de tráfico) hasta artefactos domésticos como el horno microondas.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

1.2.2. Información y Tecnologías de la información

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos, y un elemento crítico para el éxito y la supervivencia de las organizaciones es la administración efectiva de la información y las tecnologías de la información relacionada. En esta sociedad esta criticidad emerge[5] de:

- La creciente dependencia de información y en los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas
- La escala y el costo de las inversiones actuales y futuras en información y Tecnologías de Información
- El impacto de las tecnologías de información para cambiar las organizaciones y las prácticas del negocio, crear nuevas oportunidades y reducir costos.

Al constituirse la información en el recurso fundamental de toda organización requiere de esta cuente con un conjunto de medidas de seguridad orientados prioritariamente a proteger las siguientes propiedades de la información.

---

[5] Tomado de http://www.usuarios.lycos.es/keu99/delitosinformaticos.html

- **Confidencialidad:** Se define como la "condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados". La información debe ser accesada y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. A menudo se la relaciona con la Intimidad o Privacidad.
- **Integridad:** Se define como la "condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado[6]". La integridad está vinculada a la fiabilidad funcional del sistema de información (la eficacia para cumplir las funciones del sistema de organización soportado por aquél). La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar. El concepto de calidad de la información de no fallas, confiable, se encuentra incluido en esta propiedad, considerando que se traslapa con el aspecto de disponibilidad relacionadas a la seguridad y también en alguna medida relacionada a la efectividad y eficiencia. Los medidas y políticas de seguridad implementadas en la organización deben eliminar toda posibilidad que

---

[6] Tomado de http://www.arcert.gov.ar

los datos puedan ser modificados. Como ejemplo podemos mencionar la presencia de los hackers[7] o intrusos.

- **Disponibilidad:** Se define como el "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable[8]". Se asocia a menudo a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información. La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la negación de servicio proveniente de un centro de información.
- **Autenticación:** Se define como "el mecanismo que permite conocer si la persona que esta accediendo a un sistema, es realmente quien debe acceder y no un extraño". Se refiere también a los mecanismos que se utilizan por ejemplo en temas como el correo electrónico para garantizar la autenticidad del remitente (un mecanismo son las firmas digitales).

---

[7] Hackers: Entes informáticos que se dedican a infiltrarse en sistemas no seguros y causan perjuicios incalculables a los sistemas Informáticos Mundiales.

[8] Tomado de http://www.arcert.gov.ar

Para poder salvaguardar las características y propiedades de la información, será necesario tener algunas consideraciones como:

- Para leer datos y modificar un registro, etc. será necesario saber de quien se trata y si la persona está autorizada. Por lo tanto será preciso identificar a la persona o usuario (Identificación) de forma totalmente fiable (Autenticación o Verificación), y consultar un archivo, base de datos y/o algoritmo que nos permita verificar que al persona tiene o no autorización para realizar la acción demandada (Autorización).
- Se debe establecer un sistema para identificar a las personas o usuarios (Gestión de la identificación)
- Se debe definir un sistema para autentificar al usuario (uso de contraseñas), y que para cada usuario se haya definido una tabla de permisos. Cuando el usuario intente entrar en el sistema, deberá dar su identificación, que el sistema verificará si la tiene en sus tablas (Comprobación del identificador), realizar la operación pertinente para demostrar que es quien dice ser (dar su contraseña) y, el sistema comprobará que este autentificador corresponde al identificador indicado (Autenticación). Cuando el usuario intente acceder a un recurso, el sistema verificará si este usuario tiene o no el permiso correspondiente, o que su nivel y categoría le permiten realizar la acción demandada.

ESPOL
CIB-ESPOL

El administrador de seguridad será el encargado de introducir los datos de los privilegios al sistema. Los privilegios pueden darse individualmente a una persona o bien a un grupo de personas con las mismas características. También hay sistemas en los que un usuario normal da la autorización a un tercero sin la necesidad del administrador de seguridad.

1.3. Vulnerabilidad de los sistemas informáticos

Es frecuente que cada semana la prensa especializada en los sistemas de información hablen de otro fallo de seguridad: un virus que se aprovecha de las macros que manejan las herramientas del Office de Microsoft, una vulnerabilidad en Windows o UNIX, un problema de Java, un agujero de seguridad en una de las páginas principales de Internet, un ataque contra un popular cortafuegos.

Una forma común de "probar" la seguridad es realizar revisiones de seguridad. Esto es un proceso manual costoso y requiere de un tiempo. No es suficiente comprobar los protocolos de seguridad y los algoritmos de cifrado. Una revisión debe cubrir especificación, diseño, aplicación, código fuente, funcionamiento, y todo lo demás. Así como la prueba funcional no puede demostrar la ausencia de errores, una revisión de seguridad no puede demostrar que el producto sea realmente seguro.

Tomemos el siguiente ejemplo[9]: Una revisión de seguridad de la versión 1.0 dice poco sobre la seguridad de la versión 1.1. Una revisión de seguridad de un producto del software aislado no sirve necesariamente para el mismo producto en un ambiente operacional. Y cuanto más complejo sea el sistema, más compleja se vuelve una evaluación de seguridad y posiblemente habrá más fallos de seguridad.

Pensemos en el supuesto que un producto de software se desarrolla sin ninguna comprobación funcional en absoluto. Ninguna comprobación funcional de las versiones alfa o beta. Se escribe el código, se compila, y se envía. Las posibilidades de que este programa simplemente funcione incluso dejando de lado que esté libre de errores es cero. A medida que aumenta la complejidad del producto, aumentará el número de errores. Todos sabemos que las pruebas son esenciales.

Los productos se vuelven más complejos cada año, los sistemas operativos son más grandes, tienen más características, más interacciones entre los diferentes programas en Internet. Windows NT lleva buen tiempo funcionando y todavía se descubren errores de seguridad. El incremento en el uso de las computadoras y la convergencia en Internet, están aumentando

---

[9] Tomado de http://www.arcert.gov.ar

a un ritmo creciente. Los sistemas se están convirtiendo en más y más complejos, y en alguna medida, inseguros.

1.3.1. Amenazas a la seguridad de la Información

Se define como amenaza, a una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produzca una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad[10].

Las amenazas a la seguridad en una red pueden presentarse en el flujo de información desde una fuente (como por ejemplo un archivo o una región de la memoria principal) a un destino (como por ejemplo otro fichero o un usuario). Otros orígenes de estas se dan en la falencias del Sistema Operativo como tal, aspectos que serán evaluados detalladamente en los capítulos siguientes.

---

[10] Tomado de Manual de Seguridad de Microsoft

1.3.1.1. Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o controla, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, consiste[11] en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes controlados.
- Control del volumen de tráfico intercambiado entre las entidades controladas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.
- Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

---

[11] Tomado de http://www.vnunet.es/Hemeroteca/Resultados/Tema/Windows_2000

CIB-ESPOL

1.3.1.2. Ataques activos

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido, o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de Identidad**[12]**:** El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, esto es posible al sustraer la contraseña de acceso a una cuenta.
- **Repetición Indeterminada:** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de Mensajes**[13]**:** Una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir

---

[12] Tomado de http://www.vnunet.es/Hemeroteca/Resultados/Tema/Windows_2000

[13] Tomado de http://www.vnunet.es/Hemeroteca/Resultados/Tema/Windows_2000

un efecto no autorizado. Por ejemplo, el mensaje "Ingresa 10 mil dólares en la cuenta A" podría ser modificado para que diga "Ingresa 100 mil dólares en la cuenta B".

- **Degradación fraudulenta del servicio:** Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes triviales. Entre estos ataques se encuentran los de negación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

A continuación expondremos las falencias detectadas en el Windows 2000 Server y de su IIS y las medidas que debemos tomar para salvaguardar la integridad de los mismos a fin de proveer una seguridad integral a nuestros sistemas y por ende a nuestros datos que son como ya lo hemos dicho anteriormente un recurso invaluable dentro de la organización.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ESPOL
CIB-ESPOL

CAPÍTULO 2

2. INFRAESTRUCTURA DE WINDOWS 2000 SERVER

2.1. Descripción de la Arquitectura del Internet Information Server 5.0

En este capítulo se detallan las funcionalidades que Windows 2000 ofrece para la prestación de servicios en Internet, presentando brevemente algunas de las características de los mismos.

- **Origen del Internet Information Server 5.0**

Microsoft ha empezado a afianzarse en un mercado en el que, hasta hace poco, se hallaba en una posición minoritaria: el de la implantación de servidores en Internet[14]. Una clara muestra de esta tendencia es .NET, la nueva plataforma de desarrollo de aplicaciones en la que todo gira alrededor

---

[14] Tomado del Manual de Seguridad de Microsoft, publicado en Enero del 2001

de la idea de que la red, Internet, va a constituirse en el ámbito en el que las aplicaciones van a prestar sus servicios, en lugar de ser un mero mecanismo de comunicación. Es evidente que hasta hace relativamente poco tiempo, la mayoría de los servidores web estaban basados en plataformas UNIX. Esta situación ha cambiado y está cambiando, para invertirse, en buena medida, en la tendencia inversa de tal forma que muchos administradores de servidores web están abrazando la fe Windows, algo que para muchos de ellos era hasta hace poco una opción que ya la tenía incluida.

Los servicios web han pasado de ser un extra a convertirse en una prestación imprescindible. Con la publicación de Windows NT 4, dejo a la vista problemas de fiabilidad lo cual llevo a una revisión total del sistema operativo y es así que se lanza Windows NT Option Pack, un nuevo entorno que disponía de una interesante y completa plataforma de servicios de Internet.

2.1.1. La importancia estratégica de los servicios web

CIB-ESPOL

En la actualidad[15], y más aún en el futuro, Internet está convirtiéndose en "el" ámbito de negocio. Además, sus mecanismos de comunicación se están

[15] Creación Propia

trasladando a las redes locales de las corporaciones, tanto en lo referente a los mecanismos y protocolos de comunicación, como en las técnicas de desarrollo de aplicaciones y medios de acceso a la información por parte de los empleados, colaboradores y asociados. Es por todos estos motivos que un sistema operativo con vocación de liderar el mercado no puede tener éxito si no ofrece de manera nativa la posibilidad de que la información pueda compartirse, no sólo mediante los mecanismos convencionales en una red local, sino utilizando tecnología Web. Es decir, es necesario para toda plataforma que se valore, hoy en día, facilitar la creación tanto de intranets como la posibilidad de definir la presencia en Internet.

- **Windows NT 4.0 Option Pack, una opción fundamental en Windows NT 4**

En los primeros meses de 1998, Microsoft hizo público Windows NT 4.0 Option Pack[16], una extensión al sistema operativo de Microsoft que dio un auténtico vuelco a sus funcionalidades como servidor en Internet. Option Pack convierte a un servidor Windows NT en algo que se parecía poco, en el ámbito del web, a lo que incluía el paquete básico del sistema operativo, ofreciendo, a modo de resumen, los siguientes servicios básicos:

---

[16] Paquete Opcional de Windows NT 4.0 liberado en Mayo de 1998

- **Internet Information Server 4.0:** el antecesor de la versión de IIS 5.0 incluía servidores web y FTP.

- **Active Server Pages 2.0:** Microsoft proporcionó una nueva versión de la exitosa plataforma de servidor para el desarrollo de aplicaciones web utilizando técnicas de Scripting[17].

- **Servidor de noticias NNTP:** servidor de noticias compatible con el estándar Network News Transport Protocol (NNTP).

- **Servidor de correo SMTP:** el paquete incluye un servidor de correo saliente (SMTP) que principalmente nos va a permitir establecer conexiones para la transmisión de correo que, entre otras cosas, van a facilitar la inclusión en nuestro servidor de páginas web con formularios cuyos resultados serán enviados a una dirección de correo en lugar de ser procesados directamente con un CGI o página de servidor activo.

- **Microsoft Management Console:** MMC, tan familiar para los administradores en plataforma Microsoft desde Option Pack, SQL Server 7 y es definitivamente incorporada por primera vez con Windows 2000 como herramienta de administración.

---

[17] Segmentos de código escritos en otros lenguajes de programación embebidos en las páginas web.

CIB-ESPOL

- **Microsoft Transaction Server (MTS):** Primera versión realmente funcional del elemento para el desarrollo y gestión de aplicaciones en nuestro servidor que hagan uso transaccional de componentes.

- **Certificate Server:** Servidor para la creación de certificados que permitan la implementación de mecanismos de conexiones seguras de Secure Sockets Layer.

- **Site Server Express:** Versión ajustada de las herramientas de análisis de Site Server 3.0.

- **Extensiones para FrontPage 98:** Extensiones necesarias para poder crear sitios web con FrontPage 98.

2.1.2. Windows 2000 como un Servidor de Internet

Windows 2000 incorpora, en cualquiera de sus ediciones (incluyendo el exitoso Windows 2000 Professional), y sin ningún coste adicional, un servidor Internet integrado: Internet Information Server 5.0 (IIS 5.0), heredero directo de la versión 4.0 que se instalaba en Windows NT 4.0 dentro del Option Pack[18].

---

[18] Tomado de Manual de Seguridad de Microsoft

Internet Information Server 5.0 es mucho más que un servidor web. Bajo el IIS se refugian prácticamente todas las prestaciones relacionadas con Internet de Windows 2000, desde los servicios de correo SMTP y de noticias NNTP, a los servicios web y FTP, pasando incluso por los servicios de Terminal.

2.1.3. Servicios web

Evidentemente, la primera prestación de IIS[19] 5, es la de poder albergar sitios web. A continuación detallamos algunas de sus novedades.

2.1.3.1. Servidores virtuales



CIB-ESPOL

Si utilizamos el servidor web para dar servicios de Internet, es decir, si somos un proveedor de servicios de Internet (ISP),o simplemente, si deseamos en nuestro entorno Intranet hospedar más de un sitio web, necesitaremos que IIS 5 nos permita albergar servidores virtuales, es decir, diferentes sitios web. IIS 5.0 permite definir servidores virtuales que compartan una misma dirección IP, o bien que utilicen IP diferentes. Cuando una petición web llega desde un navegador, contiene un conjunto de información del servidor al que

---

[19] Internet Information Server 5.0

desea conectarse y de la página que se desea ver. Esta información contiene fundamentalmente tres partes: la dirección IP (tras la resolución de nombres DNS), el puerto de comunicación (port), y una tercera información que contiene la cadena de caracteres que el usuario ha escrito en el explorador para designar al dominio en el que desea encontrar la página, algo así como www.espol.edu.ec. Esta tercera información se denomina host header name[20] y es precisamente lo que utiliza IIS 5 para saber a cual de los servidores virtuales que comparten una dirección IP se envía la petición. Cada servidor virtual aparece como un nodo en Microsoft Management Console que se administra de manera separada. Cuando instalamos el producto se nos crean dos servidores virtuales, el Default Web Site (sitio web por defecto) y el Administration Web Site, (sitio web de Administración) que, como su nombre indica, está destinada a la administración del servidor a través del web y que se halla protegida al escuchar en un puerto diferente del 80. Cada uno de estos servidores virtuales puede administrarse separadamente en todos sus extremos. En particular, podemos indicar las tres informaciones del sitio web.

---

[20] Nombre oculto del Servidor

- **Sitios web y servidores virtuales**

Un servidor Web[21] puede hospedar varias sitios web, cada una de ellas asociada a un dominio distinto que pueden incluso compartir direcciones IP. Desde el punto de vista de los usuarios que acceden a los sitios web que comparten la máquina esta situación es absolutamente indetectable, ya que ellos se limitan a escribir en su navegador el dominio al que desean acceder. DNS resolverá ese nombre y lo convertirá en la dirección IP de la máquina compartida.

Para resolver nombres entre sitios con la misma IP, se utilizan los *host header names*, que es la información que el usuario escribe en la barra de exploración de su navegador.



CIB-ESPOL

- **Identificación de un sitio Host Header Names**

Cada sitio web de nuestro servidor viene caracterizada por tres informaciones:

- La dirección IP

---

[21] Tomado del Manual de Seguridad de Microsoft

- El número de puerto en el que la sede escucha a las peticiones de conexión.

- Un host header name es el nombre con el que los usuarios conocen el sitio web al que quieran acceder. Cuando un cliente solicita una página, el navegador pasa en la cabecera de la petición, además de la dirección IP de la máquina, la cadena de caracteres que dentro de URL que el usuario ha escrito como dirección de navegación representa al host o dominio. Esa información es detectada e interpretada por el servidor web y puede servir para determinar qué sede web desea explorar el cliente cuando varias sitios comparten una misma IP.

Cada sitio debe tener un conjunto único de esas tres informaciones, es decir, el sitio se caracteriza por el conjunto de ellas de manera que no podemos tener dos sitios en nuestro servidor que no se diferencien ni en la dirección IP, ni el puerto en el que escuchan, ni en el host header name al que atienden, ya que se produciría ambigüedad en las llamadas de los clientes.

Cuando esta situación de ambigüedad [22]se produce, es decir, cuando creamos un sitio web y no proporcionamos en la configuración una terna de valores únicos, el sitio web aparece como detenido hasta que subsanemos el error de configuración.

Conociendo esto, podemos encontrarnos con los siguientes escenarios de uso:

- Un servidor con sólo un sitio web y FTP
- Servidor con múltiples sitios y múltiples IP
- Servidor con más sitios que direcciones IP



CIB-ESPOL

- **Un servidor con sólo un sitio web y FTP :** En este caso, el sitio está asociado a la dirección IP de la tarjeta de red de la máquina, el host header name aceptable será cualquier nombre de dominio vinculado en DNS a esta dirección IP y el número de puerto será, normalmente, 80 para Web y 21 para FTP.
- **Servidor con múltiples sitios y múltiples IP :** Si tenemos tantas sitios como direcciones, esta situación en nada difiere con aquella en la que se dispone de múltiples máquinas: cada sitio tendrá asociado una dirección

---

[22] Tomado del Manual de Seguridad de Microsoft

IP, que se anotará en el DNS vinculada a su nombre de dominio. Sin embargo, es posible que tengamos más direcciones IP que sitios web. En ese caso, podremos asociar más de una dirección IP a cada sitio. Por defecto, cuando se crea un sitio web con IIS 4, tiene asociados todas las direcciones IP que aún no han sido asignadas a ninguna otra. Esta asociación, evidentemente, puede alterarse cuando se desee.

- **Servidor con más Sitios Web que direcciones IP :** Este escenario, en el que una dirección IP es compartida por varios sitios, es propio en proveedores de servicios Internet que dan servicios de Hosting[23] de sitios web. Los proveedores pueden de este modo, rentabilizar mucho mejor el costo de las direcciones IP, economizando recursos.

Los navegadores más antiguos no envían la información de host header name, por lo que no se puede utilizar este método de discriminación de sede con ellos.

---

[23] Servicio con el cual nuestras páginas web son alojadas en un Servidor que se encarga de publicarlas a través del World Wide Web

Organización de los contenidos del sitio Web

Directorio asociado a un sitio

Cada sitio web y FTP tienen asociado un directorio de inicio o directorio raíz, en el sistema de archivos del servidor. El servidor web reproduce en la organización lógica del sitio la organización física que exista en ese directorio de inicio. Es decir, todos los subdirectorios que contengan el directorio de inicio físico aparecerán como directorios web del sitio.

Para modificar el directorio de inicio de un sitio deberemos acudir a MMC para administrar el servidor web o FTP, y seleccionar el sitio al que queremos cambiar el directorio de inicio.

En esta página podemos especificar la ubicación del directorio de inicio, que puede residir en:

- Un directorio físico en un disco de nuestra máquina.
- Una ubicación lógica compartida por otra máquina (unidad de red).
- Una ubicación web caracterizada por su URL, al que se redirigirán las peticiones de documentos dirigidas a nuestro directorio.

Directorios virtuales[24]

En esa tarea de definir una estructura física y lógica y vincularlas, tendremos directorios lógicos que corresponderán con directorios físicos en otras ubicaciones que no cuelguen del directorio de inicio. Estos directorios se denominan directorios virtuales.

Los directorios virtuales se crean definiendo un alias a un directorio físico del servidor. Los clientes que naveguen por el sitio verán ese alias como si fuese un directorio físico del servidor, justo debajo del directorio de inicio.

Los directorios virtuales tienen numerosas ventajas:



CIB-ESPOL

- **Seguridad:** Oculta a los usuarios la estructura real de la información en el disco duro del servidor. La información es algo que no debemos regalar a los usuarios.
- **Flexibilidad:** Nos permiten hacer crecer el sitio más allá de los límites de un disco, dar nombres diferentes a un mismo directorio, permitiendo vías de acceso alternativas.

---

[24] Tomado del Manual de Seguridad de Microsoft

- **Hacer más fácil la navegación:** Si la ruta de directorios físicos se hace muy larga, podemos dar un nombre alternativo, con un directorio virtual con nombre más corto, fácil de recordar y de escribir.

- Permite mover directorios sin que los usuarios lo noten.



CIB-ESPOL

Aplicaciones Web

Una aplicación, desde el punto de vista de IIS es un directorio o directorios en los que se contiene una serie de archivos que van a ejecutarse en un mismo ámbito de proceso. Por ejemplo, cualquier directorio que contenga páginas Asp[25] es susceptible de ser configurado como una aplicación.

Las aplicaciones se definen especificando un punto de entrada (su directorio de inicio) y una serie de características de ejecución. Los límites de la aplicación serán todos aquellos directorios por debajo del de inicio, hasta llegar a un directorio que sea a su vez directorio de inicio de otra aplicación. Es decir, las aplicaciones son auto excluyentes, de manera que un directorio o archivo no puede pertenecer a dos aplicaciones.

---

[25] Active Server Pages (Servidor de Páginas Activas)

Además, podemos excluir subdirectorios del directorio de inicio de la aplicación sin necesidad de borrarlos o eliminarlos del disco, desde MMC. Tras esta acción, las páginas que se ejecuten dentro de este directorio y sus descendientes, no estarán en el ámbito de la aplicación.

Todos los archivos ejecutables dentro de una aplicación (ejecutables propiamente dichos, páginas activas de servidor, extensiones ISAPI, CGI scripts, aplicaciones de acceso a datos con IDC y componentes) se ejecutan en el ámbito de la misma y responden a las características definidas para ella.

2.1.3.2. Soporte para WebDAV

WebDAV[26] es una extensión al protocolo HTTP 1.1 que sigue un lema muy explícito: "makes the Web Writable". Es decir, se trata de un estándar que permite ejecutar acciones de gestión de archivos tales como escribir, copiar, eliminar o modificar, todo ello sobre una conexión HTTP. WebDAV es clave en la estrategia de convertir el web en una plataforma de desarrollo de aplicaciones. Exchange 2000, SharePoint Portal 2001 y BizTalk Server 2000 utilizan WebDAV de manera exhaustiva.

---

[26] Tomado de http://www.htmlweb.net/seguridad/tesis/tesis.html

2.1.3.3. Compresión del protocolo HTTP

El IIS 5[27] ofrece la posibilidad de comprimir los documentos previos a su envío al cliente, con el consiguiente ahorro de línea de comunicaciones. Para que esta opción sea útil, evidentemente, es preciso que el cliente admita esta posibilidad. Por otra parte, no se recomendaría a nadie que emplease la compresión sin antes someter al servidor a una prueba de estrés. La sobrecarga de procesador a la que puede someter al servidor es inaceptable en servidores con muchos impactos.



CIB-ESPOL

2.1.3.4. Aislamiento de Web Sites, aplicaciones y servicios

En IIS 4 era posible un mínimo aislamiento entre las distintas aplicaciones albergadas en un servidor. En IIS 5 esta posibilidad se ha extendido en múltiples direcciones. En primer lugar, cada aplicación web (un directorio a partir del cual hemos definido una aplicación), puede ejecutarse dentro del mismo proceso de IIS (Inetinfo), en un proceso externo (DLLHOST) o en un tercer proceso compartido por varias aplicaciones. Por otra parte, es posible limitar el tiempo de proceso que va a utilizar una aplicación, para que no afecte al resto de las hospedadas en el servidor. Además IIS 5 permite

---

[27] Tomado de http://www.htmlweb.net/seguridad/tesis/tesis.html

monitorizar (mediante anotaciones extra en los ficheros de log) cual es el uso de CPU que está haciendo cada uno de los sitios Web alojados en nuestro servidor. Un buen argumento a la hora de justificar la factura a nuestros clientes de hosting.

2.1.3.5. Servidor FTP

El servicio FTP sigue siendo necesario e Internet Information Server 5 le da soporte. El servicio ha sido mejorado, ya que IIS 5 incluye, la funcionalidad de que las descargas de ficheros desde un servidor FTP Microsoft puedan reanudarse en el punto de interrupción en caso de caída repentina de la conexión, sin necesidad de reiniciar el proceso.

- **IIS 5 como servidor FTP**

Aunque en la mayoría de las ocasiones se piensa en IIS como un servidor web no debe olvidarse que también es un servidor FTP. La razón de este olvido es que FTP, aun resultando extraordinariamente útil por su potencia y simplicidad de uso, es un protocolo poco sutil cuyo uso está en regresión. El protocolo de transmisión de archivos (File Transfer Protocol), normalmente denominado FTP, gestiona el acceso, la transferencia de archivos y la creación y gestión de directorios entre máquinas conectadas por TCP/IP.

En IIS 5, se ha introducido una novedad importante en el servicio FTP. Desde ahora, el servidor FTP permite reanudar descargas interrumpidas por caídas inesperadas de la red, algo que hacen automáticamente muchos de los clientes de FTP.

- **Configuración de un sitio FTP**



CIB-ESPOL

- **Identificación del sitio FTP**

Cada sitio FTP debe tener asociada una dirección IP y un número de puerto. Estos datos son introducidos en el momento de la creación del sitio con el asistente, pero en cualquier momento podemos necesitar modificarlos.

Entre las propiedades básicas de los sitios FTP, está la configuración de las características de las conexiones que van a poder establecerse con ella. Las conexiones FTP suelen consumir bastantes recursos, ya que los usuarios las utilizan para descargar información. Por otra parte, la dinámica de uso de estas conexiones provoca que en la práctica los usuarios se olviden de ellas muy a menudo, dejando conexiones abiertas. Podemos restringir el número límite de conexiones para protegernos ante un número excesivo de peticiones de conexión que puedan hacer que el rendimiento de nuestro servidor se vea afectado. También es configurable el tiempo de vida de

conexiones inactivas. Para liberar recursos cuando existen conexiones que no tienen actividad podemos especificar un valor en segundos, del tiempo que se permitirá que una conexión esté inactiva antes de desconectarla.



CIB-ESPOL

2.1.3.6. Servicio SMTP

IIS 5 proporciona servicio SMTP (correo electrónico saliente). Sin embargo, y a diferencia de su antecesor, los servicios no entran en conflicto con los que puedan instalarse con Exchange Server. Probablemente nosotros hemos experimentado los problemas que se producen cuando se ha instalado en un mismo equipo Windows NT, Exchange Server 5.5 junto con Windows NT Option Pack. Exchange Server 5.5 que incluye un servicio SMTP que no puede estar activo al mismo tiempo y en el mismo puerto en el que estaría el servicio SMTP incluido en el Option Pack. Por otra parte, es necesario instalar Option Pack en un servidor Exchange 5.5 si deseamos utilizar Outlook Web Access[28].

En Windows 2000, el servicio SMTP forma parte de los servicios incorporados al sistema operativo en IIS 5, igual que NNTP, si bien este último, a diferencia del primero, no se instala por defecto. Exchange 2000

---

[28] Tomado de http://www.htmlweb.net/seguridad/tesis/tesis.html

utiliza estos dos servicios, de tal forma que los requiere para proceder a la instalación. No hay conflicto, sino dependencia.

- **IIS 5 y los servicios de correo electrónico**

Internet Information Server 5 incluye además un par de servicios, SMTP y NNTP[29], que respectivamente, permiten el envío y recepción de mensajes de correo y noticias. En su versión anterior, estos servicios ya estaban incluidos en el Option Pack o paquete de opciones fundamentalmente porque los sitios web necesitan frecuentemente disponer de un servidor de correo en la misma máquina, para procesar formularios mediante el envío de mensajes de correo electrónico, por ejemplo. En IIS 5 estos servicios, fundamentalmente el de correo, no son un añadido sino prestaciones del sistema operativo reutilizadas y extendidas por Exchange Server.

Es importante destacar que estos dos servicios no poseen características que les hagan idóneos para escenarios complejos de servicios de correo y de noticias. Particularmente, no permiten la creación de buzones de correo, imprescindible para dar servicio a usuarios individuales y, por lo tanto, no es adecuado para un proveedor de servicios Internet.

---

[29] Tomado del Manual de Seguridad de Microsoft

A pesar de que el servidor de noticias posee una funcionalidad completa, sin embargo, carece de mecanismos de administración y gestión de escenarios sofisticados. Microsoft propone Exchange Server para implementar estos servicios.

- **El protocolo SMTP**

SMTP[30] es un protocolo de comunicación síncrona, es decir, que se establece entre entidades que deben estar presentes en el momento en que la información se transfiere. Es decir, para que exista una transferencia de correo entre dos servidores SMTP (que juegan el papel de MTA), ambos deben estar en línea.

Los servidores SMTP utilizan por defecto conexiones TCP en el puerto 25, el mismo puerto del servidor SMTP que suele ser un parámetro de configuración de nuestro cliente de correo. Una vez que la comunicación SMTP ha sido llevada a cabo el MTA que juega el papel de cliente (porque está enviando correo al MTA remoto, que consideraremos servidor), envía mandatos ASCII a los que el servidor remoto responde con mensajes de

[30] Creación Propia

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ESPOL
CIB-ESPOL

confirmación de recepción. Estos mandatos contienen los diferentes valores de las cabeceras del mensaje y el cuerpo del mensaje.

El servidor basa su funcionalidad en la existencia de un conjunto de directorios en el sistema de archivos de la máquina en la que reside, que van a servir de almacén para los mensajes tanto entrantes, como salientes e incluso para los que se hallen en cola o hayan sido declarados defectuosos. De este modo, la monitorización de los mensajes en proceso en el servidor puede incluso llevarse a cabo con el explorador de Windows. Todos los mensajes que lleguen al servidor son depositados en un directorio, llamado Drop directory, que actúa, de este modo, como una suerte de buzón global.

Además existe un directorio, Pickup Directory, en el que podemos depositar los mensajes que deseemos, como archivos. El servidor recoge los mensajes de este directorio y los envía. Podemos pensar en este directorio como si de un buzón global de salida se tratase.



CIB-ESPOL

- **Dominios**

IIS 5 distingue dos tipos de dominios: locales y remotos. El servidor soporta más de un servidor local, de entre los que uno será el servidor por defecto o principal (default domain) y el resto serán alias del servidor por defecto (alias

domain). El servidor por defecto es utilizado para todos aquellos mensajes que se envíen o reciban en el servidor sin especificar el dominio asociado. Cuando se recibe un mensaje destinado a un dominio local, es decir cuando se recibe un mensaje con una dirección local, el mensaje se deposita en el directorio de recepción de mensajes (Drop directory), si eso es posible, o devuelto al remitente con la indicación de que la entrega no ha sido posible.

Los mensajes con destino a dominios remotos son encaminados por IIS 5 utilizando DNS. Es posible, para cada dominio remoto, especificar un servidor auxiliar a través del cual sabemos que la ruta de encaminamiento de mensajes será más eficiente. También es posible indicar un smart host, al que se enviarán todos los mensajes destinados a dominios remotos.

- **Directorios**[31]

El servidor almacena los mensajes en un conjunto de subdirectorios en el sistema de archivos de la máquina. El directorio raíz de esta jerarquía de subdirectorios es configurable en el proceso de instalación de IIS 5, aunque el programa nos propone .\inetpub\mailroot.

---

[31] Tomado del Manual de Seguridad de Microsoft

- **Drop:** almacena los mensajes recibidos para cualquiera de los dominios locales del servidor. Debe ser diferente del directorio Pickup. Los mensajes se ordenan por dominios.

- **Pickup:** directorio en el que el servidor busca los mensajes que debe enviar. Si colocamos en este directorio un archivo de texto, el servidor lo procesa y procede a su envío.

- **Queue:** implementa la cola para almacenar aquellos mensajes que no han podido ser enviados inmediatamente. El servidor acude a este directorio a intervalos prefijados para intentar el reenvío.

- **Badmail:** almacena los mensajes que no han podido ser enviados ni devueltos al destinatario.

- **SortTemp:** archivos temporales durante el proceso de ordenación.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

Todos los mensajes que llegan a IIS, se depositan inicialmente en el directorio Queue, esperando el momento en el que podrán ser tratados. Una vez recogido el mensaje de la cola y analizado, si el mensaje llega desde un dominio remoto o desde uno local diferente al del destinatario del mensaje, el servidor lo procesa para su entrega local. Este proceso simplemente consiste en depositar el mensaje en el directorio Drop.

Existen básicamente dos maneras de provocar que IIS 5 envíe un mensaje a un dominio remoto: estableciendo una sesión SMTP directamente mediante comandos (por ejemplo, utilizando Telnet), o colocando un archivo de texto correspondiente al mensaje que deseamos enviar en el directorio Pickup. En cualquiera de los dos casos, como hemos comentado, el mensaje pasa primero por la cola.

Cuando los mensajes remotos se recogen de la cola se depositan en el directorio Sort, en el que se ordenan por dominio de destino. El siguiente paso es intentar establecer una conexión con el dominio remoto (mandatos HELO y MAIL) para proceder a la transmisión de todos los mensajes destinados a él. Si la transmisión no es posible los mensajes se devuelven a la cola en la que permanecerán hasta que se consuma un número configurable de reintentos infructuosos.

Si el servidor remoto está dispuesto para establecer la conexión, se le envían los mandatos RCPT pertinentes para verificar que los usuarios destino de los mensajes existen en el dominio remoto. Si los usuarios no existen, los mensajes son devueltos al remitente, y en caso contrario se procede a su envío.

CIB-ESPOL

- **Configuración de las conexiones**[32]

Entre las propiedades básicas del servidor está la configuración de las características de las conexiones que van a poder establecerse con nuestro servidor, bien sea de entrada o de salida de mensajes. Pueden configurarse los siguientes aspectos:

- **Número límite de conexiones:** para protegernos ante un número excesivo de peticiones de envío de correo que pueda hacer que el rendimiento de nuestro servidor se vea afectado, podemos limitar el número de conexiones entrantes.
- **Tiempo de desconexión de conexiones inactivas:** para liberar recursos cuando existen conexiones que no tienen actividad, podemos especificar un valor en segundos, del tiempo que se permitirá que una conexión esté inactiva antes de desconectarla. El valor por defecto es 1 minuto. Las conexiones de salida son aquellas que establece nuestro servidor para enviar mensajes a otros dominios.
- **Puerto TCP:** permite especificar el puerto TCP en el que nuestro servidor buscará el servidor remoto.

---

[32] Tomado del Manual de Seguridad de Microsoft

- **Número límite de conexiones:** podemos limitar el número de conexiones que se establecerán simultáneamente. Valor por defecto: 500.
- **Número límite de conexiones por dominio:** podemos limitar el número de conexiones que se establecerán simultáneamente a un dominio en particular. Valor por defecto: 100.
- **Tiempo de desconexión de conexiones inactivas:** tiempo que se permitirá que una conexión esté inactiva antes de desconectarla. El valor por defecto es 1 minuto.
- **Ubicación de mensajes erróneos:** Directorio en el que se almacenarán los mensajes erróneos (Bad Mail Directory).

- **Restricción de reenvío de correos**

Un aspecto fundamental para evitar spamming o envíos masivos e indeseados utilizando nuestro servidor de correo SMTP por parte de terceros malintencionados, es limitar el relay o reenvío de correos desde nuestro servidor. Esto podemos hacerlo basándonos en el criterio de la dirección IP o dominio del servidor que intenta enviar el correo desde nuestro SMTP.



2.1.3.7. Servicio de Noticias TNP

El servicio de noticias permite establecer en Internet, o en una red local, un foro de discusión en la que los participantes puedan exponer sus opiniones o formular abiertamente sus consultas o dudas. En este servicio se crean grupos en los que se presentan mensajes públicos a modo de notas en un tablón de anuncios. Estos grupos son denominados grupos de noticias.

Para que este grupo pueda funcionar, es necesario que exista un elemento de servidor que se encargue de recibir los mensajes y hacerlos accesibles en ese tablón virtual. Y, por supuesto, es imprescindible definir un formato de las notas y los mensajes para hacerlos inteligibles por el propio servidor y los participantes en el foro. El elemento servidor es el servidor de noticias, en nuestro caso IIS 5 y el formato de comunicación de la práctica totalidad de los servidores de noticias es el protocolo Network News Transfer Protocol (NNTP).

Los mensajes de noticias poseen una estructura similar a los de correo electrónico y constan también de una cabecera y un cuerpo. La cabecera incluye toda la información necesaria para publicar el mensaje en el tablón de noticias incluyendo el grupo o grupos en los que se desea ubicar el mensaje,

el remitente, y una descripción del tema tratado. El cuerpo del mensaje contiene la información que se desea transmitir.

- **Descripción de NNTP**[33]

La unidad de transmisión de información en el servidor de noticias es el mensaje, que en este ámbito denominaremos noticia o artículo. La unidad organizativa es el grupo de noticias que da soporte a un conjunto de noticias relacionadas desde el punto de vista temático. Los grupos, por su parte, están representados por un conjunto de directorios en el sistema de archivos de la máquina en la que reside, que van a servir de almacén para los mensajes o noticias contenidos en los grupos.



CIB-ESPOL

- **Directorios virtuales**

Como hemos comentado, el servidor almacena los mensajes en un conjunto de subdirectorios en el sistema de archivos de la máquina. Estos directorios están asociados con los grupos con una relación biunívoca y cada grupo está asociado a un directorio con el mismo nombre. Cada vez que se crea un grupo se añade un nuevo directorio.

---

[33] Tomado del Manual de Seguridad de Microsoft

- **El proceso de publicación de mensajes**

Los clientes de noticias acceden al servidor conectándose por el puerto 119, como comentamos anteriormente. Sin embargo, si se especifica que las conexiones deben ser encriptadas utilizando SSL, el puerto de comunicación es 563.

Cuando el cliente solicita la publicación de una noticia en un grupo, el servidor examina en primer lugar si el grupo en cuestión requiere la autentificación y procede a la comprobación de la identidad del usuario si la autentificación es necesaria. Si todo el proceso de identificación se culmina con éxito, se produce el flujo de mandatos entre cliente y servidor hasta que el mensaje se ha recibido completamente, tras lo cual el servidor coloca el archivo en el directorio correspondiente y actualiza los archivos de índice del grupo.



CIB-ESPOL

- **Administración de grupos de noticias**[34]

Los mensajes en un servidor de noticias se estructuran en grupos. Decimos que un grupo de noticias está moderado si existe un usuario, denominado moderador, que posee atribuciones para controlar la publicación de noticias.

Existen tres posibles estados de un grupo desde el punto de vista de la moderación.

- **Grupo no moderado:** los mensajes enviados al grupo de noticias son automáticamente publicados, sin supervisión.
- **Grupo moderado por el moderador por defecto:** antes de ser publicados los mensajes se envían a la dirección de correo. newsgroup@dominiopordefecto, que deberá ser utilizada por el moderador por defecto de nuestro servidor.
- **Grupo moderado por otro moderador:** se debe especificar la dirección de correo electrónico del usuario que actuará como administrador.



CIB-ESPOL

[34] Tomado del Manual de Seguridad de Microsoft

Cuando se envía un mensaje a un grupo de noticias moderado el servidor antes de publicarlo envía el citado mensaje al moderador. Si éste acepta el mensaje lo reenvía al servidor, que procederá a su publicación. En caso contrario, el mensaje no será publicado.



CIB-ESPOL

- **Políticas de caducidad de los mensajes**

A medida que los mensajes se van publicando en los grupos, y el tiempo va pasando, van quedando obsoletos y deberían ir eliminándose.

En servidores de noticias con gran tráfico, la gran cantidad de artículos puede hacer que tengamos problemas de almacenamiento. Para evitarlo, el servidor nos permite limitar el número máximo de mensajes que se aceptan por cada grupo de noticias.

Para que el servidor lleva a cabo esta tarea de purga de manera automática, IIS 5 nos permite definir, la fecha de caducidad de los mensajes de un grupo o el espacio máximo que un conjunto de mensajes pueden ocupar antes de que se proceda a la purga de los mismos. Estas especificaciones se denominan políticas de caducidad (Expiration Policies).

Las políticas de caducidad son aplicables a todos los mensajes del servidor o a un conjunto de grupos del mismo.



CIB-ESPOL

2.1.3.8. Active Server Pages

Active Server Pages (ASP) es un entorno de scripting que Internet Information Server proporciona para la creación de aplicaciones web. En definitiva, una página activa de servidor es un archivo con extensión .asp que contiene una combinación de código HTML y scripts que se ejecutarán en el servidor. Para que este proceso pueda llevarse a cabo es necesario que el servidor disponga de una extensión a tal efecto. Cuando un usuario solicita, en su navegador, la visión de una ASP, el servidor llama a la extensión para procesar la página. Esta extensión ejecuta los scripts de servidor, se comunica con los componentes, construye un documento HTML puro y lo envía por la red al cliente. De este modo el cliente recibe código HTML puro, sin que quede constancia alguna del script de servidor que lo ha generado.

Sin embargo, el desarrollo de aplicaciones web comienza a estar maduro para una evolución hacia técnicas de desarrollo como ASP+, que emplean los mismos paradigmas, pero haciendo un uso más racional de los conceptos de la componentización y el desarrollo orientado a objetos.

2.1.3.9. Administración mediante Web y administración delegada[35]

En IIS 5 se potencia la posibilidad de administración remota a través del WWW de cada uno de los servidores haciendo uso del navegador. Esto nos va a permitir, en primer lugar, poder resolver problemas que surjan en momentos en los que no estamos físicamente en contacto con la máquina Además, la administración basada en web va a permitir descargar en los Webmasters de cada uno de los servidores virtuales las tareas de administración de sus sitios, sin que tengan que acudir a nuestras instalaciones, algo que normalmente no suele ser deseable y que debe evitarse.

2.1.3.10. Seguridad

CIB-ESPOL

En términos de seguridad, Internet Information Server 4.0 ha demostrado ser un producto vulnerable, ya sea esto por la saña de los hackers contra productos de Microsoft o por sus propios "defectos" propios, que permiten los agujeros de seguridad en nuestros servidores, siendo así un peligroso y frágil componente del Windows 2000 Server. Por esto, es importante hacer

---

[35] Tomado del Manual de Seguridad de Microsoft

hincapié en estos problemas y específicamente la recomendación de prácticas de seguridad con el IIS 5.

A continuación reseñamos algunas de las mejoras que se han desarrollado para salvar las brechas de seguridad existentes en la versión anterior:

- Nuevos métodos de autentificación con encriptación hash.
- Mejoras a los servicios de Certificación ya incluidos en Windows NT Option Pack.
- Nuevos servicios de encriptación de 128 bits.
- Autentificación Kerberos integrada con Windows 2000



CIB-ESPOL

2.1.4. Comparación con Internet Information Server 4.0

A continuación, vamos a comparar las mejoras de seguridad del IIS 5.0 contra su predecesor IIS 4.0, a fin de establecer diferencias importantes en la evolución de estos productos y poder de esta manera conocer los beneficios que tenemos a nuestra disposición.

2.1.4.1. Internet Information Server 4.0[36]

IIS 4 fue el primer paso serio de Microsoft para dotarse de una plataforma competitiva en el ámbito de los servidores en Internet. Con la suma del Option Pack a Windows NT 4, se constituyó un nuevo sistema operativo que disponía de una interesante y completa plataforma de servicios Internet.

Desde entonces, y gracias en buena medida, a su simplicidad como plataforma de desarrollo de aplicaciones en servidor Internet Information Server ha ido ganando cuota de mercado de manera más que remarcable. Sin embargo, es necesario reconocer que el producto tenía en su versión 4 algunas carencias que era necesario subsanar si es que se deseaba competir en buenas condiciones, y sobretodo, si se deseaba estar preparado para los difíciles años venideros.



CIB-ESPOL

2.1.4.2. Servidor Internet Information Server 5.0 Incorporado[37]

Una diferencia fundamental del IIS 5.0 es que no es necesario instalarlo ya que Windows 2000 incorpora, en cualquiera de sus ediciones y sin ningún costo adicional IIS 5.0 como un servidor de Internet integrado. Internet

---

[36] Creación Propia

[37] Tomado del Manual de Seguridad de Microsoft

Information Services 5.0 es mucho más que un servidor Web. De hecho, bajo la protección de IIS se circunscriben prácticamente todas las prestaciones relacionadas con Internet de Windows 2000, desde los servicios de correo SMTP y de noticias NNTP, a los servicios Web y FTP.

2.1.4.3. Rendimiento

La primera diferencia que notamos, es que Internet Information Server ofrece un rendimiento muy superior. Y si en la estricta dinámica de servicio de páginas y ejecución de scripts de servidor la diferencia es notable, en lo referente a los servicios añadidos, tales como la Indexación o los servicios de Certificación, la mejora es radical. Certificate Services de Windows 2000 es una solución competitiva para la gestión de certificados digitales para los sitios Web que utilicen Secure Sockets Layer[38].



CIB-ESPOL

2.1.4.4. Seguridad Digest Authentication[39]

Una de las principales carencias de IIS 4 radicaba en la existencia de sólo dos métodos de autentificación: Basic Authentication y Windows NT

---

[38] Secure Sockets Layers: Protocolo diseñado por Netscape Comunications, permite cifrar la conexión y además garantiza la autentificación.

[39] Tomado del Manual de Seguridad de Microsoft

Challenge Response. La primera de ellas enviaba el nombre del usuario y su contraseña como texto sin encriptar en el proceso de autentificación. El segundo, por su parte, exigía de la utilización de Internet Explorer y, además era un problema cuando debía utilizarse en servidores Web ubicados en el interior de una red corporativa que se conectaba a Internet a través de un firewall[40] o proxy inverso. La idea es que, o perdíamos seguridad, o bien flexibilidad. IIS 5 incorpora un nuevo tipo de autentificación: Digest, que utiliza algoritmos de hashing[41] para encriptar la contraseña, pero que funciona a través de proxies y que sólo requiere que el navegador sea compatible HTTP 1.1.

2.1.4.5. Servidor de aplicaciones

En el ámbito de la estrategia .NET y sus Web Services cada vez más, los servidores Web van a constituirse en auténticos servidores de aplicaciones. IIS 4 democratizó el desarrollo de aplicaciones Web gracias a ISAPI y, sobre todo, a las páginas ASP. Internet Information Server 5 ha extendido la vocación de la versión anterior de simplicidad y facilidad de desarrollo, otorgando a la plataforma nuevos niveles de rendimiento y una mayor

---

[40] Componente de una red que impide que usuarios no autorizados accedan a nuestra red violando toda clase de seguridades.

[41] Sistema de Encriptado especial mediante el uso de cadenas de caracteres especiales.

seguridad. Las siguientes serían algunas de las mejoras incorporadas en IIS 5 respecto a un antecesor en lo que al desarrollo de aplicaciones Web se refiere:



CIB-ESPOL

- **Seguridad en la coexistencia de aplicaciones**

En IIS 4 era posible un mínimo aislamiento entre las distintas aplicaciones albergadas en un servidor. En IIS5 esta posibilidad se ha extendido en múltiples direcciones. El primer aspecto, y quizá el más reseñable, es el aislamiento de aplicaciones.

Por defecto, el servicio Web se ejecuta en un proceso propio (Inetinfo.exe), mientras que el resto de aplicaciones comparten un proceso separado de inetinfo (DLLHost.exe). En caso de caída de una de las aplicaciones que comparten dllhost, el resto de las aplicaciones también caerán, pero el servidor Web seguirá funcionando. Esta posibilidad es nueva en IIS 5. Existe una posibilidad de aislamiento aún mayor, que estriba en que cada se ejecuten en el ámbito de una instancia separada e independiente de DLLHost.dll.

La tercera posibilidad, por supuesto, es que las aplicaciones se ejecuten en el mismo proceso que los servicios Web. Esta posibilidad es la que ofrece un

mejor rendimiento, pero menos seguridad. Microsoft recomienda, que en aras del rendimiento, no se ejecuten más de 10 aplicaciones completamente aisladas[42].

- **Active Server Pages**

IIS 5 introduce diversas novedades en ASP. La primera de ellas es, en sí misma una mejora de rendimiento. En versiones anteriores del producto las páginas .htm eran procesadas más rápidamente que las .asp, por lo que si una página de servidor activo no contenía código de script era una práctica recomendable renombrarla para que tuviera la extensión asp.

La segunda novedad que comentaremos, es la integración con XML. Windows 2000 en sí, es una plataforma XML-Enabled, gracias a la incorporación del parser XML de Microsoft. IIS 5 permite, de serie, la utilización de XML en el servidor para generar documentos que puedan ser procesados para su envío al cliente o la transferencia a otros servicios, gestores de datos, aplicaciones, etc.

---

[42] Información proporcionada de los boletines de Seguridad de Microsoft

Una tercera incorporación de funcionalidad es la de poder encriptar el código asp. Si bien, en circunstancias normales, el código script de las páginas asp jamás es enviado al cliente, se han sucedido en Internet Information Server 4 numerosos agujeros de seguridad que han posibilitado a los hackers obtener el código fuente asp hasta que el administrador ha aplicado los parches o medidas correctoras adecuadas. En IIS 5 es posible codificar el código de script utilizando una herramienta que puede descargarse de msdn.microsoft.com, el Windows Scripting Encoder. Esta utilidad en línea de comandos, screnc.exe, permite la transformación de un archivo .asp en otro que contiene todo el código de script encriptado.

El motor de scripting de IIS 5 lo interpretará y decodificará directamente, previamente a su ejecución.



CIB-ESPOL

Por otra parte, IIS 5 permite la utilización de Windows Script Components, que permite tomar el código de script que tenemos en el interior de las páginas, extraerlo de las mismas y convertirlo en componentes "pseudo-COM" que se registran como si fuesen binarios y reutilizarse en las aplicaciones. En la misma web de msdn.microsoft.com/scripting se proporciona un asistente para regenerar los script components de manera sencilla, haciendo uso de especificaciones XML.

- **Administración más sencilla y potente**

IIS 5 ha crecido en dos aspectos en el ámbito de su administración. Se ha hecho más potente, pero al tiempo más sencilla.

En el ámbito de la simplicidad, IIS 5 incluye tres asistentes que van a facilitar la tarea del administrador :

- Web Server Certificate Wizard
- Permissions Wizard
- CTL Wizard.

Web Server Certificate Wizard permite la creación más sencilla de peticiones de certificados para SSL y su gestión posterior, sobre todo en lo relativo a la caducidad de ellos mismos. Cuando solicitamos la utilización de SSL en una Web, IIS 5 detecta si ya existe certificado y en caso contrario lanza el WCW.

Permission Wizard es una nueva herramienta que permite la gestión sencilla de los permisos y autentificaciones en una sede web. Todos los tipos de permisos se especifican de manera integrada en el mismo asistente.

Certificate Trust Lists (CTL) Wizard, permite la gestión de la lista de autoridades certificadoras de confianza para una cierta sede web.

La segunda novedad que comentaremos y que en este caso está dirigida al aumento de la potencia, es lo que se denomina Process Accounting o Logging. Esta nueva funcionalidad nos permite monitorizar como se están empleando los recursos del servidor en cada aplicación en términos de CPU. Se habilita o deshabilita siempre a nivel de servidor.



CIB-ESPOL

2.1.5. Seguridad en IIS 5

A continuación presentaremos un repaso general de los aspectos relativos a la seguridad de nuestros servidores Web con Windows 2000.

Sin embargo, antes de entrar en la descripción más o menos teórica de las características de seguridad, permítame abrir un cierto paréntesis ligado a la actualidad. Si hay un producto que ha sido objeto de ataques en el ámbito de Internet en los últimos meses ese es IIS. Este tipo de acciones lesivas se lleva a cabo siempre contra aquellos objetivos que pueden tener más repercusión y el éxito de Windows y de IIS se convierten en un destino apetecible para ese tipo de prácticas.

En los últimos meses se han sucedido ataques a IIS, de los cuales Code Red y Nimda son los más conocidos. En este sentido, MS ha desarrollado un nuevo paquete de servicios denominado Strategic Technology Protection Program (STPP), un programa que facilita servicios, productos y soporte para asegurar contra ataques los servidores IIS, manteniéndolos seguros a posteriori.

- **Diseño del IIS 5.0**

IIS 5.0 se lo ha diseñado de tal manera que sea mucho más seguro que su predecesor, pero puede mejorar. Todo Windows 2000 está ahora más volcado en Internet que Windows NT, y los mecanismos de seguridad del Sistema se han extendido en esta área. Windows 2000 incorpora un conjunto de nuevas tecnologías que auxilian en la tarea de hacer seguro IIS 5, a continuación las repasaremos de manera general.

- **Encriptación y Protocolos**

- **Términos Generales**

La criptografía es una disciplina compleja en la que se halla involucrada una enorme cantidad de matemática. En resumen, el objetivo de las técnicas

criptográficas es codificar mensajes de manera que cuando estos tienen que transmitirse por medios de comunicación no resistentes a intrusiones, sólo puedan ser interpretados (desencriptados) por el interlocutor, que conocerá las técnicas para deshacer la codificación llevada a cabo por el originador del mensaje. El mensaje que se encripta, y que en adelante denominaremos cifrado, no tiene porque contener texto ASCII exclusivamente, sino que puede ser un archivo binario de bases de datos, o cualquier otra información.

Cuando se encripta un mensaje, se utiliza una determinada llave criptográfica que debe ser conocida por el destinatario del mensaje para proceder a su desencriptación. De este modo, los mecanismos, esto es, los algoritmos de encriptación/desencriptación, son del dominio público, con lo que cualquier desarrollador o empresa puede generar programas que lleven a cabo las tareas citadas. En resumen, si no dispongo de la llave (en adelante clave), no puedo abrir el mensaje cifrado que aparecerá como un galimatías sin ningún sentido. De esta manera, existen dos claves: la utilizada por el remitente para cifrar el mensaje, y la utilizada por el destinatario para descifrarlo. Las claves del destinatario y el remitente pueden ser diferentes o iguales. Cuando son iguales, decimos que el algoritmo de encriptación es simétrico, mientras que cuando son diferentes decimos que son asimétricos o de clave pública. Los primeros son más eficientes desde el punto de vista de rapidez del proceso pero resultan más difíciles de usar por su falta de flexibilidad. Si utilizásemos

algoritmos simétricos en las transmisiones web deberíamos distribuir a todos los potenciales receptores una clave secreta, algo prácticamente inabordable. Es por ello que los más utilizados en es este ámbito son los algoritmos asimétricos.

Para que todo lo anterior tenga sentido, es necesario que el destinatario y el remitente del mensaje se conozcan entre sí inequívocamente, o de otro modo, que la identidad del propietario de la clave pública pueda ser conocida sin ninguna duda. Es decir, es preciso que se produzca una conexión autentificada en la que el intercambio de las claves pueda llevarse a cabo.

Evidentemente, este el segundo punto débil de nuestra comunicación y Windows 2000 Certificate Services vienen en nuestro auxilio para permitirnos solventar los problemas. El servidor, que adopta el papel de la autoridad de certificación (CA Certification Authority) tiene el papel de otorgar certificados de autenticidad a los participantes en una comunicación a través del web en la que se transfieren claves públicas. Estos certificados (Digital Certificates) son los que dan precisamente su nombre al servidor.

Los certificados son expedidos por autoridades certificadoras reconocidas por los dos sujetos de la comunicación. Un ejemplo de autoridad certificadora

es Verisign, pero cualquier servidor Windows que tenga instalados Certificate Services está facultado para crear certificados digitales.

La autoridad certificadora crea certificados que identifican al sujeto de la comunicación, una vez se comprueba su identidad. Los certificados incluyen la clave pública. Una vez el certificado ha sido creado, el sujeto certificado podrá enviar el mensaje que desee, cifrado con su clave privada, y paralela o previamente, enviará o pondrá a disposición del destinatario un certificado con su clave pública con la que podrá descifrar el mensaje.

IIS 5 incorpora un conjunto de tecnologías en las que se utiliza encriptación y certificados que no voy a comentar de manera exhaustiva, sino en sus aspectos más reseñables, y que hacen más seguro a Windows 2000.

- **Protocolos**



CIB-ESPOL

En este ámbito IIS soporta dos protocolos: SSL 3.0 y TLS (Transport Layer Security). El primero de ellos es el empleado para encriptar páginas web utilizando certificados, y es comúnmente conocido y utilizado desde IIS 4. En cuanto a TLS, se basa en SSL, y es empleado para encriptaciones a nivel más bajo que el de aplicación, es decir, por debajo del HTTP utilizado para la visualización de las páginas Web.

- **Certificados**

Los certificados digitales son una especie de DNI digitales que permiten identificar de manera inequívoca bien al cliente, bien al servidor en las comunicaciones entre ellos. SSL, PKCS #7 y PKCS#10, son protocolos en los que se utiliza de una u otra manera los certificados digitales. Los certificados suelen incluir información sobre nuestra compañía y la que generó el certificado, la autoridad certificadora.

Windows 2000 dispone de un servidor de certificados digitales incorporado que debe instalarse explícitamente, ya que no se instala cuando se emplean las opciones por defecto.

En el ámbito de IIS 5 los certificados pueden servir para autentificar al servidor, por ejemplo, para el envío de información sensible desde el cliente hacia el servidor, tal como la tarjeta de crédito. Para ello se requiere un certificado de servidor y la configuración del servidor como servidor seguro.

Además, los certificados permiten la autentificación de los clientes. Cuando un usuario que tiene un certificado digital accede a nuestro servidor, es posible mapear el mencionado certificado digital a una cuenta de Windows

de manera que no sea precisa la introducción de nombre de usuario y contraseña.



CIB-ESPOL

- **Modos de Validación**

Además de la autentificación Windows y la autentificación básica ya conocidas y utilizadas en IIS 4, IIS 5 incorpora un nuevo método de autentificación denominado Digest Authentication.

Una de las principales carencias de IIS 4 radicaba en la existencia de sólo dos métodos de autenticación: Basic Authentication y Windows NT Challenge Response. La primera de ellas enviaba el nombre del usuario y su contraseña como texto sin encriptar en el proceso de autentificación. El segundo, por su parte, exigía de la utilización de Internet Explorer y, además era un auténtico infierno cuando debía utilizarse en servidores web ubicados en el interior de una red corporativa que se conectaba a Internet a través de un cortafuegos o proxy inverso. La idea es que, o perdíamos seguridad, o perdíamos flexibilidad.

IIS 5 incorpora un nuevo tipo de autentificación: Digest, que utiliza algoritmos de hashing para encriptar la contraseña pero que funciona a través de proxies y que sólo requiere que el navegador sea compatible HTTP 1.1.

La anteriormente denominada NTLM o Windows NT Challenge/Response ahora recibe el nombre de Windows Authentication. En este tipo de validación, el nombre del usuario y la contraseña no se envían por la red, sino que lo que se transmite es algún tipo de información cifrada.

En IIS 5 esa información puede estar regida por el protocolo Kerberos, una funcionalidad estándar, asumida por el Directorio Activo (DA) en Windows 2000. Kerberos K5 ha reemplazado a NTLM como el protocolo primario para acceder a recursos con seguridad en Windows 2000. Kerberos no tiene el mismo conjunto de problemas que NTLM para la validación detrás de un firewall, ni con la compatibilidad con entornos no Microsoft, al tratarse de un protocolo estándar.



CIB-ESPOL

- **Modos de Autentificación**

Paralela y coordinadamente con los modos de validación, IIS permite diversos métodos para restringir el acceso a los contenidos basándose en la identidad del usuario. Por ejemplo, es posible que hagamos que los contenidos de una web sean públicamente accesibles facilitando el acceso anónimo, o restringirlo a ciertos usuarios.

Cuando permitimos acceso anónimo a una sede web lo que realmente estamos haciendo es no solicitar del usuario su validación y emplear para él una cuenta interpuesta, o alias, que es modificable, pero que por defecto siempre es IUSR_NombreMáquina.

Los usuarios que se conecten a un sitio web público con acceso anónimo tendrán acceso a aquellos archivos para los que la cuenta especificada tenga permisos NTFS. Si para un recurso el usuario no dispone de permisos, se le solicitará validación para que proporcione una identidad que sí los tenga.

- **Control de acceso**



CIB-ESPOL

Una vez que los usuarios han sido identificados, el siguiente paso es determinar a qué pueden acceder. El servidor web puede otorgar, para cada sitio web, subsitios, directorio virtual o archivo, permisos de acceso de lectura/escritura o ejecución. Estos son válidos para todos los usuarios que accedan a través del servidor Web.

Cada vez que otorgamos permisos en un sitio, todos los archivos y directorios de este heredarán los nuevos permisos, aunque tengan permisos individualizados asignados previamente.

Los permisos a archivos individuales y directorios deben ser establecidos con NTFS.

2.2. Seguridad en Windows 2000 Server

Mantener la seguridad de los sistemas conectados a Internet es una preocupación fundamental. Toda compañía, no importa si grande o pequeña, merece garantías de seguridad en todas las operaciones que realice a través de la red. El objetivo de esta sección es brindar pautas para mantener la seguridad usando el Strategic Technology Protection Program (STPP).

2.2.1. Introducción

CIB-ESPOL

A medida que aumenta la interconexión global del planeta, se está convirtiendo en realidad el sueño futurista de disponer de la información en cualquier lugar, en cualquier momento y en cualquier dispositivo. Las empresas y sus clientes sólo almacenarán sus datos confidenciales en Un entorno de este tipo si se les garantiza la seguridad del mismo[43].

[43] Creación Propia

Una encuesta sobre delitos y seguridad informáticos "Computer Crime and Security Survey" indica que el 85 por ciento de las grandes empresas y agencias del gobierno detectaron infracciones de seguridad[44].

En los meses recientes se ha producido una lluvia de ataques a entornos informáticos, muchos de ellos a través de Internet y a equipos con el sistema operativo Microsoft® Windows®. Sin embargo, éstos son sólo los problemas de seguridad más notorios a los que se enfrentan las empresas en la actualidad. En este estudio se describen las distintas amenazas de seguridad para dicho entorno y se explica la mejor manera de protegerse.

Independientemente de cuál sea el entorno, es muy recomendable tomarse en serio la seguridad. Muchas organizaciones cometen el error de subestimar el valor del entorno de tecnología de la información (TI), generalmente porque no tienen en cuenta costos indirectos importantes. Si el ataque es suficientemente grave, las pérdidas podrían ascender al valor de la organización. Por ejemplo, un ataque que modifique sutilmente el sitio Web corporativo para anunciar malas noticias falsas podría hundir el valor en bolsa de la corporación. Al evaluar los gastos de seguridad, debe incluirse



CIB-ESPOL

[44] Encuesta realizada por el FBI y el CSI (Computer Security Institute) en el año del 2001.

también los costos indirectos asociados a cualquier ataque, así como los costos derivados de la pérdida de funcionalidad de los sistemas de TI.

Los sistemas informáticos más seguros del mundo son los que están completamente aislados de los usuarios y de otros sistemas. Sin embargo, en el mundo real normalmente necesitamos sistemas informáticos que funcionen en red, a menudo en redes públicas. A continuación identificamos los riegos inherentes a un entorno de red y determinamos el nivel de seguridad apropiado para el entorno; también indicamos los pasos necesarios para alcanzar ese nivel de seguridad.

2.2.1.1. Microsoft Operations Framework (MOF)[45]

Para que las operaciones del entorno funcionen de la forma más eficaz, se deben administrar de forma efectiva. Para ayudarle, Microsoft ha desarrollado Microsoft Operations Framework (MOF). Las instrucciones de MOF ayudarán a garantizar la seguridad, la confiabilidad, la disponibilidad, el soporte y la capacidad de administración de sus sistemas de producción fundamentales.

---

[45] Tomado de http://www.microsoft.com/spain/technet/recursos/articulos/secmod220.mspx

El modelo de procesos MOF se divide en cuatro cuadrantes integrados de la manera siguiente:

1. Cambio.
2. Funcionamiento.
3. Soporte.
4. Optimización.

CIB-ESPOL

Juntas las fases forman un ciclo de vida en espiral, como se puede observar en la figura 2.1, que se puede aplicar a todo, desde una aplicación específica a un entorno de operaciones completo con varios centros de datos.

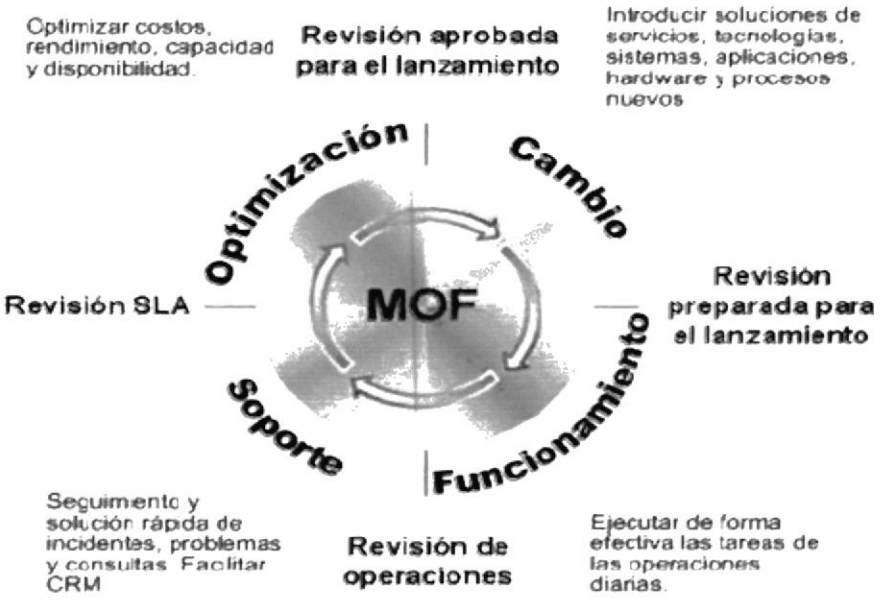


Figura 2.1. El Modelo de Procesos MOF[46]

[46] Tomada de http://www.microsoft.com/technet/itsolutions/cits/mo/mof/moftml.mspx

- **Modelo de procesos MOF**

El modelo de procesos se apoya en 20 funciones de administración de servicios (SMF, Service Management Functions) y un modelo de equipos y otro de riesgos, ambos integrados. Cada cuadrante se apoya en la revisión de administración de operaciones correspondiente (también denominada hito de revisión), en la que se valora la eficacia de las funciones de administración de servicios del cuadrante.

- **Implementar y mantener la seguridad**

En octubre de 2001, Microsoft lanzó una iniciativa denominada Programa Estratégico de Protección de Tecnología (STPP, Strategic Technology Protection Program). El objetivo de este programa es integrar los productos, los servicios y el soporte de Microsoft dedicados a la seguridad. Microsoft divide el proceso de mantener un entorno seguro en dos fases relacionadas: Implementar la seguridad y mantener la seguridad.



CIB-ESPOL

2.2.1.2. Definición de riesgo de seguridad

A medida que evolucionan los sistemas de TI, también lo hacen las amenazas a la seguridad que estos pueden sufrir. Para proteger el entorno de forma eficaz contra los ataques, es necesario conocer con detalle los peligros que se pueden encontrar. Al identificar las amenazas a la seguridad, se deben tener en cuenta dos factores principales: los tipos de ataques que seguramente se sufrirá y los lugares donde pueden tener lugar.

Muchas organizaciones no tienen en cuenta el segundo factor, pues asumen que un ataque grave sólo puede venir del exterior (normalmente, a través de su conexión a Internet).

Muchas empresas pueden no estar al corriente de que se están dando ataques internos, básicamente porque no comprueban si existen.



CIB-ESPOL

- **Administración de riesgos**

No existe un entorno de TI totalmente seguro y al mismo tiempo útil. Al examinar el entorno, se deberá evaluar los riesgos que sufre actualmente, determinar un nivel de riesgo aceptable y mantener el riesgo a ese nivel o por

debajo del mismo. Los riesgos se reducen aumentando la seguridad del entorno.

Para entender los principios de la administración de riesgos, es necesario entender algunos términos básicos utilizados en el proceso de los mismos. Estos incluyen recursos, amenazas, vulnerabilidades, explotaciones y contramedidas.

- **Recursos:** un recurso es cualquier elemento del entorno que intente proteger. Puede tratarse de datos, aplicaciones, servidores, enrutadores e incluso personas. El objetivo de la seguridad es evitar que los recursos sufran ataques.
- **Amenazas:** una amenaza es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos.
- **Vulnerabilidades:** una vulnerabilidad es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil.
- **Explotación:** una amenaza que se aprovecha de una vulnerabilidad del entorno puede tener acceso a un recurso. Este tipo de ataque se denomina explotación.

- **Contramedidas:** las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en el entorno.

2.2.1.3. Administrar la seguridad con la Directiva de Grupo de Windows 2000[47]

Una vez determinado el nivel de riesgo apropiado para el entorno y establecida la directiva de seguridad general, deberá empezar a asegurar el entorno. En un entorno basado en Windows 2000, esto se lleva a cabo principalmente por medio de la Directiva de grupo.

Muchos de los valores de configuración de la seguridad se definen en Windows 2000 a través de la Directiva de grupo, cuyo fin es controlar el comportamiento de los objetos en el equipo local y en el servicio de directorio Active Directory™. Es importante asegurarse de que estas directivas están correctamente configuradas y de que se supervisan para que no las modifiquen sin autorización previa.



CIB-ESPOL

[47] Tomado de http://www.microsoft.com/spain/technet/recursos/articulos/secmod220.mspx

2.2.1.4. Asegurar servidores basándose en su función

Se deben tener en cuenta también las directivas de línea de base que pueden definirse para todos los servidores miembros y controladores de dominio de la organización, y otras modificaciones que se pueden aplicar a funciones específicas del servidor.

Este enfoque permite que los administradores bloqueen los servidores por medio de directivas de línea base centralizadas, aplicadas de forma coherente a todos los servidores de la organización. Las directivas de línea base sólo permiten una funcionalidad mínima, pero sí permiten que los servidores se comuniquen con otros equipos en el mismo dominio y su autenticación a través de los controladores de dominio. A partir de este estado más seguro, se pueden aplicar otras directivas incrementales más, que permiten que cada servidor realice únicamente las tareas específicas definidas por su función. La estrategia de administración de riesgos determinará si es apropiado para el entorno que se lleven a cabo estos cambios.

2.2.1.5. Administrar revisiones[48]

Una de las principales medidas de protección contra ataques es mantener el entorno actualizado con todas las revisiones de seguridad necesarias, las que pueden ser necesarias tanto para servidores como para clientes. Es importante explicar la forma de obtener lo antes posible las revisiones nuevas, implementarlas rápidamente y de forma confiable en toda la organización, y confirmar que están instaladas en todos los equipos.



CIB-ESPOL

[48] Tomado de http://www.microsoft.com/spain/technet/recursos/articulos/secmod220.mspx

CAPÍTULO 3

3. COMPONENTES DE SEGURIDAD NECESARIOS PARA REALIZAR UN ANÁLISIS DE UNA ORGANIZACIÓN ORIENTADA A LA IMPLEMENTACIÓN DE WINDOWS 2000 SERVER

Este capítulo enfoca la definición de los componentes de seguridad que necesitan ser sobrentendidos para el desempeño de un análisis de seguridad en su organización. Se indican además lineamientos generales sobre cómo realizar un análisis preliminar de los recursos de su organización. Además se explica la relación entre las amenazas, exposiciones, vulnerabilidades y las medidas de seguridad.

Los conceptos básicos expuestos en este capitulo ha sido tomados del Manual de Seguridad llamado "Securing Windows 2000 Server" a fin de detallar de una manera más tecnica todo lo referente a los componentes del Sistema Operativo antes Mencionado.

3.1. Políticas básicas de Windows 2000 Server

En esta sección se detallarán los cambios necesarios para fortalecer los roles del servidor. Muchas de las configuraciones que aparecen en el MSBP[49] también son aplicadas para el controlador de dominio de los roles del servidor. Bajo este esquema, para los servidores miembros, la configuración de políticas de grupo descritas están almacenadas en la plantilla de seguridad baseline.inf. Esta plantilla se importó en el MSBP a la que se une el MSOU[50] .

El MSBP es un área estratégica de dirección de riesgo enfocada a desarrollar configuraciones comunes para todos los servidores miembros que incluyen las políticas de auditoría, la configuración de servicio, las políticas que restringen el acceso al registro, los sistemas de archivos y otras configuraciones específicas de seguridad.



CIB-ESPOL

[49] Member Server Baseline Policy

[50] Member Server Organizational Unit

3.1.1. Políticas Básicas

El proceso de configuración del nivel de dominio define las configuraciones más comunes para todos los servidores miembros. Se puede realizar esto creando un GPO[51] unido al Servidor Miembro OU[52], lo cual es conocido como una política básica. El GPO automatiza los procesos de configuración específica de seguridad en cada servidor.

3.1.1.1. Auditoría y Configuración de Eventos Log[53]

Un archivo de auditoría puede ser creado con cualquier usuario cuando este realice alguna acción específica.

Por ejemplo, la modificación de un archivo o una política puede activar una entrada en el archivo de auditoría. La auditoría muestra la acción realizada, la cuenta de usuario asociada y la fecha y hora de la acción. Se puede auditar estas acciones como exitosa o fallida.



CIB-ESPOL

---

[51] GPO: Políticas de Grupo del Windows 2000 Server

[52] OU: Unidad Organizacional

[53] Log: Archivo de auditoría donde se registran todas las operaciones realizadas por un usuario determinado en un sistema informático en un momento determinado.

El estado del sistema operativo y sus aplicaciones en una computadora es dinámico. Por ejemplo, los niveles de seguridad pueden requerirse para cambiar temporalmente la resolución de habilitación inmediata de una administración o de un problema de la red; este cambio puede a menudo ser realizado sin reserva alguna.

Esto significa que una computadora ya no puede reunir los requisitos de seguridad de la empresa. El análisis regular le permite a un administrador rastrear y asegurar un nivel adecuado de seguridad en cada computadora como parte de un programa de manejo de riesgo en una empresa. Esto le permite a un administrador tener buenos niveles de seguridad y mucho más importante, que pueda detectar cualquier falla de seguridad que pueda ocurrir en el sistema en cualquier momento.

La auditoría de seguridad es sumamente importante para cualquier sistema de una empresa, los archivos de auditoría pueden dar la indicación de que ha ocurrido alguna ruptura de seguridad.

A menudo los eventos fallidos que se registran en los archivos de auditoría son mucho más informativos que los eventos exitosos, ya que comúnmente los fracasos indican un error. Por ejemplo, si un usuario ingresa con éxito en el sistema, esto habría sido considerado normal en el archivo log. Sin

embargo, si un usuario intenta ingresar al sistema sin éxito varias veces, esto puede indicar que alguien está tratando de irrumpir en el sistema utilizando el usuario (User- ID[54]) de otra persona, lo cual se registrará en el log como un evento fallido.

El evento log registra acontecimientos sucedidos en el sistema y contiene políticas de grupo utilizadas para definir atributos relacionados a la aplicación, seguridad y auditoría del sistema, tales como un tamaño máximo del archivo, derechos de acceso para cada log y la configuración y sus métodos de retención de información. Estas configuraciones se realizan en el MSBP y se aplican a todos los servidores miembros en el dominio.



CIB-ESPOL

3.1.1.2. Fortaleciendo los procedimientos adicionales de los Servidores Miembros

La mayoría de las medidas de prevención utilizadas para fortalecer los servidores son aplicadas a través de las políticas de grupo y existen configuraciones adicionales que son difíciles o imposibles de aplicar. A continuación describiremos cómo algunos de estas medidas de prevención adicionales son implementadas manualmente, como cuentas seguras, debido

---

[54] User-ID: Identificación de un usuario dentro de una red informática, también conocido como usuario de red, que debe tener su respectiva clave de acceso.

a que estas no se pueden ejecutar a través de dichas políticas ya que no han sido configuradas para ello dentro del GPO; y cómo otras son implementadas utilizando shell scripts[55], como también filtros IPSec[56].

3.1.1.2.1. Fortaleciendo Procedimientos Manuales

- **Cuentas de Servicio Seguras**

Los servicios típicos de Windows 2000 corren bajo la cuenta del Sistema Local, pero estos también pueden correr bajo un usuario de dominio o una cuenta local. Se debería utilizar cuentas locales siempre que sea posible sobre cuentas de usuario de dominio.

Un servicio ejecutado bajo el contexto de seguridad de su cuenta de servicio es la mejor opción de seguridad, así si un atacante compromete un servicio en un servidor miembro, la cuenta de servicio puede utilizarse potencialmente para atacar a un controlador de dominio. Al determinar qué cuenta se utiliza como una cuenta de servicio, se asegura que los privilegios asignados se limiten a lo que se requiere para el funcionamiento exitoso del

---

[55] Segmentos de código que se ejecutan a nivel del núcleo del sistema operativo

[56] Protocolo Seguro de Internet

CIB-ESPOL

servicio. La tabla 3.1[57]. (Anexo D) explica los privilegios inherentes a cada tipo de cuentas de servicio.

- **Configurando Políticas IPSec**

El Protocolo Seguro de Internet (IPSec) fue inicialmente diseñado para encriptar datos cuando viajan entre dos computadoras, protegiéndolos de una modificación e intercepción si alguien lo pudiera ver en la red. IPSec es una línea importante de defensa interna, de la red privada y de ataques externos.

Aunque la mayoría de las estrategias de seguridad de red se han enfocado en prevenir ataques de afuera de la red de una organización, mucha información sensible puede perderse por ataques internos que interceptan datos en la red. La mayoría de los datos no son protegidos cuando estos viajan por la red, así que los empleados, miembros del personal de apoyo, o visitantes pueden ser capaces de obstruir su red y copiar datos para un análisis posterior.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

[57] Tomado del Manual "Securing Windows 2000 Server" Capitulo 7, pagina 250

Mientras IPSec puede ser utilizado para encriptar datos en la red, también puede utilizarse como una manera excelente de asegurar las capas de red. Esto se puede lograr utilizando políticas de IPSec para bloquear una interfase de red. Los firewalls localizados entre la red de la organización y el Internet no ofrecen ninguna protección contra las amenazas internas, así que utilizando IPSec para bloquear puertos innecesarios a un nivel significativo de seguridad para los recursos corporativos, es una buena opción de protección ante potenciales ataques.

El filtro IPSec de Windows 2000 Server no fue diseñado para reemplazar a un firewall.

Los filtros IPSec deben ser considerados como una herramienta para fortalecer servidores.

Además, los filtros IPSec pueden ayudar a contener y controlar tráfico de código malicioso de gusanos y virus.

Para obtener un nivel alto de seguridad utilizando filtros IPSec, la computadora debería ser desconectada de la red durante su reiniciación. El tiempo exacto en el que los filtros IPSec estén activos, depende de muchos factores específicos en la configuración del servidor y el tamaño de la Política

de IPSec. Una comprobación local debe ser realizada para determinar un intervalo de tiempo seguro antes de reconectar sus servidores a la red. Si el Test inicial no puede ser realizado, un firewall o router[58] debe ser utilizado para restringir tráfico entrante sólo a los puertos permitidos.

3.2. Componentes administrativos de la seguridad de riesgo.

3.2.1. La necesidad de un programa estratégico de seguridad.

La seguridad es un equilibrio entre mantener la facilidad de uso de los recursos en su organización y controlar el acceso a esos recursos. Un programa de seguridad que empuje el balance demasiado lejos hacia el mando puede molestar a los usuarios con políticas que los limiten de hacer eficazmente su trabajo. Realmente, un programa de seguridad que sea flexible puede crear una actitud satisfecha a sí mismos entre los usuarios con respecto a la seguridad en el lugar de trabajo y puede dar más oportunidades a los ataques.

---

[58] Router: Un router o ruteador permite segmentar una red informática permitiendo así una mejor distribución de las rutas por las que debe pasar la información.

La comunicación sobre la importancia de la seguridad en la organización es esencial para evitar otros problemas en la emisión de políticas de seguridad. Si las políticas y los planes de seguridad se implementan "a medias", podría haber problemas en el futuro.

Un factor de éxito crítico para el establecimiento de una infraestructura segura involucra el desarrollo de un proceso administrativo de seguridad de riesgo. A través de la identificación eficaz del riesgo, la valoración, el manejo, la mitigación y la ejecución, así como el plan de contingencia, se puede ayudar a que se reduzca la probabilidad de que un riesgo dado aparezca y se pueda minimizar el impacto o la consecuencia debido a que el riesgo de seguridad será mejor comprendido.

Realizando un análisis de riesgo de seguridad específico saldrán a flote los problemas críticos de seguridad que requieren atención y un curso de acción a implementarse para el caso de alguna eventualidad. Un riesgo de seguridad es provocado cuando una amenaza toma ventaja de una vulnerabilidad la que a su vez causa un daño a un recurso de su organización. La creación de un plan de contingencia permite crear políticas y procedimientos de seguridad para proporcionar una protección y el acceso a la reactivación de la administración de la seguridad de riesgo.

CIB-ESPOL

Al Implementar, ejecutar e ir continuamente perfeccionando los planes de seguridad de su organización se está prevenido ante alguna posibilidad de ataque o vulnerabilidad. Los programas de seguridad deben cambiar con el tiempo porque ellos requieren constante atención para supervisar su efectividad y determinar cuando las nuevas políticas y procedimientos deben ser implementados. Los programas de seguridad también deberían ser considerados para potenciales derivaciones legales a través de planes de respuestas a incidentes entallados al ambiente corporativo, como la posibilidad de conseguir un fracaso de seguridad y como esto podría presentar un problema serio. Para lograr determinar más fácilmente los costos involucrados es necesario realizar una apropiada valoración de los recursos bien definidos. El costo de la mitigación debe pesarse contra el potencial impacto de lo que puede pasar al recurso si se daña o es comprometido.

CIB-ESPOL

Si la pérdida de datos sensibles de la compañía impactara seriamente su productividad, entonces la inversión requiere una protección significativa. Si la pérdida de esos datos no es perjudicial para la organización, entonces tales datos necesitan protección mínima y la inversión para protegerlo será menor.

Las ocho consideraciones básicas que se necesitan para el proceso de valoración de seguridad de riesgo son:

1. **Requisitos de seguridad para los recursos**. Defina todos los componentes de su infraestructura organizacional que requiera cualquier nivel de protección, incluso los sistemas, redes, aplicaciones y datos comerciales. La valoración de los recursos necesita ser evaluada en una forma cuantitativa y cualitativa para un apropiado plan de medidas de prevención o resguardos.
2. **Análisis de la amenaza.** Crear una lista de exposiciones conocidas y determinar la probabilidad de una potencial amenaza que se levanta de cada una. Una exposición es un medio que puede utilizarse por una amenaza para hacer uso de una vulnerabilidad en su ambiente. Una lista compilada de las mayores agentes amenazadores en su ambiente exige que se realice un análisis apropiado de las amenazas. Una amenaza es cualquier peligro potencial a la información o a los sistemas en su entorno. Un agente de amenaza es la persona o el proceso que ataca la red a través de un puerto vulnerable en el firewall o un proceso utilizado para el acceso a los datos que en cierto modo viola su política de seguridad.
3. **Identificación de las exposiciones.** Analizar el porcentaje de pérdida de los recursos producido por cada una de las amenazas identificadas. Al

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

identificar y definir la pérdida de valor potencial de cada exposición constituye un componente crucial en el análisis de seguridad de riesgo.

4. **Valoración de vulnerabilidad**. Desarrollar una lista comprensiva de todas las vulnerabilidades conocidas que puedan utilizarse contra esos recursos y que requieran algún nivel protección. Una vulnerabilidad es alguna debilidad en un sistema de información o en sus componentes (por ejemplo, procedimientos de seguridad del sistema, diseño de hardware, diseño de software y controles internos) que podrían explotarse.
5. **Desarrollo de las Medidas de Prevención.** Desarrollar una apropiada medida de prevención para los riesgos de seguridad, significa que sea está resguardando los recursos de la organización.
6. **Prueba de penetración.** Utilizar la prueba de penetración para ayudar a identificar las maneras en que un individuo desautorizado podría ganar acceso a la organización. Los métodos comunes de pruebas de penetraciones incluyen:
   - Examinar recursos externos para identificar blancos potenciales a comprometer.
   - Ingeniería social para localizar a individuos que pueden ser engañados para que revelen sus contraseñas o alguna forma de información de seguridad que proporcionaría accidentalmente, la misma que seria clasificada como información secreta.

- Haciendo pruebas de penetraciones para determinar si el acceso físico puede ser obtenido fácilmente.

Estas pruebas son útiles para aumentar la atención que una organización debe poner en las políticas de seguridad. Una de las más grandes consideraciones para realizar una prueba de penetración está en identificar un agente externo honesto para que realice estas pruebas.

7. **Respuestas a incidentes.** Un plan de respuestas a incidentes perfilará procedimientos específicos a seguir en tanto se aprende más sobre un ataque en su organización. Generalmente, la naturaleza del ataque determinará el orden en el que se siguen los procedimientos que se definieron en su programa de seguridad.
8. **El alcance del esfuerzo de trabajo para asegurar sus recursos.** Definir la cantidad total de trabajo, incluyendo tiempo, esfuerzo y dinero requerido para proporcionar lo mejor para la seguridad y para mantener la infraestructura global utilizable desde el soporte y las perspectivas finales del usuario de la compañía. Un análisis costo-beneficio para la seguridad debería ser derivado de un análisis apropiado de la seguridad de riesgo en conjunto con los recursos para el costo total de los inversionistas o el retorno de la inversión de la organización.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

3.2.2. Recursos

Un recurso es algo en el entorno de la organización del que puede requerir algún nivel de protección. Esto podría incluir artículos del equilibrio de las aplicaciones de software o hardware y otros artículos menos tangibles como datos o incluso a las personas. El propósito de la seguridad es impedir que los recursos sean comprometidos y proteger la confidencialidad, integridad y disponibilidad de los datos. Todas las corporaciones están concientes con los riesgos que son perjudiciales cuando se consigue que sus datos sean modificados, los mismos que degradarían la integridad de la información comercial.

CIB-ESPOL

Un aspecto importante de la administración de la seguridad de riesgo está determinado por el valor de cada recurso en su organización, el valor de la información que cada recurso contiene y cómo cada recurso se relaciona con otros en su entorno.

El valor global asociado de cada recurso determinará el tiempo, esfuerzo y costo de seguridad de estos basados en el nivel de seguridad que se exige para proporcionar a cada recurso con la protección adecuada. Hay que tener presente que los recursos pueden tener un nivel asociado de dependencia. Además se debe considerar cómo estos recursos son autenticados, o cómo

los usuarios son autorizados para ganar acceso a cada recurso y los datos que están expuestos. Por ejemplo, una contraseña débil en una computadora portátil puede proponer un riesgo financiero significante si es comprometido.

Los recursos también deben ser clasificados según las medidas de protección que cada uno requiere. Estas medidas incluyen:

- Medidas de prevención: que previenen a los recursos de ser dañados, alterados, o robados. Las medidas preventivas pueden ir desde cerrar con llave una puerta del cuarto donde esta el servidor hasta un alto nivel de seguridad soportados por las políticas de seguridad.
- Medidas de detección: que permiten la detección de los recursos que han sido dañados, alterados, perdidos o robados. Las medidas de detección también incluyen mecanismos para determinar cómo estuvo comprometido un recurso y específicamente quién produjo el daño. Existen varias herramientas que están disponibles para facilitar la detección de intrusiones, daños o alteraciones y los virus.
- Medidas de reacción: que permiten la recuperación de los recursos, aun si un recurso esta perdido o dañado.

Estas se clasifican como medidas de protección y deben integrarse a los diferentes tipos de medidas de prevención, las cuales ayudan a mitigar el

riesgo potencial de un recurso que está comprometido. Una medida de prevención se diseña para eliminar una vulnerabilidad o reducir el riesgo de una amenaza que se aprovecha de una vulnerabilidad en el ambiente computacional.

Para realizar medidas de prevención para proteger los recursos de su organización, se debe en primer lugar entender cómo los recursos de su organización pueden estar comprometidos definiendo amenazas y riesgos que son relevantes para los mismos.



CIB-ESPOL

3.2.3. Relación entre las Amenazas, Exposiciones, Vulnerabilidades y Medidas de prevención.

Si un agente amenazante da lugar a una amenaza y a exposiciones de una vulnerabilidad, envuelve un ataque potencial a la seguridad. El ataque puede dañar el recurso degradando su confidencialidad, integridad, o disponibilidad. Por consiguiente, el ataque causa una exposición potencial a la pérdida de la compañía. Sin embargo, estas exposiciones pueden ser minimizadas con el uso de las medidas de prevención.

Por ejemplo, si una compañía sólo tiene un software antivirus en sus servidores y la actualización del antivirus no se realiza, esto crea una

vulnerabilidad. La compañía se vuelve vulnerable a los ataques de virus y las amenazas que un virus representa en su entorno puede interrumpir su productividad.

El riesgo es la probabilidad de que un virus se presente en el ambiente y cause daño. Porque existe la posibilidad de perder o adulterar datos en un ataque de virus, la compañía tiene ahora una exposición. Las medidas de prevención para esta situación son asegurar que el software antivirus sea instalado en todas las computadoras de la empresa y realizar las respectivas actualizaciones.

Los términos de administración de seguridad a veces pueden ser difíciles de entender. La tabla 3.2[59]. (Anexo E) proporciona una vista consolidada de los componentes de la seguridad más importantes en la administración de la seguridad.

La relación entre las amenazas, las vulnerabilidades y los riesgos pueden ser inicialmente un concepto duro de comprender. Cada amenaza y vulnerabilidad identificadas dentro de su organización deben ser calificadas y ordenadas según una norma, como baja, media, o alta. La clasificación

---

[59] Tomado del Manual "Securing Windows 2000 Server" Capitulo 7, pagina 265

ESCUELA SUPERIOR POLITECNICA DEL LITORAL ESPOL
CIB-ESPOL

jerárquica varía entre las organizaciones y a veces incluso dentro de la misma organización.

Por ejemplo, la amenaza de un terremoto es significativamente más alta para las oficinas cerca de una línea de la falla que en otra parte. Similarmente, la vulnerabilidad del daño físico a un equipo sería muy alto para una organización que produce sensitivos y frágiles circuitos electrónicos, pero el mismo nivel de vulnerabilidad para una compañía constructora puede ser más bajo.

La Matriz de la Administración de Riesgo puede ayudarle a evaluar amenazas y su impacto frente a su organización. El nivel de riesgo en su organización aumenta con el nivel de las amenazas y las vulnerabilidades, como se indica figura 3.1.:

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

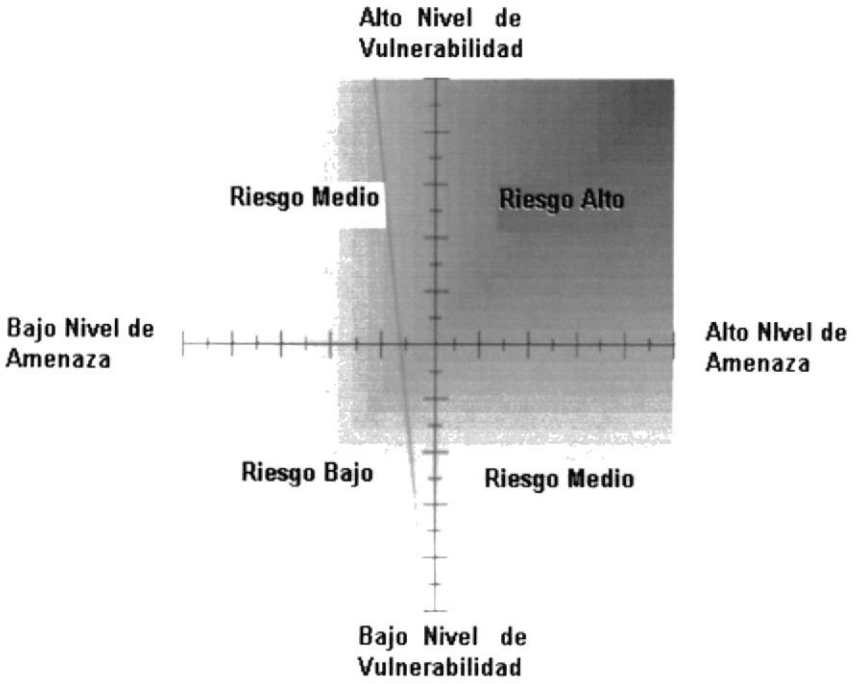


Figura 3.1. La Matriz de la Administración de Riesgo[60]

La matriz de la administración de riesgo puede utilizarse como una herramienta de la siguiente manera. Por ejemplo, su compañía podría tener dos tipos diferentes de sitios web; uno voluntario sin fines de lucro realmente un sitio informativo, o uno de servicios financieros que podría ser un sitio transaccional que proporcionaría un lugar para realizar negocios o transacciones de ventas para sus clientes.

---

[60] Tomado de http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofpm.mspx

Cada sitio web tendrá niveles de diferentes de riesgos. Por ejemplo, el sitio web informativo puede que tenga un nivel de amenaza bajo porque contiene información que si son robadas o dañadas estas no son cruciales para el funcionamiento del negocio. Esto pone al sitio web informativo en un cuadrante de riesgo bajo.

Por otro lado, el sitio web de servicios financieros podría estar en cuadrantes de riesgo medio o alto. Los atacantes pueden beneficiarse considerablemente si los datos financieros son comprometidos o robados, lo que hace que el nivel de amenaza sea alto. Sin embargo, si los servidores web tienen los apropiados service pack[61] y hotfixes[62] entonces este sitio web sería un poco menos vulnerable y puede que caiga en el cuadrante de riesgo medio. Si los servidores Web no cuentan con los service packs y hotfixes entonces el sitio web sería muy vulnerable y caería en el cuadrante de alto riesgo.

La figura 3.2. proporciona un modelo teórico que puede ser utilizado para determinar varias amenazas, motivos y objetivos, métodos, exposiciones, y vulnerabilidades que podrían manejarse contra la organización en un ataque.

---

[61] Service Pack: Parche de seguridad de algún sistema o programa informático

[62] Hotfix: Código parche para los productos informáticos.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL ESPOL
CIB-ESPOL

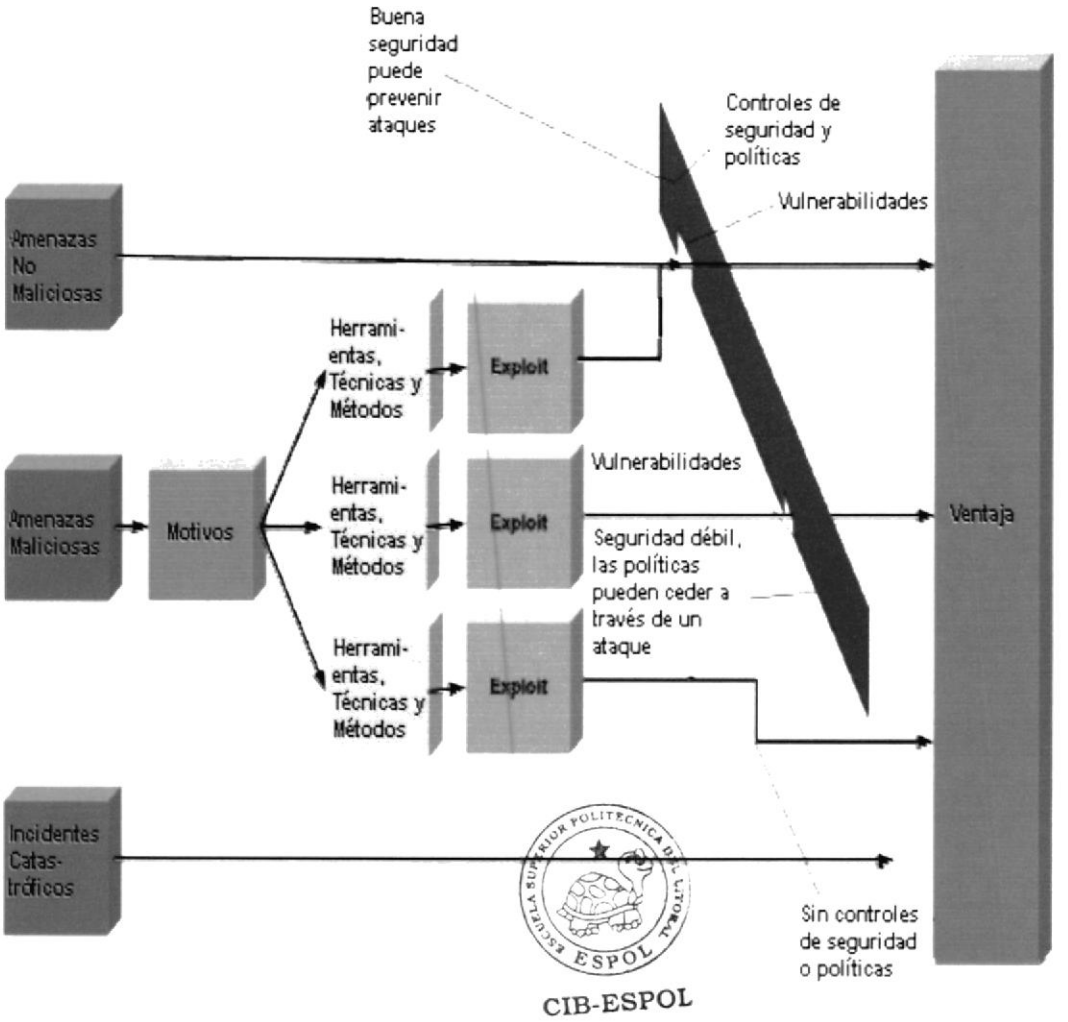


Figura 3.2. El camino para comprometer los recursos[63]

La figura 3.2. describe un simple camino lógico que muestra cómo los agentes amenazantes pueden comprometer los recursos de su compañía. Se muestran los tres tipos de clasificación de las amenazas en el lado izquierdo de la figura. La clasificación de las amenazas identifica quién es el atacante o

[63] Tomada de http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofpm.mspx

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

qué agentes amenazantes están iniciando el ataque. Éstos incluyen amenazas no maliciosas, amenazas maliciosas e incidentes catastróficos.

Los agentes amenazantes tienen motivos y objetivos típicos para lograr intentar comprometer los recursos, como alguna ganancia financiera. Los agentes amenazantes usan herramientas específicas, técnicas y métodos para aprovecharse de ciertas vulnerabilidades en la seguridad de los recursos.

Estas herramientas son en algunos casos orientadas a violar alguna vulnerabilidad específica, como también pueden afectar a muchas otras. El camino a seguir por el atacante necesariamente involucra algún método o técnica antes descrito para así poder hacerse del sistema atacado.

Para prevenir todo esto se deberían establecer políticas de seguridad que reduzcan ostensiblemente los riesgos de ataques, y de esa manera minimizar el riesgo de que sucedan hechos catastróficos como veremos mas adelante. Recordemos que la seguridad completa no existe, pero si se puede disminuir el peligro. El grafico anterior representa el camino antes descrito para poder violentar un sistema. Es importante conocer esto para poder determinar en que punto debemos implementar un método que permita asegurar nuestros recursos.

3.2.3.1. Tipos de Amenazas

Una amenaza es una persona o cosa que tiene el potencial para acceder a los recursos y causar daño. Las amenazas pueden originarse de dos fuentes primarias: los humanos y los eventos catastróficos. Las amenazas humanas pueden clasificarse en dos categorías: maliciosas y no maliciosas. Los ataques no maliciosos normalmente provienen de los usuarios y empleados que no son entrenados en el manejo de las computadoras y quiénes no son conscientes de varias amenazas de la seguridad computacional. Los ataques maliciosos normalmente vienen de personas externas o ex-empleados quienes tienen un objetivo específico a lograr. La tabla 3.3. hace referencia a los diferentes tipos de amenazas existentes:

Amenazas	Ejemplos
Incidentes Catastróficos	Fuego, Agua, Viento, Terremotos, Fallas de Voltaje, Ataques terroristas
Personas No Maliciosas	Empleados y Usuarios Desinformados
Personas Maliciosas	Atacantes, Espías Industriales, Administradores Maliciosos, Ingeniería Social

Tabla 3.3. Los tipos de Amenazas[64]

[64] Material proporcionado por el Ing. Albert Espinal, en el tópico de graduación de Seguridad en Redes Informáticas.

3.2.3.1.1. Incidentes catastróficos

Cualquier evento que se relacione a un clima extremo, fenómenos naturales, o un incidente catastrófico puede causar daño severo a la infraestructura de su organización. La información puede perderse, el hardware puede dañarse y una pérdida de productividad puede ocurrir a lo largo con la ausencia de otros servicios esenciales.

Desgraciadamente son pocas las medidas preventivas que pueden implementarse para mitigar los incidentes potencialmente catastróficos. Lo mejor para estos tipos de amenazas es tener un plan de contingencia para ayudar a minimizar los efectos de una pérdida. Teniendo preparados y listos estos planes para ir en ayuda de la organización y así reponerla a un estado anterior al ataque, entonces se puede retomar las funciones comerciales normales tan rápidamente como sea posible. Además de los eventos catastróficos naturales, también son incluidos los motines porque podrían ser difíciles de establecer en un plan de contingencia eficaz para protegerlas contra la pérdida de un recurso informativo en caso de que esto sucediera.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

3.2.3.1.2. Fracasos Mecánicos

A menudo se pasan por alto amenazas mecánicas. Éstos pueden incluir: ausencia de energía, fallas de hardware y paralizaciones de la red. La prevención de las vulnerabilidades que pueden levantarse de estas amenazas pueden llevarse a cabo a través de la planificación apropiada.

El respaldo de hardware, las fuentes de poder centralizados para los centros de cómputo y el diseño de una red robusta pueden ayudar a eliminar simples puntos de errores en su organización los cuales pueden causar fallas mecánicas. Sin embargo, implementar estas medidas de prevención puede ser sumamente caro y debe ser evaluado cuidadosamente para asegurar que el valor de los recursos garantizados estén bien resguardados utilizando dichos métodos.

Al aminorar las amenazas mecánicas se pueden descubrir riesgos adicionales a la seguridad, porque la mitigación es un paso para que puedan aumentar los ataques en el entorno. A menudo, agregando funcionalidades a un recurso informático, pueden exponerse otras vulnerabilidades de seguridad.

CIB-ESPOL

3.2.3.1.3. Amenazas Humanas

Las amenazas humanas pueden aparecer en dos variedades diferentes: maliciosas y no maliciosas. Las amenazas no maliciosas pueden causar problemas mayores con la integridad de los datos a través del error normal del usuario. La basura del software, errores de entrada de datos y los errores administrativos todos caen en esta categoría.



CIB-ESPOL

- **Ataques Maliciosos**

Las amenazas maliciosas consisten en ataques por desagrado o malicia, producidos por ex-empleados o personas que están fuera de la organización. Es probable que estas personas tengan una meta y objetivos específicos y normalmente tiene algún nivel de acceso legítimo a los sistemas de la organización. Los empleados de las compañías están mas familiarizados con las computadoras y sus aplicaciones, esto incluye el tener conocimiento de qué exposiciones y vulnerabilidades pueden causar el mayor daño a la organización. Este tipo de ataque puede ser sumamente difícil de descubrir o de proteger.

Es probable que las personas maliciosas que tengan metas y objetivos específicos usualmente tengan un acceso legítimo al sistema. Un ataque de

una persona maliciosa puede afectar todos los componentes de la seguridad computacional o sus aplicaciones. Otros tipos de crímenes de seguridad provocados por las personas maliciosas pueden involucrar soborno o la ingeniería social.

La ingeniería social es el proceso de engañar a las personas para que revelen sus contraseñas o de alguna forma sacar información de seguridad. A menudo estas acciones no son detectadas porque las auditorías se hacen de manera inadecuada, o ellas fallan al ser revisadas.



CIB-ESPOL

Un ataque malicioso también puede utilizar ingeniería social para engañar a empleados y obtener una entrada al sistema. Por ejemplo, un atacante podría hacerse pasar como un administrador del sistema y pedir contraseñas y nombres de usuarios. Empleados que no están bien entrenados y no son conscientes de la seguridad pueden caer en esta acción.

Los empleados enfadados pueden crear el mejor inconveniente o el peor sabotaje dentro de su organización. Los empleados actuales pueden causar más daño que los ex-empleados.

- **Ataques no maliciosos**

Los atacantes no son los únicos que pueden dañar una organización. La amenaza primaria a la integridad de los datos proviene de usuarios autorizados que no son conscientes de las acciones que están realizando. Los errores y omisiones pueden ocasionar a la organización una perdida, daño, o pueden alterar datos valiosos.

Los errores y omisiones son amenazas importantes a la integridad de los datos. Los errores son causados por los empleados que ingresan datos procesando cientos de transacciones por día. Muchos programas, sobre todo aquellos diseñados para usuarios que utilizan computadoras personales, están faltos de medidas apropiadas de control de calidad. Sin embargo, incluso los programas más sofisticados no pueden protegerse contra todos los tipos de errores u omisiones de entrada de datos.

Estos errores, que a menudo son llamados "bugs[65]", son realmente catastróficos. La calidad del software mejorado ha reducido pero no ha eliminado esto amenaza. En la instalación pueden mantenerse errores que también pueden originar problemas de seguridad.

---

[65] Bug: Error de programación que se suelen encontrar en los software

Las organizaciones asumen a menudo que los programas de información que sus sistemas computacionales reciben son más exactos que los que realmente son. Muchas organizaciones dirigen los errores y omisiones en su seguridad computacional, en la calidad del software y la calidad de los datos implementando políticas de seguridad.

3.2.3.2. Clasificación de las amenazas

Hay ciento de maneras de clasificar las amenazas. Microsoft desarrolló el método stride[66] para categorizar los siguientes tipos de amenazas maliciosas:

- Identidad de Spoofing
- Manipulación de datos
- Repudiación
- Divulgación de Información
- Rechazo de servicio
- Elevación de privilegio



CIB-ESPOL

[66] Método en Inglés de seguridad para categorizar amenazas (Imitación de Identidad, Manipulación de Datos, Rechazo, Revelación de Información, Denegación del Servicio y Elevación de Privilegio)

Cada componente de estos métodos son definidos a continuación:

3.2.3.2.1. Identidad de Spoofing.

La identidad del Spoofing incluye cualquier cosa que sirva para obtener o acceder ilegalmente usando la información de la autenticación de otra persona, como un nombre de usuario o una contraseña.



CIB-ESPOL

3.2.3.2.2. Manipulación de datos

La amenaza de la manipulación de los datos involucra la modificación maliciosa de datos. De estos podemos mencionar los cambios desautorizados hechos a datos persistentes, como el borrar de un sitio web la información que contenía una base de datos, o la alteración de datos cuando fluye entre dos computadoras sobre de una red abierta.

3.2.3.2.3. Repudiación

Las amenazas de la repudiación son asociadas con usuarios que niegan realizar una acción, no teniendo ninguna manera de demostrar lo contrario. Un ejemplo sería cuando un usuario realiza un operación ilegal en un sistema que falla en la habilidad de rastrear la operación prohibida.

3.2.3.2.4. No Repudio

Se refiere a la habilidad de un sistema de oponerse a amenazas de la repudiación. Por ejemplo, un usuario que compra con tarjeta de crédito un artículo tendría que firmar la factura o recibo para recibir el artículo. El vendedor puede utilizar el recibo firmado entonces como evidencia que el usuario recibió el paquete.

3.2.3.2.5. La divulgación de la información

Las amenazas de la divulgación de la información involucran la exposición de información a individuos que supuestamente no tienen acceso a ella. Los ejemplos incluyen la habilidad de usuarios de leer archivos a los cuales no se les ha concedido acceso, o la habilidad de un intruso de leer datos en tránsito entre dos computadoras.

3.2.3.2.6. Rechazo de Servicio

El ataque de denegación de servicios(Denial of Service "DOS") rompe los servicios válidos de los usuarios. Los objetivos de los ataques DOS pueden incluir el que un servidor web temporalmente sea indispuesto o inutilizable.

La protección contra ciertos tipos de amenazas DOS pueden ayudar a mejorar la disponibilidad del sistema y fiabilidad del mismo.

3.2.3.2.7. Elevación de Privilegio

En este tipo de amenaza, un usuario no privilegiado gana privilegios de acceso que lo habilita para comprometer o posiblemente destruir un ambiente de un sistema entero. Estas amenazas incluyen situaciones en las que un atacante ha penetrado a todas las defensas del sistema para explotarlas y dañarlas.

3.2.3.2.8. Exploits

Un recurso puede ser accedido a través de una amenaza donde se puede atacar una vulnerabilidad en su ambiente organizacional. La tabla 3.4.[67] (Anexo F) proporciona ejemplos de tres tipos de exploits importantes.

---

[67] Tomado del Manual "Securing Windows 2000 Server" Capitulo 8, pagina 321

3.2.3.2.9. Eliminación y Alteración de la Información.

Los ataques maliciosos que anulan o normalmente alteran la información quieren demostrar algo o tomar venganza por algo que ha sucedido. Normalmente las personas maliciosas actúan de manera rencorosa hacia la organización porque se enfadan por algo que ha pasado. Los extraños, sin embargo, pueden atacar para demostrar simplemente que es posible hacerlo, o simplemente pueden hacerlo por satisfacción de decir que ellos lo hicieron.

3.2.3.2.10. Fraude común y robo de información.



CIB-ESPOL

La tecnología de información esta incrementando las herramientas y los objetivos para el fraude y robo. Un diseño apropiado y controlado del sistema financiero puede apoyar la legislación requerida o reportar los requisitos para prevenir un fraude. Los ambientes de los sistemas financieros no son los únicos sujetos a este abuso. Otros objetivos de los atacantes son los ambientes que controlan el acceso a la información personal, como agencias de crédito o de identidad, sistemas de inventario, o sistemas de facturación por citar unos ejemplos.

Es muy difícil lograr evitar ser víctima de algún robo, pero para alcanzar una protección contra la alteración en un equipo se puede encriptar y certificar los

datos para que no puedan tener acceso a ellos aún así los roben. Si una computadora es robada, la información que contiene estará a disposición del ladrón que puede borrarla o leerla, pero se puede asegurar que la información robada sea casi inútil por que está encriptada y hace que el raptor no pueda tener acceso a la llave para poder descifrarlo.

3.2.3.2.11. Destrucción de las operaciones normales del negocio

Los atacantes pueden querer romper el normal funcionamiento comercial. Esto puede hacerse como un acto molestoso, por ejemplo, si un empleado enfadado no quiere trabajar porque él no ha sido elegido para ser ascendido.

3.2.3.3. Métodos de Ataques



CIB-ESPOL

El método en la siguiente fórmula se aprovecha de la vulnerabilidad de la organización para defenderla contra los ataques maliciosos:

- Motivos de la amenaza + Método de exposición + Vulnerabilidad del Recurso = Ataque

Pueden ganar acceso o negar servicios de numerosas maneras que incluyen a lo siguiente:

- Virus, caballos de Troya y gusanos
- Craqueando contraseñas
- Ataques de DOS
- Hackeando e-mails
- Código malicioso
- Repetición de paquetes
- Modificación de paquetes
- Ingeniería social
- Ataques de intrusiones
- IP Spoofing y sesión hijacking.

3.2.3.4. Vulnerabilidades

Una vulnerabilidad es un punto donde un recurso es susceptible a una amenaza. También puede pensarse como una debilidad. Las vulnerabilidades pueden originarse de la tecnología, las personas, o de los procesos. A menudo se ven como fallas tecnológicas en la aplicación de software o hardware, o cuando se diseña o se desarrolla un sistema.

A continuación en la tabla 3.5. tenemos una lista de posibles vulnerabilidades. Estos simplemente representan unos de los varios usos

existentes e incluye ejemplos en las áreas físicas, datos y seguridad de la red.

Vulnerabilidades	Ejemplos
Física	Puertas Desbloqueadas
Natural	Edificación grupal construido sobre una falla
Hardware y Software	Fecha expedida de software de antivirus y parches de los sistemas operativos
Medios	Interferencia eléctrica
Comunicaciones	Protocolos desencriptados
Humanas	Procedimientos definidos o aplicaciones escritas pobremente.

Tabla 3.5. Tipos de Vulnerabilidades[68]

CIB-ESPOL

3.2.3.5. Riesgos

Un riesgo es la probabilidad de que un agente amenazante se aprovecha de una vulnerabilidad y a la pérdida potencial de un recurso. Si un firewall tiene

[68] Material proporcionado por el Ing. Albert Espinal, en el tópico de graduación de Seguridad en Redes Informáticas.

varios puertos abierto, hay un riesgo más alto que un intruso utilizara uno de los puertos para que acceda a la red por un método desautorizado.

Si los usuarios en su entorno no están especializados en los procesos y procedimientos, hay un riesgo más alto a que un empleado cometa un error e involuntariamente destruyera los datos. Si un sistema de divulgación de intrusión no se lleva a cabo en una red, hay un riesgo más alto que un ataque pase inadvertido hasta que sea demasiado tarde.

3.2.3.6. Medidas de Prevención



CIB-ESPOL

Las medidas de prevención o resguardos, reducen el riesgo potencial. Una medida de prevención es algo como una configuración de software, hardware, o procedimientos que cuando se implementa neutraliza una amenaza o una vulnerabilidad para reducir el riesgo en un ambiente computacional.

Los ejemplos de medidas de prevención incluyen: Creación de contraseña fuertes, un alto grado de seguridad, mecanismos de control de acceso dentro de un sistema operativo, la aplicación de contraseñas en el sistema básico de entrada y salida (BIOS) y el entrenamiento para el entendimiento de la seguridad.

Si la compañía sólo tiene hotfixes de seguridad en sus servidores y los mismos no se actualizan, esto crea una vulnerabilidad. La amenaza es un acto de un usuario malicioso o no malicioso en el entorno que rompe la productividad. Sin el hotfixes actualizado, un sistema no esta protegido y hay una posibilidad de pérdida o adulteración de datos. La medida de prevención en esta situación es instalar cualquier service pack que son requisitos previos en todas las computadoras de su organización y entonces actualizarlos con cualquiera de los hotfixes que se incluyeron en estos service packs. La relación entre las amenazas, vulnerabilidades, y las medidas de prevención se muestra en la figura 3.3.

CIB-ESPOL

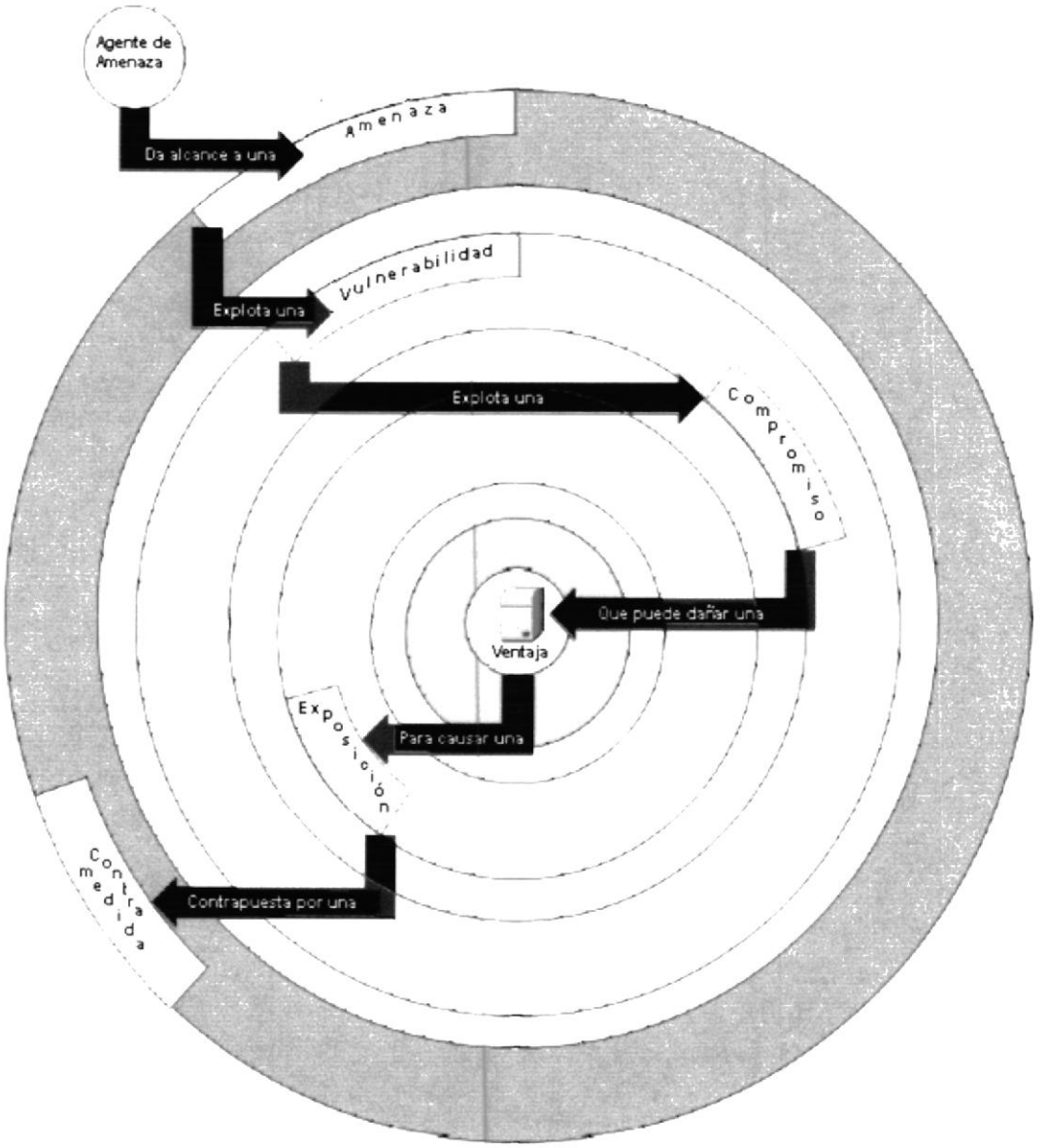


Figura 3.3. Relaciones entre los componentes de seguridad[69]

[69] Tomada de http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofpm.mspx

3.3. Gestión de Parches

Los sistemas operativos y las aplicaciones son a menudo inmensamente complejos. Estos pueden consistir de millones de líneas de código, escritos por muchos programadores diferentes. Por estas razones, es esencial que el software trabaje fiablemente y no comprometa la seguridad o estabilidad de su sistema. Para minimizar cualquier problema, se prueban los programas completamente. Sin embargo, los hackers se esfuerzan continuamente encontrando debilidades en el software, haciendo imposible anticiparse a todos los ataques en el futuro.



CIB-ESPOL

Las compañías de software generan parches para resolver debilidades en código o aplicaciones, esto claro esta después de la comercialización del producto. Un parche es un pedazo de código que se inserta en un programa ejecutable como un apuro temporal a un ataque por ejemplo de un virus.

Cada vez se generan más ataques a la seguridad de los sistemas y así mismo los hackers emplean métodos mas sofisticados para romper estas seguridades y modificar el ambiente de estos programas. Entonces se crean nuevos parches de seguridad. Sin embargo, al implementar los parches también pueden referirse simplemente a agregar funcionalidad a un producto determinado.

El manejo de parches de seguridad presenta un desafío específico a la mayoría de las organizaciones. Una vez que la debilidad ha sido expuesta en software, los atacantes generalmente extenderán información sobre eso rápidamente a lo largo de su comunidad. Las compañías de software se esfuerzan por soltar un parche de seguridad para cerrar la vulnerabilidad lo más pronto posible. Pero hasta que se implemente el parche, la seguridad puede comprometerse severamente.



CIB-ESPOL

3.3.1. Service Packs

Los Service Packs guardan el estándar del producto, la solución a los problemas reportados y también pueden extender la funcionalidad de su entorno. Estos se empaquetan convenientemente para su transmisión e incluyen herramientas y drivers[70] actualizados.

Los Service Packs son productos específicos, y los hay separados para cada producto. Sin embargo, el mismo Service Pack generalmente se utilizará para las diferentes versiones del mismo producto. Por ejemplo, el mismo service pack se utiliza para actualizar Windows 2000 Server y Windows 2000 Profesional.

---

[70] Driver: Software encargado de configurar partes especificas de hardware tales como tarjetas, y cualquier elemento informático que así lo requiera.

Los service packs también son acumulativos. Cada nuevo service pack contiene todas las soluciones implementadas en versiones anteriores, así como cualquier nuevo problema reportado. No se necesita instalar un service pack anterior antes de instalar la última versión.



CIB-ESPOL

3.3.2. Hotfixes o QFEs

Los QFEs son un equipo dentro de Microsoft que produce hotfixes. Se proporcionan Hotfixes o QFEs a clientes individuales cuando ellos experimentan problemas críticos para los que ningún workaround factible está disponible.

Los Hotfixes no sufren regresión extensa y son orientados a problemas específicos. Solo se debe aplicar uno si se experimenta un problema crítico y se está utilizando la versión actual del software con el último service pack.

Los grupos de hotfixes están periódicamente incorporados en los service packs al tiempo que estos sufren verificaciones más rigurosas y se hacen disponibles a todos los clientes.

3.3.3. Parches de seguridad

Se diseñan parches de seguridad para eliminar vulnerabilidades de seguridad. Los atacantes que quieren irrumpir en los sistemas pueden aprovecharse de estas vulnerabilidades. Éstos son similares a los hotfixes pero se clasifican obligatorios, si se necesita ser implementado rápidamente.

Muchas actualizaciones de seguridad son para el lado del cliente (a menudo el browser[71]).

3.3.4. Manejo de parches en las organizaciones

La gestión de parches dependerá fundamentalmente del tamaño y complejidad de su organización. Sin embargo, es vital que se entienda la importancia de esto y cómo encajar en la estrategia de gestión de riesgo global para su compañía.

Por ejemplo, si se decide que el riesgo debe minimizarse a toda costa, se podría seguir la estrategia de cerrar todos los sistemas de producción cada vez que una nueva vulnerabilidad aparece en su software. Se puede escoger

---

[71] Browser: Software que nos permite la navegación en el Internet.

no empezar los sistemas nuevamente hasta solucionarlo con el parche de seguridad y ser implementado a lo largo de su organización. Esto consume mucho tiempo y resulta caro por lo que será completamente impráctico para muchas organizaciones.

A lo largo del proceso de gestión de parches, se necesitará evaluar los riesgos contra los costos de realizar las medidas de seguridad apropiadas. Después de que una vulnerabilidad de seguridad se ha descubierto, puede haber un periodo corto antes de que se divulgue un parche. Se necesitará evaluar el riesgo producido por la vulnerabilidad y determinar las medidas a tomar antes de aprobar e implementar el parche.

Estas medidas pueden incluir el desactivar servicios, poner fuera de servicio a los sistemas, o restringir los accesos a los usuarios interiores u otros grupos como sea necesario. Una vez que un parche se libera, se necesita determinar el riesgo de implementarlo inmediatamente, contra el costo de guardar los servicios mientras se realiza una prueba y se asegura que el parche no afecte negativamente al sistema. Si se decide probar, se necesitará determinar cuándo probarlo; con lo que pueden permitirse el lujo de hacer esto ante el riesgo de no implementarlo.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

3.3.4.1. Evaluar el ambiente actual

A menudo, se aplican parches incoherentemente en una organización y no hay documentación de por qué, cuando y donde se han implementado. Antes de que se pueda manejar la seguridad de su ambiente apropiadamente, se debe conocer su estándar en detalle. Se debe saber:

- Qué sistemas están en su ambiente, incluyendo sistemas operativos y sus versiones.
- Aplicaciones en uso a lo largo de su ambiente.
- Mantener información sobre los individuos o grupos responsables de proteger cada sistema.
- Qué recursos están presentes en su ambiente y su valor relativo.
- Identificar las amenazas conocidas y los procesos que se tienen que identificar y que involucren cambios del nivel de amenaza.
- Identificar las vulnerabilidades conocidas.
- Qué medidas de seguridad se han implementado en su entorno.

3.3.4.2. Servicio de actualización de software



CIB-ESPOL

En muchos ambientes, puede ser beneficioso haber especializado a las computadoras para el proceso de gestión de parches. Estos sistemas

proporcionan situaciones especializadas por el hecho de guardar herramientas de seguridad, parches, hotfixes, service packs y documentación.

Se puede preparar a estos sistemas para realizar análisis y recuperación de parches.



CIB-ESPOL

3.3.4.3. Actualizar los servicios de seguridad

Se debe asegurar que los sistemas de actualización de seguridad estén funcionando.

Los sistemas de actualización de seguridad generalmente no necesitan ser servidores. Sin embargo, la alta disponibilidad es muy importante, como éstos, las computadoras formarán la base que pondrá al corriente su ambiente con el último parche.

Para implementar un sistema de actualización de seguridad apropiadamente, la computadora necesitará directa o indirectamente internet para acceder y poder transmitir la última información del parche a las fuentes, así como acceder a la computadora que sea responsable para guardar la versión actual.

3.3.4.4. Comunicación

Si su compañía es pequeña, entonces sólo una persona puede necesitar encargarse de guardar parches actualizados, probarlos, instalarlos y leer los varios archivos que estos generen. Sin embargo en ambientes más grandes habrán generalmente, varias personas en el cargo con aspectos diferentes en la gestión de parches de seguridad.

Es muy importante que todos aquellos involucrados en la gestión de parches se comuniquen eficazmente.

Esto ayudará a asegurar que se tomen decisiones sin producir esfuerzo y que ningún paso del proceso se pierda.

3.3.5. Proceso de Gestión de Parches

La gestión de parches es justamente un subconjunto de cambios. Si ya se tiene un cambio de procedimiento de gestión en su organización, no se tendrá que crear completamente un nuevo proceso para la gestión de parches. A continuación se proporcionará información específica del proceso de gestión de parches que pueden utilizarse para mejorar una organización

3.3.5.1. Mejorar el Proceso de Gestión

Análisis: Mirar el ambiente actual y las amenazas potenciales. Determinar el parche que se debe implementar para reducir las amenazas en su entorno.

Planeación: Determinar qué parches deben implementarse para detener las potenciales amenazas y vulnerabilidades que se han identificado. Identificar quién realizará las pruebas, ka implementación y los pasos involucrados.

Pruebas: Repasar los parches disponibles y clasificarlos para su entorno. Probar todos los parches que se han identificado para asegurarse que estos trabajarán dentro de su ambiente sin ningún efecto colateral. Se debe entender que hace el parche y cómo afecta a su entorno, también hay que verificar que se este realizando como se lo planeó.

Implementación: Implementar los parches correctos para reforzar su entorno.

Monitoreo: Verificar todos los sistemas después de implementar los parches.

Revisión: Como parte del proceso, se necesita repasar los nuevos parches rutinariamente. Si durante la revisión se encuentra que se necesitan nuevos parches, se debe regresar al primer paso.

3.3.6. El Analizador Básico de Seguridad de Microsoft (MBSA)

El Analizador Básico de Seguridad de Microsoft (MBSA) se ha diseñado para examinar a las computadoras que están ejecutando Windows NT 4.0, Windows 2000, Windows XP Profesional y Windows XP Home Edition. El MBSA puede ejecutarse en cualquier computadora que utilice cualquiera de estas plataformas.

Es crítico conocer qué parches se han aplicado a su sistema y, más pretenciosamente, cuales no tiene. La herramienta de MBSA hace esto, ya que utiliza HFNetChk (Anexo B) la popular herramienta que Microsoft liberó en Agosto del 2001 para que verifique las brechas de seguridad.

3.3.7. Plan de parches



CIB-ESPOL

No necesariamente toda amenaza o vulnerabilidad propone un riesgo significativo a su entorno. Cuando se leen las notificaciones del sistema

operativo acerca de las potenciales vulnerabilidades, se debe evaluar si estas vulnerabilidades aplican a su entorno particular.

Por ejemplo, si la vulnerabilidad aplica al servicio en Windows 2000 del protocolo de transferencia de archivos (FTP) y nunca se habilita el mismo, entonces la vulnerabilidad no se aplica.

Si se responde a las amenazas y vulnerabilidades que no aplican a su entorno, no se tendrá un beneficio significativo.

Cuantas nuevas amenazas y vulnerabilidades salgan, se debe leer cualquier información de apoyo sobre estas. Una de las primeras alternativas será no tomar ninguna acción, desactivar el servicio al riesgo o implementar un parche.



CIB-ESPOL

3.3.7.1. Clasificando los parches

Cuando cada nuevo parche está disponible, se debe determinar la importancia para su entorno. Esto determinará entonces pronto lo que se necesitará para implementarlos y cuando probarlos.

Microsoft mantiene evaluaciones de cada vulnerabilidad las cuales describe en un artículo que denomina boletín de seguridad. El sistema de evaluación clasifica las vulnerabilidades según su impacto potencial si es explotada y la probabilidad de que suceda este acontecimiento.

Se puede utilizar este sistema de evaluación como un asesoramiento para clasificar parches. Finalmente, se necesitará clasificarlos basados en su propio ambiente.

3.3.7.2. Probando los Parches

Como con cualquier software, los parches no pueden trabajar perfectamente en cada entorno. Con suerte, se debe probar cualquier parche completamente antes de instalarlo en el ambiente.

Sin embargo, muchos parches de seguridad necesitan ser instalados rápidamente para arreglar problemas serios.

En muchos casos, se encontrará que el procedimiento de comprobación es un compromiso entre la necesidad de que se resuelva un problema de seguridad y la necesidad de asegurar que el parche sea estable en su ambiente.

Como parte de el procedimiento de gestión de riesgo, se necesitará determinar que se realice completamente cada paso. Si se salta algunas fases debido a la urgencia y se debe todavía continuar, se obliga a completarlos en un laboratorio de prueba para encontrar potenciales problemas antes de que estos ocurran.

Toda la comprobación debe ocurrir en equipos que se parezcan a los servidores de producción tan parecido como sea posible.



CIB-ESPOL

3.3.7.3. Evaluando el Parche

A un mínimo, la valoración del parche debe consistir en los siguientes pasos:

- **Identificar al dueño del parche:** Para todos los parches, se debe tener un dueño identificado, quién es responsable para la evaluación del parche.
- **Revisar toda la documentación:** Antes de aplicar cualquier Service Pack, hotfix, o parche de seguridad, toda la documentación pertinente debe leerse.
- **Verificar la categoría del parche:** Después de la valoración del parche, se puede necesitar cambiar la categoría. Esto afectará a otros

aspectos de la comprobación. Cuando se revise la documentación hay que buscar respuestas a las siguientes preguntas:

- ¿Es la actualización pertinente y se resolverá un problema eficazmente?
- ¿Hay dependencias que relacionan a la actualización? (Por ejemplo, hay ciertas características que necesitan ser habilitados o desactivados para que la actualización sea eficaz?)
- ¿Se necesita realizar inmediatamente acciones al implementar la actualización?

3.3.7.4. Instalando los parches

Se debe asegurar que el parche se instale correctamente, incluso si el parche requiere una reiniciación, se debe saber cuánto espacio requiere (incluso un desinstalador), entender qué opciones están disponibles para el usuario y así sucesivamente. También se debe leer cualquier documentación de apoyo para información adicional.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

3.3.7.5. Funcionamientos del servidor

Una vez que el parche es instalado, se necesita asegurar que el servidor continúa trabajando normalmente.

Hay que probar todas las funciones del servidor y asegurarse que todo opera normalmente.

3.3.7.6. Funcionamientos de la aplicación

Como parte del procedimiento de comprobación, es importante verificar el parche con cualquier aplicación coexistente en los servidores e identificar cualquier problema con dependencias. Después de instalar el parche, se debe verificar que todas las aplicaciones continúan trabajando como antes.

3.3.7.7. Desinstalar el parche



CIB-ESPOL

Es posible que a pesar de su comprobación, después de instalar el parche se pueda encontrar con problemas. Entonces se necesitará el desinstalador del parche. Es importante, por consiguiente, probar que el desinstalador funcione correctamente. Después de desinstalarlo, se debe verificar que el servidor continúa corriendo como lo había esperado.

3.3.7.8. Crear un Plan de Reversión

Aún cuando su comprobación proceda completamente sin novedades, todavía es posible que haya problemas cuando se implemente el parche. Se necesita un plan de acción para restaurar el sistema a su estado original antes de que el parche fuera implementado.

En algunos casos, esto consiste en tomar un respaldo del servidor antes de que la instalación ocurra, para que si hay problemas el servidor pueda restaurarse muy rápidamente.

3.3.7.9. Implementar Parches

Asumiendo que la comprobación funciona fácilmente, se debe estar listo para implementar el parche para la organización. Hay varias maneras de hacer esto, ya sea manualmente o por medio de políticas de grupo.

3.3.7.10. Supervisar los parches

Después de que se ha instalado los parches en su entorno de producción, se necesita continuar supervisando los servidores.

También, si se implementara un parche sin un análisis completo que pruebe el tiempo-crítico, se debe probar el parche después en un ambiente de prueba.

Así como se supervisa cuando existen servidores, es muy importante que se controle el ambiente en conjunto para asegurar que esos nuevos servidores estén con los parches necesarios antes de salir a producción.

CAPÍTULO 4

4. ANÁLISIS DE LAS VULNERABILIDADES DE WINDOWS 2000 SERVER Y EL SERVICIO IIS 5.0

En este capítulo se procederá a realizar inicialmente un estudio general de las vulnerabilidades para tener una idea de como estas afectan a las organizaciones y como las empresas valoran la seguridad de sus sistemas, para luego efectuar el análisis de algunas de las más conocidas vulnerabilidades existentes en el Windows 2000 Server y el servicio IIS 5.0.

4.1. Estudio General de las Vulnerabilidades

4.1.1. Estadísticas de Ataques a las Vulnerabilidades

A nivel mundial, cada día se registran nuevos casos de penetraciones a todo tipo de empresas. La mayoría de los casos van desde los muy conocidos virus y gusanos, hasta la explotación de las vulnerabilidades que poseen algunos sistemas operativos entre ellos, Windows 2000 Server.

Según estadísticas del CERT[72] en lo que va del 2005 se han reportado 1220 casos de vulnerabilidades a nivel mundial. Eso demuestra como cada vez los sistemas operativos, en especial los de Microsoft, presentan nuevas fallas que son aprovechadas por hackers para causar perjuicios millonarios.

La tabla 4.1. y la figura 4.1 muestran un cuadro estadístico de casos de vulnerabilidades reportadas desde el año 2000 hasta la fecha, a fin de definir la tendencia que marca este problema en los Sistemas Operativos.

Año	**2000**	**2001**	**2002**	**2003**	**2004**	**1TRI,2005**
Vulnerabilidades	1.090	2.437	4.129	3.784	3.780	1.220
Total de Vulnerabilidades Reportadas (2000 - 2005):						16.440

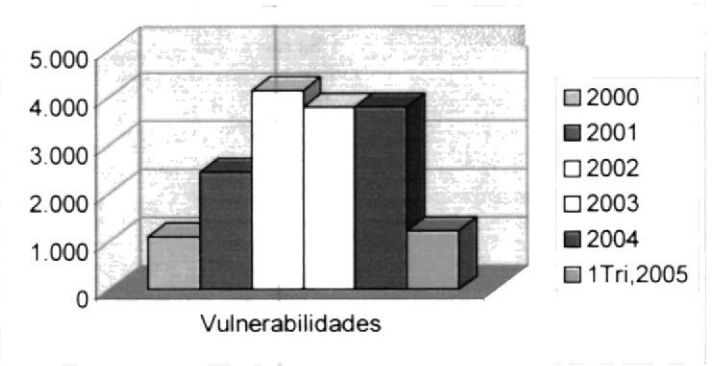
Tabla 4.1. Casos reportados de vulnerabilidades en los últimos cinco años.[73]



CIB-ESPOL

[72] Computer Emergency Readiness Team

[73] Datos tomados de las estadísticas anuales del CERT



CIB-ESPOL

Figura 4.1. Cuadro Estadístico de casos reportados de vulnerabilidades en los últimos cinco años. [74]

Como se puede observar la tendencia ha sido creciente en los últimos cinco años, teniendo su punto máximo en el año 2002 con 4.129 casos de vulnerabilidades reportadas; en los años posteriores se refleja una condición un poco inferior pero muy cercana a ese nivel, lo cual se muestra en las estadísticas del primer semestre del 2005 que ya supera el total de vulnerabilidades reportadas solo en el año 2000.

Es por esto que se hace necesario poner atención a las medidas de seguridad que pueden ser implementadas dentro de nuestras organizaciones.

---

[74] Datos tomados de las estadísticas anuales del CERT

Para poder tener un conocimiento completo de como enfrentar estas vulnerabilidades, es necesario conocer en que medida estas afectan a los diferentes productos disponibles en el amplio mercado Informático, donde gracias a la competencia tenemos varias opciones de diferentes proveedores de tecnología lo cual nos permite poder escoger la mejor alternativa que sea aplicable a nuestro entorno organizacional.



CIB-ESPOL

Sin embargo como al fin y al cabo todo sistema informático es realizado por humanos y como tal está propenso a tener errores y por ende vulnerabilidades, sin embargo estas pueden ser mitigadas dependiendo de su nivel de incidencia o el impacto que provoque en nuestra empresa.

Dentro del siguiente listado, que se muestran en la tabla 4.2. y la figura 4.2, encontraremos las aplicaciones más utilizadas dentro de las organizaciones, en el cual podremos medir el impacto que sobre estos se ciernen con los diferentes problemas de seguridad.

El CERT anualmente pone a disposición estos datos estadísticos de tal forma que los administradores de tecnología, así como también los usuarios finales tengan el conocimiento de cuan vulnerable puede ser el sistema que están utilizando, para tener una idea de las diferentes medidas de seguridad que se

deben tomar para minimizar los riesgos de ataques a las diferentes vulnerabilidades que se presenten.

Aplicaciones	Porcentajes	Numero de Casos
Microsoft Windows NT/2000Server/XP	43%	7.069
Microsoft Windows 95/98/ME	29%	4.768
UNIX Generic	10%	1.644
Linux Red Hat	7%	1.151
Oracle	6%	986
Cisco	4%	658
Solaris	1%	164

Tabla 4.2. Casos reportados de vulnerabilidades por aplicaciones en los últimos cinco años.[75]



CIB-ESPOL

[75] Datos tomados de las estadísticas anuales del CERT

CIB-ESPOL

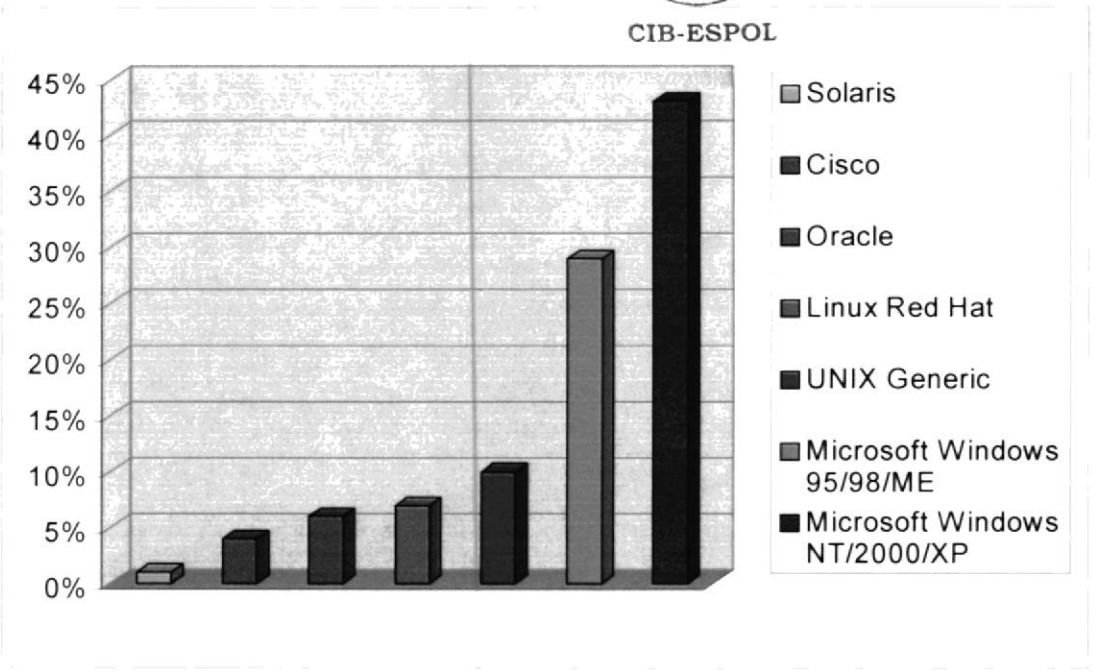


Figura 4.2. Cuadro estadístico de los casos reportados de vulnerabilidades por aplicaciones en los últimos cinco años. [76]

Como es de conocimiento público los sistemas de Microsoft son los más utilizados a nivel mundial, pero así también son los que más vulnerabilidades presentan, siendo los sistemas operativos para servidores los que representan casi el 50% del total de vulnerabilidades reportadas, obviamente entre esos está incluido el Windows 2000 Server.

[76] Datos tomados de las estadísticas anuales del CERT

4.1.2. Percepción de seguridad en las organizaciones

Antes de hacer un análisis en las vulnerabilidades del Windows 2000 Server para determinar como se incrementan los riesgos en nuestras organizaciones y aplicar soluciones a los problemas que se pueden suscitar, es necesario establecer como perciben los usuarios y los administradores de tecnología el asunto de la seguridad. Este punto en particular es la base de todo, ya que si las organizaciones no conciben la importancia debida a lo que representa la seguridad, entonces resultaría infructuoso tratar de concienciar el grado en que las vulnerabilidades ponen en riesgo el recurso mas valioso de la empresa como es la información hasta cuando es demasiado tarde.

Dentro de las organizaciones se manejan diversos criterios acerca de la seguridad, a continuación se muestra la tabla 4.3. y la figura 4.3. donde se muestra la tendencia de la percepción de las organizaciones sobre el valor de la seguridad.

Valor de la Seguridad	Porcentajes
Manejo de Riesgos	49%
Protege el Negocio	33%
Estrategia de Negocio	28%
Mal Necesario	24%
No es Visible	12%

Tabla 4.3. Percepción del valor de la seguridad en las organizaciones[77]

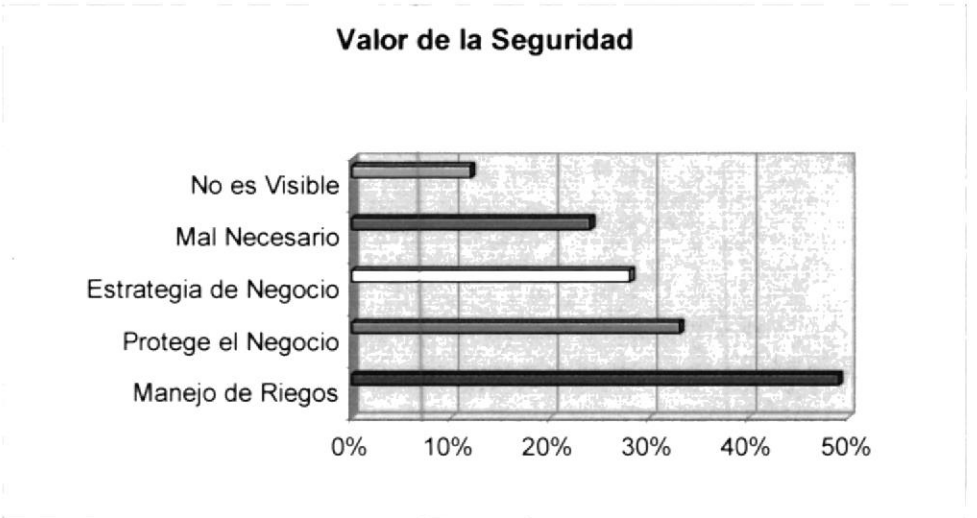


Figura 4.3. Cuadro estadístico de la percepción del valor de la seguridad en las organizaciones[78]

CIB-ESPOL

[77] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

[78] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

Producto de esta información, podemos determinar que dentro de las organizaciones, el tema de la seguridad se lo enfoca en su mayoría dentro de los procesos que implican manejo de riesgos. En segundo lugar, esta como un elemento protector del negocio. Otros lo ven como una estrategia de negocio, en especial cuando se trata de empresas orientadas a brindar un servicio con un mínimo de riesgos.

Para usuarios un tanto pesimistas, lo ven como un mal necesario, debido a que piensan que esto es algo con lo que no se puede dejar de coexistir y cuando se presentan problemas se convierte en algunos casos en un dolor de cabeza. Para otros en realidad este punto no es visible.

Como se puede apreciar el 49% de los encuestados opina que es un factor indispensable para el manejo de riesgos, pero que tanto se conoce de las medidas de seguridad. A continuación se muestra la tabla 4.4. y la figura 4.4. que nos permite determinar tal información.

Criterios de Medidas de Seguridad en las empresas		Porcentajes
Grupo A	Disponen de Medidas de Seguridad	38%
Grupo B	No saben si sus Medidas de Seguridad son Efectivas	10%
Grupo C	No Disponen de Ningún Tipo de Medida de Seguridad	52%

Tabla 4.4. Criterios de medidas de seguridad en las empresas[79]

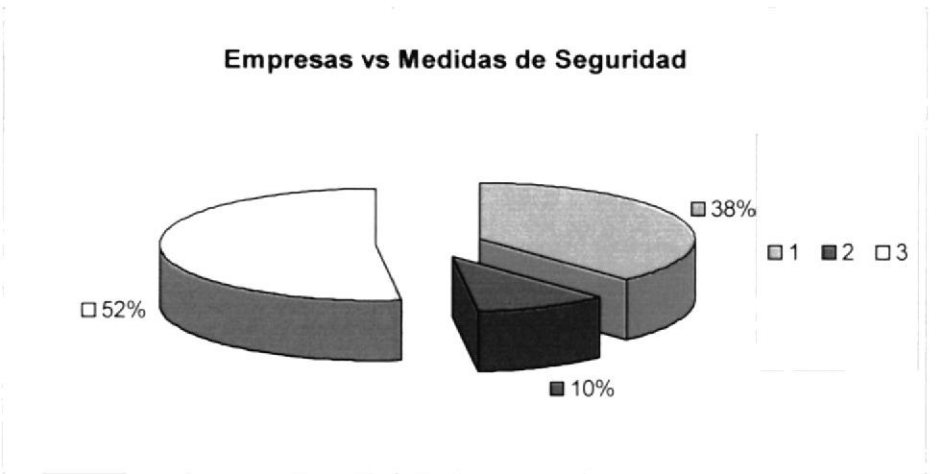


Figura 4.4. Gráfico estadístico de los criterios de medidas de seguridad en las empresas[80]

CIB-ESPOL

[79] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

[80] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

Según estas estadísticas, el 52% de las empresas no disponen de ningún tipo de seguridad. Esto da a notar el gran riesgo que corren las organizaciones y por ende lo vulnerable que estas son.

Un factor muy importante a considerar y que constituye a no dudarlo, el dirimente principal al momento de establecer la tecnología de seguridad ideal para nuestra organización son los costos destinados para este fin.

Como se puede observar, la mayoría de las organizaciones no posee ningún tipo de seguridad y esto se debe principalmente a la percepción del gasto que se destina a estos proyectos dentro de las empresas. A continuación en la tabla 4.5. y la figura 4.5., se presenta los resultados de una encuesta sobre la percepción que tienen las empresas sobre la inversión en seguridad informática:

Percepción	Porcentaje
Costo Necesario del Negocio	63%
Gasto Discreto	22%
Infraestructura Básica	13%
Gasto suprimible	1%
No opinan	1%

Tabla 4.5. Percepción de las empresas sobre la inversión en seguridad informática[81]

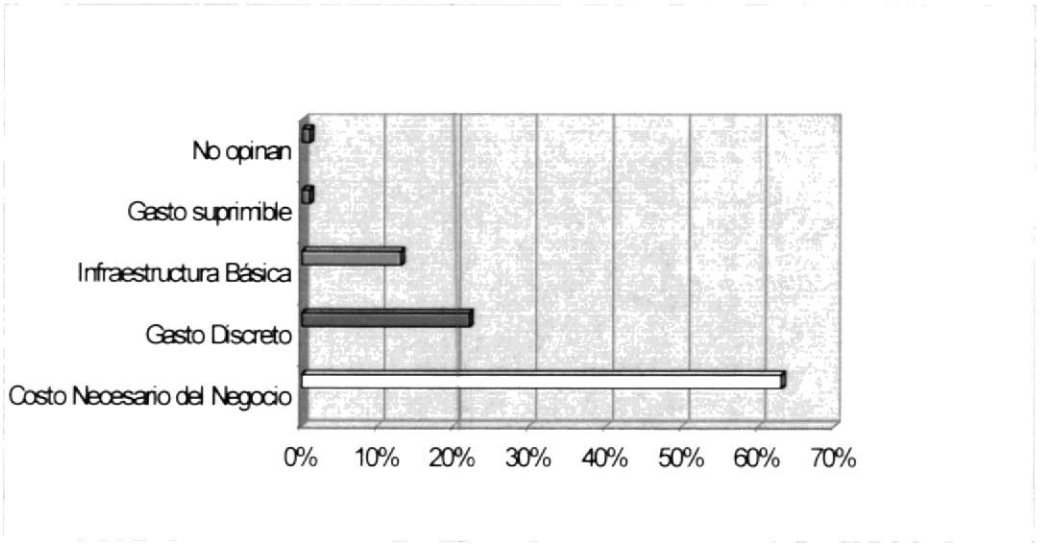


Figura 4.5. Cuadro estadístico de la percepción de las empresas sobre la inversión en seguridad informática[82]

[81] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

[82] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

Al momento de establecer las soluciones a las diferentes vulnerabilidades del Windows 2000 Server, es importante conocer el grado en que estas comprometen nuestra información. La mayoría de las empresas encuestadas tienen opiniones divididas en cuanto a los niveles de información comprometida de acuerda a los tipos de ataques que se pueden presentar, como se puede apreciar en la tabla 4.6. y la figura 4.6.

Tipo de Ataque	**Información Comprometida**			
	No Confidencial	Algo Confidencial	Muy Confidencial	Extrema Confidencialidad
Internos	18%	44%	27%	5%
Externos	3%	35%	40%	13%

Tabla 4.6. Niveles de información comprometida por tipo de ataques[83]

[83] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

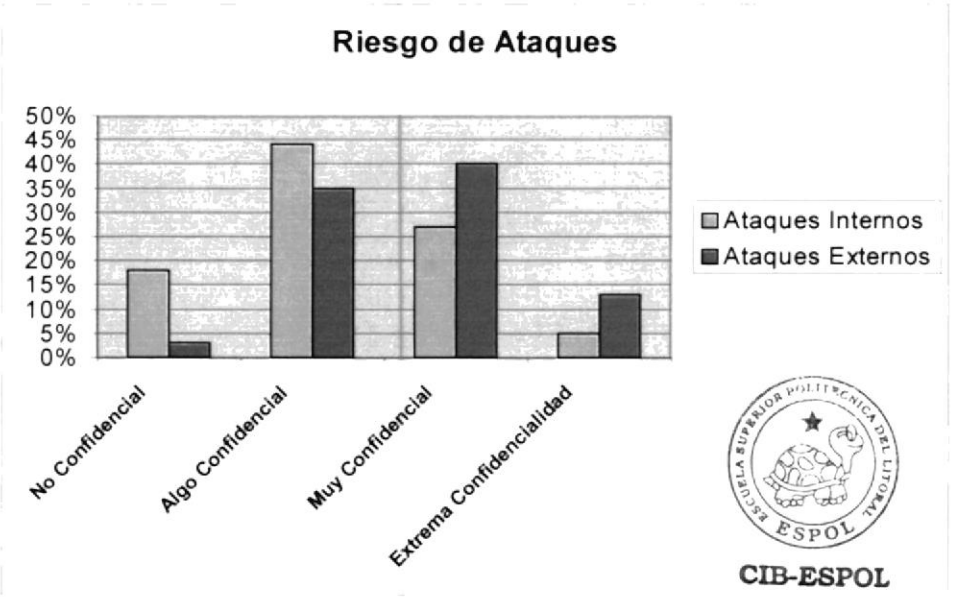


Figura 4.6. Gráfico de los Niveles de información comprometida por tipo de ataques[84]

Como se puede apreciar, un grupo opina que la mayoría de los ataques provienen de fuentes internas, de los cuales tan solo un 5% ven comprometida información de extrema confidencialidad. Otros opinan que la mayoría de los ataques proviene de fuentes externas de los cuales un 13% ven comprometida información de extrema confidencialidad que constituyen un dato más significativo dentro de esta estadística y por lo tanto merece nuestra atención al momento de establecer soluciones.

---

[84] Datos tomados del estudio Global Security Survey realizado por Deloitte Touche Tohmatsu

Esta información depende esencialmente desde la óptica de donde se la mire, ya que para quienes han sufrido ataques de seguridad internos pensaran que es una de las mayores amenazas frente a los ataques externos. Otros dirán que son los ataques externos aquellos que representan mayor incidencia en la seguridad organizacional. En todo caso es importante establecer las políticas necesarias para hacerle frente a estas formas de ataques.

4.1.3. Estadísticas de Ataques de Vulnerabilidades de Windows 2000 Server y del IIS 5.0

En esta parte se muestran las estadísticas de las vulnerabilidades más críticas reportadas a nivel mundial en el sistema operativo Windows 2000 Server y el Internet Information Server 5.0., lo cual nos puede dar una idea de la importancia de prestar atención a las vulnerabilidades más significativas, de tal manera que se pueda tomar precauciones tales como un plan de contingencia para solucionar o prevenir cualquier eventualidad que pueda suscitarse en nuestra organización.

Cabe recalcar que la información contenida en esta sección así como lo anteriormente expuesto en este capítulo ha sido recopilada desde empresas especializadas en el análisis de estas amenazas que provienen de países

como: EE.UU., Inglaterra donde la importancia que se le da a estos problemas informáticos es mayor a la que se le da en países en vías en desarrollo como los latinoamericanos y muy especialmente en nuestro país, lo cual nos da a notar la poca preocupación que sobre este tema se tiene en el Ecuador y en Latinoamérica en general.

Es necesario destacar que la poca importancia que en nuestros países se tiene acerca de estas vulnerabilidades es tal que no existen estudios relativos a estos casos, mas bien el único estudio encontrado a nivel de Latinoamérica señala que la mayor preocupación en cuanto a la seguridad informática se refiere, la constituyen los hackers que como todos sabemos provocan la mayor cantidad de ataques a redes y sistemas informáticos.

Seria muy importante que se hicieran estudios a nivel de Latinoamérica y muy en especial en nuestro país para tener una percepción del alcance que pueden tener las vulnerabilidades de los sistemas operativos y su nivel de impacto en la estructura organizacional de nuestras empresas.

Por todo lo antes mencionado, no se ha podido establecer un estudio comparativo entre lo reportado por el CERT y la realidad latinoamericana acerca de este asunto y menos aun ha sido posible compararla con nuestro país.

A continuación en la tabla 4.7. y en la figura 4.7. se muestran los porcentajes de ataques calculados por el CERT según una métrica que evalúa cada vulnerabilidad y sobre la cual se puede determinar el nivel de incidencia que esta tiene. La métrica es un valor dado entre 0 y 180 y que incluye entre otras cosas: el conocimiento de la vulnerabilidad, la facilidad para ser explotada, el riesgo que conlleva, el impacto que produce y que se requiere para explotar la vulnerabilidad.

Vulnerabilidades	Porcentaje Ataques
A. Overflow DCOM Servicio RPCSS	94,50%
B. Microsoft Index Server / IIS 5.0	69,30%
C. Directorio Vulnerable IIS 5.0	68,40%
D. Overflow Buffer Windows 2000 Server	67,50%
E. Overflow Buffer Chunked Encoding para ASP en IIS 5.0	62,43%
F. Vulnerabilidad Servicio NNTP IIS 5.0	30,05%

Tabla 4.7. Los porcentajes de ataques de las vulnerabilidades más críticas del Windows 2000 Server y del IIS 5.0. según el CERT[85]

[85] Datos tomados del CERT

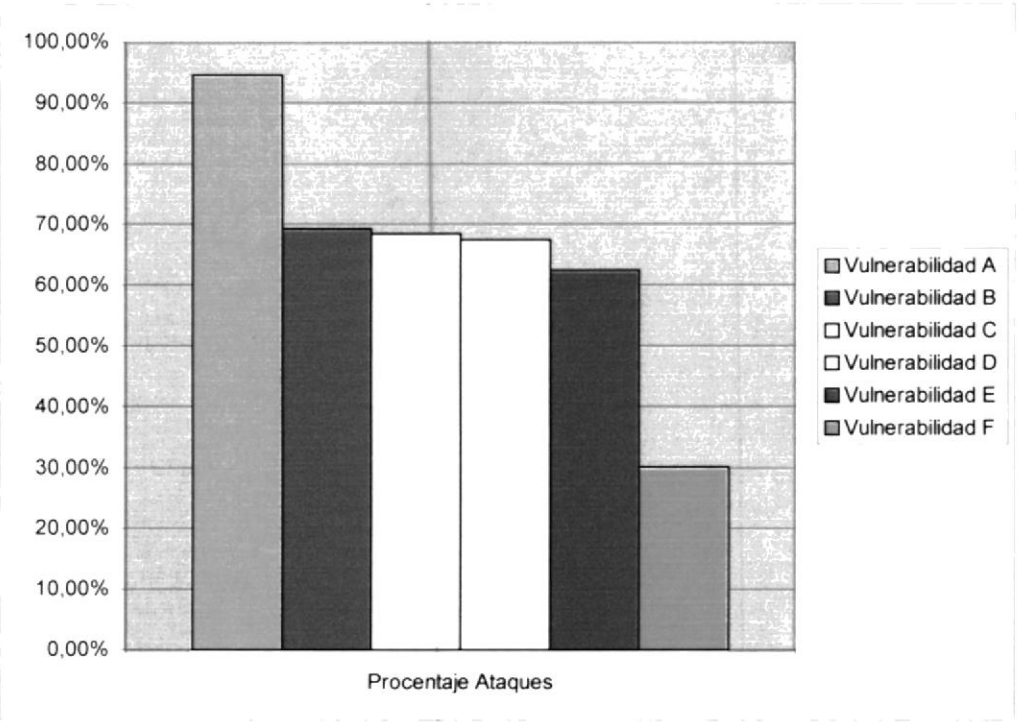


Figura 4.7. Gráfico de los porcentajes de ataque de las vulnerabilidades más críticas del Windows 2000 Server y el IIS 5.0. según el CERT[86]

4.2. Vulnerabilidades del Windows 2000 Server

CIB-ESPOL

A continuación se detallan las vulnerabilidades más comunes que tiene el sistema operativo Windows 2000 Server. La información aquí presentada ha sido tomada de diversas fuentes publicadas en el Internet, de casos reportados a nivel mundial y de la página web de Microsoft.[87]

---

[86] Datos tomados del CERT

[87] Todas las fuentes están señaladas en la bibliografía

4.2.1. Vulnerabilidades en los Servicios

- **Desbordamiento de memoria a través del RPCSS**

Descripción

Un desbordamiento de memoria remotamente explotable podría permitir a un intruso ejecutar código arbitrario con privilegios del sistema lo cual causaría una denegación de servicio.

El Servicio RPCSS de Microsoft es responsable de administrar mensajes RPC (Remote Procedure Call). Las fallas del tipo desbordamiento de memoria ocurren en secciones de código que manejan la activación de mensajes DCOM enviados al servicio RPCSS.

Explotando la vulnerabilidad de denegación de servicio, los intrusos podrían causar inestabilidad de forma remota a través de la utilización del servicio RPCSS. Esto podría resultar en una inestabilidad general del sistema lo cual requerirá reiniciar el mismo.

Servicios Afectados: Servicio RPCSS (Remote Service Call System Service)

Impacto: Al explotar la vulnerabilidad, intrusos remotos podrían ser capaces de ejecutar código arbitrario con privilegios de la cuenta Local System. de forma remota a través de la utilización del servicio RPCSS, con lo cual provocaría que el sistema colapse.

Nivel de incidencia: Crítica

Solución:

1. Aplicar una Actualización de Microsoft como se indica en el Boletín de Seguridad MS03-039.[88]
2. Bloquear el Tráfico en los Puertos RPC
3. Deshabilitar DCOM
4. Deshabilitar COM Internet Services y RPC sobre HTTP

- **Ejecución de código remoto a través de un buffer no comprobado en el Locator**

Descripción

El servicio Locator de Microsoft es un servicio de calificativos que mapea nombres lógicos a nombres específicos de red. Se puede producir una vulnerabilidad de seguridad de un buffer sin comprobar en el servicio Locator,

---

[88] Consultar http://www.microsoft.com/spain/technet/seguridad/boletines/MS03-039-IT.asp

cuando un atacante intente construir una llamada RPC que haga uso del servicio Locator para resolver un nombre lógico y utilice una llamada RPC para pasar los datos mal construidos.

Servicios Afectados: Servicio Locator

Impacto: Mediante el envío de una petición mal construida al servicio Locator, un atacante puede provocar la caída del servicio, o incluso la ejecución de código en el sistema.

Nivel de Incidencia: Critica

Solución: Aplicar una Actualización de Microsoft como se describe en el boletín de seguridad MS03-039

- **Denegación de Servicios a través del Windows Media Services**

Descripción



CIB-ESPOL

Los componentes que se cargan cuando se instala Windows Media Services son: Windows Media Unicast Services, Windows Media Station Service, Windows Media Program Service y Windows Media Monitor Service. Una falla surge debido a la forma en que los componentes Windows Media Station Service y Windows Media Monitor Service, manejan las conexiones TCP/IP.

Servicios Afectados: Windows Media Services

Impacto: Un usuario malicioso puede provocar que el Windows Media Station Service deje de aceptar nuevos requerimientos, aunque esté disponible para transferir conexiones TCP que ya hayan sido realizadas, y no aceptará nuevas peticiones. Para recobrar el estado original el administrador debe reiniciar el servicio.

Nivel de Incidencia: Moderada

Solución

1. Aplicar una Actualización de Microsoft como se indica en el boletín MS04-008[89]

2. Bloquear los puertos 7007 y 7778, si se utliza un firewall en su organización.

3. Administrar el Windows Media Services desde la consola o a través de una sesión de terminal

4. Remover Windows Media Services



CIB-ESPOL

[89] Consultar http://www.microsoft.com/spain/technet/seguridad/boletines/MS04-008-IT.asp

- **Overflow de Enteros en la Biblioteca DirectX MIDI**

Descripción

Existe una vulnerabilidad del tipo overflow de enteros contenido en la biblioteca DirectX en Microsoft Windows. A través de la explotación de esta vulnerabilidad un intruso podría ejecutar código arbitrario en los equipos, o provocar un ataque de negación de servicio.

Servicios Afectados: Biblioteca DirectX MIDI

Impacto: Un archivo MIDI especialmente creado podría causar un integer overflow, llevando a un incorrecto direccionamiento de memoria y a una corrupción de heap.

Cualquier aplicación que utilice DirectX/DirectShow para procesar archivos MIDI podría ser afectada por esta vulnerabilidad.



CIB-ESPOL

Nivel de Incidencia: Crítica

Solución:

1. Aplicar un parche como se especifica en el Boletín de Seguridad de Microsoft MS03-030[90].

---

[90] Consultar http://www.microsoft.com/spain/technet/seguridad/boletines/MS03-030-IT.asp

2. Modificar la configuración de Internet Explorer, deshabilitando Active scripting , Run ActiveX controls and plug-ins, Play sounds in web pages, Play videos in web pages

- **Buffer Overflow en Biblioteca de Conversion de HTML de Microsoft Windows**

Descripción

Existe una vulnerabilidad del tipo overflow en el motor de interpretación de código HTML en el Internet Explorer, lo que puede llegar a permitir la ejecución de código o causar una denegación de servicio.

Impacto: Un intruso puede hacer que el IE[91] copie el elemento <HR> en el portapapeles y cargar la biblioteca. El intruso podría lograr esto convenciendo a una víctima que vea un pagina Web de HTML o un mensaje de correo electrónico con formato HTML en el IE, Outlook u Outlook Express en una zona en donde la característica de Active scripting y Allow paste operations vía script estén habilitadas.

Nivel de Incidencia: Crítica

---

[91] IE: Internet Explorer

Solución:

1. Aplicar el parche según lo especificado por el boletín de Seguridad de Microsoft MS03-023[92].

2. Modificar la configuración de la zona de la seguridad del Internet Explorer.

- **Buffer Overflow en IIS 5.0**

Descripción

Existe una vulnerabilidad de buffer overflow en Microsoft IIS 5.0 ejecutándose en Microsoft Windows 2000. IIS 5.0 es instalado y ejecutado de forma predeterminada en los sistemas Microsoft Windows 2000. Esta vulnerabilidad puede permitir a un intruso remoto ejecutar código arbitrario en la máquina víctima.

Una exposición está disponible al público para esta aprovechar esta vulnerabilidad, lo cual aumenta la urgencia para que los Administradores apliquen la actualización correspondiente al sistema.

---

[92] Consultar http://www.microsoft.com/spain/technet/seguridad/boletines/MS03-023-IT.asp

Impacto: Una vulnerabilidad de buffer overflow existe en ntdll.dll (una porción de código utilizada por el componente WebDAV de IIS). Al enviar una solicitud al servidor IIS 5.0, un intruso puede ser capaz de ejecutar código arbitrariamente en el contexto de seguridad del Sistema Local, esencialmente dando al intruso un control completo sobre el sistema.



CIB-ESPOL

Nivel de Incidencia: Crítico

Solución:

Aplicar una actualización de Microsoft que está disponible en:

http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69D32AC929B&displaylang=en

- **Desbordamiento de memoria en el servicio NetDDE de WINDOWS**

Descripción

Un desbordamiento de búfer en el servicio NetDDE de WINDOWS explotable en remoto puede permitir la ejecución de código arbitrario en el sistema

Por fortuna, el servicio NetDDE (Network Dynamic Data Exchange) no se encuentra activo por defecto, por lo que un sistema podría presentar componentes vulnerables sin que la vulnerabilidad pueda explotarse.

Servicios Afectados: Servicio NetDDE

Impacto: Un intruso podría ejecutar código arbitrario causando una inestabilidad general en el sistema que podría dejar inoperable el servidor

Nivel de Incidencia: Crítica

Solución:

1.Desactivar el servicio NetDDE

2 Aplicar una actualización como se indica en el boletín de seguridad de Microsoft MS04-31 [93]

4.2.2. Vulnerabilidades en los protocolos

- **Ejecución remota de código a través de la Validación IP**

Descripción

Existe una vulnerabilidad de ejecución remota de código que podría permitir que un atacante enviara un mensaje IP creado especialmente para tal propósito a un sistema afectado. Un intruso que aprovechara esta vulnerabilidad podría provocar la ejecución remota de código con el sistema afectado. Sin embargo, lo más probable es que los intentos de aprovechar esta vulnerabilidad tuvieran como consecuencia la denegación de servicio.

---

[93] Consultar: http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx

Protocolos Afectados: TCP/IP

Impacto: Ejecución de Código remoto en el sistema.

Nivel de Incidencia: Crítica

Solución:

1. Aplicar una Actualización de Microsoft como se indica en el boletín de seguridad MS03-023

2. Utilizar un servidor de seguridad personal

- **Denegación de servicio a través de una conexión ICMP[94]**

Descripción

Existe una vulnerabilidad de denegación de servicio que podría permitir que un atacante enviara un mensaje ICMP creado especialmente para tal propósito a un sistema afectado.

Protocolos Afectados: TCP/IP, ICMP

Impacto: Un intruso que aprovechara esta vulnerabilidad podría provocar que el sistema afectado restableciera las conexiones TCP existentes.

Nivel de Incidencia: Crítica

---

[94] Protocolo de Control de Mensajes de Internet

Solución: Aplicar una Actualización de Microsoft como se indica en el boletín de seguridad MS03-023

- **Denegación de servicio a través de la unidad MTU[95] de ruta del protocolo ICMP**

Descripción

Existe una vulnerabilidad de denegación de servicio que podría permitir que un atacante enviara un mensaje de Protocolo de mensajes de control de Internet (ICMP) creado especialmente para tal propósito a un sistema afectado, lo que daría lugar a un deterioro del rendimiento de la red y a la posibilidad de que el sistema afectado dejara de responder a las solicitudes.

Protocolos Afectados: TCP/IP, ICMP

Impacto: Provocará denegación de servicio

Nivel de incidencia: Crítica

Solución: Aplicar una Actualización de Microsoft como se indica en el boletín de seguridad MS03-023

---

[95] MTU: Unidad máxima de transferencia

4.2.3. Vulnerabilidades del Sistema Operativo

- **Desbordamiento de memoria en el núcleo de Windows**



CIB-ESPOL

Descripción

Un atacante que logre aprovecharse del desbordamiento de memoria del núcleo de Windows, puede conseguir el control completo sobre el sistema vulnerable.

El núcleo del sistema operativo es el centro del mismo. Este centro ofrece a los programas de aplicación, servicios para acceder a los recursos existentes.

Se ha descubierto que los núcleos de los sistemas operativos Windows NT 4.0, 2000 y XP contienen un error en la forma en que se tratan determinados mensajes que son enviados al depurador. Este error puede provocar una vulnerabilidad de seguridad.

De manera más especifica, la función LpcRequestWaitReplyPort(), que es utilizada por el núcleo del sistema operativo, confía en que un proceso que

se ejecuta en el espacio de memoria de usuario facilitará correctamente el tamaño de un mensaje devuelto al núcleo.

Mediante la utilización de esta vulnerabilidad, un atacante puede ejecutar código en el anillo 0 (el mismo anillo dónde se ejecuta el núcleo del sistema operativo y en donde no se aplica la separación de procesos ni la protección de memoria). Esto permite saltarse cualquier mecanismo de seguridad existente y un acceso ilimitado a cualquier recurso del sistema. El código que se ejecuta en este anillo dispone incluso de más privilegios que el usuario administrador de la máquina.

Esta vulnerabilidad no es explotable de forma remota. Únicamente puede ser aprovechada por un atacante que disponga de la capacidad de conectarse al sistema, ya sea en una sesión interactiva (utilizando el teclado y monitor del ordenador) o a través de una sesión de terminal.

Componentes Afectados: Función LpcRequestWaitReplyPort() del Núcleo de Windows

Impacto: Al explotar esta vulnerabilidad, el atacante podrá ejecutar código malicioso provocando inestabilidad en el núcleo de Windows.

Nivel de Incidencia: Intermedia

Solución: Aplicar una Actualización de Microsoft como se indica en el Boletín de Seguridad MS03-007[96]

- **Desbordamiento de memoria en el cmd.exe**

Descripción

El sistema de archivos NTFS permite la creación de rutas de longitud prácticamente ilimitada, pero la API de Windows no permite rutas mayores de 256 bytes. Según la documentación de la API de Windows se puede evitar la comprobación de la ruta solicitada con el prefijo \? para el nombre de archivo.

El cmd.exe de Windows NT se ve afectado por un desbordamiento de memoria en el comando cd si la ruta destino es mayor de 256. Esta vulnerabilidad puede ser explotada fácilmente para lograr la ejecución de código.

El cmd.exe de Windows 2000 no se ve afectado por un desbordamiento de memoria, sin embargo si se cambia a un directorio mayor de 256 caracteres, cmd.exe quedará encerrado en dicho directorio, impidiendo cambiar a

---

[96] Consultar http://www.microsoft.com/spain/technet/seguridad/boletines/MS03-007-IT.asp

cualquier otro (fallará incluso el comando cd). Esto puede provocar un ataque de denegación de servicio contra scripts de mantenimiento.

Componentes Afectados: Comando cmd.exe

Impacto: Esto puede provocar un ataque de denegación de servicio contra scripts de mantenimiento.

Nivel de incidencia: Critica

Solución: Aplicar una Actualización de Microsoft como se indica en el Boletín de Seguridad MS03-007

4.3. Vulnerabilidades del Internet Information Server 5.0

A continuación se detallan las vulnerabilidades más comunes que tiene el servicio Internet Information Server 5.0 del sistema operativo Windows 2000 Server.

4.3.1. Vulnerabilidades en los Servicios

- **Posibilidad de un ataque de denegación de servicios cuando la petición de URL excede el máximo de la longitud permitida.**

Descripción



CIB-ESPOL

Los intrusos pueden ser capaces de hacer que el servicio de IIS fallara enviando una petición particular de URL demasiado larga.

ISAPI es una interfaz de programa de IIS que puede ser utilizado para modificar o extender el comportamiento de IIS. Los programas escritos usando ISAPI son conocidos también como filtros o extensiones, dependiendo de la manera en que estos sean implementados. Una de las diferencias primarias es que las extensiones sólo se ejecutan cuando son llamados (por una referencia en un URL) mientras que los filtros ejecutados por cada URL son sometidos al servidor.

Un intruso podría hacer que el servicio IIS fallara. En IIS 5.0 y 5.1 el servicio se reiniciará automáticamente, aunque un ataque pudiera ser ejecutado relativamente fácil; IIS 4.0 tendría que ser reiniciado manualmente.

Servicios afectados: Interfaz ISAPI

Impacto: Cuando IIS intenta procesar la página con una URL demasiado larga (para enviar esto al cliente como un mensaje de error) resulta una violación. Otros filtros ISAPI pueden tener un comportamiento similar, lo que provocaría la misma vulnerabilidad.

Nivel de Incidencia: Crítico

Solución: Aplicar un parche como el que se describe en el Boletín de Seguridad MS02-018[97] de Microsoft

- **Desbordamiento de memoria en la interfaz ISAPI**



CIB-ESPOL

Descripción

Un desbordamiento de memoria en la extensión HTR de la interfaz ISAPI sobre servidores IIS podría permitir a un intruso interrumpir la operación normal del servicio o posiblemente ejecutar un código arbitrario con los privilegios de dicha extensión.

HTR es una tecnología server-side scripting[98] para IIS que en gran parte ha sido suplantado por ASP.

---

[97] Consultar http://www.microsoft.com/technet/security/bulletin/MS02-018.mspx

[98] Secuencia de comandos que se ejecutan del lado del servidor

Servicios afectados: Interfaz ISAPI

Impacto: Un intruso puede interrumpir la operación normal del servidor IIS y puede ser capaz de utilizar esta vulnerabilidad para ejecutar un código arbitrario con los privilegios de la extensión HTR del interfaz ISAPI. Sobre IIS 4.0, esto permite al control administrativo del sistema operativo; sobre IIS 5.0 y 5.1, esto permite el acceso con los privilegios de la cuenta IWAM_COMPUTERNAME.

Nivel de Incidencia: Crítica

Solución:

1. Aplicar un parche como se describe en el Boletín de Seguridad de Microsoft MS02-018

2. Inhabilitar la extensión HTR de la interfaz ISAPI

- **Cross-site scripting[99] en la opción de búsqueda de Archivos de Ayuda de IIS.**

Descripción

Los visitantes a los sitios web que utilizan Microsoft IIS 5.0 y 5.1 son vulnerables a un ataque de cross-site scripting en la opción de búsqueda de archivos de ayuda de IIS.

Muchos sitios web de Internet pasan por alto la posibilidad en la que un cliente puede enviar datos malévolos intentado ser utilizado sólo por sí mismo, sin darse cuenta que esto es un error fácil de atacar.

Sin embargo, esta situación puede ocurrir cuando el cliente confía en una fuente de información de poca confianza cuando se solicita una petición.
IIS es un servidor web muy popular y cualquier cliente que tiene una relación de confianza con un sitio web IIS puede ser vulnerable si este sitio devuelve un mensaje de error.

Servicios afectados: Opción de Búsqueda de Archivos de Ayuda del IIS

---

[99] El cross-site scripting es una forma de ataque en la cual el intruso abusa de la confianza entre una víctima y un sitio web.

Impacto: Cuando un usuario confiado pulsa sobre un link determinado, el URL enviado puede incluir un código malicioso y de esta manera puede ser ejecutado de improviso sobre el cliente.

Nivel de Incidencia: Crítico

Solución: Aplicar un parche de seguridad de Windows como se indica en el boletín de seguridad MS02-018

- **Los nombres largos de archivos inválidos provocan un desbordamiento de memoria en el servicio server-side includes (SSI)**

Descripción



CIB-ESPOL

Un desbordamiento de memoria en IIS podría permitir a un intruso ejecutar un código arbitrario con los privilegios del ASP.DDL.

Server-side includes files (SSI files) son los archivos que residen sobre un servidor web y que están incluidos por scripts, programas o páginas web. Los archivos SSI a menudo son utilizados para proporcionar cabeceras comunes o gráficos a través de páginas web múltiples, o reutilizar código en páginas web múltiples. Los browsers no pueden solicitar que un archivo particular sea incluido, pero pueden ser capaces de influir en cuando y como un archivo debe ser incluido.

Expresamente, esto realiza una operación sobre el nombre del archivo que sólo debería tener éxito si el nombre del mismo es válido.

Una vulnerabilidad de seguridad se presenta porque es posible aceptar una petición que incluya un nombre muy largo de archivo, pero hacerlo de esta manera tiene dos efectos. Primero, la extensión ASP de la interfaz ISAPI concluye que el nombre del archivo tiene que ser procesado como parte de un archivo ASP y un archivo server-side includes. Segundo, el nombre del archivo evade la comprobación de seguridad. El resultado es que el nombre de archivo – que es más largo que el buffer asignado para soportarlo – causa una extensión de buffer en el archivo ASP cuando este es procesado.

Servicios afectados: Extensión ASP de la interfaz ISAPI, Server-side includes (SSI)

Impacto: Un intruso puede ejecutar código arbitrario en el sistema, causando su inhabilitación.

Nivel de Incidencia: Crítico

Solución:

1. Aplicar un parche como se describe en el Boletín de Seguridad de Microsoft MS02-018.
2. Inhabilitar la extensión ASP de la interfaz ISAPI
3. Utilizar la herramienta IIS Lockdown

- **Posibilidad de un ataque de Denegación de Servicios por medio del WebDAV**

Descripción



CIB-ESPOL

Existe una vulnerabilidad importante en el componente WebDAV del servidor web de Internet Information Server (IIS) de Microsoft. Esta vulnerabilidad es considerada crítica ya que permite la ejecución de código arbitrario en el servidor. Además se tiene constancia que está siendo activamente explotada, por lo que se hace necesaria una actuación inmediata por parte de los administradores de servidores vulnerables.

WebDAV (World Wide Web Distributed Authoring and Versioning) es una extensión del protocolo HTTP versión 1.1, que proporciona un estándar para la edición y administración de archivos entre ordenadores vía Internet.

Se ha descubierto la existencia de una vulnerabilidad de seguridad en un componente de Windows utilizado por WebDAV, provocada por la existencia de búfer sin analizar. WebDAV es un componente incluido en la instalación por defecto de IIS.

Como la vulnerabilidad es fácilmente explotable, es de prever que gusanos con capacidad de auto propagación que hagan uso de esta vulnerabilidad.

Servicios afectados: Componente WebDAV

Impacto: La vulnerabilidad puede ser aprovechada por un atacante remoto mediante el envío de una petición HTTP especialmente construída en una máquina que ejecute Internet Information Server (IIS). La petición podrá provocar la caída del servidor o incluso la ejecución del código enviado por el atacante. El código se ejecutará en el contexto de seguridad del servicio IIS (por defecto, LocalSystem).

Nivel de Incidencia: Crítico

Solución:

1. Aplicar un actualización de Microsoft como se indica en el Boletín de Seguridad MS03-007
2. Deshabilitar WebDAV
3. Utilizar IIS Lockdown
4. Instalar URLScan

- **Desbordamiento de memoria en el servicio Indexing Service causado por el virus Code Red**



CIB-ESPOL

Descripción

El virus "Code Red" es una réplica de un código malicioso que explota los recursos del host sobre el Indexing service.

El virus "Code Red" ataca a través del puerto 80 sobre el protocolo TCP, una vez realizada la conexión con éxito, envía requerimientos HTTP GET hacia la victima causando un desbordamiento de memoria sobre el Indexing Service. Estos requerimientos se realizan de forma randómica a los diferentes hosts de la red y se esparce de forma natural como un gusano. Una vez que el ataque haya sido un éxito, el host victima experimenta una respuesta única a los requerimientos solicitados al Server

Servicios Afectados: Indexing service, Protocolos TCP y HTTP

Impacto: El ataque de un virus "Code Red" causa una degradación al sistema afectado al mismo tiempo esto puede ser el punto de partida para que un gusano infecte a múltiples máquinas. El escaneo de los sistemas y redes pueden causar que este gusano realice un ataque malicioso de

denegación de servicios en muy corto tiempo, esto ocurre por que en cada instancia que el gusano "Code Red" usa un generador randómico de número que crea una lista de direcciones IP para ser escaneadas.

Nivel de Incidencia: Crítico

Solución:

Aplicar un parche de seguridad como se describe en los boletín de seguridad MS01-044[100]

- **Desbordamiento de memoria en una sección que codifica mecanismos de transferencia para ASP.**

Descripción

Una vulnerabilidad de desbordamiento de memoria en IIS 4.0 y 5.0 podría permitir a un intruso ejecutar un código malicioso contra un servidor IIS con los privilegios de la extensión ASP de la extensión ISAPI.

Chunked encoding es la transferencia de unidades de datos de tamaño variable (llamados chunks) desde un cliente web a un servidor web.

---

[100] Consultar: http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Los buffer utilizados para almacenar chunks son localizados sobre un depósito y por lo tanto se puede llamar a esta vulnerabilidad un depósito basado en desbordamiento de memoria. La explotación de un desbordamiento basado en un deposito de buffer para ganar el control de un sistema a veces puede ser más difícil que la explotación de otras clases de desbordamientos de buffer para ganar control. Sin embargo, el fracaso es más dirigido a la ganancia del control del sistema que otros desbordamientos típicos basados por depósitos de buffer.

Además de provocar el tamaño incorrecto del buffer, el error aritmético también previene del IIS 4.0 y 5.0 de colocar cualquier límite verdadero sobre el tamaño de un chunk. Por consiguiente, esto sería fácil para un cliente que envíe un chunk que podría sobrescribir más o toda la memoria del sistema.

Esto es un punto crítico, porque va al centro de esta vulnerabilidad que plantea una amenaza tan seria a los servidores. Esta vulnerabilidad es un ejemplo de supuestos depósitos invadidos; estos son con frecuencia difíciles o imposibles de explotar, debido a la naturaleza dinámica de la memoria del sistema. Los datos sobre el servidor pueden cambiar posiciones de un momento a otro, impidiendo la capacidad del atacante de sobrescribir programas o datos seleccionados. Sin embargo, en este caso, el atacante no necesita conocer donde los programas fueron localizados, pero podría en

cambio simplemente superponer grandes partes de la memoria del sistema indiscriminadamente.

Servicios afectados: Extensión ASP de la interfaz ISAPI

Impacto: Hay un error aritmético en la manera de calcular el tamaño de un buffer de IIS utilizado para almacenar un chunk. El resultado es que IIS asigna un buffer que es demasiado pequeño, permitiendo a un intruso hacer un desbordamiento de memoria.

Nivel de Incidencia: Crítico

Solución:

1. Aplicar un parche como el descrito en el Boletín de Seguridad de Microsoft MS02-018.
2. Inhabilitar la extensión ASP de la interfaz ISAPI
3. Utilizar la herramienta IIS Lockdown

- **Problemas de Seguridad en el Servicio RDS (Remote Data Service)**

Descripción

Diversos errores de seguridad en el Remote Data Services (RDS) permiten a un atacante ejecutar comandos con privilegios de administrador. Esto puede

acarrear serios problemas en nuestro servidor ya que de esta manera la información se ve expuesta y seriamente comprometida.

Servicios Afectados: Servicio RDS (Remote Data Service)

Impacto: Se pierda fiabilidad al servicio atacado, y se corre el riesgo de perder la información que se posee en las cuentas de los usuarios.

Nivel de incidencia: Crítico

Solución:

1. Aplicar el parche de seguridad disponible en http://www.microsoft.com/Downloads/Release.asp?ReleaseID=456231

- **Ejecución de código remoto a través del Directorio Transversal Extendido Unicode**

Descripción



CIB-ESPOL

Una vulnerabilidad existente puede permitir a un atacante visitar el sitio web del IIS, y podrá ejecutar código arbitrario con los privilegios de la cuenta USR_<Nombre de la Maquina>. Esta vulnerabilidad tiene características similares que han sido explotadas en el pasado. Si no se toman las medidas necesarias, los sistemas con esta vulnerabilidad se ven comprometidos.

Servicios Afectados: Directorio Transversal Extendido Unicode

Impacto: Usuarios remotos podrán ejecutar comandos con los privilegios de la cuenta USR_<nombre de la Maquina>

Nivel de Incidencia: Critico

Solución:

2. Aplicar un parche de actualización como se describe en el boletín de seguridad MS01-044.
3. Aplicar permisos sobre los archivos NTFS para permitir solo el acceso de los archivos contenidos en el Web Server.

- **Ejecución de Ataques Remotos a través del servicio NNTP**

Descripción

Una vulnerabilidad en el componente de IIS puede permitir un ataque remoto para comprometer un sistema, provocando una inestabilidad en el sistema afectado.

El servicio NNTP (Network News Transport Protocol) es el encargado de publicar nuevos articulo en la red. La vulnerabilidad se da en el comando XPAT que tiene como función extraer las cabecera de esos artículos basados en la comparación de esas cabeceras. Esta función da como resultado una

vulnerabilidad cuando un atacante envía mensajes erróneos al servidor afectado.

Servicios Afectados: Servicio NNTP

Impacto: Un ataque remoto sin autenticar puede permitir la ejecución de código con privilegios administrativos sobre el sistema afectado.

Nivel de Incidencia: Critico

Solución:

1. Aplicar el parche de seguridad publicado en el boletín MS04-036[101]
2. Desinstalar el Servicio NNTP

4.3.2. Vulnerabilidades en los protocolos

- **Denegación de Servicios a través de una petición de estado de conexión FTP mal creada.**

Descripción

---

[101] Consultar: http://www.microsoft.com/technet/security/bulletin/MS04-036.asp

Una vulnerabilidad en IIS podría permitir a un intruso interrumpir las operaciones ordinarias de FTP como los servicios web contra servidores vulnerables IIS.

Los intrusos pueden detener la operación de los servidores IIS vulnerables. Sobre IIS 5.0 e IIS 5.1, el servicio comenzará automáticamente de nuevo, aunque el intruso pueda ser capaz de repetir el ataque indefinidamente. Sobre IIS 4.0, el servicio puede ser restaurado manualmente.



CIB-ESPOL

Protocolos afectados: Servicios FTP y HTTP

Impacto: Un intruso que envía un requerimiento mal creado para el estado de una conexión existente podría provocar que el servidor IIS fallara, resultando en la pérdida de los servicios FTP y HTTP.

Nivel de Incidencia: Crítico

Solución: Aplicar un parche como el descrito en el boletín MS02-018

- **Desbordamiento de memoria vía comprobación inexacta de los delimitadores en los campos de cabecera HTTP.**



CIB-ESPOL

Descripción

Un desbordamiento de buffer en IIS podría permitir a un intruso ejecutar código arbitrario con los privilegios de la extensión ASP de la interfaz ISAPI.

Un buffer no chequeado correctamente en el mecanismo de procesamiento de los encabezados HTTP en todas las versiones de IIS puede ser aprovechado para sobrescribir los encabezados que recibe el servidor.

Como todos los servidores web, IIS analiza cabeceras HTTP y los descompone en partes constituyentes. Como parte de este procesamiento, IIS comprueba delimitadores que, como se supone, están marcados dentro de las cabeceras. Creando una cuidadosa elección de petición HTTP, el intruso puede provocar un incorrecto análisis del IIS para una cabecera HTTP y colocar resultados erróneos dentro de un buffer que sea demasiado pequeño.

Componentes afectados: Protocolo HTTP y la extensión ASP de la interfaz ISAPI

Impacto: Un intruso puede interrumpir la operación ordinaria de un servidor vulnerable IIS o ejecutar código arbitrario con los privilegios de la extensión ASP de la interfaz ISAPI, ASP.DLL. Sobre IIS 4.0, ASP.DLL corre como parte del sistema operativo así que permite a un intruso tomar el control total administrativo. Sobre IIS 5.0 y 5.1, ASP.DLL corre con los privilegios de la cuenta IWAM_COMPUTERNAME.

Nivel de Incidencia: Crítico

Solución:

1. Aplicar un parche como se describe en el Boletín de Seguridad de Microsoft MS02-018.
2. Inhabilitar la extensión ASP de la interfaz ISAPI
3. Utilizar la herramienta IIS Lockdown (Anexo B)
4. Utilizar la herramienta Urlscan (Anexo B)

- **Desbordamiento de memoria a través del protocolo IPP**

Descripción

La vulnerabilidad tiene lugar cuando se hace una petición del ISAPI .printer, pero en lugar de el host, se manda una cadena de aproximadamente 420 bytes, que es mas de lo que la pila puede soportar.

El desbordamiento tiene lugar por causa del filtro .printer de ISAPI que se encuentra en la DLL sw3prt.dll situada en la carpeta system32, esta es la DLL que da soporte al IPP (Internet Printing Protocol) que trata varios aspectos de impresión en red basados en web.

Servicios afectados: Protocolo IPP e interfaz ISAPI

Impacto: Producto de esta falla, se ve comprometido el soporte IPP para imprimir archivos remotamente vía HTTP produciendo un desbordamiento.

Nivel de incidencia: Critico

Solución:

1.Aplicar actualización de Microsoft disponible en http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321

2. Desinstalar el servicio ISAPI

4.4. Casos de estudio orientados al Análisis de las Vulnerabilidades más críticas del Windows 2000 Server y el IIS 5.0.

El propósito de esta sección es el exponer los casos de estudios más importantes dentro de las vulnerabilidades del Windows 2000 Server y del Internet Information Server 5.0. , a fin de contribuir al estudio de estas vulnerabilidades y concienciar a la comunidad informática de los peligros que

se ciernen sobre los sistemas operativos de las organizaciones, ya que en el Ecuador como lo hemos reiterado no existen entidades responsables de proporcionar dicha información. Se ha tomado como referencia información obtenida desde las empresas objeto de este análisis.

A continuación se presentan dos casos de estudio realizados a dos empresas en el Ecuador: Burger King Co. Ecuador y Ecuacotton S.A.

En estos casos analizaremos las consecuencias que se dieron en estas empresas después de sufrir un ataque sobre las vulnerabilidades en el servidor Windows 2000 Server y del servicio Internet Information Server 5.0.

Además de presentar una descripción general tanto de la organización, así como del ataque mismo, se plantearán soluciones a corto, mediano y largo plazo que estas empresas podrían aplicar para evitar o contrarrestar los efectos de un ataque de este tipo dentro de su organización, las mismas que fueron desarrolladas por quienes elaboramos este trabajo producto de un análisis de algunas estructuras de seguridad y contramedidas aplicables dentro del marco teórico de este documento.



CIB-ESPOL

Caso de Estudio Burger King Co. Ecuador[102]

- **Vulnerabilidad explotada**

Desbordamiento de Memoria a través del Servicio RPCSS



CIB-ESPOL

- **Antecedentes**

Burger King Co. cuenta con 17 locales en todo el Ecuador. Todos ellos se conectan a su servidor matriz localizado en Guayaquil, el mismo que cuenta con Windows 2000 Server.

Para realizar la conexión con los locales disponen de un enlace dedicado compartido a través de la empresa Transferdatos.

Como medidas de protección, cuentan con una licencia corporativa de Norton Antivirus 2004 que se actualiza vía Internet y se distribuye a cada PC conectado al Servidor. Se calcula que cuenta con 100 usuarios recurrentes.

- **Detalles de la explotación de la vulnerabilidad**

---

[102] Datos obtenidos por Anl. Mauricio Granda, Gerente de Sistemas de Burger King Co. Ecuador

Como se abordó anteriormente, el servicio RPCSS es el encargado de administrar los mensajes de llamadas a procedimientos. Este ataque se realizó en 2 partes:

1. El atacante logró tener acceso al servidor central de Burger King y aprovechó la brecha existente en este servicio y empezó a provocar una denegación de servicio mediante el envió de RPC masivos provocando inestabilidad al sistema en general, haciendo que el administrador reinicie el Sistema
2. El atacante obtuvo privilegios de administrador, bloqueó los accesos al administrador del sistema y ejecutó sentencias que alteraron toda las configuraciones de los sistemas instalados en el servidor y se eliminaron todos los accesos de los usuarios. Finalmente incomunicó todos los puertos de conexión provocando la inoperancia total del sistema.

- **Efectos del ataque**

1. Caída total del servidor provocando la inhabilitación de los sistemas de facturación de los locales, así como también de la conectividad con los proveedores internacionales, y por ende esto también afectó al sistema de inventario.

2. Al no contar con un servidor secundario, se paralizaron las importaciones de las materias primas para la distribución a los locales, produciendo un retraso general.

3. Se perdió la comunicación con los locales originando una congestión a nivel operativo.

4. Se recurrió a facturar con sistemas locales alternos que cada local dispone produciendo información inconsistente en algunos casos.

- **Pérdidas económicas ocasionadas por el ataque**

Producto de este ataque, Burger King estuvo inoperante alrededor de 8 horas, dado que la vulnerabilidad explotada es considerada como critica y esta empresa no contaba con las medidas necesarias para enfrentarla.

En la tabla 4.8. se presentan los ingresos estimados por ventas de la empresa Burger King Co. Ecuador

Número de Locales	Ingreso Promedio Diario por Local	Promedio Diario General	Ingreso por hora General (16 horas diarias)	Promedio Mensual	Promedio Anual
17	$ 1.000,00	$ 17.000,00	$ 1.062,50	$ 510.000,00	$ 6.120.000,00

Tabla 4.8. Ingresos estimados por ventas de Burger King Co. Ecuador[103]

En la tabla 4.9. y en las figuras 4.8. y 4.9. se muestran los costos aproximados que fueron asumidos por Burger King producto del ataque antes mencionado, considerando que con una vulnerabilidad con un nivel de incidencia crítico se perdieron 8 horas de productividad y los posibles costos que se pueden asumir ante vulnerabilidades con un nivel de incidencia medio y moderado, si no se toman las medidas correspondientes.

CIB-ESPOL

[103] Creación propia

Riesgos vs. Costos					
Nivel de incidencia Vulnerabilidad	Off Line (Horas)	Porcentaje	Pérdida Diaria	Pérdida Mensual	Pérdida Anual
Critica	8	50%	$ 8.500,00	$ 255.000,00	$ 3.060.000,00
Media	4	25%	$ 4.250,00	$ 127.500,00	$ 1.530.000,00
Moderada	2	13%	$ 2.125,00	$ 63.750,00	$ 765.000,00

Tabla 4.9. Riesgos vs. Costos Estimados de Burger King Co. Ecuador[104]

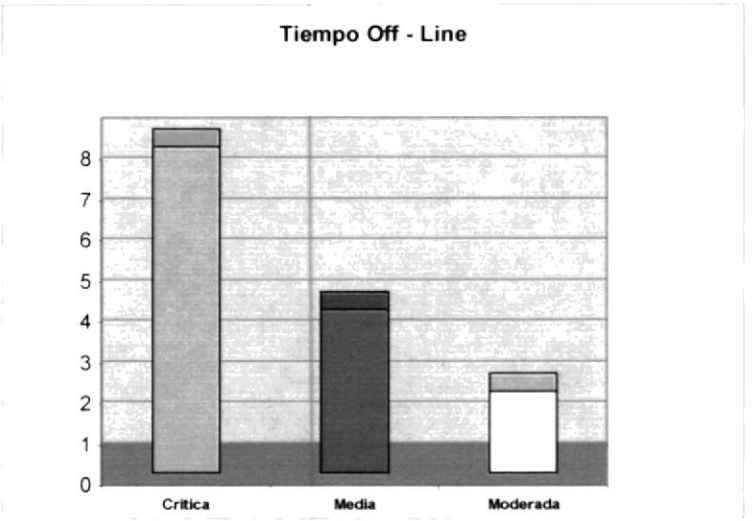


Figura 4.8. Cuadro estadístico del tiempo no productivo por cada nivel de incidencia de una vulnerabilidad para Burger King Co. Ecuador[105]

[104] Creación propia

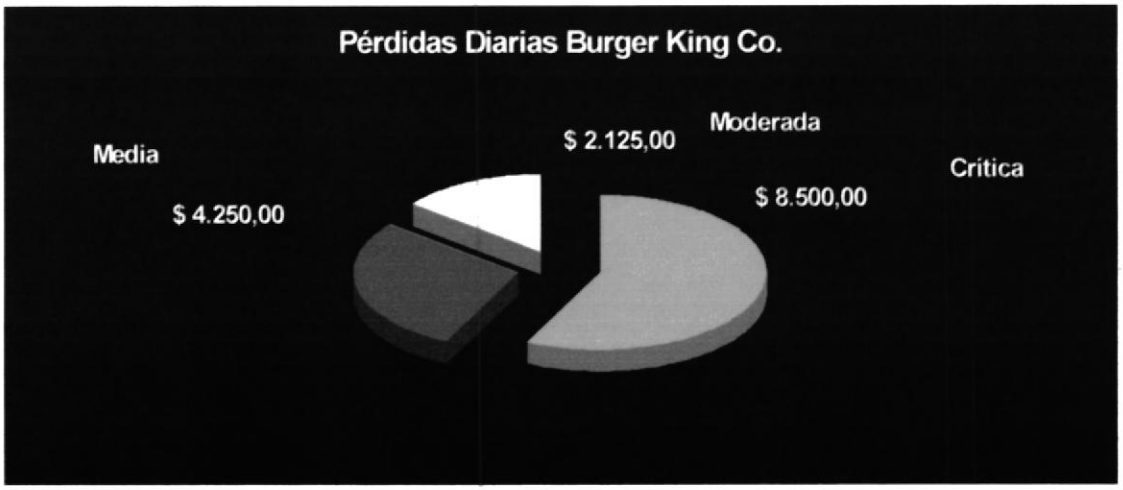


Figura 4.9. Gráfico estadístico de pérdidas estimadas por nivel de incidencia de una vulnerabilidad en Burger King Co. [106]

Como resultado de este ataque, Burger King registró en tan solo ese día una pérdida aproximada de $8.500 dólares, valor que en realidad se duplicaría al añadir al costo directo otros rubros como el derivado del tiempo no operativo, de la reducción de la productividad de los empleados y el costo de las medidas a tomar de forma inmediata para recuperarse del incidente, además del perjuicio causado a la reputación de la empresa. Es decir, que el costo estimado producto de este ataque representa solo la punta del iceberg.

---

[105] Creación propia

[106] Creación propia

- **Soluciones Propuestas**

Corto plazo:

1. Actualizar el servidor con las ultimas actualizaciones.

2. Instalar un servidor "Mirror"[107] que entre a funcionar en el momento en que el servidor principal este fuera de servicio.

3. Realizar un chequeo general de las conexiones para determinar cual es la que está siendo utilizada por el atacante. En el Anexo B se detallan algunas herramientas que podrían ser útiles para este efecto.

Mediano plazo:

1. Establecer Políticas de Actualización de los Servidores de la Organización

2. Elaborar un Plan de Contingencia que contemple las acciones a realizar para los casos en que se presenten catástrofes como la anteriormente descrita. El Anexo A detalla los pasos a seguir para le elaboración y mantenimiento del plan de contingencia.



CIB-ESPOL

[107] Servidor Mirror: Es un servidor con una copia exacta del servidor principal, que se utiliza como respaldo de la información y que puede ser puesto fácilmente como principal ante cualquier eventualidad.

Largo plazo:

1. Contemplar la implementación de una estructura de seguridad robusta a la medida de las posibilidades de la organización. La implementación de Firewalls de Seguridad o de algún medio de protección para evitar así que usuarios ajenos a nuestra red penetren en ella

- **Consideraciones Generales**

Como se ha podido notar, el problema que tuvo Burger King se pudo haber evitado o en todo caso minimizado si los encargados de la Administración de la Seguridad hubieran tomado mayor empeño en implementar una infraestructura de seguridad que permitiera brindar seguridad a los sistemas de uso frecuente y los sistemas llamados "críticos", es decir, aquellos que no pueden fallar. Es necesario hacer tomar conciencia a la Gerencia de cuan importante es la seguridad dentro del negocio y del posible impacto que pudiera causar la violación de las mismas.



CIB-ESPOL

Caso de estudio Ecuacotton S.A.[108]

- **Vulnerabilidad explotada**

Denegación de Servicio producida por el gusano "CODE RED II" al Service Index del IIS 5.0

- **Antecedentes**

Ecuacotton S.A es una empresa exportadora de Textiles situada en Guayaquil. Esta compañía centra su negocio en la elaboración de prendas que son comercializadas en el mercado latinoamericano, en países como Chile, Argentina y México, así como también en el mercado norteamericano donde grandes cadenas de ropa son sus principales consumidores tales como Hidary, WallMart, Such A Tees entre otras. En Guayaquil específicamente son proveedores de T-Shirts-To-Go.

Como su principal mercado es el internacional, Ecuacotton implementó un Sistema de toma de Pedidos vía Internet para facilitar a los compradores la realización del pedido para la elaboración de las prendas que serán

---

[108] Datos obtenidos por Lsi. Humberto Ledesma, Jefe de Sistemas de Ecuacotton S.A.

comercializadas por estos clientes. Además se instaló un Sistema de Negociación, el cual cumple con la función de establecer un contacto más personalizado con los consumidores a fin de establecer costos de mano de obra , costos directos e indirectos de fabricación.

Para esto se implementó un Servidor con Windows 2000 Server y para el tratamiento de las paginas ASP del Sistema vía internet, el servidor web incluido en este sistema operativo, Internet Information Server 5.0. La base de datos esta bajo tecnología Informix Dynamic Server y los aplicativos de uso cotidiano como Contabilidad, Nomina, Compras, etc. son programas en C++. La conectividad con Internet la realizan mediante un enlace dedicado proporcionado por la empresa Telconet.

- **Detalles de la explotación de la vulnerabilidad**

Ecuacotton S.A. sufrió un ataque devastador del gusano "Code Red II" a través del puerto 80 del Servidor. Una vez infiltrado, envía una petición HTTP al Servidor para explotar la vulnerabilidad del Service Index. Este ataque dejó como resultado:

- La denegación de servicio al servidor atacado.
- La desconfiguración total de los servicios preinstalados.
- Datos inconsistentes en la base de datos.

- Inoperancia total del Servidor.

- **Efectos del ataque**

1. Caída total del servidor, perdiéndose toda la información de pedidos de los clientes de ese día.
2. Al no contar con un servidor secundario, se paralizaron las importaciones de las materias primas para la elaboración de las camisetas de los pedidos, y las exportaciones de las prendas confeccionadas a los diferentes mercados.
3. Se perdió la comunicación con los potenciales clientes, producto de la caída del servidor.
4. Se produjo una inhabilitación operativa, ya que el servidor de aplicaciones se encontraba realizando un backup de la información del servidor de Internet lo cual produjo retrasos en el área administrativa.
5. Todas las cuentas de correo electrónico fueron borradas.
6. No se pudo facturar las cuentas de embarques ya realizados a los clientes, produciéndose así un déficit económico durante el tiempo que duró la recuperación de los sistemas administrativos.



CIB-ESPOL

- **Pérdidas económicas ocasionadas por el ataque**

Producto de este ataque, Ecuacotton S.A, no pudo realizar pedidos por alrededor de 10 horas ya que no contaban con las seguridades necesarias para enfrentar los riesgos que conlleva implícito un ataque al Windows 2000 Server y al Internet Information Server 5.0, incluso después de haber recuperado el sistema tuvieron 2 ataques consecutivos que afectaron al servidor de correos.

En la tabla 4.10. se presentan los ingresos estimados por pedidos de la empresa Ecuacotton S.A.



CIB ESPOL

# Pedidos Promedio Mensual	Piezas por Pedido	Costo por Unidad	Costo Total promedio por Pedido	Promedio Mensual Pedidos	Promedio Anual Pedidos
9	150000	$ 2,50	$ 375.000,00	$ 3.375.000,00	$ 40.500.000,00

Tabla 4.10. Ingresos estimados por pedidos de Ecuacotton S.A. [109]

[109] Creación propia

En la tabla 4.11. y en las figuras 4.11. y 4.12. se muestran los costos aproximados que fueron asumidos por Ecuacotton luego de ocurrido el ataque, considerando que con una vulnerabilidad con un nivel de incidencia crítico se perdieron 10 horas de productividad y los posibles costos que se pueden asumir ante vulnerabilidades con un nivel de incidencia medio y moderado, si no se toman las medidas correspondientes.

Nivel de Incidencia de Vulnerabilidad	Tiempo Off Line (Horas)	Porcentaje	Pérdida Mensual Promedio	Pérdida Anual Promedio
Critica	10	83%	$ 312.500,00	$ 3.750.000,00
Media	5	42%	$ 156.250,00	$ 1.875.000,00
Moderada	3	25%	$ 93.750,00	$ 1.125.000,00

Tabla 4.11. Riesgos vs. Costos estimados de Ecuacotton S.A. [110]

[110] Creación propia

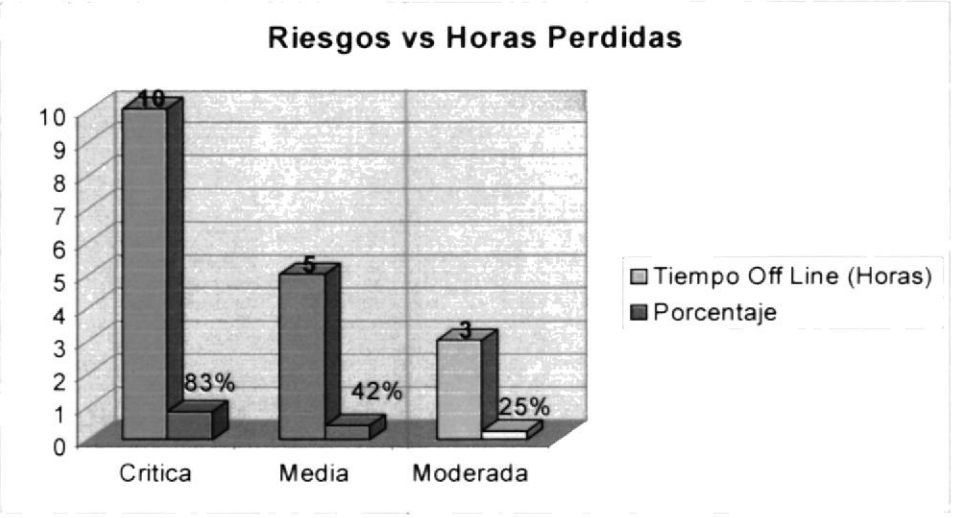


Figura 4.10. Cuadro estadístico del tiempo no productivo por cada nivel de incidencia de una vulnerabilidad para Ecuacotton[111]

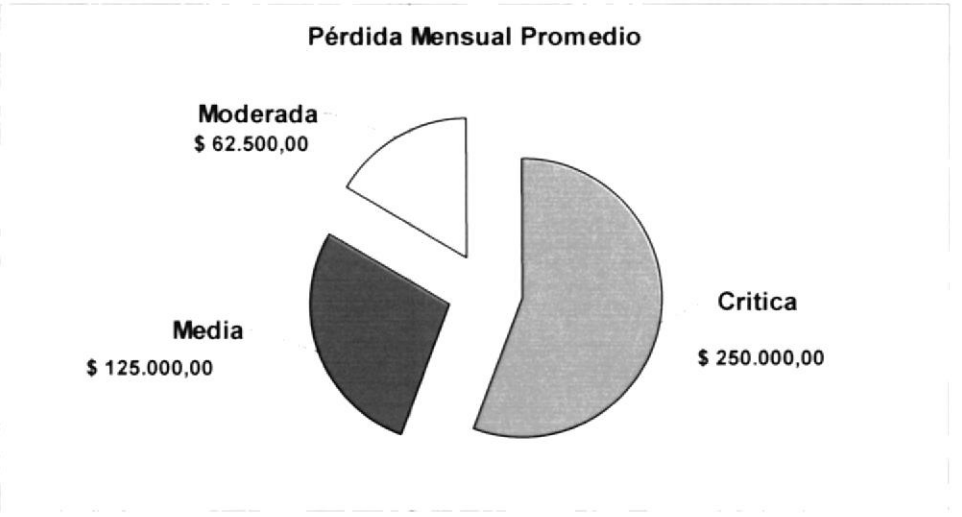


Figura 4.11. Gráfico estadístico de pérdidas estimadas por nivel de incidencia de una vulnerablilidad para Ecuacotton[112]

---

[111] Creación propia

Como resultado de este ataque, Ecuacotton S.A vio reflejado en sus ingresos mensuales una pérdida significativa de $250.000,00 dólares, la misma que pudo ser controlada si esta empresa hubiera contado con una infraestructura básica de seguridad.

- **Soluciones Propuestas**

Corto plazo:

1. Actualizar el servidor con las últimas actualizaciones publicadas para esta vulnerabilidad.
2. Proceder a realizar una revisión general de los Sistemas antes de proceder a cambiar el servidor afectado para evitar que no existan residuos del ataque .
3. Realizar un chequeo general de las conexiones para determinar cual es la que está siendo utilizada por el atacante. En el Anexo B se detallan algunas herramientas que podrían ser útiles para este efecto.

Mediano plazo:

1. Establecer Políticas de Actualización de los Servidores de la Organización

---

[112] Creación propia

2. Elaborar un Plan de Contingencia que contemple las acciones a realizar para los casos en que se presenten catástrofes como la anteriormente descrita. El Anexo A detalla los pasos a seguir para le elaboración y mantenimiento del plan de contingencia.

Largo plazo:

1. Contemplar la implementación de una estructura de seguridad robusta a la medida de las posibilidades de la organización. La implementación de Firewalls de Seguridad o de algún medio de protección para evitar así que usuarios ajenos a nuestra red penetren en ella



CIB-ESPOL

- **Consideraciones generales**

El problema causado por es "Code Red II" se pudo haber prevenido si la empresa hubiera tomado las medidas necesarias para combatir estas amenazas. La toma de conciencia es el punto básico por el cual todas las organizaciones deben partir para el análisis de la seguridad y sobre todo analizar el costo que nos puede representar un ataque como los descritos anteriormente nos pueden ocasionar frente a los beneficios que implica la implementación de medidas eficaces para enfrentar estos problemas donde se ve en juego el activo mas importante de la empresa: "La Información"

CAPÍTULO 5



CIB-ESPOL

5. CONCLUSIONES Y RECOMENDACIONES

Después del estudio realizado, hemos podido darnos cuenta de algunos aspectos básicos que no debemos olvidar al momento de implementar un esquema encaminado a la administración de recursos informáticos orientados al Internet:

- Los riesgos de seguridad al momento de emplear un determinado sistema operativo, en este caso Windows 2000 Server.

- El estudio de esos riesgos y el impacto dentro de nuestras organizaciones.

- El manejo de esas vulnerabilidades y la aplicación de las debidas medidas correctivas y preventivas.

- La elaboración de planes de contingencia en caso de que se explote alguna de las vulnerabilidades detectadas.

Generalmente no tomamos en cuenta ciertas normas básicas al momento de escoger una plataforma de trabajo que satisfaga las necesidades de la empresa y nos enfocamos hacia la facilidad de su administración o implementación. Recordemos que está en juego el recurso más importante dentro de una organización como lo es la "Información", y vale recordar que este es "Invaluable", de tal manera que debemos llevar el cuidado necesario para mantener a salvo mencionados recursos.

Dentro de este trabajo se encuentra especificado todos y cada una de las principales vulnerabilidades de Windows 2000 Server y su servidor IIS, así como también las contramedidas para fortalecer esas brechas de seguridad que tiene este sistema operativo.

Como conclusión final podríamos afirmar que la seguridad completa no existe y por ello, lo más importante para mantener un esquema de seguridad es reducir los riesgos y tomar las medidas necesarias para en lo posible minimizar el impacto de estas vulnerabilidades y aplicar las soluciones propuestas en los capítulos anteriores.

No debemos olvidar de lo importante que debe ser el análisis de todas las variables al momento de definir una herramienta como lo es Windows 2000 Server, ya que de eso depende sustancialmente la seguridad que su

organización vaya a implementar y como coexistir con los riesgos que eso implica.

Esperamos que la documentación antes descrita sirva para asegurar las vulnerabilidades de este sistema operativo y a su vez salvaguardar los recursos de las organizaciones.



CIB-ESPOL

ANEXOS

CIB-ESPOL

ANEXO A

PLAN DE CONTINGENCIA ORIENTADO AL MANEJO Y FORTALECIMIENTO DE LA SEGURIDAD DEL WINDOWS 2000 SERVER Y EL SERVICIO IIS

A continuación se muestran las principales actividades requeridas para la planificación e Implementación de una capacidad de recuperación de desastres.

- Identificación de riesgos
- Evaluación de riesgos
- Asignación de prioridades a las aplicaciones
- Establecimiento de los requerimientos de recuperación
- Elaboración de la documentación
- Verificación e implementación del plan
- Distribución y mantenimiento del plan

Identificación de riesgos

La primera fase del plan de contingencia, el análisis de riesgos, nos sitúa en el lugar de un asesor de una compañía de seguros. En esta fase, la

preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo?, ¿Qué puede ir mal? y ¿cuál es la probabilidad de que suceda?
Un inventario completo de una red muestra de manera clara la complejidad de ésta. Cualquiera que realice inventarios de componentes para redes, comprende los problemas en el seguimiento del hardware y software utilizado por los usuarios finales. Afortunadamente, existen algunos productos disponibles, como los de las compañías Seagate Software, McAfee y otros, que facilitan la construcción de un inventario de los sistemas.

Una omisión en el inventario fácilmente puede dar lugar a una recuperación fallida tras un desastre. El sistema de aplicación puede no encontrarse preparado para su uso si alguno de sus componentes no está disponible; en tal caso, es aconsejable estar constantemente a la expectativa de los nuevos elementos que pueden haberse olvidado. Por ejemplo, una aplicación para acceso remoto no funcionaría si los cables no están disponibles para conectar los módem.

Los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

Evaluación de riesgos

Es el proceso de determinar el costo para la organización de sufrir un desastre que afecte su actividad. Si una inundación impidiera la actividad comercial durante cinco días, la compañía perdería cinco días de ventas, además del deterioro físico de los edificios e inventario. En el caso de los sistemas informáticos, la preocupación principal es comprender la cantidad de pérdida financiera que puede provocar la interrupción de los servicios, incluyendo los que se basan en las redes.

Asignación de prioridades en las aplicaciones



CIB-ESPOL

Después de que acontezca un desastre y se inicie la recuperación de los sistemas, debe conocerse qué aplicaciones recuperar en primer lugar. No hay que perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad empresarial necesita primero sus aplicaciones esenciales.

Esto implica la necesidad de determinar por anticipado cuáles son las aplicaciones fundamentales del negocio. Si la empresa es como la mayoría, se tendrán aplicaciones "muy importantes" dependiendo de a quién se le pregunte. El departamento de recursos humanos afirmará que el sistema de

nóminas es el más importante, el departamento de ventas dirá que es su sistema de entrada de pedidos, el departamento de producción insistirá en su control de inventario y el departamento de compras asignará el papel de más importante a su sistema de facturación. Desgraciadamente, no todos estos sistemas pueden ser el más importante; por lo tanto, es fundamental que la dirección ayude a determinar el orden en que los sistemas serán recuperados.



CIB-ESPOL

Establecimiento de requisitos de recuperación

La clave de esta fase del proceso de elaboración del plan de migración es definir un periodo de tiempo aceptable y viable para lograr que la red esté de nuevo activa. El personal directivo de la organización deseará saber cuándo estarán sus aplicaciones funcionado para planificar la actividades de la compañía.

Es muy importante concederse una cantidad de tiempo adecuada y no realizar estimaciones poco realistas sobre las propias posibilidades. No es el deseo de nadie tener a un montón de gente alrededor esperando la finalización de las operaciones de recuperación; una distracción de este tipo probablemente perturbe las labores. El término para este objetivo es tiempo de recuperación objetivo o en inglés TRO (Recovery Time Objective).

Elaboración de la documentación

Crear un documento que mucha gente pueda tener como referencia es quizás lo más difícil del plan de contingencia. Implicará un esfuerzo significativo para algunas personas, pero ayudará a aprender cosas sobre el sistema y puede que algún día salve la empresa.

Los recursos necesarios para escribir y mantener un plan de contingencia representan más de lo que puede realizarse en ratos libres y después de horas de oficina. La dirección de la organización debe apoyar la iniciativa para que sea un éxito. Uno de los problemas del plan de contingencia en un entorno de comunicaciones es que la tecnología de redes cambia tan rápidamente que resulta difícil permanecer al día. Esto incluye nuevos dispositivos, así como nuevos sistemas de aplicación que introducen su propio nivel de complejidad en este campo.

Contenido del plan de contingencia

El plan de contingencia debe intentar definir las cinco áreas siguientes:

- Listas de notificación, números de teléfono, mapas y direcciones
- Prioridades, responsabilidades, relaciones y procedimientos

- Información sobre adquisiciones y compras
- Diagramas de las instalaciones
- Sistemas, configuraciones y copias de seguridad en cinta

Hay que cerciorarse de que se sabe a quién notificar en primer lugar cuándo ocurre un desastre. Por ejemplo, si hay un incendio, llamar primero a los bomberos y luego al director general. Pueden existir otras personas o organizaciones identificadas con características o conocimientos especiales que puedan ayudar a minimizar el daño. Si no se dispone de números de teléfono o direcciones actualizados, se puede pasar muy mal contactando con las personas afectadas.

Mapas mostrando las ubicaciones del centro de operaciones temporal y la instalación externa pueden ahorrar mucho tiempo. También puede ser útil mostrar itinerarios alternativos de acceso para el caso de que las rutas principales no se encuentren disponibles.

Verificación e Implementación del plan

Una vez redactado el plan, hay que probarlo. Hay que estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico sobre el propio trabajo, de manera que pueda uno probarse a sí mismo que funciona.

Psicológicamente, esto no es fácil porque con toda probabilidad se ha invertido una gran cantidad de tiempo y energía personal en este proceso, aunque lo mejor sería, si es posible, situarse de manera imparcial ante la confiabilidad del plan. Por consiguiente, han de realizarse las pruebas para encontrar problemas, no para verificar que el plan funciona. Si existen errores en la información, tómese nota de ellos y corríjase el plan.



CIB-ESPOL

Comprobación del plan por partes

No se puede tumbar el sistema algún día para ver si se es capaz de recuperarlo. Existen muchas y mejores formas de verificar un plan de contingencia sin utilizar mayores interrupciones en el trabajo de la organización. Algunas de las cosas en las que habitualmente no se piensa a la hora de comprobar pueden ahorrar mucho tiempo posteriormente. Por supuesto, también es necesario verificar los procedimientos que se emplearán para recuperar los datos. Compruébese el software para la realización de las copias de seguridad para confirmar si pueden recuperarse las aplicaciones de mayor prioridad de la manera esperada. Esto debería hacerse en una red aislada para evitar problemas con el servidor de licencias. Una vez recuperada la información, verifíquese si el usuario puede acceder a ella. Esto requiere de algunas estaciones de trabajo conectadas a la red para simular auténticos usuarios finales con cuentas en los servidos

originales. En este punto, puede ser necesario actualizar el plan para incluir información sobre el establecimiento de cuentas de usuario. Compruébese cada una de las operaciones del plan individualmente y examínese entonces si, como resultado, se tiene un sistema de red en funcionamiento. No está de más verificar el plan con otras personas de la organización que se encuentren tan familiarizadas con los productos o procedimientos empleados.



CIB-ESPOL

Distribución y mantenimiento del plan

Por último, cuando se disponga de un plan definitivo ya verificado, es necesario distribuirlo a las personas que necesitan tenerlo. Inténtese controlar las versiones del plan, de manera que no exista confusión con múltiples versiones. Así mismo, es necesario asegurar la disponibilidad de copias extra del plan para su depósito en la instalación exterior a en cualquier otro lugar además del lugar de trabajo. Manténgase una lista de todas las personas y ubicaciones que tienen una copia del plan. Cuando se actualice el plan, sustituya todas las copias y recoja las versiones previas.
El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más

importantes para la organización. Las modificaciones a esta parte del plan utilizarán modificaciones consecutivas a los procedimientos de recuperación.

ANEXO B

HERRAMIENTAS DE PROTECCIÓN DE LA SEGURIDAD DENTRO DE WINDOWS 2000 SERVER

URLScan

UrlScan es una herramienta de seguridad que restringe los tipos de peticiones HTTP que puede procesar Internet Information Services. Al bloquear peticiones HTTP concretas, la herramienta de seguridad UrlScan previene la posibilidad de que peticiones potencialmente dañinas puedan alcanzar el servidor. UrlScan 2.5 se puede instalar directamente sobre servidores con IIS4.0 o versión superior.

La herramienta de seguridad UrlScan consta de dos archivos: UrlScan.dll y UrlScan.ini, que juntos componen el paquete UrlScan.exe. La última actualización de UrlScan 2.5 ofrece a los administradores mayor control sobre la configuración de UrlScan y proporciona funcionalidades que ayudan a reforzar la seguridad del servidor.

UrlScan 2.5 introduce las siguientes funcionalidades, que no estaban disponibles en versiones anteriores:

- Cambio del directorio del archivo de log
- Log de URLs largas
- Restricción del tamaño de las peticiones

Windows Server 2000 incorpora muchas características de seguridad que permiten proteger los servidores IIS5.0. UrlScan aporta algunas funcionalidades adicionales, como el control de verbos, más allá de lo que ofrece IIS5.0. También sucede que algunas organizaciones han integrado ciertas funcionalidades de UrlScan en sus prácticas de administración de IIS y para otros servidores de Microsoft. Si desea utilizar las funcionalidades y características adicionales de UrlScan 2.5 o simplemente mantener su administración de seguridad actual, entonces puede considerar la posibilidad de instalar y utilizar UrlScan con IIS5.0.

IIS Lockdown Tool



CIB-ESPOL

La herramienta, conocida como IIS Lockdown Tool, permite hacer la configuración más adecuada de un servidor web de forma rápida y sencilla, de manera que el servidor provee únicamente aquellos servicios que el

administrador desea. Los clientes pueden utilizar esta herramienta para proteger instantáneamente sus sistemas contra las amenazas de seguridad.

La herramienta ofrece dos modos de operación. El modo por defecto es express el cual, con un simple clic de ratón, configura el servidor una avanzada seguridad apropiada para la mayoría de los servidores web básicos. Para aquellos administradores que deseen configurar particularmente sus servidores, la herramienta provee un modo avanzado. El sistema entrega una ayuda la cual provee información y recomendación para seleccionar la mejor configuración y además permitir que la última configuración sea reversada.

Considere esto: un servidor web configurado usando express lockdown puede ser completamente protegido contra virus y gusanos como "Code Red" y contra prácticamente todas las vulnerabilidades conocidas para IIS 4.0 o 5.0, incluso sin las actualizaciones para aquellas vulnerabilidades.



CIB-ESPOL

Software Update Services

Microsoft Software Update Services (SUS) está diseñado para simplificar el proceso de mantener sistemas basados en Windows con la última actualización crítica de seguridad. SUS habilita a los administradores para desplegar rápidamente y de forma segura las actualizaciones de seguridad en sus plataformas de servidor Windows 2000 Server así como en las

plataformas de escritorio Windows 2000 Professional y Windows XP Professional.

SUS provee ahora los Service Packs de Windows además de las actualizaciones críticas de seguridad. SUS incluirá Windows XP SP1, Windows 2000 SP4, y todos los futuros Service Packs de Windows 2000, Windows XP y la familia de productos de Windows Server 2003.



CIB-ESPOL

HFNetChk

Un elemento especialmente importante a la hora de hacer que un sistema sea seguro es mantenerse al día en cuanto a los parches de seguridad. Es crucial saber qué parches se han aplicado a sus sistema y, aún más importante, cuáles no se han aplicado. Microsoft ha lanzado una herramienta llamada HFNetChk que supondrá una ayuda significativa para los administradores de sistema en esta tarea. HFNetChk v3.81 está disponible a través de la interfaz de línea de comandos del Microsoft Baseline Security Analyzer (MBSA).

HFNetChk es una herramienta de línea de comando que permite al administrador comprobar el estado de los parches de todas las máquinas de una red desde una ubicación central. La herramienta actúa llamando a una

base de datos XML que Microsoft actualiza constantemente. HFNetChk puede ser ejecutado en sistemas Windows NT 4.0 o Windows 2000 y rastrea el sistema local o sistemas remotos en busca de parches para los siguientes productos:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Todos los servicios del sistema incluido Internet Information Server 4.0 y 5.0
- SQL Server 7.0 y 2000 (incluido Microsoft Data Engine)
- Internet Explorer 5.01 y posteriores
- Exchange 5.5 y 2000
- Windows Media Player 6.4 y posteriores

MBSA y HFNetChk han sido desarrollados para Microsoft por Shavlik Technologies LLC[113].

---

[113] Consultar http://www.shavlik.com/

MBSA

Microsoft ha desarrollado el Microsoft Baseline Security Analyzer (MBSA) como parte del Programa de estrategia de Protección Tecnológica, y en respuesta directa a las necesidades de los usuarios para un método dinámico de identificación de vulnerabilidades se seguridad.

MBSA Versión 1.2 incluye un gráfico y una interfaz de líneas de comando que permite ejecutar, local o remotamente, un escáner de los sistemas basados en Windows. MBSA se ejecuta en Windows 2000, Windows XP y Windows Server 2003 y puede buscar revisiones que faltan y vulnerabilidades de la seguridad en los siguientes productos: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS), SQL Server, Internet Explorer (IE) y Office.



CIB-ESPOL

ANEXO C

CASO DE ESTUDIO

"PENETRACIÓN DE VIRUS NIMDA A TRAVES DE VULNERABILIDAD DE WINDOWS 2000"

NIVEL DE ATAQUE: Alto



CIB-ESPOL

DETALLES DEL ATAQUE:

Nimda intenta introducirse de forma automática en los servidores Web basados en Internet Information Server explotando varias vulnerabilidades a través de peticiones GET vía HTTP, bien buscando tener acceso al intérprete de comandos, CMD.EXE, o al archivo ROOT.EXE, un troyano que ya habría sido introducido con anterioridad al ser infectado por los gusanos Code Red II o Sadmind.

Si el servidor es vulnerable a algunos de los ataques que Nimda lleva a cabo, aprovecha para ejecutar una sesión de TFTP y así descarga en el servidor Web el archivo ADMIN.DLL, que contiene el código vírico. Este archivo se copiará en las unidades C:, D: y E:

Para evitar que Nimda pueda explotar la vulnerabilidad de Internet Explorer, e impedir así que se ejecute de forma automática el archivo "readme.exe" al visualizar un mensaje infectado, debemos tener nuestro navegador correctamente actualizado.

Las versiones vulnerables son Internet Explorer 5.01 y 5.5 que no tengan instalado el Service Pack 2 o la actualización específica que Microsoft distribuyó para este problema. Los usuarios de Internet Explorer 6 no tienen que instalar ningún parche, no están afectados por esta vulnerabilidad.

Esta vulnerabilidad, fue corregida por Microsoft, que facilitó un parche específico para ella. En lugar de ese parche, recomendamos instalar una actualización acumulativa posterior donde ya se corrigen otras vulnerabilidades además de la que hoy nos ocupa:

Internet Explorer 5.01

Internet Explorer 5.5

Si tenemos el Internet Explorer correctamente actualizado, evitaremos que Nimda pueda infectarnos de forma automática, con tan sólo visualizar el mensaje en el que nos llega. Sin embargo, este parche no debe darnos una falsa sensación de seguridad total contra Nimda, ya que nos infectaríamos si abrimos el archivo adjunto.

Por tanto, una vez más, debemos seguir recordando la regla de oro de no abrir archivos adjuntos no solicitados.

Infección en Servidores

En servidores Windows, Nimda explota varias vulnerabilidades, en especial las relacionadas con la escalada de directorios a través de caracteres Unicode en la URL.

Para lograr una protección contra todas las vulnerabilidades que intenta explotar, lo mejor es instalar el último parche acumulativo disponible según versión en:

IIS 4.0

IIS 5.0

Asimismo, no debemos olvidar inspeccionar nuestro servidor en busca de troyanos, remanentes de una infección previa del Code Red y a los que Nimda intenta acceder para lograr la infección.

Además de las acciones que ya hemos ido comentando, Nimda se copia como "mmc.exe" en el directorio de Windows, como "load.exe" en el directorio de sistemas, sobreescribe la biblioteca "riched20.dll" del directorio de sistema y realiza una copia de la biblioteca infectada en todos los

directorios que contengan documentos (.doc). Por último, se copia repetidas veces en el directorio temporal de Windows con nombres de archivo aleatorios que empiezan por "mep" o "ma" y terminan con las extensiones .TMP o .TMP.EXE.

La biblioteca de windows riched20.dll es utilizada por los procesadores de texto como Word o WordPad. La sustitución de esta biblioteca por una infectada hace que el Nimda se ejecute cada vez que se utilice uno de estos procesadores de texto.

Asimismo se asegura su ejecución mediante una modificación en el system.ini:



CIB-ESPOL

[boot]

shell=explorer.exe load.exe -dontrunold

En Windows 9x/Me las unidades estarán compartidas sin ninguna clave de acceso, mientras que en Windows NT/2000 a la cuenta GUEST le da derechos de los grupos Administrators (máximos privilegios) y Guests (invitados).

En Windows NT/2000 elimina la clave que instaura la seguridad para compartir de recursos:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\

lanmanserver\Share\Security

Otras claves son creadas o modificadas para ocultar archivos y extensiones:

HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\Explorer\Advanced\HideFileExt

HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\Explorer\Advanced\Hidden

HKEY_CURRENT_USER\Software\Microsoft\Windows\

CurrentVersion\Explorer\Advanced\ShowSuperHidden

La infección continúa infectando archivos .EXE, anteponiendo su código, con la excepción del archivo Winzip.exe al que no infecta.

Aunque es posible intentar la limpieza manual, a base de restaurar las claves del registro, eliminar archivos infectados o instalar de nuevo los modificados, son tantos pasos los que hay que dar que, para no eternizar esta noticia y evitar descuidos, aconsejamos el uso de las utilidades que los antivirus están facilitando para realizar la desinfección de manera automática.

Esta penetración se dio en el servidor de correo y archivos de Hilantex S.A en el 2004 produciendo una pérdida de los sistemas Informáticos ya que no se contaba con ningún tipo de plan de contingencia y los debidos procedimientos para recuperación de desastres en especial contra este virus ya que no existía toda la documentación necesaria así como también se desconocía de las herramientas existentes en la actualidad para mantener el servidor actualizado con las últimas versiones de parches de seguridad.

ANEXO D

Tabla 3.1. Privilegios de Diferentes Tipos de Cuentas en Ambientes Windows 2000

Servicio de Autenticación sobre Windows 2000 Server	Intraforest solo en Windows 2000 Server	Multiforest con confianza NTLM entre dominios
Local user service account	Sin recursos de red, solo acceso local bajo privilegios de cuentas asignadas	Sin recursos de red, solo acceso local bajo privilegios de cuentas asignadas
Domain user service account	Acceso de red como usuario de dominio, acceso local bajo privilegios de usuario	Acceso de red como usuario de dominio, acceso local bajo privilegios de usuario
LocalSystem	Acceso de red como cuenta autenticada de usuario de computadora, acceso local bajo LocalSystem	Sin recurso de red período de red, acceso local bajo LocalSystem

CIB-ESPOL

ANEXO F

Tabla 3.2. Componentes Importantes de Seguridad

Componente	Definición
Amenaza	Una amenaza es un potencial peligro para la información o el sistema.
Agente de Amenaza	Un agente de amenaza es la persona o proceso atacando la red a través de un puerto vulnerable en el firewall, o un proceso utilizado para datos de acceso en una manera que viola las políticas de seguridad.
Vulnerabilidad	Una vulnerabilidad es un software, hardware o debilidad procesal que puede proveer a un atacante o agente de amenaza con una oportunidad para entrar a una computadora o red y ganar acceso desautorizado para recursos sin el ambiente.
Riesgo	Un riesgo es la posibilidad de que un agente de amenaza tome ventaja de una vulnerabilidad. Esto es potencial para perder o la probabilidad que una amenaza explotaría una vulnerabilidad.
Exposición	Una exposición ocurre cuando un agente de amenaza expone una ventaja de la compañía para pérdida potencial. Una vulnerabilidad puede causarle a una organización a ser expuesta a posibles daños.
Medidas de Prevención	Una medida de prevención o salvaguarda mitiga un riesgo. Una medida de prevención incluye configuración de software, hardware o procedimientos que eliminan una vulnerabilidad o reducen el riesgo de un agente de amenaza que puede ser explotado por una vulnerabilidad.

ANEXO G

Tabla 3.4. Componentes Importantes de Seguridad

Exploit	Ejemplo
Exploit de vulnerabilidad técnica	Buffer Overflow Desconfiguración Ataque Repetido Sesión Hijacking
Obteniendo Información	Identificación de dirección Mostrando documentos Identificación OS Escaneo de Puertos Análisis de respuestas Ingeniería Social Probando aplicaciones y servicios Enumeración de usuarios Escaneo de vulnerabilidades Fuga radiofónica
Denegación de Servicio (DoS)	Daño físico Recursos modificados Saturación de recursos Buffer Overflow

CIB-ESPOL

ANEXO H

Listado de las Vulnerabilidades más comunes en el Windows 2000 Server

No.	Vulnerabilidad	Nivel de Incidencia
1	Ejecución remota de código y denegación de servicios a través del TCP/IP	Crítica
2	Ejecución de código remoto a través de hiperlink object library	Crítica
3	Ejecución de código a través del control ActiveX DHTML	Crítica
4	Ejecución de código remoto a través de los componentes Ole y COM	Crítica
5	Ejecución de código remoto a través del servicio Server Message Block	Crítica
6	Ejecución de código remoto a través del servicio License Logging Service	Crítica
7	Desbordamiento de memoria en el servicio PNG	Crítica
8	Ejecución de código remoto a través del	Crítica

CIB-ESPOL

	manejador de formato de íconos y cursores	
9	Ejecución de código a través de la ayuda de archivos HTML	Crítica
10	Ejecución de código remoto a través del WINS (Windows Internet Naming Service)	Crítica
11	Elevación de privilegio en el Kernel de Windows y en el servicio LSASS	Crítica
12	Ejecución de código a través de HyperTerminal	Crítica
13	Ejecución de código remoto a través del protocolos NNTP	Crítica
14	Ejecución de código remoto a través de NetDDE	Crítica
15	Denegación de servicio a través del servicio WebDAV	Crítica
16	Ejecución de código a través del Programador de Tareas	Crítica
17	Denegación de servicio a través de Windows Media Services	Crítica
18	Desbordamiento de memoria en Microsoft Frontpage Server Extensions podría permitir	crítica

	ejecución de código remoto	
19	Desbordamiento de memoria en WorkStation Service podría permitir ejecución de código remoto	Crítica
20	Desbordamiento de memoria en la ayuda de Windows y Centro de Soporte podría comprometer el sistema	Crítica
21	Desbordamiento de memoria en el control Activex de Windows Troubleshooter podría permitir ejecución de código	Crítica
22	Ejecución de código remoto en la verificación de autenticación	Crítica
23	Desbordamiento de memoria en el servicio RPCSS podría permitir ejecución de código remoto	Crítica
24	Un buffer no chequeado en directX podría comprometer el sistema	Crítica
25	Desbordamiento de memoria en la interface RPC podría permitir ejecución de código remoto	Crítica
26	Desbordamiento de memoria en el convertidor	Crítica

CIB-ESPOL

	HTML podría permitir ejecución de código remoto	
27	Flaw en Microsoft VM podría comprometer el sistema	Crítica
28	Flaw en Windows Script Engine podría permitir ejecución de código.	Crítica
29	Buffer no chequeado en Windows Component podría comprometer el servidor	Crítica
30	Buffer no chequeado en el servicio Locator podría permitir ejecución de código	Crítica
31	Ejecución de código remoto a través de un buffer no comprobado en el Locator	Crítica
32	Ejecución remota de código a través de validación IP	Crítica
33	Denegación de servicios a traves de una conexión ICMP	Crítica
34	Denegación de servicios a través de la unidad MTU de ruta del protocolo ICMP	Crítica
35	Desbordamiento de memoria en el núcleo de Windows	Crítica
36	Desbordamiento de memoria en el cmd.exe	Crítica

37	Ejecución remota de código a través del servicio Web View	Media
38	Elevación de privilegios y denegación de servicios a través del kernel de windows	Media
39	Ejecución de código a través de la cola de mensajes	Media
40	Ejecución de código remoto a través del shell de Windows	Media
41	Error en la validación de ruta de archivos ASP	Media
42	Ejecución de código remoto a través del Wordpad	Media
43	Ejecución de código remoto a través de POSIX	Media
44	Ejecución de código a través del componente Utility Manager	Media
45	Ejecución de código a través de Microsoft Jet Database Engine	Media
46	Desbordamiento de memoria en Función MDAC podría permitir ejecución de código	Media
47	Desbordamiento de memoria en los controles ListBox y ComboBox podría permitir ejecución	Media

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

	de código	
48	Un buffer no chequeado en función MDAC podría comprometer el sistema	Media
49	Flaw en el manejador de mensajes de Windows a través del utility manager podría permitir una elevación de privilegio	Media
50	Desbordamiento de memoria en windows podría permitir corrupción de datos	Media
51	Flaw en la interfaz ISAPI para Windows Media Services podría originar ejecución de código.	Media
52	Flaw en RPC Endpoint Mapper podría permitir ataques de denegación de servicio	Media
53	Flaw en Windows WM TIMER podría habilitar elevación de privilegio	Media
54	Denegación de servicio a través del DirectPlay	Moderada
55	Desbordamiento de memoria en el Servicio de Messenger podría permitir ejecución de código	Moderada
56	Flaw en el NetBIOS podría permitir informacion inconsistente	Moderada
57	Flaw en SMB podría habilitar las políticas de grupo para ser habilitadas	Moderada

ANEXO I

Listado de las Vulnerabilidades más comunes en el Internet Information Server 5.0.

No.	Vulnerabilidad	Nivel de Incidencia
1	Posibilidad de un ataque de denegación de servicios cuando la petición de URL excede el máximo de la longitud permitida.	Crítica
2	Desbordamiento de memoria en la interfaz ISAPI	Crítica
3	Cross-site scripting en la opción de búsqueda de Archivos de Ayuda de IIS	Crítica
4	Los nombres largos de archivos inválidos provocan un desbordamiento de memoria en el servicio server-side includes (SSI)	Crítica
5	Posibilidad de un ataque de Denegación de Servicios por medio del WebDAV	Crítica
6	Denegación de Servicios a través de una petición de estado de conexión FTP mal creada.	Crítica
7	Desbordamiento de memoria vía comprobación	Crítica

	inexacta de los delimitadores en los campos de cabecera HTTP.	
8	Desbordamiento de memoria en una sección que codifica mecanismos de transferencia para ASP.	Crítica
9	Desbordamiento de memoria a través del protocolo IPP	Crítica
10	Problemas de Seguridad en el Servicio RDS (Remote Data Service)	Crítica
11	Cross-site scripting en la página de resultados de un error http	Media
12	Cross-site scripting en el mensaje de respuesta a una redirección	Media



CIB-ESPOL

ABREVIATURAS

ABREVIATURA	SIGNIFICADO
API	Interface de programación de aplicaciones
ASCII	Código Americano Estándar para Intercambio de Información
ASP	Active Server Pages
BIOS	Basic Input Output System
CA	Certification Authority
CGI	Common Gateway Interface
CIS	COM Internet Services
CPU	Central Process Unit
CSI	Computer Security Institute
CTL	Certificate Trust Lists
DC	Domain Controler
DCOM	Modelo de Objeto Componente Distribuido
DDL	Biblioteca de vínculos dinámicos
DNS	Domain Name Server
DOS	Denial of Service
EFS	Sistema de cifrado de archivos

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
ESPOL
CIB-ESPOL

FBI	Federal Bureau of Investigation
FPSE	FrontPage Server Extensions
FRS	File Replication Service
FTP	File Transfer Protocol
HTML	Hyper Text Markage Language
HTTP	Hyper Text Transfer Protocol
IAS	Internet Autentication Service
ICMP	Internet Control Message Protocol
ID	Identification
IDC	Internet Data Center
IDS	Sistema de detección de Intrusos
IIS	Internet Information Server
IP	Internet Protocol
IPSEC	Protocolo Seguro de Internet
ISA	Microsoft Internet Security and Acceleration
ISAPI	Interface de programación de aplicaciones para servicios de Internet
ISP	Proveedor de Servicios de Internet
LAN	Local Area Network
LM	LAN Manager
MACS	Microsoft Audit Collection System
MCIS	Microsoft Comercial Internet System

CIB-ESPOL
ESPOL ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

MMC	Microsoft Management Console
MOF	Microsoft Operations Framework
MOM	Microsoft Operations Manager
MSOU	Member Server Organizational Unit
MTA	Mail Transfer Agent
MTS	Transaction Server
MTU	Maxium Transfer Unit
NNTP	Network News Transport Protocol
NT	Windows NT
NTFS	New Technology File System
NTLM	Windows NT Challenge/Response
NTP	Protocolo de Tiempo de Red
OS	Operating System
OU	Unidad Organizacional
PC	Personal Computer
PDC	Primary Domain Controller
PIN	Número de identificación personal
RADIUS	Remote Authentication Dial-In User Service
RCPT	Recipient
RPC	Remote Procedure Call
RPCSS	Administrador de Mensajes RPC
SAM	Security Accounts Manager

SID	Specific Security Identifier
SMB	Server Message Block
SMF	Service Management Functions
SMTP	Simple Mail Transfer Protocol
SQL	Structure Query Language
SSI	Server-side includes
SSL	Secure Socket Layer
WebDAV	World Wide Web Distributed Authoring and Versioning
SSP	Proveedor de asistencia de seguridad
STPP	Strategic Technology Protection Program
TCP	Transfer Control Protocol
TCP/IP	Transfer Control Protocol / Internet Protocol
TGS	Ticket Granting Service
TI	Tecnología de Información
TLS	Transport Layer Security
UDP	User Data Protocol
URL	Universal Resolution Link
W3C	World Wide Web Consortium
WAN	World Area Network
WINS	Servicio de nombres de Internet de Windows
XML	Extensible Markup Language
XP	Windows XP

BIBLIOGRAFÍA

Direcciones en Internet:

- www.tec-mex.com.mx/downloads/dl_previa.htm
- http://www.htmlweb.net/seguridad/tesis/tesis.html
- http://usuarios.lycos.es/keu99/delitosinformaticos.html
- http://www.alfa-redi.org/upload/revista/10503--20-41-Delitos%20Informaticos%20-%20Blossiers.pdf
- http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SeguridadWin2000.PDF
- http://www.vnunet.es/Hemeroteca/Resultados/Tema/Windows_2000
- http://www.agapea.com/Seguridad-en-Microsoft-Windows-2000-Referencia-tecnica-n8648i.htm
- http://www.arcert.gov.ar/webs/webdocs.html
- http://www.abcdatos.com/tutoriales/software/servidores.html
- http://www.abcdatos.com/tutoriales/tutorial/o470.html
- http://desarrollo.ethek.com/Desarrollo/contenido.asp?IDContenido=86
- http://www.htmlpoint.com/

- http://www.conocimientosweb.net/portal/directorio-cat-27.html&orderby=dateD
- http://www.maxitrucos.com/Manuales/M_win2000.htm
- http://www.microsoft.com/spain/technet/recursos/articulos/secmod220.mspx
- http://www.hispasec.com/unaaldia/1630
- http://www.sincables.net/modules.php?name=News&file=print&sid=907
- http://www.error500.net/modules/news/article.php?storyid=850

Fuentes Consultadas

- Datos Estadísticos del Cert http://www.kb.cert.org/vuls/id/668916
- Ecuacotton S.A. Km. 7 ½ vía a Daule Lsi. Humberto Ledesma
- Burger King Co. C.C. Dicentro Anl. Mauricio Granda
- Hilantex S.A Km. 7 ½ vía a Daule Ing. Jorge Ortega López



CIB-ESPOL