

UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA



ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

INGENIERÍA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

TEMA

Diseño, análisis, pruebas e implementación de un esquema de seguridad para la plataforma Windows

*Tesis de grado previa a la obtención del
Título de: Ingeniero en Sistemas
Informáticos y Computación*

AUTOR

Diego Geovanny Ordóñez Bazarán

DIRECTOR

Ing. Janneth Chicaiza

LOJA – ECUADOR

2008

CERTIFICACIÓN

Ingeniera

Janneth Chicaiza

DIRECTORA DE TESIS

CERTIFICA:

Que el presente trabajo de investigación previo a la obtención del título de **INGENIERO EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN**, ha sido dirigido, supervisado y revisado en todas sus partes, cumpliendo con todas las exigencias y requisitos legales establecidos por la Universidad Técnica Particular de Loja, quedando autorizada su presentación.

Loja, octubre del 2008

Ing. Janneth Chicaiza

AUTORÍA

El presente proyecto de tesis con cada una de sus observaciones, conceptos, ideas, opiniones, conclusiones y recomendaciones vertidas, son de absoluta responsabilidad del autor.

Además, es necesario indicar que la información de otros autores empleada en el presente trabajo está debidamente especificada en fuentes de referencia y apartados bibliográficos.

Diego Geovanny Ordóñez Bazarán

CESIÓN DE DERECHOS

Yo, Diego Geovanny Ordóñez Bazarán declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: ***“Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.***

Diego Geovanny Ordóñez Bazarán

AGRADECIMIENTO

Agradecer a la Universidad Técnica Particular de Loja, por haberme brindado los medios y conocimientos necesarios en mi formación tanto a nivel personal como académica que me permitirán desarrollarme profesionalmente.

A la escuela de Ciencias de la Computación por todos los conocimientos impartidos durante el proceso de mi formación profesional.

A mi directora de Tesis Ing. Janneth Chicaiza, por el asesoramiento, dirección, sugerencias y enseñanzas que han sido de mucha utilidad para el desarrollo y culminación de este proyecto de investigación.

A mis familiares, amigos, compañeros y todas aquellas personas que colaboraron brindándome su apoyo durante el desarrollo de mi tesis.

EL AUTOR

DEDICATORIA

Primeramente al Todo Poderoso por darme la oportunidad de vivir la vida.

De manera muy especial a la memoria de mi hermano, que fue el que me motivo a estudiar y más que nada me enseñó a perseverar en la vida y que es a quien guardaré infinita admiración, respeto y gratitud por las palabras de aliento que me brindo mientras estuvo en esta vida.

A mis padres y hermanos que siempre han confiado y brindado el apoyo que me impulsa a mejorar día tras día.

A todos mis amigos que con su alegría y palabras de aliento han contribuido hacer realidad esta investigación.

Diego

ESQUEMA DE CONTENIDOS

CERTIFICACIÓN.....	II
AUTORÍA.....	III
CESIÓN DE DERECHOS	IV
AGRADECIMIENTO	V
DEDICATORIA.....	VI
ESQUEMA DE CONTENIDOS.....	VII
DESCRIPCIÓN DEL PROBLEMA	XI
OBJETIVOS.....	XII
1. INVESTIGACIÓN PRELIMINAR	1
1.1 INTRODUCCIÓN.....	3
1.2 GENERALIDADES DE LAS PLATAFORMAS WINDOWS	3
1.3 CARACTERÍSTICAS DE SEGURIDAD GENERALES QUE OFRECEN LAS PLATAFORMAS WINDOWS.....	7
1.3.1 Sistema de Autenticación	8
1.3.2 Sistemas Operativos de Servidor	8
1.4 ANÁLISIS DE LAS CARACTERÍSTICAS DE SEGURIDAD DE LAS PLATAFORMAS WINDOWS MÁS UTILIZADAS.....	8
1.4.1 CARACTERÍSTICAS DE SEGURIDAD DE PLATAFORMAS WINDOWS PARA PC's	9
1.4.1.1 <i>La Seguridad en Windows XP y Windows Vista</i>	9
1.4.2 CARACTERÍSTICAS DE SEGURIDAD DE PLATAFORMAS WINDOWS PARA SERVIDORES.....	12
1.4.2.1 <i>Seguridad que posee Windows NT</i>	12
1.4.2.2 <i>Seguridades características de la plataforma Windows 2000 Server</i>	12
1.4.2.3 <i>Seguridad de Windows Server 2003 y Windows Server 2008</i>	13
1.5 TENDENCIAS DE ATAQUES A LAS PLATAFORMAS WINDOWS	16
1.6 PROBLEMAS DE SEGURIDAD COMUNES Y ESPECÍFICOS DE LAS PLATAFORMAS WINDOWS	18
1.7 ASPECTOS Y COMPONENTES DE UN ESQUEMA DE SEGURIDAD PARA ENTORNOS WINDOWS	19
1.7.1 Definición de Esquema de seguridad.....	19
1.7.2 Componentes que debe abarcar un esquema de seguridad Windows	19
1.8 VENTAJAS DE UN ESQUEMA DE SEGURIDAD	21
1.9 ESTÁNDARES A SEGUIR EN INFRAESTRUCTURAS DE SEGURIDAD WINDOWS.....	21
1.9.1 Buenas Prácticas para la Seguridad Corporativa.....	23
1.9.2 Seguridad para Servidores Windows	24
1.9.2.1 <i>Estándares para infraestructuras de seguridad de Servidores Basados en Windows</i>	24
1.10 PUNTUALIZACIONES.....	28
2. TÉCNICAS DE CONFIGURACIÓN E INSTALACIÓN.....	29
2.1 INTRODUCCIÓN.....	31
2.2 ANÁLISIS DE VULNERABILIDADES Y ATAQUES A SISTEMAS WINDOWS SERVERS.....	31
2.2.1 Definición de Vulnerabilidad.....	31
2.2.2 Análisis y mitigación de servicios afectados por las vulnerabilidades en Windows.....	33
2.2.3 Amenazas y ataques a los sistemas informáticos	38
2.2.4 Categorías de Amenaza en plataformas Windows	39
2.2.5 Agentes de la Amenaza en Windows.....	40
2.3 CONFIGURACIONES DE LÍNEA BASE PARA LOS SERVIDORES WINDOWS	40
2.3.1 Directivas	41
2.3.1.1 Directivas de Domino	43
2.3.1.2 Directivas de Línea de Base para los Servidores Miembros	43
2.3.1.3 Otras Opciones de Seguridad	44
2.3.1.4 Grupos Restringidos	50
2.3.1.5 Configuración de seguridad adicional	51
2.3.1.6 Directivas de Línea de Base para el Controlador de Domino	53
2.3.2 Seguridad de cada función del servidor.....	56
2.3.3 Herramienta Microsoft Security Baseline Analyzer (MBSA) y validación de configuración de puertos.....	56
a. <i>Herramienta MBSA</i>	56

<i>b. Validación de la configuración de puertos</i>	57
2.4 POLÍTICAS DE UTILIZACIÓN DE WINDOWS UPDATE EN UN SERVIDOR WINDOWS	57
2.5 RESUMEN Y CHECKLIST DE LAS TÉCNICAS DE CONFIGURACIÓN E INSTALACIÓN DE SEGURIDADES EN LAS PLATAFORMAS WINDOWS	58
2.6 PUNTUALIZACIONES.....	70
3. IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD	71
3.1 INTRODUCCIÓN.....	73
3.2 DESCRIPCIONES GENERALES QUE COMPRENDE UN ESQUEMA DE SEGURIDAD.....	73
3.2.1 Consideraciones previas	73
3.2.2 Proceso sugerido de implementación.....	73
3.2.3 Medidas de seguridad para servidores Windows	75
3.2.4 Consideraciones de seguridad referentes al Sistema Operativo	77
3.2.5 Conceptos a considerar en la elaboración de un esquema de seguridad	79
3.3 DISEÑO DEL ESQUEMA DE SEGURIDAD.....	83
3.3.1 Diseño de la Seguridad de los Servidores Windows	83
3.3.2 Esquema de los servidores Windows de la UTPL.....	85
3.3.3 Rol de los servidores y aplicaciones de acuerdo a su nivel de exposición y criticidad	87
3.3.4 Evaluación de necesidades, objetivos y servicios que presta la UTPL.....	90
3.3.5 Evaluación de requerimientos de seguridad adecuados para los servidores Windows de la UTPL.....	91
3.3.6 Medidas de seguridad aplicables a los servidores Windows del GDS de la UTPL	94
3.4 IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD.....	94
3.4.1 Detalle de configuraciones que abarca el Esquema de Seguridad.....	94
3.4.2 Evaluación de Resultados del Esquema y Herramientas utilizadas.....	102
3.5 APLICACIÓN DE CONFIGURACIONES AL GDS.....	103
3.5.1 Políticas a activar para el GDS.....	103
3.5.2 Servicios básicos que se deben ejecutar en los servidores del GDS.....	104
3.5.3 Revisiones de recursos compartidos en los servidores del GDS	106
3.5.4 Nivel de seguridad que deben mantener los servidores del GDS que están directamente conectados a Internet	106
3.5.5 Configuración de Políticas de Seguridad a nivel firewall para los servidores del GDS	106
3.5.6 Recomendaciones sobre el número de cuentas de usuario que se debe tener por servidor en el GDS	107
3.5.7 Novedades de diseño en la creación de una línea base de seguridad para los servidores miembros del GDS	107
3.6 PUNTUALIZACIONES.....	108
4. EVALUACIÓN DE RESULTADOS DEL ESQUEMA DE SEGURIDAD PARA EL GDS DE LA UTPL	109
4.1 INTRODUCCION.....	111
4.2 LABORATORIO	111
4.2.1 Descripciones Generales.....	111
4.2.2 Desarrollo	113
4.2.3 Herramientas Utilizadas.....	115
4.2.4 Evaluación.....	115
4.2.5 Resultados	116
4.3 PASOS SEGUIDOS EN LA EVALUACIÓN Y PRUEBAS DE FUNCIONALIDAD DEL ESQUEMA DE SEGURIDAD DE LOS SERVIDORES VIRTUALES WINDOWS SIMILARES A LOS DEL GDS	117
4.4 ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS OBTENIDOS DE LAS PRUEBAS DE FUNCIONALIDAD DEL ESQUEMA DE SEGURIDAD.....	119
4.5 CHECKLIST A CONSIDERAR EN LA CONFIGURACIÓN DE SEGURIDAD DE UN SERVIDOR WINDOWS SERVER 2003	124
4.6 PUNTUALIZACIONES.....	126
5. CONCLUSIONES Y RECOMENDACIONES	127
5.1 CONCLUSIONES	128
5.2 RECOMENDACIONES	130
6. BIBLIOGRAFIA	132

7. ANEXOS..... 136

ANEXO 1.1	CARACTERÍSTICAS DE SEGURIDAD DE SISTEMAS OPERATIVOS WINDOWS PARA PC'S	137
PLANTILLA 3.1	CHECKLIST HARDWARE DE SERVIDORES WINDOWS PREVIO A INSTALAR WINDOWS SERVER 2003.....	139
ANEXO 3.1	CONFIGURACIÓN DE ACTIVE DIRECTORY	141
ANEXO 3.2	DETALLE PERSONALIZADO DE CONFIGURACIÓN DE LA PLANTILLA DE SEGURIDAD PARA UN SERVIDOR MIEMBRO DE UN DOMINIO	150
ANEXO 3.3	CONVERSIÓN DE SERVIDORES MIEMBROS EN CONTROLADOR DE DOMINIO PRIMARIO Y DE BACKUP.....	169
ANEXO 3.4	CONFIGURACIÓN DE FIREWALLS EN CADA SERVIDOR MIEMBRO DEL GDS DEL DOMINIO UTPL.....	183
ANEXO 3.5	CREACIÓN DE UNA LÍNEA BASE DE SEGURIDAD DE SERVIDORES MIEMBRO	186
ANEXO 4.1	PRUEBAS DE SEGURIDAD DE LOS SERVIDORES WINDOWS DEL GDS.....	196
ANEXO 4.2	TEST DE ESCANEAMIENTO Y FUNCIONALIDAD DE LOS SERVIDORES WINDOWS DEL GDS.....	201

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS PARA CONFIGURAR SEGURIDADES EN WINDOWS SERVER 2003..209

INDICE DE TABLAS

CAPITULO I

Tabla 1.1.	Estadísticas de los sistemas operativos más utilizados hasta el 31 de agosto del 2008	4
Tabla 1.2.	Características de seguridad de las ediciones de Windows XP	9
Tabla 1.3.	Características de seguridad y sus beneficios en Windows Vista	10
Tabla 1.4.	Seguridades relevantes que posee la plataforma Windows 2000 Server	13
Tabla 1.5.	Seguridades de Windows Server 2003 y 2008	14
Tabla 1.6.	Servicios, puertos y protocolos que sufren ataques con frecuencia en Windows.....	17
Tabla 1.7.	Problemas comunes y específicos de Windows.....	18
Tabla 1.8.	Estándares de Seguridad para la Información	22

CAPITULO II

Tabla 2.1.	Tipos de vulnerabilidades comunes.....	32
Tabla 2.2.	Vulnerabilidades 2007: Top 10	33
Tabla 2.3.	Servicios afectados por vulnerabilidades críticas en plataformas Windows	34
Tabla 2.4.	Índice de gravedad de vulnerabilidades	37
Tabla 2.5.	Herramientas para realizar escaneos de vulnerabilidades en plataformas Windows	37
Tabla 2.6.	Definiciones de ataques a sistemas de información	39
Tabla 2.7.	Categorías de Amenaza	39
Tabla 2.8.	Categorías de Amenaza	40
Tabla 2.9.	Directivas básicas para un servidor miembro	44
Tabla 2.10.	Recomendaciones sobre las entradas del Registro de TCP/IP	44
Tabla 2.11.	Configuración de Afd.sys agregada al registro por la directiva de línea de base para los servidores miembros.....	47
Tabla 2.12.	Entradas del registro que se recomienda configurar	48
Tabla 2.13.	Sistema de archivos a asegurar.....	50
Tabla 2.14.	Configuración de derechos de usuarios agregados manualmente	51
Tabla 2.15.	Configuración de Terminal Server	53
Tabla 2.16.	Configuración de asignación de derechos de usuarios recomendada	54
Tabla 2.17.	Opciones de seguridad recomendadas en un controlador de dominio	55
Tabla 2.18.	Configuración de derechos de usuarios adheridos manualmente.....	55
Tabla 2.19.	Descripción de validaciones de seguridad permitidas con la herramienta MBSA	57
Tabla 2.20.	Puertos a los que escuchará un servidor miembro después de aplicar la directiva de línea de base para servidores miembros	57
Tabla 2.21.	Configuraciones de Seguridad en Windows Server 2003	59

CAPITULO III

Tabla 3.1. Medidas de seguridad Windows.....	75
Tabla 3.2. Configuraciones de seguridad.....	78
Tabla 3.3. Servicios que se instalan por defecto en Windows Server 2003	80
Tabla 3.4. Nivel de medición del riesgo en los servidores del GDS	89
Tabla 3.5. Criticidad de los servidores del GDS	90
Tabla 3.6. Descripción de servidores del ambiente de Producción	92
Tabla 3.7. Descripción de servidores del entorno de Desarrollo y Pruebas	93
Tabla 3.8. Descripción Hardware de los Servidores Windows del GDS	96
Tabla 3.9. Directivas de Seguridad que difieren entre el DC y un Servidor miembro del GDS	98
Tabla 3.10. Servicios a habilitarse en el DC del GDS.....	99
Tabla 3.11. Configuración de permisos de archivos ejecutables de Windows	100
Tabla 3.12. Aseguramiento de carpetas adicionales del DC.....	100
Tabla 3.13. Configuraciones de Seguridad a nivel de Dominio para el GDS	101
Tabla 3.14. Puertos utilizados por aplicaciones o servicios del GDS	101
Tabla 3.15. Herramientas de configuración de seguridad de Windows Server 2003	102
Tabla 3.16. Servicios Básicos	104

CAPITULO IV

Tabla 4.1. Detalles Hardware y Software de la máquina Host	112
Tabla 4.2. Descripción de máquinas virtuales	113
Tabla 4.3. Herramientas utilizadas en la implementación del Esquema de Seguridad	115
Tabla 4.4. El antes y después de aplicar seguridades a un Sistema Operativo Windows Server 2003.....	116

INDICE DE FIGURAS

CAPITULO I

Figura 1.1. Evolución de Microsoft Windows	4
Figura 1.2. Detalle del proceso como se perpetra un ataque a un sistema operativo	18
Figura 1.3. Componentes de un Esquema de Seguridad Global.....	20

CAPITULO II

Figura 2.1. Análisis de los riesgos en un sistema informático	38
Figura 2.2. Entornos de seguridad existentes y planeados	41
Figura 2.3. Cuadro sinóptico de tipos básicos de directivas en Plataformas Windows	42
Figura 2.4. Directivas de configuración para un dominio	43

CAPITULO III

Figura 3.1. Modelo de creación de un Esquema de Seguridad	74
Figura 3.2. Forma en que opera un PDC conjuntamente con el BDC	85
Figura 3.3. Diagrama de red de los servidores Windows que operan en el ambiente de Producción	86
Figura 3.4. Diagrama de red de los servidores Windows del ambiente de Desarrollo y Pruebas	87
Figura 3.5. Diagrama de Seguridad de los Servidores Windows	95

CAPITULO IV

Figura 4.1. Detalle del proceso de implementación de seguridades en las plataformas Windows.....	114
Figura 4.2. Comparación de políticas configuradas de las aplicadas.....	116
Figura 4.3. Cambios en las políticas de auditoría al configurar seguridades en un servidor Windows	117
Figura 4.4. Relación Costo grado de seguridad	117
Figura 4.5. Resultados de análisis de Windows Server 2003 sin seguridades configuradas.....	120
Figura 4.6. Datos informativos de las vulnerabilidades de seguridad del servidor NODO1SGA del entorno de producción del DGS de la UTPL.....	120
Figura 4.7. Resultado del análisis de Windows Server 2003 con seguridades configuradas	121
Figura 4.8. No presentación del último usuario logeado en el sistema.....	122
Figura 4.9. Cumplimiento de políticas fuertes de cambio de contraseñas.....	123
Figura 4.10. Cumplimiento de políticas de deshabilitación de cuentas	123

DESCRIPCIÓN DEL PROBLEMA

La seguridad informática es un proceso continuo que requiere una evolución permanente de los mecanismos de seguridad implementados, con el propósito de mejorarlos constantemente de acuerdo a las necesidades empresariales

Los esquemas de seguridad garantizan seguridad a nivel físico, a nivel de datos, usuarios finales, aplicaciones, equipos, red, etc., para esto se debe basar en estándares que garanticen el cumplimiento de políticas y procedimientos, que permitan tener un ambiente confiable.

La finalidad de esquematizar la seguridad de la información es por la identificación y aseguramiento de todos los activos y procesos esenciales que posee una entidad para su desarrollo, para lo cual debe implementar medidas y controles tanto preventivos como proactivos, planes de contingencia, de operatividad, y de recuperación para proceder cuando se ha materializado un ataque, y de esta manera minimizar al máximo las pérdidas de la información.

La Universidad Técnica Particular de Loja como entidad que brinda servicios de Educación Superior, necesita garantizar la seguridad en todos los niveles de TI, uno de ellos es su infraestructura de servidores que operan bajo la plataforma Windows, ya que en esta plataforma existen varios sistemas de información que están en producción, tal es el caso del Sistema de Gestión Académico que está ejecutándose sobre servidores Windows 2003 Server. Éste sistema maneja información crítica, por lo que requiere de un esquema de seguridad apropiado para cada entorno de despliegue del sistema (producción, desarrollo y pruebas) para de esta forma asegurar la confidencialidad, integridad, disponibilidad y autenticidad de la información que maneja día a día en sus actividades a las cuales está orientado dicho sistema.

Para lograr tal propósito, se propone el análisis, diseño, pruebas e implementación de un esquema de seguridad que trabaje en plataformas Windows, ajustado a las características y necesidades específicas de la Universidad Técnica Particular de Loja.

OBJETIVOS

Objetivo General

- Implementar un esquema de seguridad para plataformas Windows.

Objetivos Específicos

- Estudiar las diversas seguridades de las plataformas Windows.
- Analizar las mejores medidas de seguridad aplicables a los servidores que operan bajo plataformas Windows.
- Estudiar el estado actual de los servidores Windows de la UTP
- Definir y evaluar los requerimientos de seguridad adecuados para cada servidor Windows.
- Probar mecanismos y métodos eficaces con enfoque activo hacia la seguridad en un servidor Windows.
- Seleccionar la alternativa o mecanismo apropiado a utilizar en un esquema de seguridad de servidores Windows.
- Proporcionar las mejores prácticas de protección para servidores, con la finalidad de brindar soluciones óptimas a la vulnerabilidad de los servidores Windows.
- Presentar una serie de políticas y procedimientos para el desempeño satisfactorio de un servidor Windows.
- Elaborar una descripción detallada de todas las consideraciones que se debe tomar en cuenta, previo a la puesta en marcha de un servidor Windows.

CAPITULO I
INVESTIGACIÓN PRELIMINAR

Objetivos

- Investigar las características comunes de seguridad en plataformas Windows
- Establecer ventajas de un esquema de seguridad para plataformas Windows
- Analizar estándares de seguridad para infraestructuras de seguridad Windows



1.1 INTRODUCCIÓN

Las diversas características de seguridad en plataformas Windows están orientadas a ayudar a una organización a lograr un nivel adecuado de seguridad, que le lleve a mantener asegurados sus sistemas de cómputos actuales y futuros.

Una cosa es crear un ambiente que está seguro desde un inicio, sin embargo, una vez que el ambiente está funcionando, es algo totalmente diferente mantener el ambiente seguro en el tiempo, tomar acciones preventivas contra amenazas y después responder a éstas de manera efectiva cuando ocurre.

Por todas las tareas de seguridad que se tienen que considerar en Esquemas de seguridad, se hace un recuento de algunas generalidades de las plataformas Windows desde que hicieron su aparición hasta la actualidad, de igual forma se analiza las características de seguridad de manera global de todas las versiones Windows que con anterioridad han salido al mercado, incluido Windows Vista y Windows Server 2008.

Se analiza las diversas formas en que las plataformas Windows son atacadas, y cuáles son los problemas de seguridad más comunes y específicos de éstos sistemas operativos.

También se analiza aspectos generales que debe abarcar un Esquema de Seguridad, las ventajas que brinda y los estándares a seguir o tomar en consideración cuando se elabora Esquemas de Seguridad Windows.

1.2 GENERALIDADES DE LAS PLATAFORMAS WINDOWS

Las diferentes versiones de las plataformas Microsoft Windows empezaron haciendo su aparición por el año 1985 con la versión **Windows 1.0**, en un inicio tenía pocas funcionalidades, pero con el paso del tiempo fue mejorando hasta convertirse hoy en día en el sistema operativo más utilizado a nivel mundial, existen estadísticas que confirman a las plataformas Windows como las que tienen mayor acogida en los últimos años por los usuarios finales.



Tabla 1.1. Estadísticas de los sistemas operativos más utilizados hasta el 31 de agosto del 2008
Fuente: <http://www.w3counter.com/globalstats.php>

Operating Systems		
1	Windows XP	74.31%
2	Windows Vista	11.30%
3	Mac OS X	4.93%
4	Windows 2000	2.37%
5	Linux	2.00%
6	Windows 2003	0.72%
7	Windows 98	0.66%
8	Windows ME	0.26%
9	SymbianOS	0.08%
10	Windows NT	0.03%

Windows es desarrollado por la empresa Microsoft y el éxito de su acogida, se debe a que es un sistema operativo que está basado en gráficos (ventanas), lo que es muy atractivo e intuitivo para el usuario final. A continuación en el gráfico se puede apreciar cómo ha evolucionado el sistema operativo Windows desde su aparición.

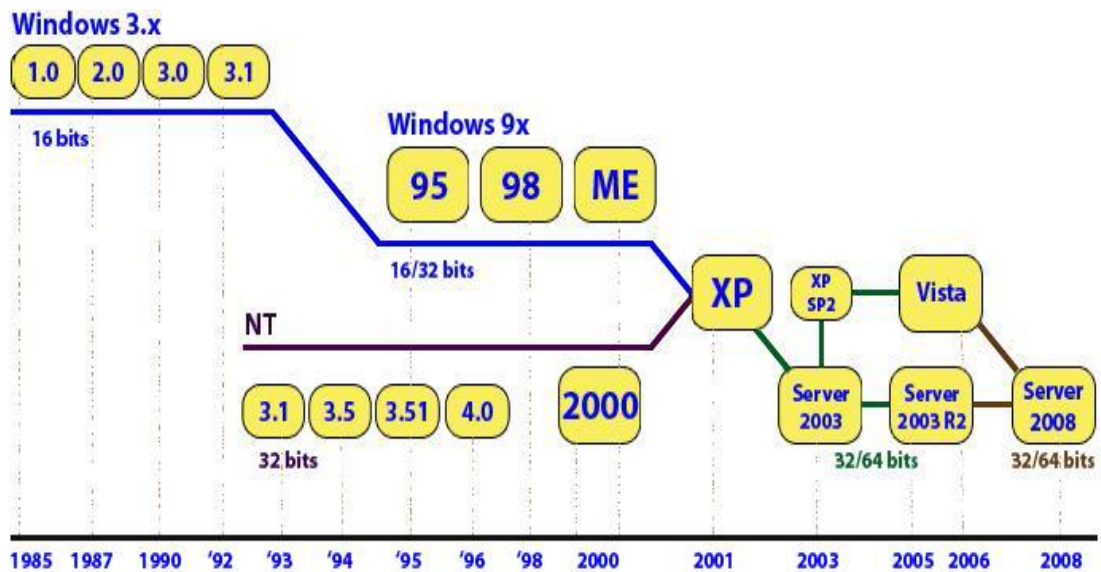


Figura 1.1. Evolución de Microsoft Windows
Fuente: <http://www.alegsa.com.ar/Notas/139.php>

Desde la primera versión del sistema operativo Windows, hasta la actualidad, ha ido mejorando de manera integral de versión a versión, las versiones iniciales de Windows si bien era cierto que se las consideraba como sistemas operativos, no se convertían en tales por el hecho de que dependían del sistema operativo MS-DOS (Microsoft Disk Operating System), por ello siempre se hablaba o se lo concebía a Windows como una interfaz gráfica para el MS-DOS ya que necesitaba la instalación previa de éste para su funcionamiento. Pero a partir del año 1993 con la salida de **Windows NT 3.1**,



este sistema comienza a repuntar y a ser considerado como un autentico sistema operativo, este Windows contaba con algunas especificaciones para el trabajo en red así como para realizar comunicaciones punto a punto.

En el año 1995 se lanza al mercado un sistema operativo Windows para PC's basados en IBM (International Business Machines) llamado **Windows 95** con un entorno gráfico real, este sistema rápidamente se convierte en el más utilizado y se caracterizaba por utilizar el acceso a ficheros de 32 bits, que le permitía nombres largos de archivos, tenía un sistema de archivos FAT16 (File Allocation Table), disponía de un DOS propio, llamado MS-DOS 7.0 y los requerimientos de instalación eran bajos y su rendimiento bastante aceptable.

Al sistema operativo se lo fue mejorando con el paso del tiempo y se le incluyo muchas más funcionalidades como la incorporación de Internet Explorer, soporte para USB (Universal Serial Bus), sistema de archivos FAT32, soporte para DMA (Direct Memory Access) y se mejoró el rendimiento y fiabilidad del sistema en general. La instalación de este Windows se la podía realizar desde la unidad de CD o desde disquetes.

En el año 1998 se lanza una nueva versión del sistema operativo Windows bajo el nombre de **Windows 98** que al año siguiente se lanzaría como Windows 98 segunda edición, este tipo de sistema operativo se basa en el sistema operativo Windows 95, las características principales del Windows 98 fueron, reafirmar y mejorar las utilidades que se habían incluido en el sistema Windows 95, además se le agregó un nuevo controlador denominado Win32, el cual incluye el soporte para USB, DVD y el IEEE (Institute of Electrical and Electronics Engineers) 1394, éste sistema mejora la gestión de memoria e incluye soporte para una variedad de procesadores de la época. Así el Windows 98 y en especial la segunda edición, se ha convertido en el sistema operativo más estable que Microsoft ha elaborado y es ideal para instalar en equipos poco potentes, ya que aprovecha de muy buena manera los recursos del equipo.

En el 2000 Microsoft saca el sistema operativo **Windows Millenium**, pues este tipo de sistema operativo se caracterizó por ser un sistema de transición, no tuvo muchas innovaciones, todos los complementos que le incluyeron al sistema terminaron por dar muchas confusiones y problemas, terminó por convertirse en el sistema operativo Windows de más corta vida en el mercado.

En temas referentes a sistemas operativos aplicables a entornos empresariales, Microsoft desarrollo el **Windows NT**, que empezó por el año 1993 con sus primeras versiones pero es en el año 1996 que Microsoft lanzó el sistema operativo **Windows NT 4.0** que a la final sería el último de la familia NT, éste sistema operativo se caracterizó por utilizar el sistema de archivos NTFS (New Technology File System), usaba una arquitectura de 32 bits y fue el primer sistema Windows aplicado para la gestión de redes e independientemente de sistemas operativos Unix. NT fue desarrollado para ordenadores potentes, pues necesitaba de gran cantidad de recursos para su operación.

Windows 2000 Server, sistema operativo que apareció en el año 2000 y fue el sucesor del sistema operativo Windows NT 4.0, de igual manera éste sistema operativo fue diseñado para entornos



empresariales y de manera concreta para servidores, éste Windows se caracterizó por estar desarrollado a base de las mejores ideas concebidas de los sistemas Windows 9x (Windows 95, 98, ME) así como lo mejor del sistema operativo Windows NT acompañado de una gran capacidad Plug and Play, de las que carecían las versiones anteriores de NT.

Microsoft sacó al mercado algunas versiones del sistema operativo Windows 2000 Server las cuales fueron las siguientes:

- ✓ Windows 2000 Server
- ✓ Windows 2000 Advanced Server
- ✓ Windows 2000 Datacenter Server
- ✓ Windows 2000 Small Business Server

Además de las citadas versiones de Windows 2000 Server, también existe una versión para computadores de escritorio denominada Windows 2000 Professional. Todas las versiones del sistema se caracterizan por ser ideales para grandes empresas ya que tienen mucha estabilidad y fiabilidad.

En el año 2001 Microsoft hace el lanzamiento del sistema operativo **Windows XP** (eXPerience - experiencia), que hasta la actualidad es el sistema operativo Windows que se mantiene con mucha acogida entre los usuarios finales, Windows XP se desarrollo y caracterizó por ser el sistema destinado al público en general, pues es un sistema netamente para computadores de escritorio, aunque también es utilizado para portátiles. XP está basado en Windows NT como en Windows 2000, por eso, éste sistema es multitarea y multiusuario, acompañado de configuraciones de seguridad para el acceso de los usuarios, lo que lo lleva a ser un sistema bastante eficiente, aunque para su funcionamiento apropiado sea necesario disponer de altas prestaciones hardware.

En el año 2003 hace la aparición **Windows Server 2003**, que es un sistema sucesor a Windows 2000 Server y que fue desarrollado en base al núcleo de Windows XP, al cual se le agregan servicios necesarios y se deshabilitan servicios innecesarios, de tal manera que sea un sistema idóneamente para servidores, el objetivo de Windows Server 2003 es aprovechar al máximo las prestaciones de un servidor en donde se lo instale, y con ello obtener un máximo rendimiento del mismo. Las características principales que tiene integrado Windows Server 2003 son: Sistema de archivos NTFS, encriptación de archivos, carpetas o unidades completas, autenticación Kerberos 5, gestión de backup mejorado y jerarquizado, configuración de cuotas de utilización de disco, Active Directory basado en LDAP (Lightweight Directory Access Protocol), políticas de seguridad mejoradas con respecto a Windows 2000 y una serie de mejoras de servicios de servidor que le permiten cumplir algunas funciones de manera eficiente. Windows Server 2003 viene en cuatro versiones:

- ✓ Windows Server 2003 Standard Edition
- ✓ Windows Server 2003 Web Edition
- ✓ Windows Server 2003 Enterprise Edition
- ✓ Windows Server 2003 Datacenter Edition



Este sistema operativo de servidor no ha salido para estaciones de trabajo y desde su aparición hasta la actualidad se han liberado dos Service Pack y un Release en el 2005 en donde se integra algunas nuevas mejoras que lo hacen mucho más productivo y seguro.

En lo referente a plataformas para computadores de escritorio y portátiles, a principios del año 2007 Microsoft lanza al mercado el **Windows Vista** que entre las nuevas características que trae integrado, es una mejor seguridad con el modo de usuario restringido llamado "Control de Cuenta de Usuario", la interfaz gráfica de usuario llamada AERO (Auténtico, Energético, Reflexivo y Abierto) que es muy impactante pero consume bastantes recursos, además también incluye una versión mejorada del Internet Explorer y otras aplicaciones adicionales que lo hacen bastante atractivo.

Existe una planificación por parte de la Empresa Microsoft para hacer otros lanzamientos de sistemas operativos en un futuro, los cuales se llamarían: Windows Home Server (de nombre en código Quattro), y posteriormente Windows "Vienna".

1.3 CARACTERÍSTICAS DE SEGURIDAD GENERALES QUE OFRECEN LAS PLATAFORMAS WINDOWS

Las plataformas Windows desde su aparición han ido mejorando el nivel de seguridad, por esto se puede hablar de una evolución que ha dependido o ha estado en función de la evolución del sistema operativo en sí. Por ello existen características comunes de seguridad entre las plataformas Windows pero no de manera absoluta sino más bien de manera relativa, debido a que en versiones **Windows 3.x** no se puede dar mayor referencia o detalle de seguridad, porque son versiones muy básicas y no se contemplaba la seguridad en el diseño de las mismas.

Si se analiza cómo se maneja la seguridad desde las primeras versiones de Windows, se encuentra que son bastante vulnerables tanto la generación de Windows 3.x y Windows 9.x, no siendo así las plataformas Windows NT, Windows 2000 Server, XP, Windows Server 2003 y Windows Vista, en estas versiones la seguridad tiene un nivel bastante aceptable que las familias de Windows iniciales.

Las plataformas **Windows 9.x** carecen de una autenticación de usuario para iniciar sesión, pues con un **ESC**, cuando pide una contraseña es suficiente para acceder al sistema, por lo que es muy sencillo ingresar a una máquina con éstas plataformas, tanto localmente como desde la red.

Las verdaderas características de seguridad aparecen desde las plataformas **Windows NT** y desde entonces se han ido incrementando y mejorando dichas seguridades, es por ello que a partir de esas generaciones de Windows se puede hablar de una seguridad que tiene variadas cosas en común con las generaciones que salieron luego de estas plataformas, y que hasta la actualidad están siendo utilizadas.



1.3.1 Sistema de Autenticación

Todas las versiones Windows a partir de las NT cuentan con un sistema de autenticación, lo que ya permite controlar y frenar de cierta manera el ingreso de personas no autorizadas al sistema operativo. Toda la autenticación en estos sistemas está basada en contraseñas.

1.3.2 Sistemas Operativos de Servidor

Algunas otras características de seguridad que son comunes entre los sistemas operativos Windows de servidor y que están basadas en Windows NT son:

- ✓ Sistema de archivos NTFS
- ✓ Para controlar la seguridad de una manera más adecuada, manejan cuentas de usuario y grupo y sobre ellas se aplican permisos que les dan a las plataformas Windows Server una mayor capacidad de gestión, control y seguimiento.
- ✓ Maneja políticas de seguridad, las cuales pueden aplicarse al sistema mediante el uso de directivas.
- ✓ Se realiza el control de acceso a objetos, datos o recursos del sistema por parte de los usuarios.
- ✓ Se permite auditar los eventos del sistema, usuarios, grupos, operaciones, cuentas, etc.
- ✓ Encriptación de datos lo que conlleva un intercambio de información segura entre empleados, usuarios, clientes, etc., de una empresa determinada.
- ✓ Se brinda el servicio de firewall incorporado en el propio sistema operativo de servidor
- ✓ Los sistemas tienen incorporados protocolos de seguridad que son útiles para navegar por internet de forma segura, éstos protocolos por mencionar algunos son: SSL¹, SET², Kerberos, entre otros.
- ✓ Las versiones de Windows Server, pueden actualizarse mediante el uso de Windows Update.

Se puede decir además, que de las características mencionadas, aunque con algunas variantes, también son comunes a los sistemas operativos Windows de escritorio como son Windows XP y Windows Vista de manera específica.

1.4 ANÁLISIS DE LAS CARACTERÍSTICAS DE SEGURIDAD DE LAS PLATAFORMAS WINDOWS MÁS UTILIZADAS

Si bien es cierto que toda la familia de plataformas Windows tienen muchas características en común, debido a que parten de un mismo sistema operativo origen, no se puede considerar de manera idéntica las características de seguridad de las plataformas Windows de escritorio frente a las de servidores, difieren en algunos aspectos, debido a que cada plataforma está desarrollada

¹ SSL: Secure Sockets Layer - Nivel de Transacciones seguras

² SET: Secure Electronic Transaction - Transacciones Electrónicas Seguras



acorde al trabajo que va a brindar, radicando ahí la diferencia entre plataformas Windows de escritorio con las plataformas Windows de Servidor.

1.4.1 CARACTERÍSTICAS DE SEGURIDAD DE PLATAFORMAS WINDOWS PARA PC's

Los rasgos de seguridad en las plataformas Windows se dan a partir de Windows 98 y Windows Millennium, que hoy en día son plataformas que están casi en desuso (algunas de las características de seguridad que incluían están descritas en el **ANEXO 1.1**).

1.4.1.1 La Seguridad en Windows XP y Windows Vista

Las características de seguridad de las plataformas Windows XP y Windows Vista, son mucho más mejoradas que en versiones anteriores de plataformas de escritorio, existen algunas similitudes como diferencias concernientes a la seguridad entre estas dos últimas plataformas Windows. De igual manera tanto XP como Vista poseen algunas ediciones correspondientes a la misma plataforma, pero con la diferencia de que cada edición tiene sus propias características de seguridad, instalación, utilidad, y ejecución. La plataforma Windows XP cuenta con las ediciones:

- ✓ Windows XP Home Edition
- ✓ Windows XP Professional Edition
- ✓ Windows XP Tablet PC Edition
- ✓ Windows XP Media Center Edition

Las distintas ediciones de **Windows XP** poseen características en común y diferencias a la vez, a continuación en la siguiente tabla se detallan algunos aspectos de la seguridad que posee la edición Home Edition y la Professional Edition:

Tabla 1.2. Características de seguridad de las ediciones de Windows XP
Fuente: <http://www.zonagratis.com/a-cursos/windows/SeguridadWindowsXP.htm>

Características Home Edition	Características Profesional Edition
Compatibilidad mejorada con software y hardware	
Inicio de sesión simplificado con la "Pantalla de Bienvenida"	
Intercambio rápido de usuarios	
Nuevo interfaz de usuario, con vistas web y tareas sensibles al contenido de carpetas	
Soporte mejorado para medios digitales (videos, imágenes, música)	
Librerías multimedia DirectX 8.1 para juegos	
Seguridad simplificada. Todos los usuarios formarán parte del grupo local Propietario	Seguridad basada en grupos: Operadores de copia de seguridad, Usuarios avanzados, replicadores...
Cuenta invitado activa por defecto	Cuenta invitado deshabilitada por defecto
Compartición de recursos limitada y simplificada	Dispone de recursos ocultos compartidos para administradores (C\$, etc.)
Asistencia remota	Asistencia remota / Escritorio remoto
Versión de 32 bits	Versiones de 32 y 64 bits (para Itanium)

**Tabla 1.2.** Características de seguridad de las ediciones de Windows XP (... continuación)

Soporta actualización desde Windows 98, 98 SE, o Millennium Edition	Soporta actualización desde Windows 98, 98 SE, Millennium Edition, Windows NT 4.0 Workstation, o Windows 2000 Professional
Soporte monoprocesador	Soporte biprocesador
Herramienta de Backup opcional en el CD de instalación	Backup and Automated System Recovery (ASR) integrados
Soporte para discos simples	Soporte para discos dinámicos
Herramienta de fax opcional en el CD de instalación	Herramienta de fax integrada
	Internet Information Services/ Servidor Web Personal
	Sistema de cifrado de archivos
	Control de acceso a nivel de archivos
	Certificación "C2" de seguridad

De manera similar **Windows Vista** también cuenta con algunas ediciones que son:

- ✓ Windows Vista Starter
- ✓ Windows Vista Home Basic
- ✓ Windows Vista Home Premium
- ✓ Windows Vista Business
- ✓ Windows Vista Enterprise y
- ✓ Windows Vista Ultimate

Estas ediciones de Windows Vista presentan nuevas e importantes avances concernientes a seguridad, pues protege mejor los datos tanto personales como de la corporación en donde se esté utilizando este sistema, de esta forma se evita daños, divulgación o alteración de información causados por personas desautorizadas o atacantes de la privacidad de una persona o una corporación.

Windows Vista reduce a gran escala la superficie de ataque a los intrusos que pretenden ingresar al sistema, para llevar a cabo estas tareas ha implementado en su estructura nuevas o modificadas características de seguridad, las cuales se detallan en la tabla siguiente:

Tabla 1.3. Características de seguridad y sus beneficios en Windows Vista

Fuente: <http://www.microsoft.com/latam/technet/productos/windows/windowsvista/mngsec.msp>

Características	Beneficios
Firewall	Mejora el firewall de Windows para que evite de forma activa la propagación de programas malintencionados y que se pongan en riesgo datos personales
Endurecimiento de Servicios de Windows	Proporciona más resistencia contra ataques de software malintencionado al limitar las acciones que los usuarios o el software pueden realizar después de afectar un servicio de Windows
Exploración confiable	Proporciona una experiencia más segura y confiable al explorar el Web
Inicio y ejecución seguros	Asegura que la integridad de Windows Vista esté protegida contra ataques con conexión y sin ella
Cliente de protección de acceso a la red	Permite aislar el equipo y explorar su estado de mantenimiento antes de que se le otorgue acceso a una red corporativa. Esta característica requiere una funcionalidad auxiliar en Windows Vista Server
Mejoras en la actualización de seguridad	Permite ver el estado de seguridad utilizando un agente del lado del cliente y reduce la cantidad de reinicios necesarios para las revisiones de seguridad
Centro de seguridad de Windows	Los usuarios pueden conocer rápidamente el estado de seguridad de su equipo y recibir alertas cuando el equipo se encuentre sin protección
Protección de cuentas de usuario	Windows Vista facilita la implementación de un equipo con acceso de usuario con el menor número de privilegios, sin que los usuarios finales necesiten poseer derechos administrativos en sus equipos

**Tabla 1.3.** Características de seguridad y sus beneficios en Windows Vista (... continuación)

Autenticación	Proporciona protocolos, proveedores de inicio de sesión y una estructura de autenticación escalable y extensible
Autorización	Admite la expresión y evaluación de directivas enriquecidas para admitir capacidades de extensibilidad y delegación
Administración de credenciales	Proporciona servicios de administración de identidades mejorados y que pueden administrarse, provisión de testigos, y administración del ciclo vital
Servicios de criptografía	Ofrece operaciones mejoradas de cifrado y firmas para aplicaciones que deben proteger datos

La seguridad de la plataforma **Windows XP** frente a la seguridad de la plataforma **Windows Vista** integra algunas diferencias destacables, pero no se puede decir que sean unas grandes diferencias entre estas dos. Analizando de manera detallada la seguridad desarrollada en cada plataforma se llega a observar que en verdad Windows Vista trae algunas características nuevas con respecto a la seguridad, las más destacables son:

- ✓ Control de cuenta de usuario (UAC)
- ✓ Cifrado de unidad BitLocker
- ✓ Servicios de Módulo de plataforma segura (TPM)
- ✓ Windows Defender

Describiendo cada una de estas nuevas características de seguridad de Windows Vista, se tiene que: “El **Control de cuenta de usuario (UAC)** es un nuevo conjunto de tecnologías de infraestructura de esta versión de Windows que permite a las organizaciones implementar un escritorio mejor administrado y mitigar el impacto del malware³. UAC requiere que todos los usuarios ejecuten aplicaciones y tareas con una cuenta de usuario estándar, limitando el acceso de administrador a procesos autorizados. También permite el bloqueo de escritorios, lo que evita la instalación de aplicaciones no autorizadas e impide que los usuarios estándar realicen cambios por error en la configuración del sistema.

El **Cifrado de unidad Bitlocker** es una nueva característica de seguridad integral que proporciona un elevado nivel de protección de los datos y del sistema operativo sin conexión para el equipo. BitLocker garantiza que no se revelen los datos almacenados en el equipo a ningún usuario que altere el equipo mientras el sistema operativo instalado esté sin conexión.

El Cifrado de unidad Bitlocker funciona conjuntamente con el Módulo de plataforma segura (TPM) mediante el cifrado del volumen de Windows entero, lo que garantiza la integridad de componentes y la protección de datos desde el principio del arranque. El Cifrado de unidad Bitlocker está diseñado para ofrecer una experiencia de usuario transparente al inicio de sistemas que disponen de una BIOS y un microchip TPM compatibles.” [Microsoft *TechNet*, 2008].

“Los **Servicios de Módulo de plataforma segura (TPM)** son un nuevo conjunto de características de esta versión de Windows que sirve para administrar el hardware de seguridad TPM del equipo. La arquitectura de Servicios de TPM suministra la infraestructura de la seguridad basada en hardware

³ Malware: Programa maligno diseñado para causar daños al hardware, software, redes, etc. (virus, troyanos, gusanos, nukas, etc.)



proporcionando acceso a TPM y garantizando el uso compartido de TPM por parte de las aplicaciones. Esto significa que el uso compartido de aplicaciones puede integrarse a través del desarrollo de software y que los servicios se pueden administrar a través de una interfaz gráfica de usuario.” [Windows Vista *TechCenter*, 2007].

Con la herramienta **Windows Defender**, Windows Vista detecta el malware, spyware⁴ u otros programas no deseados que intenten instalarse en un equipo, también Windows Defender elimina el software malicioso que detecta, esta herramienta tiene que estar actualizada para su correcto funcionamiento, por ello hace uso de la utilidad de Windows Update. Windows Defender es una herramienta que ofrece protección al equipo en tiempo real.

1.4.2 CARACTERÍSTICAS DE SEGURIDAD DE PLATAFORMAS WINDOWS PARA SERVIDORES

1.4.2.1 Seguridad que posee Windows NT

“El sistema operativo Microsoft Windows NT cuenta con excelentes funciones de seguridad para una empresa. Un solo acceso al dominio de Windows NT permite que el usuario acceda a los recursos que se encuentran en cualquier parte de una red corporativa. Las herramientas del administrador fáciles de utilizar para la política de seguridad y administración de cuentas reducen los costes de implementación de Windows NT. El modelo de dominio Windows NT es flexible y soporta una amplia gama de configuraciones de red, desde un solo dominio en una ubicación a dominios multimaestros que hay en todo el mundo.” [Windows 2000 Server – SEGURIDAD, 2007]

Las características de seguridad básicas que brinda Windows NT se las lista a continuación:

- ✓ Autenticación de acceso
- ✓ Seguridad a nivel de objeto
- ✓ Derechos de usuario

Sobre estas tres características se fundamenta toda la seguridad del sistema operativo Windows NT, y también es el origen de las seguridades para las demás plataformas Windows que se basan en el sistema operativo NT.

1.4.2.2 Seguridades características de la plataforma Windows 2000 Server

“**Windows 2000**, (conocido también como **Win2K**) sistema operativo de Microsoft que se puso en circulación en el año 2000 con un cambio de nomenclatura para su sistema NT. Así, Windows NT 5.0 se pasa a llamar **Windows 2000**.” [WIKIPEDIA, 2008]

La familia Windows 2000 Server es la siguiente generación de los sistemas operativos Windows NT Server. La familia Server consiste en sistemas operativos de red multipropósito con una alta

⁴ **Spyware**: programa espía que se utiliza para el robo de información de una computadora sin que se dé cuenta el usuario del computador.



capacidad de escalabilidad, ya sea para negocios pequeños como para sitios Web con grandes cantidades de transacciones, Windows 2000 le ofrece un sistema de funcionamiento y una plataforma para las más demandadas aplicaciones de comercio electrónico y de la línea de negocios.

Tabla 1.4. Seguridades relevantes que posee la plataforma Windows 2000 Server
Fuente: <http://www.lavioleta.net/Capitulo1.html>

Características de seguridad de Windows 2000 server
Autenticación Kerberos v5 y NTLM ⁵
Múltiples métodos de autenticación para usuarios internos y externos
Servidor de certificados de clave pública basado en X.509
Infraestructura de tarjeta inteligente y credenciales para la seguridad de usuario
Protocolo de seguridad IP (IPSec) que da protección de datos transmitidos a través de la red usando encriptación
Sistemas de archivos encriptados (NTFS, EFS ⁶)
Propiedades de control de acceso para objetos
Relación de confianza transitiva entre dominios
Infraestructura de llave pública (PKI)

Problemas y Limitaciones

Windows 2000 Server mantiene compatibilidad con clientes de versiones anteriores (Windows NT 4.0, Windows 95 y Windows 98), así utiliza el NTLM y LM como protocolos de autenticación para inicios de sesión. Esto significa que la fuerte autenticación de Kerberos v5 no es utilizada para esos sistemas. Como NTLM y LM son aún usados, así las contraseñas de esos usuarios pueden ser comprometidos.

1.4.2.3 Seguridad de Windows Server 2003 y Windows Server 2008

Windows Server 2003

“Windows Server 2003 se centra en proporcionar un conjunto de elementos de ayuda, herramientas y plantillas para mejorar la seguridad de Windows Server 2003 en muchos entornos. Aunque este producto ya es altamente seguro desde su instalación por defecto, existen un cierto número de opciones de seguridad que pueden configurarse posteriormente en función de requerimientos concretos.” [Microsoft *TechNet*, WS2003]

Windows Server 2003 cuenta con una serie de nuevas características de seguridad que dan a las distintas empresas muchas capacidades de crear soluciones que se adapten a sus necesidades y objetivos y así protejan los activos de información.

Windows Server 2008

⁵ NTLM: NT LAN Manager – Administración de red de área local NT

⁶ EFS: Sistema de archivo encriptado



Microsoft Windows Server 2008, es una nueva plataforma para servidores, “está diseñado para ofrecer a las organizaciones la plataforma más productiva para virtualización de cargas de trabajo, creación de aplicaciones eficaces y protección de redes. Ofrece una plataforma segura y de fácil administración, para el desarrollo y alojamiento confiable de aplicaciones y servicios web. Windows Server 2008 incluye nuevas funciones de gran valor y eficacia y mejoras impactantes en el sistema operativo base.”[Microsoft *TechNet*, 2007]

Windows Server 2008 es un sistema operativo que proporciona a los profesionales de TI una serie de tecnologías nuevas que están orientadas a ofrecer más control, mayor protección y mayor flexibilidad lo que genera una eficiencia y aprovechamientos de recursos en una organización determinada.

Windows Server 2008, en temas referentes a la seguridad, incluye muchos nuevos componentes en comparación con su antecesor Windows Server 2003, a continuación se analiza las características de seguridad entre Windows Server 2003 y Windows Server 2008.

Tabla 1.5. Seguridades de Windows Server 2003 y 2008

Fuente: <http://www.microsoft.com/latam/technet/windowsserver/longhorn/evaluate/whitepaper.mspx>

CARACTERÍSTICAS DE SEGURIDAD	
WINDOWS SERVER 2003	WINDOWS SERVER 2008
CONTROLADORES DE DOMINIO	
<ul style="list-style-type: none"> ➤ Utiliza Active Directory para almacenar datos y administrar las interacciones entre el usuario y el dominio, incluidos los procesos de inicio de sesión de los usuarios, la autenticación y las búsquedas en directorios. ➤ Se permite aplicar una única política de passwords igual para todos los usuarios del dominio. ➤ Si los usuarios tienen que autenticarse con un controlador de dominio sobre una WAN⁷ no pueden, porque no existe tal alternativa. 	<p>Controladores de dominio de sólo lectura (RODC)</p> <ul style="list-style-type: none"> ➤ Utiliza Active Directory Domain Services (AD DS) para mantener la información de usuarios, máquinas y dispositivos de red. AD DS es una utilidad necesaria para ciertas aplicaciones como Microsoft Exchange Server y para tecnologías de gestión centralizada, como las políticas de grupo. ➤ Permite definir diferentes políticas de password y bloqueo de cuenta para distintos grupos de usuarios dentro de un dominio. ➤ Diseñado para implementarse principalmente en entornos de sucursales. ➤ Puede reducir los riesgos de implementar un controlador de dominio en ubicaciones remotas, como sucursales, donde no se puede garantizar la seguridad física. ➤ Un Controlador de Dominio de Solo-Lectura (RODC) es un nuevo tipo de controlador disponible con el sistema operativo Windows Server 2008. Un RODC mantiene particiones de solo-lectura de la base de datos de Active Directory Domain Services. ➤ Los administradores pueden parar y reiniciar los servicios de Active Directory Domain Services utilizando los complementos de la Microsoft Management Console (MMC⁸) o la línea de comandos. ➤ Mejoras en la capacidad de administración de Active Directory.

⁷ WAN: Wide Area Network – Red de Área Extensa

⁸ MMC: Microsoft Management Console – Consola de Administración Microsoft



Tabla 1.5. Seguridades de Windows Server 2003 y 2008 (... continuación)

CARACTERÍSTICAS DE SEGURIDAD	
WINDOWS SERVER 2003	WINDOWS SERVER 2008
CONTROL DE ACCESO	
<ul style="list-style-type: none"> ➤ Control de acceso basado en roles. Usada frecuentemente para forzar directivas ➤ Control de acceso basado en URL. Controla el acceso a las aplicaciones expuestas en la Web ➤ Directiva de Restricción de software (SRP). Controla la ejecución de una aplicación en un sistema, permitiendo así controlar el software desconocido o no fiable. 	<ul style="list-style-type: none"> ➤ El control de acceso y seguridad de red se hace aplicando diversas tecnologías y protocolos, como el Servidor de Política de Red (NPS, Network Policy Server), el servicio Routing and Remote Access Service (RRAS), Health Registration Authority (HRA) y el protocolo HCAP (Host Credential Authorization Protocol). Aislamiento de servidor y dominio <ul style="list-style-type: none"> ➤ Permite limitar el acceso a equipos autenticados y autorizados. ➤ Evita que equipos y programas no autorizados obtengan acceso a recursos de manera inapropiada. ➤ Existen dos tipos de aislamiento para proteger una red: Aislamiento de servidor.- se configuran mediante directivas de IPSec para aceptar sólo comunicaciones autenticadas de otros equipos, Aislamiento de dominio.- garantiza que los equipos que sean miembros de un dominio sólo acepten comunicaciones autenticadas y protegidas.
AUDITORÍA	
<ul style="list-style-type: none"> ➤ Auditoría basada en operaciones ➤ Auditoría selectiva por usuario ➤ Auditoría mejorada de inicio/cierre de sesión y administración de cuentas ➤ Servicio de recopilación de auditoría de Microsoft 	<ul style="list-style-type: none"> ➤ Windows Server 2008 establece un proceso de auditoría de Active Directory Domain Services (AD DS) con una nueva subcategoría de política de auditoría (Directory Service Changes) capaz de registrar los valores previos y posteriores a un cambio realizado sobre un objeto de AD DS y sus atributos. ➤ La política global de auditoría "Audit directory service access" en Windows Server 2008 está habilitada por defecto.
RED	
<p>Seguridad de red</p> <ul style="list-style-type: none"> ➤ Mejoras en el protocolo de seguridad de internet (IPSec) ➤ Control de acceso a la red por cuarentena, que retrasa el acceso remoto normal a una red privada hasta que la configuración del ordenador de acceso remoto ha sido examinada y validada. ➤ Soporte integrado para el protocolo de autenticación IEEE 802.1x ➤ El firewall no está habilitado, el administrador debe encargarse de habilitarlo y elaborar reglas de filtrado de tráfico para que proteja los datos entrantes como salientes. ➤ Configuración flexible de red <p>Servicio de autenticación de internet (IAS)</p> <ul style="list-style-type: none"> ➤ IAS soporta completamente el protocolo Remote Access Dial-in User Server (RADIUS) que gestiona la autenticación como la autorización de usuarios remotos e inalámbricos. ➤ Entorno de confianza. Permite a los usuarios acceder de forma segura a los recursos ➤ Administrador de credenciales. Proporciona almacenamiento seguro para los nombres de usuarios o contraseñas. ➤ Delegación restringida. Delimita servicios concretos para controlar qué recursos específicos puede usar el servicio o el ordenador. ➤ Transición de Protocolo. ➤ Integración entre .NET Passport y Directorio Activo. <p>Encriptación de datos</p> <ul style="list-style-type: none"> ➤ Soporte multiusuario. Compartir archivos encriptados es una forma útil y fácil de permitir la colaboración sin que los usuarios tengan que compartir claves privadas. ➤ El sistema de archivos encriptado combinado con las carpetas Web-based Distributed Authoring and Versioning (WebDAV) proporciona modos simples y seguros para compartir datos delicados entre redes 	<p>Protección de acceso a redes (NAP)</p> <ul style="list-style-type: none"> ➤ Evita que equipos que no se encuentren en buen estado tengan acceso a la red de la organización y la pongan en peligro. ➤ Con NAP los administradores pueden configurar directivas de estado (requisitos de software, requisitos de actualización de seguridad y opciones de configuración necesarias) ➤ Los métodos de cumplimiento de NAP admiten cuatro tecnologías de acceso a redes que funcionan junto con NAP: El cumplimiento de seguridad de protocolo de internet (IPSEC), el cumplimiento de 802.1, el cumplimiento de red privada virtual (VPN) y el cumplimiento de protocolo de configuración dinámica de host (DHCP) <p>Servicios de Acceso y Directivas de Red (NPAS)</p> <ul style="list-style-type: none"> ➤ NPAS es un servicio "one-stop" para todas las políticas de seguridad de la red y servicios de control de acceso. ➤ Es posible desplegar los servidores de VPN, máquinas de Dial-Up y router. Es factible instalar un servidor RADIUS y crear políticas de acceso remoto a través del Connection Manager Administration Kit. ➤ NPAs también permite configurar conexiones seguras, ya sea a través de cableado o de forma inalámbrica, para proteger mejor las comunicaciones sobre la red. <p>Funcionalidad de seguridad avanzada de Firewall de Windows</p> <ul style="list-style-type: none"> ➤ Bloquea el tráfico de red según su configuración y aplicaciones que se encuentren en ejecución. ➤ El firewall esta activado por defecto y todo el tráfico entrante es bloqueado igualmente por defecto a menos que sea tráfico solicitado o permitido por alguna regla creada para tal fin. El tráfico saliente igualmente es analizado, el objetivo del firewall es bloquear todo el tráfico que se envía a puertos específicos, como los que son utilizados por software de virus. ➤ Es posible crear excepciones de firewall y reglas de IPsec superpuestas, mediante configuración integrada evitando así configuraciones contradictorias.



Tabla 1.5. Seguridades de Windows Server 2003 y 2008 (... continuación)

CARACTERÍSTICAS DE SEGURIDAD	
WINDOWS SERVER 2003	WINDOWS SERVER 2008
<ul style="list-style-type: none"> ➤ Encriptación más sólida. <p>Infraestructura de clave pública</p> <ul style="list-style-type: none"> ➤ Soporte de certificación cruzada ➤ Listas delta de anulación de certificados ➤ Registro automático ➤ Solida seguridad incluyendo Kerberos perfeccionados ➤ Administración unificada <p>Acceso remoto e inalámbrico seguro</p>	<p>PKI de empresa (PKIView)</p> <ul style="list-style-type: none"> ➤ Aumento de la capacidad de administración en todos los aspectos de Windows PKI. ➤ Protocolo de estado de certificados en línea (OCSP) ➤ Servicio de inscripción de dispositivos de red (NDES) ➤ Inscripción web <p>Directiva de grupo y PKI.</p>
SISTEMA DE ARCHIVOS	
<p>Servicio de instantáneas de volumen (VSS)</p> <ul style="list-style-type: none"> ➤ Permite la creación de copias de seguridad instantáneas de un volumen de información determinado. ➤ VSS mantiene un conjunto de versiones anteriores de los archivos, llamados instantáneas o Shadow copies, las cuales pueden ser utilizadas para la recuperación de información cuando un archivo sea dañado a causa de un error humano. <p>Sistema de archivos NTFS</p> <p>Sistema de Archivos Distribuidos (DFS)</p> <ul style="list-style-type: none"> ➤ DFS hace que los archivos sean más fáciles de encontrar. ➤ DFS puede ayudarle a reemplazar o a integrar su estructura de ficheros existentes en una sola jerarquía que sea fácil de utilizar y mantener. 	<p>Particiones fuertes</p> <ul style="list-style-type: none"> ➤ Permite crear maquinas virtuales (VM), que funcionan como un contenedor independiente de sistema operativo. <p>Seguridad para el hardware</p> <ul style="list-style-type: none"> ➤ Prevención de ejecución de datos (DEP), evita la ejecución de los virus y los gusanos más predominantes. <p>Windows Server virtualization</p> <ul style="list-style-type: none"> ➤ Ayuda a evitar la exposición de las máquinas virtuales que contienen información confidencial. <p>Base de equipos de confianza mínima</p> <ul style="list-style-type: none"> ➤ Superficie de ataque reducida y una arquitectura de virtualización simplificada y ligera, con lo que mejora la confiabilidad de equipos virtuales basados en Windows Server virtualization.
SISTEMA DE ARCHIVOS	
<p>Seguridad y recuperación de información</p> <ul style="list-style-type: none"> ➤ Servicio de cifrado de archivos (EFS), permite a los usuarios cifrar su información para prevenir accesos accidentales o maliciosos por personas no autorizadas. ➤ Recuperación automática del sistema (ASR), es una característica que ofrece una solución sencilla para la recuperación de la información. 	<p>Fuerte aislamiento</p> <ul style="list-style-type: none"> ➤ Asignación flexible de memoria ➤ Adición dinámica de hardware <p>Cifrado de unidad BitLocker</p> <ul style="list-style-type: none"> ➤ Característica clave de Windows Server 2008, ayuda a proteger servidores, estaciones de trabajo y equipos móviles. ➤ BitLocker cifra el contenido de una unidad de disco, evitando de esta manera que un intruso que ejecuta un sistema operativo paralelo, salte las protecciones de archivo y sistema o que visualice los archivos almacenados. ➤ BitLocker incluye cifrado del volumen de sistema y comprobación de integridad en componentes de pre inicio. ➤ BitLocker resuelve las amenazas de robo o exposición de datos de un equipo perdido, robado o retirado de manera inapropiada de servicio activo. <p>Criptografía de nueva generación (CNG)</p> <ul style="list-style-type: none"> ➤ Criptografía flexible que permite a los profesionales de TI crear, actualizar y usar algoritmos personalizados de criptografía en aplicaciones relacionadas con criptografía, como Servicios de Certificate Server de Active Directory, Capa de sockets seguros (SSL) y Seguridad de Protocolo Internet (IPSEC) ➤ CNG permite que las organizaciones y los desarrolladores usen sus propios algoritmos criptográficos o implementaciones de algoritmos criptográficos estándar. ➤ CNG ofrece compatibilidad con algoritmos de criptografía de curva elíptica (ECC)

1.5 TENDENCIAS DE ATAQUES A LAS PLATAFORMAS WINDOWS

Las plataformas Windows por basarse en sus inicios en la idea de ser una plataforma no ideada para la seguridad a gran escala, durante su periodo de vida hasta la actualidad a sufrido muchos ataques de diversa índole, pero la tendencia de la mayoría de los ataques a estas plataformas ha venido



desde la red de redes (Internet), esto implica que existe una baja protección de la pila de protocolos TCP/IP. Los atacantes se valen de la baja seguridad que brindan los sistemas operativos Windows a los protocolos de conexión de red y aprovechan esas vulnerabilidades para lanzar sus ataques, por ello se detalla a continuación algunos servicios y protocolos con sus respectivos puertos que han sufrido una mayor tendencia a ser atacados en los últimos tiempos bajo las plataformas Windows.

Tabla 1.6. Servicios, puertos y protocolos que sufren ataques con frecuencia en Windows
Fuente: <http://www.cert.org.mx/areciento/>

Nombre del Servicio	Puerto/Protocolo	Información Relacionada
ftp	21/tcp 21/udp	Una clase de vulnerabilidades en IE permite que un script malicioso de un dominio se ejecute en un dominio diferente, el cual también podría ejecutarse en una zona diferente de IE
ssh	22/tcp	Pueden generar un desbordamiento de búfer que a un intruso le permite influir en ciertas variables internas al programa
telnet	22/tcp 23/tcp	Causan problemas de denegación de servicio, descubrimiento de información y elevación de privilegios
domain	23/tcp 23/udp 53/tcp 53/udp	Vulnerabilidades Múltiples en BIND ⁹
netbios-ns	137/udp	Microsoft Windows Server Message Block (SMB) falla al manejar adecuadamente paquetes SMB_COM_TRANSACTION requiriendo transacciones NetServerEnum2
netbios-dgm	138/udp	
netbios-ssn	139/tcp	
microsoft-ds	445/tcp	Puede generar una negación de servicio, y a un atacante le permitiría enviar continuas cadenas nulas de 10K al sistema
ICMP echo	Ninguno/ICMP type 8	Ataques de Negación de Servicio IP de "smurf" ¹⁰
ICMP echo reply	Ninguno/ICMP type 0	

Detallando las formas de cómo se llevan a cabo las diferentes tendencias de ataques informáticos en los diversos sistemas operativos existentes en la actualidad, se tiene la siguiente figura que describe como procede un atacante.

⁹ BIND: Berkeley Internet Name Domain

¹⁰ Smurf: Es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con spoofing para inundar un objetivo

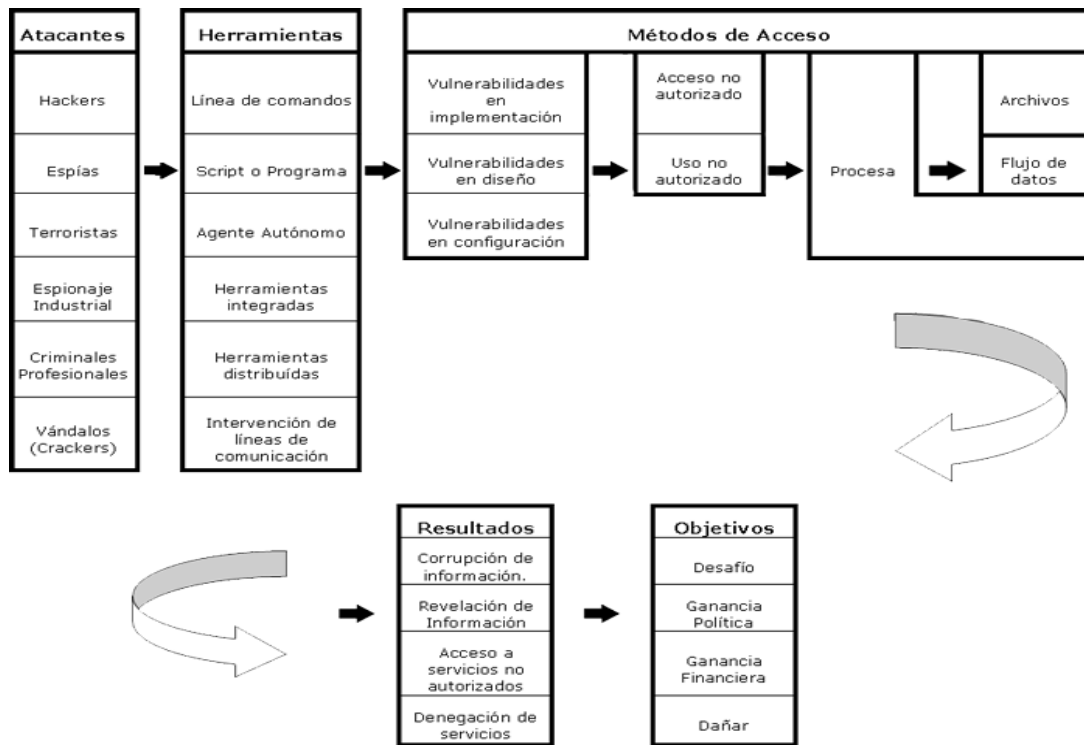


Figura 1.2. Detalle del proceso como se perpetra un ataque a un sistema operativo
Fuente: <http://www.segu-info.com.ar/ataques/ataques.htm>

1.6 PROBLEMAS DE SEGURIDAD COMUNES Y ESPECÍFICOS DE LAS PLATAFORMAS WINDOWS

Las plataformas Windows por ser una de las plataformas más populares a nivel mundial están expuestas a millones de piratas informáticos que día a día están tratando de encontrarles errores, vulnerabilidades o agujeros de seguridad con la finalidad de comprometer al sistema, es por esta razón que en verdad las plataformas Windows se han visto comprometidas con problemas de seguridad, que de no seguir un proceso de aseguramiento de las mismas, se verá comprometida la información que se maneje bajo la utilización de estos sistemas operativos, a continuación se detalla los problemas más comunes y específicos que atentan contra estas plataformas:

Tabla 1.7. Problemas comunes y específicos de Windows
Fuente: <http://www.somoslibres.org/modules.php?name=News&file=print&sid=307>

Problemas de seguridad comunes y específicos en plataformas Windows
Sistemas Windows de Escritorio
Desbordamiento de búfer Denegación de servicio (DoS) Problemas de control de acceso Ejecución remota de código Ataques mediante el uso de mensajería instantánea Ataques utilizando programas de correo Ocultación de extensiones de archivos permite ataques de virus



Tabla 1.7. Problemas comunes y específicos de Windows (... continuación)

Problemas de seguridad comunes y específicos en plataformas Windows		
Windows XP	Windows Vista	
Llamada a procedimiento remoto (RPC)	Problemas en compartición de información	
Autenticación de Windows		
Sistemas Windows de Servidor		
Desbordamiento de búfer Denegación de servicio (DoS) Llamada a procedimiento remoto (RPC) Problemas de control de acceso Ejecución remota de código Ataques utilizando programas de correo Instalación de servicios innecesarios Ocultación de extensiones de archivos permite ataques de virus Bajo aseguramiento de la pila TCP/IP		
Windows NT 4.0	Windows 2000 Server	Windows Server 2003
Problemas en conexión remota	Problemas en conexión remota	Problemas en compartición de información

1.7 ASPECTOS Y COMPONENTES DE UN ESQUEMA DE SEGURIDAD PARA ENTORNOS WINDOWS

1.7.1 Definición de Esquema de seguridad

“Un **Esquema de Seguridad** es la integración de dispositivos informáticos bajo determinadas políticas de seguridad que les respalda y fortalece ante cualquier ataque. Pues la finalidad primordial de un esquema de seguridad es garantizar que los recursos de una empresa estén disponibles para que cumplan los propósitos de dicha entidad, y con ello evitar que la información sea alterada o dañada por circunstancias o factores externos.” [Ciberhabitat, 2008].

1.7.2 Componentes que debe abarcar un esquema de seguridad Windows

Un esquema de seguridad en general engloba algunos componentes que van desde la seguridad de la organización, seguridad lógica, seguridad física, seguridad legal entre otros, se puede decir que los componentes de un esquema de seguridad están en función de los objetivos, propósitos o metas que persigue una entidad determinada, por ello al hablar de **componentes de un esquema de seguridad Windows** se delimita y se hace más referencia a la seguridad lógica, que si bien es cierto, tiene una relación directa con la seguridad física (Hardware), debido a que ningún sistema operativo o software se ejecuta sin un hardware de por medio.

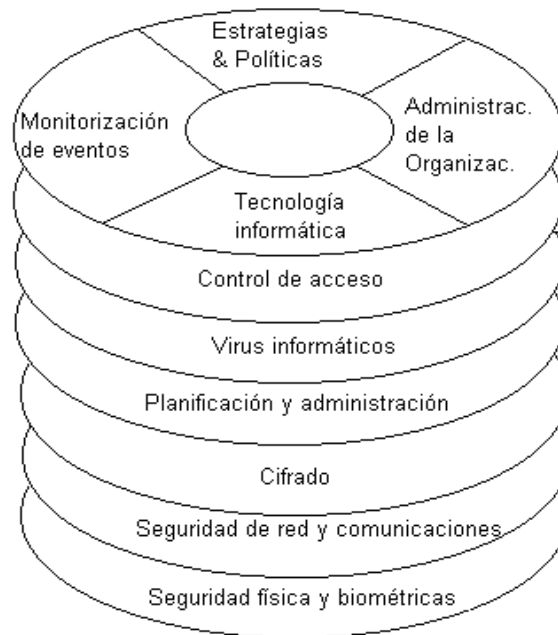


Figura 1.3. Componentes de un Esquema de Seguridad Global

Fuente: <http://www.monografias.com/trabajos14/riesgosinfor/Image416.gif>

De esta manera los objetivos que se persigue con la implementación de un esquema de seguridad son:

- ✓ Disminuir costes de Tecnologías de Información
- ✓ Mejorar el servicio de Tecnologías de Información
- ✓ No exponer la empresa a riesgos

Una vez definidos los objetivos de un esquema de seguridad, se debe citar los componentes que abarca el esquema, así se tiene que en un **esquema de seguridad Windows** se contempla los siguientes componentes:

- ✓ Seguridad a nivel de dominio
- ✓ Consolidación de seguridad de los servidores miembros y controladores de dominio
- ✓ Configuración de firewalls de manera individual tanto para estaciones de trabajo, servidores, enrutadores y demás equipos que ejecuten sistemas Windows.
- ✓ Configuración de un firewall perimetral que garantice conexiones de red confiables y seguras
- ✓ Seguridad a nivel de datos, aplicaciones, etc.
- ✓ Directivas de seguridad
- ✓ Seguimiento de sucesos (auditoría) referentes a procesos, usuarios, ejecución de tareas, etc.
- ✓ Políticas y estándares de seguridad

Un entorno de seguridad, puede implicar muchos componentes adicionales a los citados con anterioridad ya que están en juego varios aspectos dependientes a cada organización o empresa en sí. Los aspectos a considerar, por mencionar algunos pueden ser: Las aplicaciones que necesitan



seguridad, formas de dar protección a determinados servicios ante los usuarios, nivel en el que se va a proporcionar la seguridad (aplicación, datos, niveles inferiores, etc.).

1.8 VENTAJAS DE UN ESQUEMA DE SEGURIDAD

- ✓ Optimizar recursos
- ✓ Los procedimientos se adecuarían y administrarían por un mismo personal administrador de infraestructura y controles, lo que ahorraría tiempo.
- ✓ Permite asegurar los activos de información
- ✓ Disponibilidad de los servicios que presta una organización de manera confiable.
- ✓ Se facilita el control, auditoría, gestión de riesgos, etc. de aplicaciones
- ✓ Enfoque directo en las necesidades del área
- ✓ Permite ver la seguridad de la información como un componente de la gestión del negocio.
- ✓ Involucra niveles superiores (directivos) de una organización
- ✓ Permite interactuar con diferentes áreas de la organización
- ✓ Esta en relación directa con la continuidad del negocio
- ✓ Centralizar la administración de los servidores

1.9 ESTÁNDARES A SEGUIR EN INFRAESTRUCTURAS DE SEGURIDAD WINDOWS

Los estándares internacionales que regulan la **seguridad de la información** en los diversos ambientes que permanecen interconectados mediante el Internet, basan su protección en una serie de conceptos que han sido debidamente analizados y aprobados por entidades que se dedican al estudio y generación de estándares de seguridad aplicables a los activos de información. A continuación se describe la estructura del estándar que regula la seguridad de la información y que son dados por la **ISO¹¹/IEC¹² 17799** bajo la denominación de **Código de Prácticas para la Gestión de la Seguridad de la Información**, los cuales se deben tener muy en cuenta cuando se elabora un **Esquema de seguridad** para asegurar los activos de información de una organización en particular.

¹¹ ISO: International Organization for Standardization - Organización Internacional de Estandarización

¹² IEC: International Electrotechnical Commission - Comisión Electrotécnica Internacional



Tabla 1.8. Estándares de Seguridad para la Información
Fuente: <http://seguridad-de-la-informacion.googlegroups.com/web/iso-17799-2005-castellano.pdf?gda>

Estructura del Estándar de seguridad de la Información		
Nro.	Nombre de Cláusula	Objetivos de Cláusula
1	Política de Seguridad	<p>Proporciona a la Gerencia, dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.</p> <p>La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.</p>
2	Organización de la Seguridad de la Información	<p>Manejo de la seguridad de la información dentro de la organización.</p> <p>Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.</p> <p>Si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Se debieran desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información.</p>
3	Gestión de Activos	<p>Lograr y mantener una apropiada protección de los activos organizacionales.</p> <p>Todos los activos debieran ser inventariados y contar con un propietario nombrado. Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea conveniente, pero el propietario sigue siendo responsable por la protección apropiada de los activos</p>
4	Seguridad de Recursos Humanos	<p>Asegurar que los empleados, entiendan sus responsabilidades y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.</p> <p>Las responsabilidades de seguridad debieran ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.</p> <p>Los antecedentes de todos los candidatos al empleo, contratistas y terceros deberán ser adecuadamente investigados, especialmente para los trabajos confidenciales.</p> <p>Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información deberán firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.</p>



Tabla 1.8. Estándares de Seguridad para la Información (... continuación)

Estructura del Estándar de seguridad de la Información		
Nro.	Nombre de Cláusula	Objetivos de Cláusula
5	Seguridad Física y Ambiental	Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.
6	Las Comunicaciones y Operaciones	Asegurar la operación correcta y segura de los medios de procesamiento de la información.
7	Control de Acceso	Controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.
8	La Adquisición, Desarrollo y Mantenimiento de Sistemas de información	Garantizar que la seguridad sea una parte integral de los sistemas de información.
9	El Manejo de Incidentes de Seguridad de la Información	Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.
10	Gestión de la Continuidad Comercial	Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna. Las fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se debieran desarrollar e implementar planes para la continuidad del negocio para asegurar la reinundación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización
11	Conformidad	Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país

1.9.1 Buenas Prácticas para la Seguridad Corporativa

La seguridad de los datos y transacciones es de vital importancia en esta época de rápida expansión de las redes informáticas comerciales y oficiales, y de la nueva economía basada en Internet. Los retos que se derivan de la seguridad se han convertido en los más importantes en todas aquellas compañías que hacen uso de las tecnologías de la información.



El término seguridad informática es una generalización para un conjunto de tecnologías que ejecutan ciertas tareas relativas a la seguridad de los datos. El uso de estas tecnologías de forma eficiente para asegurar una red corporativa requiere que se integren dentro de un plan global de seguridad. El proceso de planificación para su implantación correcta supone:

- Adquirir una comprensión en detalle de los riesgos potenciales del entorno (por ejemplo, virus, hackers y desastres naturales).
- Realizar un análisis proactivo de las consecuencias y mediciones de los posibles agujeros de seguridad en relación con los riesgos.
- La creación de una estrategia de implantación cuidadosamente planificada para integrar las medidas de seguridad dentro de todos los aspectos de una red corporativa, en base a esa comprensión y análisis.

1.9.2 Seguridad para Servidores Windows

1.9.2.1 Estándares para infraestructuras de seguridad de Servidores Basados en Windows

Existen numerosos pasos que un administrador de sistemas puede seguir para proteger sus servidores de ataques. El incremento en el número y severidad de hacking en años anteriores recientes, a inducido a que se formen muchas organizaciones que ofrecen consultaría sobre problemas de seguridad computacional; Muchas de estas organizaciones ofrecen listas de recomendaciones denominadas “las mejores prácticas” para contrarrestar el problema de hacking. Examinando estos documentos y basándose en datos actuales disponibles se tiene el conjunto de recomendaciones siguientes, que lleva a prevenir o minimizar ataques a la seguridad de una organización:

La lista de **recomendaciones** está detallada en orden de importancia, pero no por ello se debe seguirse de manera obligatoria el orden, sino depende de las necesidades de las organizaciones que las adopten. [UCRIVERSIDE SECURITY, 2008]

1. Chequear semanalmente todos los servidores para constatar el cumplimiento respecto a todos los Service Packs, parches y situaciones problemáticas que comprometan al servidor.

Esta es la más importante acción a tomar para reducir la probabilidad de un ataque. Una vez que un bug o vulnerabilidad se hace pública, los hackers empiezan a buscar sistemas que no han sido debidamente parcheados. La posibilidad de un intento de ataque aumenta con cada día que pasa. Los Administradores del sistema deberían hacer este literal el de más alta prioridad.



2. Verificar que todos los usuarios (especialmente aquellos usuarios con permisos de administrador) tengan contraseñas fuertes. Hacer cumplir las políticas de contraseñas fuertes.

La única cosa que se interpone entre un posible intruso y el completo control de un servidor es el password, si un intruso obtiene la habilitación de la cuenta password de administrador, tendrá todos los privilegios para hacer cualquier cosa. Por eso cada uno y cada cuenta administrador deben de mantener contraseñas fuertes. Las cuentas de usuarios individuales también deben de tener las contraseñas fuertes, pero hay factores humanos que pueden limitar la habilidad de dar fuerza a las políticas de la contraseña de manera más estricta. Es delicado lograr el equilibrio para implementar políticas de contraseñas ya que se puede crear una carga sobre los usuarios y realmente llevarían a una pérdida neta de la protección. Si se obliga a los usuarios a que cambien su contraseña a menudo, ellos pueden acudir a escribirlas en papel o adherirlas sobre sus monitores. Las características de contraseñas fuertes se pueden consultar en **PL02**.

3. Mantener un nivel mínimo de seguridad física para todos los servidores.

Seguridad Física Mínima:

- ✓ Cada servidor debe estar detrás una puerta cerrada con llave y con acceso limitado sólo a individuos que tienen una necesidad legítima para el acceso.
- ✓ Cuando no haya nadie trabajando en la consola del servidor, la sesión de la consola debe terminar de operar o bloquearse a fin de pedir una contraseña para acceder nuevamente.
- ✓ El cuarto de servidores debe estar ubicado en cierta forma que las personas que están fuera del cuarto no puedan ver el teclado (evite así ver las contraseñas de usuarios administradores).
- ✓ La evidencia escrita de identificación de usuarios y contraseñas, no debe dejarse o yacer en el interior del cuarto de servidores.

4. Aplicar procedimientos de copia de seguridad para todos los sistemas.

- ✓ Cree y mantenga copias de seguridad **por lo menos de los archivos de datos** en todos los servidores. Deben crearse los respaldos regularmente usando procedimientos bien conceptualizados que deben incluir alguna forma de almacenamiento fuera del sitio de medios de respaldo, esto en caso de la pérdida de la instalación.
- ✓ Cree y mantenga un disco de reparación de emergencia actualizado (ERD) para todos los sistemas. **Esta medida a menudo es pasada por alto, pero es tan importante como respaldar los archivos de datos.**
- ✓ Regularmente pruebe los procedimientos de recuperación para verificar que los respaldos son válidos y restituibles.



5. Utilizar Software Antivirus Actualizado.

El software antivirus en un servidor no puede parar su actividad, ya que pueden detectar y descubrir muchos troyanos, programas de hackers que usan a menudo para hurtar dentro de los sistemas. Después de instalar el software antivirus, éste debe ser actualizado frecuentemente y así asegurar que el software sea capaz de detectar todos los virus, incluso los más recientemente descubiertos.

6. Bloquear el acceso hacia/desde cualquier puerto TCP/UDP innecesario.

Existen más de 65000 puertos TCP y UDP en cualquier servidor dado, la mayoría puede utilizar el mismo camino para ida y vuelta por lo que un atacante puede lograr el acceso no autorizado a un sistema. Use cualquier manera posible para bloquear el acceso a los puertos sobre el servidor donde no haya ningún uso legítimo. La manera más común y eficaz de bloquear el acceso a éstos puertos es mediante el uso de un cortafuego (Firewall). Los cortafuegos pueden dividirse en dos categorías:

Cortafuego Personal

Un cortafuego personal puede instalarse en el propio servidor y puede ser sumamente efectivo para bloquear el tráfico no deseado hacia y desde el servidor. Algunos productos de esta categoría son:

- ✓ ZoneAlarm Pro
- ✓ BlackICE Server Protection
- ✓ Sygate Personal Firewall Pro 5

Cortafuego de Red

Este tipo de cortafuego se pone en la red del campus, entre el servidor y el resto del mundo. El trabajo del cortafuego de la red es bloquear el acceso hacia/desde cualquier puerto particular en el servidor. Calcula las comunicaciones que ofrecerán el servicio al cortafuego en los próximos meses.

Los cortafuegos no pueden prevenir cada tipo de ataque, ellos pueden ser algo difíciles de configurar. Determinar cuáles puertos de salida están abiertos para permitir el tráfico requerido y cuales bloquear para filtrar el tráfico que no se requiere puede ser un proceso largo y tedioso.

7. Habilitar la seguridad al loguearse sobre todos los servidores.

“La prevención es ideal, pero la detección es un deber” es un axioma normalmente repetido en el mundo de la seguridad computacional. Por ello, la argumentación de seguridad es una de las muchas claves a afianzar en los servidores basados en Windows. Activando las características de auditoría en los servidores basados en Windows pueden reforzar ésta habilidad para



determinar cómo se intenta, como se llevo a cabo y hasta qué punto se dio un ataque, así se determina hasta que punto estuvo expuesto el sistema. Auditar puede además ayudar a los administradores a descubrir los ataques infructuosos para así poder hacer cambios de las configuraciones, a fin de defenderse contra futuros ataques.

Recuerde los siguientes eventos:

- ✓ El Ingreso y salida – Satisfactorios y Fallidos
- ✓ El Acceso a archivos y objetos – Fallas únicamente
- ✓ El Uso de derechos de usuario – Fallas únicamente
- ✓ La administración de usuario y grupo – Satisfactorios y Fallidos
- ✓ Los cambios de política de seguridad – Satisfactorios y Fallidos
- ✓ Reinicio y apagado del sistema – Satisfactorios y Fallidos
- ✓ El seguimiento de procesos

8. Desactivar los servicios innecesarios.

Si realizó una instalación por defecto, Windows NT/2000 server se configuran para ejecutar muchos servicios, muchos de los cuales no son requeridos. Ejecutar servicios innecesarios sobre servidores es como tener puertas en una casa por donde nadie pasa en la vida. ¿Por qué arriesgarse alguien reforzando la entrada cuando la puerta puede ser eliminada en su totalidad? ¿Examine cada servidor y vea cada servicio que está corriendo y pregúntese “Este servicio es realmente necesario”? Si la respuesta es no, entonces desactive o quite el servicio. Existen herramientas de libre distribución que le pueden ayudar a identificar los servicios que deben correr en un servidor y sobre que puertos TCP/UDP asocian su labor tales servicios.

9. Desactivar la enumeración de cuentas de usuario anónimas.

Por defecto sobre todos los sistemas Windows NT y en algunos sistemas Windows 2000, un usuario puede ingresar sin un nombre de usuario ni contraseña y pueden listar todos los nombres de cuentas de usuarios del sistema. Además pueden enumerar los nombres de usuario, un atacante puede aprovechar esto para obtener información necesaria para determinar que cuentas listadas tienen privilegios de administrador. Este agujero de seguridad ha sido usado recientemente contra los servidores de campus, permitiendo así a hackers adquirir acceso a la lista de nombres de usuarios de servidores NT/2000, incluyendo información relativa a las cuentas que tienen privilegios de administrador. Usando la restricción anónima del registro de entrada, puede bloquear el acceso rutinario a la información del usuario.



10. Usar NTFS

Todo sistema Windows NT y Windows 2000 debe ser formateado usando NTFS y no FAT/FAT32. Ningún FAT ni FAT32 utilizan un nivel de seguridad de archivos y usarlos entonces representaría un riesgo sustancial y comprometedor.

1.10 PUNTUALIZACIONES

- ✓ Las características de seguridad de cada sistema operativo Windows Server se ha ido mejorando día a día lo que contribuye a una mayor producción de las empresas que adopten este tipo de sistemas operativos para sus servidores, además prestan una excelente facilidad de manejo por estar basadas en su entorno Windows, así mismo incluyen una manera fácil de administrar la seguridad porque todo lo concerniente a la seguridad se la puede manejar basándose en plantillas, y estas plantillas se las puede generar de una manera guiada.
- ✓ Las ventajas que trae consigo implementar un esquema de seguridad, son varias, pero siempre se destaca la centralización de la administración, lo que es beneficioso para un administrador.
- ✓ Los servidores Windows que no pertenecen a un esquema de seguridad, corren mayor riesgo de ser atacados por intrusos, por el hecho de no beneficiarse de las seguridades que otorga y abarca un esquema de seguridad.
- ✓ Seguir un proceso basado en estándares es muy beneficioso ya en los estándares se detalla todos los pasos correctos que se deben seguir en la configuración de una infraestructura de seguridad.

CAPITULO II
TÉCNICAS DE CONFIGURACIÓN E INSTALACIÓN

Objetivos

- Analizar vulnerabilidades y ataques a sistemas operativos Windows Server
- Verificar las configuraciones de un servidor Windows
- Analizar políticas de utilización de Windows Update, así como manejar las actualizaciones de un servidor que está en operación



2.1 INTRODUCCIÓN

Hoy en día, no se puede garantizar una seguridad absoluta en los diferentes sistemas operativos de servidores o estaciones de trabajo que permanecen interconectados formando redes de área local, menos aún si éstos forman parte de redes de área extensa.

Al mismo ritmo de crecimiento de las redes de computadores han ido apareciendo, nuevos peligros y amenazas para la información que es transportada y almacenada en medios digitales; en el mundo informático de manera continua surgen ataques a las diversas plataformas con las cuales trabajan ya sea una PC o servidor. Por tanto, el tema de seguridad debe ser seguido y garantizado día a día, para ello es necesario analizar el entorno en donde se opera, los ataques más frecuentes, las vulnerabilidades descubiertas, formas de manejar las actualizaciones de un sistema operativo, etc. Es una tarea esencial a la hora de realizar las configuraciones de seguridad de un servidor o estación de trabajo en particular.

En este capítulo se analiza las vulnerabilidades y configuraciones que se deben realizar, y métodos de actualización del sistema operativo que está instalado en un servidor Windows, todas estas tareas son de mucha relevancia dentro del marco de un esquema de seguridad Windows.

2.2 ANÁLISIS DE VULNERABILIDADES Y ATAQUES A SISTEMAS WINDOWS SERVERS

2.2.1 Definición de Vulnerabilidad

Una **vulnerabilidad** es “un error, debilidad o mala configuración del software que puede utilizarse o atacarse directamente por parte de un intruso para ganar acceso a un sistema operativo o de información”. La materialización de las vulnerabilidades afecta los principios fundamentales de seguridad de la información: confidencialidad, disponibilidad e integridad; bien sea a nivel organizacional o particular. [ALEGSA - Diccionario Informático, 1998-2007]

Lo que más se manifiesta en los sistemas informáticos no es la seguridad, sino más bien la inseguridad o vulnerabilidad, por ello no se puede llegar a concebir la idea de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos. [Seguridad Informática, 2001]

Los **tipos de vulnerabilidades** que afectan a un sistema, se detallan en la siguiente tabla:



Tabla 2.1. Tipos de vulnerabilidades comunes

Fuente: <http://www.tecnoxarxavalles.com/drivers/Infotec/Manuals/>

Tipo de vulnerabilidad	Descripción
Física	Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.
Natural	Es el grado en que el sistema puede verse afectado por desastres naturales que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.
Hardware y Software	<i>Desde el punto de vista del hardware</i> , ciertos tipos de dispositivos pueden ser más vulnerables que otros, por lo que requieren de algún tipo o herramienta para poder ser accedidos. <i>Desde el punto de vista del software</i> , ciertos fallos o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos fiable. Comprende todos los bugs en los sistemas operativos, u otros tipos de aplicaciones que permiten atacarlos.
Emanación	Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios que interceptan estas emanaciones y descifran o reconstruyen la información almacenada o transmitida.
Comunicaciones	Las comunicaciones son una vulnerabilidad por el hecho de que pueden ser interceptadas, lo que añade el riesgo de: <ul style="list-style-type: none"> ❖ Se puede ingresar al sistema a través de la red ❖ Interceptar información que es transmitida desde o hacia el sistema
Humana	Representa la mayor vulnerabilidad del sistema. Toda la seguridad del sistema descansa sobre un administrador el cual tiene acceso a todo el sistema sin restricción alguna. Los usuarios del sistema representan un gran riesgo para los mismos, ellos son los que acceden directamente al sistema por lo que pueden manipularlo a su conveniencia, estudios indican que más del 50% de ataques son debidos a los propios usuarios.

Las formas en que las vulnerabilidades se las puede llegar a detectar son mediante reportes, documentos e informes previos de valoraciones de riesgos, requerimientos de seguridad y resultados de pruebas de seguridad que arrojan las herramientas que se utilizan para escanear vulnerabilidades (MBSA, Nessus, Retina Network Security Scanner, etc.). Basándose en este tipo de estudio se puede concluir una lista de vulnerabilidades, los cuales a mayor cantidad se encuentren, dan un mayor nivel de riesgo organizacional, pero al ser identificadas a tiempo se puede llegar a disminuir el riesgo e impacto que conllevan para la organización.

Las vulnerabilidades en los sistemas de información y en los sistemas operativos representan problemas graves para la información que almacenan o manipulan de manera cotidiana dichos sistemas, por eso que importante es mantener un sistema operativo **actualizado con todas las normas de seguridad existente**, que impidan y combatan el ingreso a los posibles atacantes de la información.

La siguiente tabla revela el porcentaje de vulnerabilidades publicadas durante el primer semestre de 2007, en la cual se detalla que los cinco primeros fabricantes o distribuidores de sistemas operativos son responsables del 12.6% de las vulnerabilidades existentes en la actualidad.



Tabla 2.2. Vulnerabilidades 2007: Top 10
Fuente: <http://www.kriptopolis.org/top-10-vulnerabilidades-2007>

Vendor	Percentage of 1H 2007 Vulnerabilities
Microsoft	4.2 %
Apple	3.0 %
Oracle	2.0 %
Cisco	1.9 %
Sun	1.5 %
IBM	1.3 %
Mozilla	1.3 %
XOOPS	1.2 %
BEA	1.1 %
Linux Kernel	0.9 %

Por lo general las vulnerabilidades de los sistemas operativos son aprovechadas por herramientas llamadas **exploits** las cuales permiten a un intruso ingresar al sistema operativo y así el sistema puede quedar obsoleto o inhabilitado porque está a expensas del atacante.

2.2.2 Análisis y mitigación de servicios afectados por las vulnerabilidades en Windows

Es importante analizar los servicios que son afectados por las vulnerabilidades de un sistema operativo Windows para evitar habilitar ciertos servicios que sean propensos a una vulnerabilidad o de igual forma darles un mayor cuidado, protección y mitigación a aquellos que involucran la seguridad integral de una plataforma Windows.

“El análisis de vulnerabilidades se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro del sistema de gestión de la seguridad de la información.”

[Análisis Vulnerabilidades, 2007]

Todos los sistemas operativos y de información poseen algún tipo de vulnerabilidad, ya que están expuestos para servir a un usuario, lo que se debe procurar es que las vulnerabilidades descubiertas en un sistema, sean siempre del más bajo impacto posible, es por ello que los servidores que trabajan con sistemas operativos Windows no se escapan a las vulnerabilidades. A continuación se describen algunos **servicios afectados por vulnerabilidades** y las propias **vulnerabilidades críticas de las plataformas Windows**. [TECNOLOGIAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACION, 2007].



Tabla 2.3. Servicios afectados por vulnerabilidades críticas en plataformas Windows
Fuentes: <http://www.acis.org.co/fileadmin/Articulos/TecnicasAtaqueComputacionForense.pdf>
<http://www.uned.es/csi/sistemas/secure/vulne/index.htm>

Vulnerabilidad	Servicios afectados	Mitigación
Vulnerabilidades de desbordamiento de buffer	✓ Internet Explorer	✓ Instalar las actualizaciones y parches de seguridad.
	✓ Internet Information Server (IIS)	✓ Verificar el IIS Lockdown ¹³ que fortalece la configuración del servidor. ✓ Valorar la posibilidad de instalar URLScan que permite bloquear las peticiones contra el servidor utilizadas para explotar esta vulnerabilidad. ✓ Instalar URL Buffer Size Registry Tool 1.0 que permite restringir el tamaño del búfer utilizado por IIS para recibir las peticiones que explotan esta vulnerabilidad.
	✓ Windows Media Player	✓ Desinstalar del equipo la versión Windows Media Player ✓ Eliminar la extensión .ASX ✓ Modificar las propiedades de la extensión para que los archivos no se abran automáticamente.
Vulnerabilidades de condición de carrera (race condition)	✓ Internet Explorer al usar JavaScript no seguro	✓ Configurar filtros anti-phishing
	✓ Llamada al subsistema de procedimiento remoto (RPCSS)	✓ Restringir el acceso a los puertos: 135/TCP, 139/TCP, 445/TCP, 593/TCP, 135/UDP, 137/UDP, 138/UDP, 445/UDP. ✓ Crear capas de seguridad redundante ✓ Bloquear el acceso de redes externas
Vulnerabilidades de Cross Site Scripting (XSS)	✓ Internet Information Server 5.0 y 6.0	✓ Restringir acceso de ingreso a las aplicaciones desde redes externas inseguras ✓ Fijar passwords para proteger directorios
Vulnerabilidades de Inyección de Caracteres (CRLF)	✓ Internet Explorer 6.0	✓ No navegar desde el servidor por sitios que no sean de confianza (sitios de descarga de seriales, música, programas utilitarios, etc.)
Vulnerabilidades de denegación del servicio (DoS)	✓ Terminal Services ✓ Remote Desktop ✓ Internet Explorer, controles ActiveX	✓ Instalar parches de seguridad los más actuales posibles. Ver PLO1 . ✓ Bloquear el puerto TCP/3389 en el firewall, desactivar Terminal Services o Remote Desktop sino son necesarios, o utilizar IPsec o VPN para las conexiones a éstos servicios. ✓ No seguir enlaces no solicitados ✓ Desactivar ActiveX para sitios que no son de confianza ✓ Configurar de manera personalizada el Internet Explorer para hacerlo más seguro
Vulnerabilidades de ventanas engañosas o mistificación de ventanas (Window Spoofing)	✓ HTTP ¹⁴ en Internet Explorer 7	✓ Reforzar la secuencia de predicción de números de secuencia TCP ✓ Eliminar las relaciones de confianza basadas en la dirección IP ✓ Cifrado y filtrado de conexiones de red
Vulnerabilidades de elevación de privilegios	✓ Servicios de cuentas: "Local Service" y "Network Service"	✓ En la actualidad no se conocen exploits para esta vulnerabilidad, estas cuentas se deben monitorear con frecuencia. MBSA es una buena herramienta para realizar monitoreo.
Vulnerabilidades de fallo de validación	✓ Internet Explorer 7 (IE7)	✓ No seguir enlaces no confiables

¹³ Desactiva características innecesarias de software

¹⁴ HTTP: HyperText Transfer Protocol - Protocolo de Transferencia de HyperTexto



Tabla 2.3. Servicios afectados por vulnerabilidades críticas en plataformas Windows (... continuación)

Vulnerabilidades críticas que afectan las plataformas Windows		
Vulnerabilidad/S.O. Afectado	Descripción	Mitigación
Gusano "Zotob" Microsoft Windows Server 2003, Windows XP y Windows 2000	✓ Aprovecha vulnerabilidad en Plug and Play de Windows	✓ Actualizar el sistema con los paquetes ubicados en el Boletín de seguridad de Microsoft MS05-039, disponible en la siguiente dirección web: http://www.microsoft.com/spain/technet/seguridad/boletines/MS05-039-IT.msp
Explorador de Windows 2000 Microsoft Windows 2000 SP3 y SP4, 98, 98SE y ME.	✓ Vulnerabilidad de ejecución remota de código en la forma en que la función de Vista Web del Explorador de Windows trata determinados caracteres HTML en los campos de vista previa	✓ Instalar las actualizaciones del Boletín de seguridad de Microsoft MS05-024, disponible en la siguiente dirección web: http://www.microsoft.com/latam/technet/seguridad/boletines/ms05-024.msp
Actualización de seguridad acumulativa para Internet Explorer Microsoft Windows 98, 98SE, ME, 2000, XP, 2003	✓ Esta vulnerabilidad podría lograr el control completo de un sistema afectado, mediante la ejecución remota de código.	✓ Instalar las actualizaciones disponibles en el Boletín de seguridad de Microsoft MS05-020, que están ubicados en la dirección web siguiente: http://www.microsoft.com/latam/technet/seguridad/boletines/MS05-020.msp
LSASS¹⁵ Microsoft Windows Server 2003, Windows XP, Windows 2000 y Windows NT 4.0, NetMeeting	✓ Permite la ejecución remota de código, es una vulnerabilidad muy grave y es utilizada por multitud de gusanos para propagarse.	<ul style="list-style-type: none"> ✓ Utilizar un servidor de seguridad como el servidor de seguridad de conexión a internet que está incluido en Windows XP y Windows Server 2003. ✓ Habilitar el filtrado TCP/IP avanzado en sistemas que admitan esta característica. ✓ Bloquear los puertos afectados mediante el uso de IPSec en los sistemas afectados. ✓ Todos los procesos e información adicional de mitigación de esta vulnerabilidad están disponibles en el Boletín de seguridad de Microsoft MS04-011, se pueden consultar en la dirección web: http://www.microsoft.com/spain/technet/seguridad/boletines/ms04-011-it.aspx
RPC-DCOM Microsoft Windows Server 2003, Windows XP, Windows 2000 y Windows NT 4.0	✓ Permiten la ejecución arbitraria de código, denegación de servicio y saturación de búfer.	<ul style="list-style-type: none"> ✓ Bloquear y deshabilitar servicios COM ✓ Utilizar servidores de seguridad de conexión a internet ✓ Bloquear los puertos afectados con un filtro IPSEC y deshabilitar servicios RPC sobre HTTP que escuchan en los puertos 80 y 443. ✓ Deshabilitar DCOM en todos los equipos afectados ✓ Instalar las actualizaciones comprendidas en el Boletín de Seguridad de Microsoft MS03-039, disponibles en el siguiente enlace Web: http://www.microsoft.com/spain/technet/seguridad/boletines/ms03-039-it.aspx
WebDAV¹⁶ Microsoft Windows Server 2003, Windows XP, Windows 2000 y Windows NT 4.0	<ul style="list-style-type: none"> ✓ Es una vulnerabilidad que pone en grave riesgo a miles de servidores que utilizan el servidor web de Microsoft Internet Information Server (IIS). ✓ Existe un desbordamiento de búfer en la 	<ul style="list-style-type: none"> ✓ Deshabilitar el servicio vulnerable ✓ Instalar las actualizaciones correspondientes al boletín de seguridad de Microsoft MS03-007 que está disponible en el siguiente enlace web: http://www.microsoft.com/technet/security/bulletin/ms03-007.msp

¹⁵ LSASS: Servicio de Subsistema de Autorización de Seguridad Local¹⁶ WebDAV: World Wide Web Distributed Authoring and Versioning



Tabla 2.3. Servicios afectados por vulnerabilidades críticas en plataformas Windows (... continuación)

Vulnerabilidades críticas que afectan las plataformas Windows		
Vulnerabilidad/S.O. Afectado	Descripción	Mitigación
	librería "ntdll.dll" que es utilizada por el componente WebDAV de IIS.	
Desbordamiento de búfer en el servicio de Estación de Trabajo Microsoft Windows 2000 SP2, 3 y 4, Microsoft Windows XP Gold, SP1 Microsoft Windows XP 64-Bit Gold, SP1	✓ Vulnerabilidad que lleva a la saturación de un búfer en el servicio Workstation, con lo que permite la ejecución de código de manera remota.	<ul style="list-style-type: none"> ✓ Bloquear los puertos UDP 138, 139 y 445 y los puertos 138, 139 y 445 del servidor de seguridad ✓ Utilizar un servidor de seguridad como el servidor de seguridad de conexión a internet. ✓ Habilitar el filtrado TCP/IP avanzado en los sistemas basados en Windows 2000 y Windows XP ✓ Deshabilitar el servicio de estación de trabajo ✓ Todas la actualizaciones están incluidas en el boletín de Seguridad de Microsoft MS03-049, y están en la siguiente dirección web: http://www.microsoft.com/latam/technet/seguridad/boletines/MS03-049-IT.aspx
Desbordamiento de búfer en el Servicio Mensajero Microsoft Windows Server 2003, Windows XP, Windows 2000 y Windows NT 4.0	✓ El problema consiste en que el servicio Mensajero no valida correctamente la longitud de un mensaje antes de transferirlo al búfer adecuado.	<ul style="list-style-type: none"> ✓ Utilizar un servidor de seguridad personal, como el servidor de seguridad de conexión a internet. ✓ Deshabilitar el servicio mensajero ✓ Todas la actualizaciones de seguridad están disponibles en el boletín de Seguridad de Microsoft MS03-043, las cuales se pueden conseguir en la siguiente dirección web: http://www.microsoft.com/spain/technet/seguridad/boletines/ms03-043-it.aspx
Servicio Localizados Microsoft Windows XP, Windows 2000 y Windows NT 4.0	✓ Permite que un intruso remoto ejecute código arbitrario en un sistema vulnerable enviando una gran carga de requerimientos a dicho servicio.	<ul style="list-style-type: none"> ✓ Aplicar actualizaciones del distribuidor. ✓ Deshabilitar el servicio vulnerable. ✓ Deshabilitar el acceso a NetBIOS. ✓ Las actualizaciones están contenidas en el boletín de Seguridad de Microsoft MS03-001, el enlace web donde puede encontrar información relacionada es: http://www.clcert.cl/show.php?xml=xm/alertas/doc_CLCERT-2003-003.xml&xsl=xsl/alertas.xsl
Universal Plug-and-Play Microsoft Windows 98, 98SE, ME, XP	✓ Es una vulnerabilidad de saturación del búfer.	<ul style="list-style-type: none"> ✓ Actualizar los sistemas operativos con el boletín de Seguridad de Microsoft MS01-059, la web que contiene este tipo de información está disponible en el siguiente enlace web: http://www.microsoft.com/technet/security/bulletin/ms01-059.msp
Microsoft SQL Server Microsoft Windows XP, Windows 2000 y Windows NT 4.0	<ul style="list-style-type: none"> ✓ La Clave de Registro de la Cuenta de Servicio de Microsoft SQL Server tiene Permisos Débiles que Permiten Elevación de Privilegios ✓ Microsoft SQL Server Contiene un Buffer Overflow en la Función pwdencrypt() y de igual forma los procedimientos de almacenamiento extendido. ✓ Microsoft SQL Server 2000 Contiene un Buffer Overflow de Heap en el SSRS (SQL Server Resolution Service) ✓ Microsoft SQL Server 2000 Contiene un Buffer Overflow de Pila en el SSRS (SQL Server Resolution Service) 	<ul style="list-style-type: none"> ✓ La Clave de Registro de la Cuenta de Servicio de Microsoft SQL Server tiene Permisos Débiles que Permiten Elevación de Privilegios ✓ Bloquear el Acceso Externo a los Puertos del Microsoft SQL Server ✓ Todas las actualizaciones de las vulnerabilidades están disponibles en el boletín de Seguridad de Microsoft MS02-039, o también se encuentra información relevante en la siguiente dirección web: http://www.clcert.cl/show.php?xml=xm/alertas/doc_CLCERT-2002-022.xml&xsl=xsl/alertas.xsl



De acuerdo a las gravedades de cada una de las vulnerabilidades, éstas se clasifican conforme se detalla en la siguiente tabla:

Tabla 2.4. Índice de gravedad de vulnerabilidades
Fuente: <http://www.microsoft.com/technet/security/policy/rating.asp>

Término	Definición
Crítica	Una vulnerabilidad cuya explotación podría permitir la propagación de un gusano de Internet sin intervención del usuario.
Importante	Una vulnerabilidad cuya explotación podría poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o la integridad o disponibilidad de los recursos de proceso.
Moderada	Su explotación está mitigada en un alto grado por factores como la configuración predeterminada, la auditoría o la dificultad de la explotación.
Baja	Una vulnerabilidad cuya explotación es extremadamente difícil o cuyo impacto es mínimo.

Las vulnerabilidades descritas en la tabla 2.3, producen que un atacante las aproveche y corrompa el sistema operativo con toda la información que esté manejando al momento del ataque, por tanto, es importante escanear y analizar las vulnerabilidades de cada plataforma para de esa manera fortalecer el sistema con la finalidad que en un futuro no se produzcan ataques por intrusos y con ello la pérdida de los activos de información que son en la actualidad el activo más elemental de una empresa, organización o entidad.

Existen algunas herramientas consideradas para hacer escaneos de vulnerabilidades de un sistema operativo Windows, seguidamente se detalla las herramientas que tienen una mayor credibilidad para hacer escaneos.

Tabla 2.5. Herramientas para realizar escaneos de vulnerabilidades en plataformas Windows

Escaneadores de Vulnerabilidades	
Herramienta	Descripción
GFILANguard Network Security Scanner	Es una herramienta que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de una red. Disponible en: http://www.gfihispana.com/
Windows Live OneCare Safety Scanner	Es un servicio gratuito que permite a los usuarios de ordenadores revisarlos, eliminar virus y llevar a cabo análisis para mejorar el rendimiento del computador. Disponible en: http://onecare.live.com/scan
Nessus	Es uno de los más potentes programas que existen para escanear vulnerabilidades y publicado bajo licencia GPL ¹⁷ . Esta herramienta detecta vulnerabilidades que permiten que un hacker acceda a datos sensibles en un sistema, también facilita chequear configuraciones incorrectas o falta de parches en un sistema. Disponible en: http://www.nessus.org/nessus/
Security System Analyzer (SSA)	Escáner no intrusivo ideal para las auditorías de seguridad informática. Además detecta los parches que faltan en el sistema Windows. Disponible en: http://www.security-database.com/ssa.php
Nmap	Escaneador de puertos que permite además determinar el S.O de la máquina remota. Permite escanear servicios TCP, UDP, ICMP, RPC, etc. Es uno de los escaneadores más completos que existen. Disponible en: http://www.rediris.es/cert/tools/
Otros	En la dirección Web siguiente se encuentra una lista completa de herramientas de seguridad donde consultar y optar por la más adecuada para una plataforma en particular. URL: http://insecure.org/tools/tools-es.html

¹⁷ GPL: General Public License – Licencia Pública General

2.2.3 Amenazas y ataques a los sistemas informáticos

Por lo general una **amenaza** se conceptualiza como “una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese 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 especificar los servicios y mecanismos de seguridad necesarios.” [delitosinformaticos, 2002].

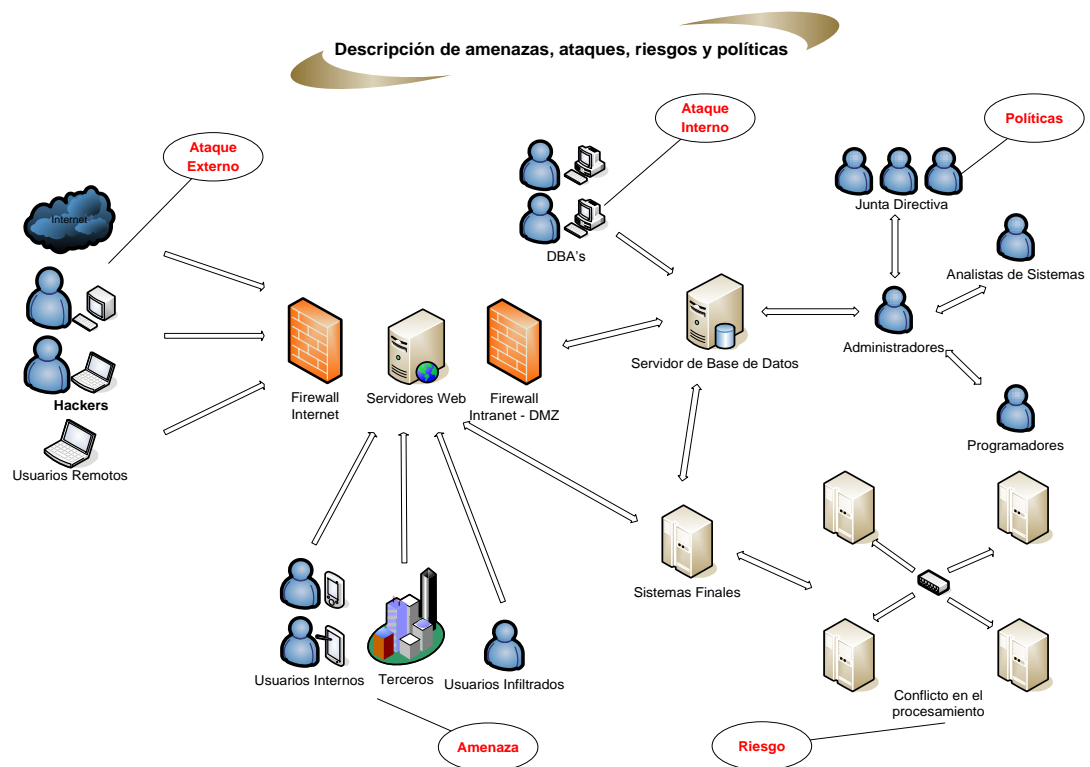


Figura 2.1. Análisis de los riesgos en un sistema informático

“Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.” [delitosinformaticos, 2002]

Un **ataque** no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas y las dos formas de ataques a un sistema operativo son las siguientes:



Tabla 2.6. Definiciones de ataques a sistemas de información
Fuente: <http://www.delitosinformaticos.com/seguridad/clasificacion.shtml>

Clasificación y tipos de ataques en sistema de información		
Amenazas	Descripción	
Interrupción	Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad	
Intercepción	Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador	
Modificación	Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad	
Fabricación	Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad	
Ataques		
Pasivos: Un atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida	Obtención del origen y destinatario de la comunicación	Lee las cabeceras de los paquetes monitorizados
	Control del volumen de tráfico entre las entidades monitorizadas	Obtiene información acerca de la actividad o inactividad inusuales
	Control de las horas habituales de intercambio de datos entre las entidades de la comunicación	Extrae información acerca de los periodos de actividad
Activos: Implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos	Suplantación de identidad	El intruso se hace pasar por una entidad diferente
	Re actuación	Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado
	Modificación de mensajes	Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado
	Degradación fraudulenta del servicio	Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones (Denegación de Servicio)

2.2.4 Categorías de Amenaza en plataformas Windows

“Microsoft Windows cuenta con modelos para categorizar las amenazas de software, tales categorías, con frecuencia suelen usarse para describir las vulnerabilidades de seguridad de las plataformas Windows y así publicar los boletines de seguridad, a continuación se describe como se categorizan las amenazas para plataformas Windows.” [Microsoft, 2003].

Tabla 2.7. Categorías de Amenaza
Fuente: <http://www.microsoft.com/mspress/books/5957.asp>

Término	Definición
Suplantación de identidad	Obtención de acceso y uso ilegales de la información de autenticación de otra persona, como el nombre de usuario y la contraseña.
Manipulación de datos	Modificación maliciosa de los datos.
Rechazo	Se asocia con los usuarios que niegan haber realizado una acción, aunque no hay forma de probarlo. El <i>No rechazo</i> se refiere a la capacidad de un sistema de contrarrestar las amenazas de rechazo (por ejemplo, firmar por un paquete recibido para poder usar como evidencia la firma).
Revelación de información	Exposición de la información a sujetos que no deben tener acceso a ella; por ejemplo, acceder a los archivos sin tener los permisos apropiados.
Denegación de servicio	Intento explícito de impedir que los usuarios legítimos usen un servicio o sistema.
Elevación de privilegios	Se produce cuando un usuario sin privilegios obtiene acceso privilegiado. Un ejemplo de elevación de privilegios sería un usuario sin privilegios que consigue que se le agregue al grupo de Administradores.



2.2.5 Agentes de la Amenaza en Windows

“Las **amenazas maliciosas** son ataques desde dentro o desde fuera de la red que tienen la intención de dañar o deteriorar una empresa. Las **amenazas sin intención de dañar** provienen generalmente de empleados sin formación que no son conscientes de las amenazas y vulnerabilidades de seguridad. La tabla siguiente describe varios agentes de amenazas maliciosas.” [Microsoft, 2003].

Tabla 2.8. Categorías de Amenaza

Fuente: <http://www.microsoft.com/mspress/books/5957.asp>

Término	Definición
Virus	Programa que infecta los archivos de los ordenadores insertando copias de código que se auto replican y suelen borrar archivos críticos o ejecutan alguna otra acción que daña los datos o el ordenador en sí.
Gusano	Programa que se auto replica, a menudo malicioso como un virus que puede propagarse entre ordenadores, por lo general residen en memoria y es difícil de eliminar.
Troyano	Software o correo electrónico que parece ser útil y benigno, pero que de hecho cumple algún objetivo destructivo o facilita el acceso al atacante.
Correo bomba	Un correo electrónico malicioso enviado a un receptor confiado. Cuando el receptor abre el correo o ejecuta el programa, el correo bomba realiza alguna acción maliciosa sobre el ordenador.
Atacante	Persona u organización que lleva a cabo el ataque a una organización determinada.

2.3 CONFIGURACIONES DE LÍNEA BASE PARA LOS SERVIDORES WINDOWS

Crear una línea base de seguridad para un servidor con sistema operativo Windows Server 2003, “permite que los administradores bloqueen los servidores por medio de directivas de línea de base centralizadas, aplicadas de forma coherente a todos los servidores de la organización. Las directivas de línea de base sólo permiten una funcionalidad mínima, pero si 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” [Seguridad en Windows 2000 Server, 2002]

Implementar un entorno de seguridad con Windows Server 2003, se lo puede realizar de algunas formas o tomando en consideración tres tipos de entornos diferentes:

- ✓ **Ciente heredado (LC).**- Es un entorno en el que la seguridad no está lo suficientemente elevada, pero es una seguridad aceptable.
- ✓ **Ciente de empresa (EC).**- Este tipo de entorno de seguridad es más sólido y por ende se lo puede utilizar a nivel empresarial, además tiene una mayor compatibilidad con versiones de sistemas operativos más actuales.
- ✓ **Seguridad especializada:** Funcionalidad limitada (SSLF).- Este tipo de entorno ofrece una seguridad más sólida y elevada que los dos entornos anteriores, ya que cumple estrictas



directivas de seguridad, aunque esto le signifique una pérdida de funcionalidad, administración y compatibilidad con aplicaciones.

A continuación se muestra los tres tipos de entornos de seguridad y los clientes compatibles en cada uno de ellos:

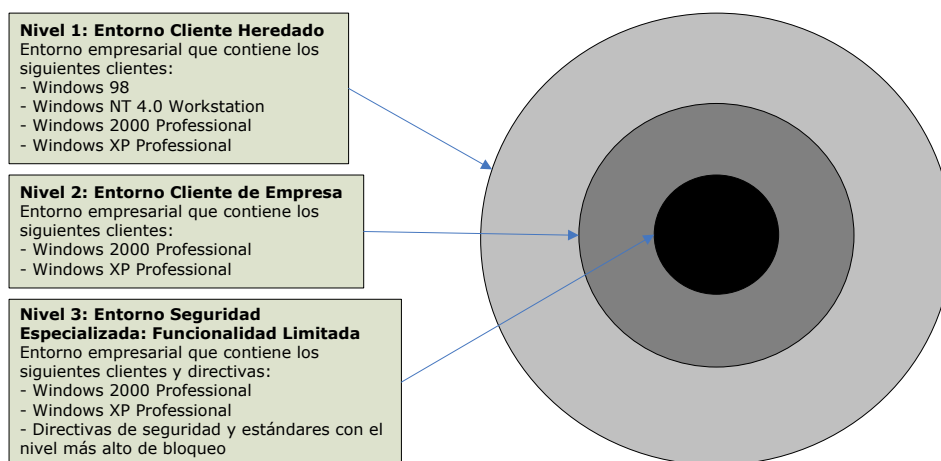


Figura 2.2. Entornos de seguridad existentes y planeados

Fuente: <http://www.microsoft.com/spain/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch01.msp>

2.3.1 Directivas

Definición.- “Una directiva es un conjunto de una o varias políticas de un sistema, en la cual cada política del sistema establece una configuración del objeto al que afecta, así se puede tener políticas para instalar actualizaciones de un sistema operativo, políticas de contraseñas para los usuarios, para los grupos, para la definición de auditorías de eventos, etc.” [Multinglés, 2007]

Dentro de sistemas operativos Windows se distinguen dos tipos de directivas base, las cuales se describen a continuación en el cuadro sinóptico:

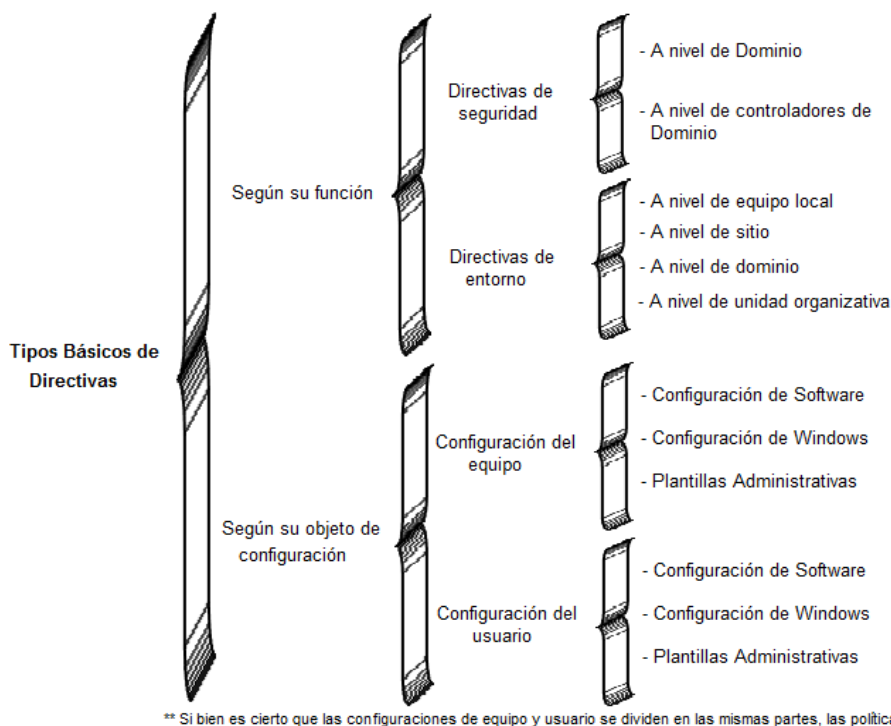


Figura 2.3. Cuadro sinóptico de tipos básicos de directivas en Plataformas Windows

Fuente: <http://multingles.net/docs/GPOS.htm>

En una línea base de seguridad para servidores, la implementación de las diferentes directivas con sus correspondientes políticas, se deben organizar de la siguiente manera: [Microsoft TechNet, WS2000]

- ✓ **Directiva para todo el dominio.** Aborda los requisitos de seguridad comunes, como las directivas de cuentas que se deben aplicar para todos los servidores y estaciones de trabajo.
- ✓ **Directivas para el controlador de dominio.** Directivas que se aplican a la OU¹⁸ de los controladores de dominio. En particular, la configuración afecta a las directivas de auditoría, las opciones de seguridad y la configuración de servicios.
- ✓ **Directivas de línea de base para los servidores miembros.** La configuración común para todos los servidores miembros, como las directivas de auditoría, la configuración de servicios, las directivas que restringen el acceso al registro, el sistema de archivos y otros parámetros de seguridad específicos, como borrar el archivo de páginas de la memoria virtual al apagar el sistema.
- ✓ **Directivas para la función del servidor.** Se definen las directivas de acuerdo a las distintas funciones del servidor. Para cada función, se describen necesidades y configuraciones de seguridad específicas.

¹⁸ Organizational Unit: Unidad Organizativa



2.3.1.1 Directivas de Domino

Dentro de una línea base de seguridad específica a nivel de dominio, se debe considerar muchos parámetros, tal es el caso de la longitud de la contraseña, que varían dependiendo de las directivas de seguridad globales de cada organización. Pero es muy importante que se defina esta configuración de manera apropiada.

En la configuración de las directivas de dominio se debe tener en cuenta las siguientes pautas que se describen en la siguiente figura:

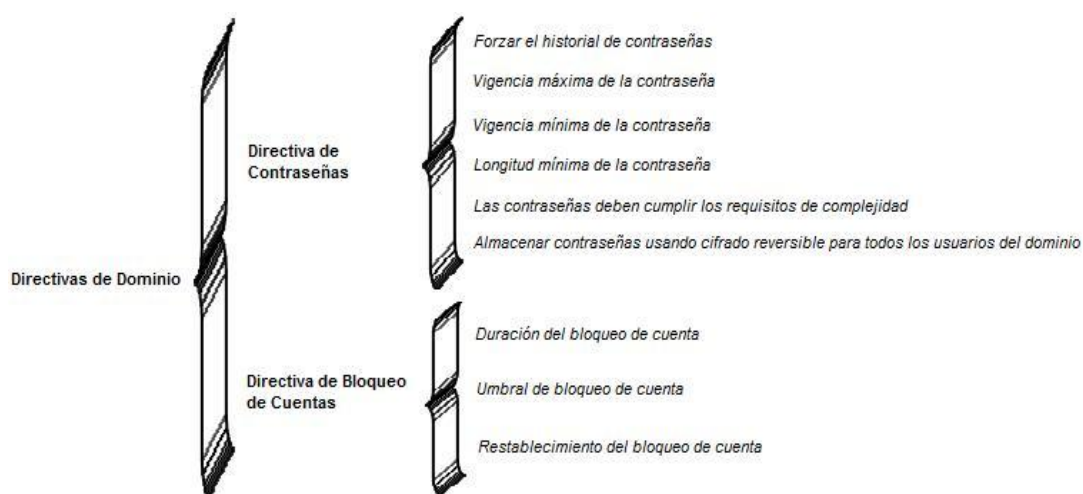


Figura 2.4. Directivas de configuración para un dominio

Fuente: <http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx>

2.3.1.2 Directivas de Línea de Base para los Servidores Miembros

Configurada la seguridad a nivel de dominio, lo siguiente es definir la configuración común para todos los servidores miembros del dominio, se lo puede realizar a través de un GPO¹⁹ en la Unidad Organizativa del servidor miembro, conocido como directiva de línea de base. Un GPO común automatiza el proceso de configuración de parámetros de seguridad específicos en cada servidor. También deberá aplicar manualmente cierta configuración de seguridad adicional que no se puede aplicar mediante directivas de grupo.

La configuración de la directiva de línea de base para los servidores miembros de un dominio engloba un conjunto de directivas las cuales se deben configurar y son las que se detallan en la siguiente tabla:

¹⁹ Group Policy Object - Objeto de Directiva de Grupo

**Tabla 2.9.** Directivas básicas para un servidor miembroFuente: <http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx>

Directiva de Grupo de Línea de Base para los Servidores Miembros	
Directiva	Descripción
Auditoría	Abarca todas las políticas de auditoría en un servidor, las cuales registran los sucesos del sistema, de seguridad y de las aplicaciones que se desee, esta directiva debe estar configurada en todos los servidores miembros del dominio. La configuración de la directiva de auditoría requiere un espacio de disco determinado en megabytes.
Opciones de Seguridad	Determina opciones concretas de seguridad tales como: permitir, denegar, cambiar, restringir, autenticar tareas, actividades de un usuario en particular.
Configuración de Servicios	En ésta directiva se configuran habilitando o deshabilitando los servicios necesarios que un servidor miembro de un dominio debe tener inicializados

2.3.1.3 Otras Opciones de Seguridad

Este tipo de configuraciones de seguridad se deben agregar de manera adicional a la configuración de la plantilla de seguridad de línea de base

Consideraciones de Seguridad Sobre los Ataques en Red.- Algunos ataques de denegación de servicio pueden ser una amenaza para la pila TCP/IP en servidores basados en Windows Server 2003. Ataques de este tipo hacen que equipos o servicios determinados no se encuentren disponibles para los usuarios de la red, además estos ataques son difíciles de detectar. Las configuraciones se describen en **PR01**.

Tabla 2.10. Recomendaciones sobre las entradas del Registro de TCP/IPFuentes: <http://www.microsoft.com/spain/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch01.mspx>
<http://www.microsoft.com/spain/technet/recursos/articulos/secmod57.mspx>

Nombre	Descripción
DisableIPSourceRouting	Nivel de protección del enrutamiento de origen IP. El enrutamiento de origen IP es un mecanismo que permite al remitente determinar la ruta IP que un datagrama debe tomar a través de la red. Vulnerabilidad. - Un atacante podría utilizar paquetes enrutados de origen para ocultar su identidad y ubicación. El enrutamiento de origen permite que un equipo envíe un paquete para especificar la ruta que sigue.
EnableDeadGWDetect	Permitir la detección automática de puertas de enlace de red extintas (podría dar lugar a DoS). Cuando se habilita la detección de puertas de enlace inactivas, TCP puede pedir a IP que cambie a una puerta de enlace de reserva si varias conexiones experimentan dificultades. Vulnerabilidad. - Un atacante puede forzar al servidor a cambiar de puerta de enlace, posiblemente a una no prevista.
EnableICMPRedirect	Permite la redirección ICMP para anular rutas generadas con OSPF. Las redirecciones del protocolo ICMP (Protocolo de mensajes de control de Internet) hacen que la pila instale rutas de host. Estas rutas reemplazan las rutas generadas con OSPF (Abrir primero la ruta de acceso más corta). Vulnerabilidad. - El problema es que el período de tiempo de espera de 10 minutos para las rutas instaladas de redirección ICMP crea un agujero negro temporal para la red afectada en que el tráfico ya no se enrutará correctamente para el host afectado.
EnablePMTUDiscovery	Permitir la detección automática del tamaño de MTU²⁰ (DoS posible por un atacante mediante un pequeño MTU). Cuando se habilita este valor predeterminado, la pila TCP intenta determinar automáticamente la unidad de transmisión máxima (MTU) o el tamaño de paquete más grande a través de la ruta de acceso a un host remoto. Vulnerabilidad. - Si no se establece este valor en 0, un atacante puede hacer que la MTU tenga un valor muy pequeño y sobrecargar la pila al forzar al servidor a fragmentar un gran número de paquetes.

²⁰ **MTU:** Maximum Transfer Unit – Unidad máxima de transferencia



Tabla 2.10. Recomendaciones sobre las entradas del Registro de TCP/IP (... continuación)

Nombre	Descripción
EnableSecurityFilters	Determina tanto los filtros como los caracteres de sincronización para los datagramas TCP/IP. Vulnerabilidad. - Sin habilitar la opción de filtrar el tráfico de red, existe el riesgo que se otorgue indebidamente a un atacante el acceso al equipo y así la posibilidad de ejecutar código malicioso en lugares privilegiados de seguridad.
KeepAliveTime	Con que frecuencia se mantienen activos los paquetes que son enviados en milisegundos. Este valor controla con qué frecuencia TCP intenta comprobar que una conexión inactiva sigue intacta, enviando un paquete de mantenimiento de conexión. Si todavía se puede tener acceso al equipo remoto, confirma el paquete de mantenimiento de conexión. Vulnerabilidad. - Un atacante capaz de conectarse a aplicaciones de red podría causar una condición DoS al establecer numerosas conexiones.
PerformRouterDiscovery	Permitir IRDP para detectar y configurar direcciones de puertas de enlace por defecto. Este valor de configuración se utiliza para habilitar o deshabilitar IRDP (Internet Router Discovery Protocol). IRDP permite al sistema detectar y configurar direcciones de puerta de enlace automáticamente. Vulnerabilidad. - Si un atacante consigue el control de un sistema en el mismo segmento de red, puede configurar un equipo de la red para suplantar a un enrutador. A continuación, otros segmentos con IRDP habilitado intentarían enrutar su tráfico a través del sistema comprometido.
SynAttackProtect	Syn ataque al nivel de protección (protege contra DoS). Este valor de registro hace que TCP ajuste la retransmisión de SYN-ACK ²¹ . Al configurar este valor, las respuestas de conexión exceden el tiempo de espera más rápidamente en caso de un ataque de solicitud de conexión (SYN). Vulnerabilidad. - En un ataque masivo SYN, el atacante envía una corriente continua de paquetes SYN a un servidor y éste deja las conexiones semiabiertas hasta que queda desbordado y ya no puede responder a solicitudes legítimas.
TcpMaxConnectResponseRetransmissions	SYN - ACK de las retransmisiones cuando una solicitud de conexión no es reconocida. Este valor determina el número de veces que TCP retransmite un SYN antes de anular el intento. El tiempo de espera de retransmisión se dobla con cada retransmisión sucesiva en un intento de conexión concreto. El valor de tiempo de espera inicial es de tres segundos. Vulnerabilidad. - En un ataque masivo SYN, el atacante envía una secuencia continua de paquetes SYN a un servidor y éste deja las conexiones semiabiertas hasta que se desborda y ya no puede responder a solicitudes legítimas.
TcpMaxConnectRetransmissions	Esta entrada determina cuántas veces TCP retransmite las solicitudes de nuevas conexiones. Al enviar datos sobre las conexiones existentes, el número máximo de retransmisiones se determina por el valor de la entrada TcpMaxDataRetransmissions. Vulnerabilidad. - Evitar ataques del hombre en el medio, con menos tiempos de retransmisiones entre un host y un servidor en intento por conexión, elimina la posibilidad que un atacante suplante la identidad de un servidor.
TcpMaxDataRetransmissions	Cuántas veces no es reconocida la retransmisión de datos. Este parámetro controla el número de veces que TCP retransmite un segmento de datos individual (segmento sin conexión) antes de anular la conexión. El tiempo de espera de retransmisión se duplicará con cada retransmisión sucesiva en una conexión. Se restablece cuando se reanudan las respuestas. El valor base de tiempo de espera está determinado de forma dinámica por el tiempo de recorrido completo medido en la conexión. Vulnerabilidad. - En un ataque masivo SYN, el atacante envía una secuencia continua de paquetes SYN a un servidor y éste deja las conexiones semiabiertas hasta que se desborda y ya no puede responder a solicitudes legítimas.
TCPMaxPortsExhausted	A cuantas solicitudes de conexión baja se inicia la protección de ataque SYN. Este parámetro controla el punto en que la protección de SYN-ATTACK ²² empieza a funcionar. La protección de SYN-ATTACK empieza a funcionar cuando el sistema rechaza las solicitudes de conexión TcpMaxPortsExhausted porque el registro disponible de conexiones se ha establecido en 0. Vulnerabilidad. - En un ataque masivo SYN, el atacante envía una secuencia continua de paquetes SYN a un servidor y éste deja las conexiones semiabiertas hasta que se desborda y ya no puede responder a solicitudes legítimas.

²¹ **SYN-ACK:** SYNCHRONIZE-ACKNOWLEDGEMENT – Sincronización de Acuse de recibo

²² **SYN-ATTACK:** SYNCHRONIZE-ATTACK – Sincronización de ataque



“Afd.sys controla los intentos de conexión a las aplicaciones de Windows Sockets²³, como los servidores de FTP y de Web. Afd.sys se ha modificado para que admita un gran número de conexiones en estado semiabierto, sin denegar el acceso a los clientes legítimos. Esto se logra al permitir al administrador configurar una copia de seguridad dinámica. La versión de Afd.sys que se incluye con Windows Server 2003 soporta cuatro parámetros de registro que se pueden utilizar para controlar el comportamiento de la copia de seguridad dinámica.” Las configuraciones a realizar se encuentran en **PR02**. [Microsoft Soluciones de Microsoft para la seguridad, 2003]

AFD.sys es un archivo que incluye dos modificaciones: [YoREPARO, 2006]

- ✓ Fija el tamaño de la trama de transferencia de red a 4 KB si AFD.SYS se ejecuta sobre Workstation y a 64 KB si éste controlador de dispositivo se ejecuta sobre Server. Un tamaño mayor significa que las comunicaciones normalmente serán más rápidas, pero también que los buffers colocados tendrán un impacto negativo en la memoria disponible del sistema. El archivo controlador de AFD se encuentra cargado en la ruta `\SystemRoot\System32\drivers\afd.sys`
- ✓ modifica una variable de acuerdo con el tipo de producto. Este cambio ocurre donde este controlador fija el límite de transferencias de ficheros de red simultáneas a 2 si se está ejecutando sobre Workstation. Sobre Server, AFD.SYS chequea la entrada del Registro `\HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\SERVICES\AFD\PARAMETERS\MAXACTIVETRANSMITFILECOUNT` para el límite. Esta variación existe puramente para limitar la funcionalidad de Workstation más que para optimizar el rendimiento.

²³ **Socket:** Objeto que conecta una aplicación a un protocolo de red y hace uso de una dirección IP, un protocolo y un número de puerto.



Tabla 2.11. Configuración de Afd.sys agregada al registro por la directiva de línea de base para los servidores miembros
Fuente: <http://www.microsoft.com/security>

Nombre	Descripción
DynamicBacklogGrowthDelta	Número de conexiones a crear cuando se necesitan conexiones adicionales para aplicaciones Winsock²⁴. Este valor de configuración controla el número de conexiones libres que se deben crear cuando se necesitan conexiones adicionales. Tener cuidado con este valor, ya que un valor elevado puede causar asignaciones explosivas de conexiones libres. Vulnerabilidad.- En un ataque masivo SYN, el atacante envía una secuencia continua de paquetes SYN a un servidor y éste deja las conexiones semiabiertas hasta que se desborda y ya no puede responder a solicitudes legítimas.
EnableDynamicBacklog	Habilitar la reserva dinámica para aplicaciones Winsock. Se trata de un modificador global para habilitar o deshabilitar el registro dinámico. El valor predeterminado es 0 (deshabilitado). Si se establece en 1, la característica de registro dinámico nuevo se habilita. Vulnerabilidad.- Las aplicaciones Windows Sockets pueden ser susceptibles a ataques DoS.
MinimumDynamicBacklog	El número mínimo de conexiones libres para las aplicaciones Winsock. Este valor de configuración controla el número mínimo de conexiones libres que se permiten en un extremo de escucha. Si el número de conexiones libres se sitúa por debajo de este valor, se coloca un subproceso en cola para crear conexiones libres adicionales. Este valor no debe ser demasiado elevado, ya que el código de registro dinámico se emplea cuando el número de conexiones libres está por debajo de este valor. Un valor demasiado elevado puede provocar una reducción de rendimiento. Vulnerabilidad.- Las aplicaciones Windows Sockets pueden ser susceptibles a ataques DoS.
MaximumDynamicBacklog	El número máximo de conexiones “casi-libres” para las aplicaciones Winsock. Este valor de configuración controla el número máximo de conexiones semilibres que se permiten en un extremo de escucha. Las conexiones semilibres incluyen el número de conexiones libres más las conexiones en estado semiconectado (SYN_RECEIVED ²⁵). No se realiza ningún intento por crear conexiones libres adicionales si esto implica superar este valor. Vulnerabilidad.- Las aplicaciones Windows Sockets pueden ser susceptibles a ataques DoS.

Otras entradas recomendadas del registro a parte de las ya especificadas y que son necesarias configurarlas para fortalecer la seguridad de los servidores miembros de un dominio, son las que se especifican a continuación en la siguiente tabla a nivel conceptual y en **PRO3** se describe todas las configuraciones a realizarse en un servidor.

²⁴ **WinSock:** Interface que permite conectarse con el Internet desde el entorno Windows

²⁵ **SYN_RECEIVED:** Recibido sincronismo



Tabla 2.12. Entradas del registro que se recomienda configurar
Fuentes: <http://www.microsoft.com/spain/technet/security/topics/serversecurity/tcg/tcgch10n.mspix>
<http://www.microsoft.com/spain/technet/recursos/articulos/secmod57.mspix>

Nombre de Clave	Descripción
AutoAdminLogon	<p>Habilitar inicio de sesión automático (no recomendable). Por defecto, esta entrada no está habilitada de forma predeterminada y no debe usarse nunca en un servidor, prácticamente en ninguna circunstancia imaginable.</p> <p>Vulnerabilidad.- Si configura un equipo para inicio de sesión automático, cualquiera que pueda obtener acceso físicamente al equipo puede obtener acceso también a todo lo que está en el equipo, incluidas las redes a las que está conectado el equipo. Además, si habilita el inicio de sesión automático, la contraseña se almacena en el registro en texto sin formato. La clave de Registro específica que almacena este parámetro puede leerla de forma remota el grupo de Usuarios autenticados. Por lo tanto, esta entrada sólo es apropiada si el equipo está protegido físicamente y si se asegura de que los usuarios que no son de confianza no puedan consultar de forma remota el Registro.</p>
AutoReboot	<p>Permite que Windows se reinicie automáticamente después de una caída del sistema (recomendado salvo para entornos de alta seguridad). Cuando esta entrada está habilitada, un servidor puede reiniciarse automáticamente tras un bloqueo grave. Está habilitada de forma predeterminada, lo que no es recomendable para los servidores altamente seguros.</p> <p>Vulnerabilidad.- Existe la inquietud de que un equipo podría quedarse atascado en un bucle interminable de errores y reinicios. Sin embargo, la alternativa a esta entrada tampoco es muy atractiva: el equipo simplemente dejará de funcionar.</p>
AutoShareWks	<p>Habilitar comparticiones Administrativas (se recomienda a excepción de entornos de alta seguridad). De forma predeterminada, cuando las funciones de red de Windows están activadas en un servidor, Windows crea recursos compartidos administrativos ocultos, lo que no es recomendable en servidores altamente seguros.</p> <p>Vulnerabilidad.- Debido a que estos recursos compartidos administrativos integrados son muy conocidos y están presentes en la mayoría de los equipos con Windows, los usuarios malintencionados a menudo se concentran en ellos para sus ataques de fuerza bruta que intentan adivinar las contraseñas así como otros tipos de ataques.</p>
DisableSavePassword	<p>Prevenir el guardado dial-up de contraseñas. De forma predeterminada, Windows ofrecerá la opción de guardar las contraseñas para las conexiones de acceso telefónico y VPN, lo que no es recomendable en un servidor.</p> <p>Vulnerabilidad.- Un atacante que roba el equipo portátil de un usuario podría conectarse automáticamente a la red de la empresa si la casilla de verificación Guardar esta contraseña está activada para la entrada de marcado.</p>
Hidden	<p>Ocultar el ordenador de la lista de búsquedas (no se recomienda salvo para entornos de alta seguridad). Puede configurar un equipo para que no envíe anuncios a exploradores en el dominio. Si lo hace, ocultará el equipo de la lista de exploración; no se anuncia a otros equipos en la misma red.</p> <p>Vulnerabilidad.- Un atacante que sabe el nombre de un equipo puede reunir más fácilmente información adicional acerca del mismo. Si habilita esta entrada, elimina un método que un atacante puede utilizar para reunir información acerca de equipos en la red. Además, si habilita esta entrada, puede ayudar a reducir el tráfico de la red. Sin embargo, la vulnerabilidad es menor porque los atacantes pueden utilizar métodos alternativos para identificar y localizar posibles objetivos.</p>
NoDefaultExempt	<p>Habilitar IPSec para proteger el tráfico Kerberos RSVP (recomendado). Esta subclave configura filtros que permiten el funcionamiento de Intercambio de claves de Internet (IKE) y del protocolo de autenticación Kerberos. Los filtros también permiten que se señale (RSVP) la calidad de servicio (QoS) de la red cuando el tráfico de datos está protegido mediante IPSec, así como el tráfico que IPSec no puede proteger (como el tráfico de multidifusión o difusión).</p> <p>Vulnerabilidad.- Puesto que IPSec se utiliza cada vez más para el filtrado de paquetes básico de anfitrión a servidor de seguridad, especialmente en situaciones de exposición a Internet, el efecto de estas suposiciones predeterminadas no se ha comprendido completamente. Algunos administradores de IPSec pueden crear directivas IPSec que consideran seguras, pero que en realidad no lo son, contra ataques entrantes que utilizan las suposiciones predeterminadas. Los atacantes podrían falsificar tráfico de red que parecería contener paquetes legítimos de IKE, RSVP o Kerberos, pero que los dirige a otros servicios de red en el anfitrión.</p>
NtfsDisable8dot3NameCreation	<p>Activar la PC para detener la generación de nombres de archivo de estilo 8.3. Windows Server 2003 soporta formatos de nombre de archivo 8.3 para compatibilidad hacia atrás con aplicaciones de 16 bits. La convención de nombre de archivo 8.3 es un formato de nombramiento que permite nombres de archivo de hasta 8 caracteres de longitud.</p> <p>Vulnerabilidad.- Esto significa que un atacante sólo necesita ocho caracteres para hacer referencia a un archivo que puede tener 20 caracteres de longitud. Por ejemplo, se puede hacer referencia a un archivo denominado EsteEsUnNombreDeArchivoLargo.doc con su nombre de archivo 8.3 EsteEs~1.doc. Si evita utilizar aplicaciones de 16 bits, puede desactivar esta característica. Al deshabilitar la generación de nombres cortos en una partición de sistema de archivos NTFS (NTFS), también se incrementa el rendimiento de enumeración del directorio.</p>



Tabla 2.12. Entradas del registro que se recomienda configurar (... continuación)

Nombre de Clave	Descripción
	Los atacantes pueden utilizar nombres de archivo cortos para tener acceso a los archivos de datos y aplicaciones con nombres de archivo largos que normalmente resultarían difíciles de localizar. Un atacante que haya conseguido acceso al sistema de archivos puede tener acceso a los datos o ejecutar aplicaciones.
NoDriveTypeAutoRun	<p>Desactivar Autoejecutar para todas las unidades. Autoejecución empieza a leer desde una unidad en su PC tan pronto como se le inserta el medio. Como resultado, el archivo de instalación de los programas y el sonido en los medios de audio inician inmediatamente.</p> <p>Vulnerabilidad.- Para evitar que se inicie un programa malicioso al insertar un medio, la directiva de grupo deshabilita la ejecución automática en todas las unidades. Un atacante que consiga acceso físico al sistema podría insertar un DVD o CD habilitado para ejecución automática en el equipo, con lo que ejecutaría código malicioso automáticamente. Dicho programa malicioso puede contener cualquier código que desee el atacante.</p>
NoNameReleaseOnDemand	<p>Permitir a la PC ignorar las solicitudes de liberación de nombres NetBIOS excepto de los servidores WINS. NetBIOS sobre TCP/IP es un protocolo de red que entre otras cosas proporciona un medio para resolver fácilmente los nombres NetBIOS registrados en los sistemas basados en Windows para las direcciones IP configuradas en esos sistemas. Este valor determina si la PC libera su nombre NetBIOS cuando recibe una solicitud de liberación de nombre.</p> <p>Vulnerabilidad.- NetBIOS sobre TCP/IP (NetBT) se ha diseñado para no utilizar ningún método de autenticación y, por lo tanto, es vulnerable a la imitación. La imitación es la práctica de hacer creer que la transmisión procede de un usuario distinto al que ha realizado la acción. Un usuario malicioso puede explotar la naturaleza sin autenticación del protocolo para enviar un datagrama nombre-conflicto a un equipo de destino y provocar que abandone su nombre y deje de responder a las solicitudes que reciba.</p>
SafeDllSearchMode	<p>Activar el modo de búsqueda seguro de DLLs (se recomienda). El orden de búsqueda de DLLs se puede configurar para buscar DLLs solicitadas por procesos en ejecución en una de dos maneras:</p> <ul style="list-style-type: none"> ✓ Buscar primero en las carpetas especificadas en la ruta del sistema, y luego buscar en la carpeta de trabajo actual. ✓ Buscar primero en la carpeta de trabajo actual, y luego buscar en las carpetas especificadas en la ruta del sistema. <p>El valor de registro se configura a 1. Con una configuración de 1, el sistema primero busca en las carpetas que se especifican en la ruta del sistema y luego busca la carpeta de trabajo actual. Con una configuración de 0, el sistema primero busca en la carpeta de trabajo actual y luego busca en las carpetas que se especifican en la ruta del sistema.</p> <p>Vulnerabilidad.- Si un usuario ejecuta inconscientemente código hostil y este código se ha empaquetado con archivos adicionales que incluyen versiones modificadas de archivos DLL del sistema, el código hostil puede cargar sus propias versiones aumentando potencialmente el tipo y grado de daño que puede producir dicho código.</p>
ScreenSaverGracePeriod	<p>El tiempo en segundos antes de que expire el periodo de gracia del protector de pantalla. Windows incluye un periodo de gracia entre el momento en que se lanza el protector de pantalla y la consola se asegura realmente de manera automática cuando está activado el bloqueo del protector de pantalla.</p> <p>Vulnerabilidad.- El período de gracia predeterminado permitido para el movimiento del usuario antes de que surta efecto el bloqueo del protector de pantalla es de cinco segundos. Con el período de gracia predeterminado, el equipo es vulnerable a ataques potenciales de alguien que se dirija a la consola para intentar iniciar sesión en el sistema antes de que el bloqueo surta efecto. Se puede realizar una entrada en el registro para ajustar la duración del período de gracia.</p>
WarningLevel	<p>Umbral de porcentaje para el registro de sucesos de seguridad en el cual el sistema generará una advertencia. Esta opción empezó a estar disponible con SP3 para Windows 2000, una función nueva para generar una auditoría de seguridad en el registro de sucesos de seguridad cuando el registro de seguridad alcanza un umbral definido por el usuario. Por ejemplo, si este valor se configura a 90, entonces mostrará una entrada de suceso para eventID 523 con el siguiente texto cuando el registro de seguridad alcance el 90% de la capacidad: "El registro de sucesos de seguridad está completo al 90%".</p> <p>Nota: Si las configuraciones del registro se configuran para Sobrescribir sucesos según sea necesario o Sobrescribir sucesos que pasen de x días, no se generará este suceso.</p> <p>Vulnerabilidad.- Si se llena el registro de seguridad y no se ha configurado el equipo para sobrescribir sucesos como sea necesario, los sucesos más recientes no se escribirán en el registro. Si dicho registro se llena y el equipo se ha configurado para apagarse cuando ya no pueda registrar sucesos en el registro de seguridad, el equipo se apagará y ya no podrá proporcionar servicios de red.</p>



2.3.1.4 Grupos Restringidos

Esta función grupos restringidos, permite administrar la pertenencia a grupos, valiéndose de mecanismos de directiva, con ello se impide la deliberación de derechos de grupos o usuarios potentes, para hacer uso y aplicar esta función se debe analizar muy bien las necesidades de su organización para de esa manera determinar que grupos o usuarios se desea restringir.

Seguridad del Sistema de Archivos.- “El sistema de archivos NTFS²⁶ en Windows Server 2003 se ha mejorado por lo que la mayoría de permisos predeterminados para NTFS son adecuados para la mayoría de las organizaciones. A continuación se describe algunos **archivos** que **deben ser asegurados** a un mayor nivel, los cuales se encuentran en la carpeta **%SystemRoot%\System32**, a todos los archivos que se detallan se les concede los permisos de: **Administradores:** Control total y **Sistema:** Control total.” [Guía de Seguridad de Windows Server 2003, 2005]

Tabla 2.13. Sistema de archivos a asegurar
Fuente: <http://technet.microsoft.com/es-es/default.aspx>

Nombre de archivo	Descripción
regedit.exe	El Editor del Registro es una herramienta desarrollada para usuarios avanzados. Sirve para ver y cambiar la configuración del Registro del sistema, que contiene información acerca de cómo se ejecuta el equipo. Windows consulta esta información y la actualiza cuando se hacen cambios en el equipo.
arp.exe	Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el Protocolo de Resolución de Direcciones (ARP) .
at.exe	El comando AT programa la ejecución de comandos y programas en un equipo a una hora y fecha especificadas. El servicio de programación debe estar en ejecución para utilizar el comando AT.
attrib.exe	Muestra o cambia los atributos de los archivos: + (establece un atributo), - (borra un atributo), R (sólo lectura del archivo), A (atributo de archivo de almacenamiento), S (atributo de archivo del sistema), H (atributo de archivo oculto), I (no atributo de archivo indizado de contenido).
cacls.exe	Es una herramienta de la línea de comandos que muestra o edita las listas de control de acceso (ACL) de archivos o carpetas.
debug.exe	Se trata de una utilidad interactiva de exploración de bajo nivel, pero que también puede utilizarse para ciertas funciones, entre ellas las de traducir sentencias ensamblador a lenguaje máquina.
edlin.exe	Es un editor de líneas de texto que se puede utilizar para crear y cambiar archivos ASCII.
eventcreate.exe	Esta herramienta de línea de comandos permite a un administrador crear un Id y mensaje de evento personalizados en el registro de eventos especificado.
eventtriggers.exe	Es una herramienta de la línea de comandos que permite a un administrador visualizar y configurar “Eventos disparadores” sobre un sistema local o remoto.
ftp.exe	Transfiere archivos a y desde un equipo que ejecute un servicio de servidor de FTP (a veces conocido como demonio). FTP se puede usar interactivamente.
nbtstat.exe	Muestra las estadísticas del protocolo y las conexiones actuales de TCP/IP usando NBT (NetBIOS sobre TCP/IP).
net.exe	Engloba muchos servicios que usan comandos de red que empiezan por la palabra net. Tales comandos tienen algunas propiedades en común que los hacen útiles en entornos de red.
net1.exe	Es un proceso que pertenece al Microsoft Windows Operating System y ofrece funciones adicionales a su red de área local vía la línea de comando del DOS.
netsh.exe	Es un programa de la línea de comandos que le permite, de forma local o remota, mostrar o modificar la configuración de red de un equipo que está en funcionamiento. Netsh también proporciona una característica de secuencias de comandos que le permite ejecutar un conjunto de comandos en lotes en un equipo especificado. Netsh también puede guardar una secuencia de comandos de configuración en un archivo de texto con el propósito de realizar funciones de archivo o para configurar otros servidores.
netstat.exe	Muestra estadísticas del protocolo y conexiones TCP/IP actuales.
nslookup.exe	Muestra información que puede usar para diagnosticar la infraestructura de DNS (Sistema de nombres de dominio). Para utilizar esta herramienta, debería familiarizarse con el funcionamiento de DNS. El comando Nslookup sólo está disponible si se ha instalado el protocolo TCP/IP. Este protocolo se instala junto con el sistema operativo.
ntbackup.exe	Puede realizar operaciones de copia de seguridad en el símbolo del sistema o con un archivo por lotes mediante el comando ntbackup seguido de diversos parámetros.
rcp.exe	Copia archivos a y desde computadoras que corran el servicio RCP.

²⁶ New Technology File System: Nueva tecnología del Sistema de Archivos



Tabla 2.13. Sistema de archivos a asegurar (... continuación)

Nombre de archivo	Descripción
reg.exe	Agrega, modifica y muestra la información de las subclaves del Registro y los valores de las entradas del Registro.
regedt32.exe	Comando utilizado para conectar, manipular o ejecutar el editor del registro del sistema.
regini.exe	Es un comando que se lo utiliza para manipular el registro del sistema
regsvr32.exe	Este programa de la línea de comandos registra archivos .dll como componentes en el Registro.
rexec.exe	Ejecuta comandos en hosts remotos ejecutando el servicio REXEC. Rexec autentica el nombre del usuario sobre el host remoto antes de ejecutar el comando especificado.
route.exe	Manipula tablas de enrutamiento de red.
rsh.exe	Ejecuta comandos en hosts remotos ejecutando el servicio RSH.
sc.exe	SC es un programa de línea de comandos usado para comunicarse con el Administrador de control de servicios y con los servicios. El Servicio de Control de utilidad se instala con Windows Server 2003.
secedit.exe	Configura y analiza la seguridad del sistema al comparar la configuración actual con al menos una plantilla.
subst.exe	Asocia una ruta de acceso con una letra de unidad.
systeminfo.exe	Esta herramienta muestra información de configuración del sistema operativo de un equipo local o remoto, incluidos los niveles de Service Pack.
telnet.exe	Telnet es un sencillo programa basado en texto que le permite conectarse a otro equipo a través de Internet. Si el administrador o el propietario del equipo le conceden el derecho de conectarse a otro equipo, Telnet le permitirá utilizar comandos para obtener acceso a los programas y servicios del equipo remoto, como si estuviera sentado delante de él. Telnet puede utilizarse para realizar muchas tareas, como obtener acceso a correo electrónico, bases de datos o archivos.
tftp.exe	Transfers files to and from a remote computer running the TFTP service.
tlntsvr.exe	Permite que un usuario remoto inicie sesión en el equipo y ejecute programas, y sea compatible con varios clientes de Telnet TCP/IP, incluyendo los equipos basados en UNIX y Windows. Si este servicio se detiene, es posible que el acceso al usuario remoto no esté disponible. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse.

Asegurar los archivos descritos con anterior, es parte del fortalecimiento del sistema operativo de un servidor, ello permite que un usuario por desconocimiento, error o mala intención los borre y así el sistema de alguna manera quede vulnerable a ataques realizadas por intrusos.

2.3.1.5 Configuración de seguridad adicional

Derechos de Usuario.- Existen algunas configuraciones que aplicando directivas no es posible configurar en un servidor de línea de base, por ello estas configuraciones se deben realizar de forma manual.

En la siguiente tabla se describen algunas asignaciones de **derechos de usuario** agregadas manualmente.

Tabla 2.14. Configuración de derechos de usuarios agregados manualmente

Fuente: <http://go.microsoft.com/fwlink/?linkid=14846>

Nombre del parámetro en IU	Alta seguridad	Vulnerabilidad Mitigada
Deny access to this computer from the network	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts	Usuarios que accedan al computador desde la red sin la debida autorización ponen en riesgo al equipo.
Deny log on as a batch job	Support_388945a0 and Guest	Usuarios normales no necesitan tener habilitada esta característica, este parámetro solo está disponible para administradores.
Deny log on through Terminal Services	Built-in Administrator; Guests; Support_388945a0; Guest; all NON-operating system service accounts	Vulnerabilidades de autenticación, con ello se puede ejecutar código arbitrario por parte de un atacante.



Todas las cuentas de servicio que NO son del sistema operativo, son cuentas de servicio para aplicaciones empresariales específicas. Esto no incluye las cuentas del SISTEMA LOCAL, SERVICIO LOCAL o del SERVICIO DE RED que son cuentas integradas para el sistema operativo. [Microsoft, 2003].

Para agregar manualmente los grupos de seguridad mencionados en la tabla anterior a la Política de línea de base de configuración de Servidor miembro, siga los pasos que se detallan en **PR04**.

Aseguramiento de las cuentas más conocidas.- “Windows Server 2003 tiene varias cuentas integradas de usuario que no se pueden eliminar, pero cuyo nombre se puede cambiar. Dos de las cuentas integradas más conocidas en Windows Server 2003 son Invitado y Administrador.

De manera predeterminada, la cuenta Invitado está desactivada en un servidor miembro y en los controladores de dominio. No se debe cambiar esta configuración. Se debe cambiar el nombre de la cuenta integrada del Administrador y se debe modificar la descripción para ayudar a evitar que los agresores pongan en peligro un servidor remoto utilizando una cuenta bien conocida.

Muchas variaciones de código malicioso utilizan la cuenta integrada del administrador en un intento inicial de poner en peligro a un servidor.” [Microsoft TechNet, 2005].

Todo el procedimiento de aseguramiento de las cuentas en Windows Server 2003, se describen en **PR05**.

Asegurar las cuentas de servicio.- “Nunca configurar un servicio para que se ejecute bajo el contexto de seguridad de una cuenta de dominio, a menos que sea absolutamente necesario. Si se pone en peligro físico un servidor, se puede obtener fácilmente las contraseñas de la cuenta de dominio al descargar los secretos de LSA²⁷.” [Microsoft TechNet Home, 2005].

El aseguramiento de las cuentas de servicio se lo maneja desde la consola de administración de Usuarios y Equipos de Active Directory, desde donde se puede verificar, limitar o conceder privilegios a usuarios o grupos de usuarios de un dominio.

Formatear las particiones con formato NTFS a cada servidor de dominio, permite la admisión de ACL²⁸ en los niveles de archivo y carpeta, sino se han formateado con ese formato de archivo, se puede emplear la utilidad de conversión, pero se debe tener presente que en una conversión de formatos como puede ser de FAT²⁹ a NTFS, las listas ACL de la unidad convertida se configura en **Todos**: Control total. [Microsoft TechNet, 2003]

En equipos que ejecutan Windows Server 2003 con SP1 existen dos plantillas de seguridad referentes a las listas ACL, las cuales debes ser aplicarlas de manera individual tanto a los servidores controladores de dominio, como a los servidores miembros del dominio.

Estas plantillas están ubicadas en el directorio: **%windir%\inf**.

%windir%\inf\defltsv.inf.- Plantilla aplicable a un servidor miembro del dominio

²⁷ LSA: Autoridad de seguridad local

²⁸ Lista de Control de Acceso

²⁹ File Allocation Table - Tabla de Ubicación de Ficheros



%windir%\inf\defltdc.inf.- Plantilla aplicable a un servidor controlador de dominio

Configuración de los Servicios de Terminal Server.- Los servicios de Terminal Server deben ser configurados a nivel empresarial y para la alta seguridad, habilitando o seleccionando los valores que se especifican en la tabla siguiente.

Tabla 2.15. Configuración de Terminal Server
Fuentes: <http://go.microsoft.com/fwlink/?LinkId=16286>
<http://support.microsoft.com/kb/895433/es>

Nivel de cifrado de los servicios de Terminal Server		
Nivel de cifrado	Descripción	
Nivel Alto	Permite utilizar un cifrado de 128 bits, lo que impide que los atacantes intercepten las sesiones de los servicios de terminal server. Es recomendable utilizar el nivel de cifrado alto cuando se esté trabajando en un entorno que incluya clientes que también utilicen un cifrado de 128 bits, como los clientes de conexión a escritorio remoto.	La configuración de los niveles de cifrado de Terminal Server, se describen en PR06
Compatible con el Cliente	Admite una fuerza máxima de cifrado en función de la que admita el cliente, ideal para entornos con clientes mixtos y heredados.	
Nivel Bajo	Cifra los datos enviados del cliente al servidor con un cifrado de 56 bits, pero los datos enviados del servidor al cliente no están cifrados, no es recomendable utilizar para conexiones de servicios de terminal server.	

Informe de errores.- Microsoft recomienda habilitar la opción de informe de errores de Windows, ya que así puede dar seguimiento a los errores del sistema, esto queda a criterio de la empresa dependiendo de las políticas de seguridad y confidencialidad de la información que maneje. El proceso de configuración se describe en **PR07**.

2.3.1.6 Directivas de Línea de Base para el Controlador de Dominio

Los controladores de dominio cumplen un papel muy importante en la tarea de aseguramiento de un ambiente empresarial en la cual existen servidores, computadores de escritorio, computadores portátiles, y otros dispositivos que de alguna manera estén ejecutando Windows Server 2003, un controlador de dominio utiliza el servicio de Active Directory, por lo que cualquier pérdida de un controlador de dominio, podría llegar a generar muchos contratiempos para los clientes, aplicaciones y demás equipos que dependan de los controladores de dominio.

Todos los controladores de dominio creados en el dominio se asignan automáticamente a la OU de controladores de dominio. Los controladores de dominio nunca deben moverse fuera de esta OU, ya que en ella se aplican ACL de seguridades específicas.

La OU de controladores de dominio es una OU de nivel superior y, por tanto, no aplica la configuración definida en la directiva de línea de base para los servidores miembros. Por este motivo, se ha creado una directiva de línea de base distinta para los controladores de dominio.



La configuración implementada en la directiva de línea de base para los controladores de dominio afecta a los apartados siguientes de la directiva:

- ✓ Directiva de auditoría
- ✓ Opciones de seguridad
- ✓ Configuración de servicios

Las políticas configuradas en las directivas de línea de base para un controlador de dominio tienen mucha relación con las políticas base de servidores miembros, la diferencia radica en que las políticas para un servidor controlador de dominio están vinculadas a la unidad organizacional de controladores de dominio. [Seguridad Windows 2000 Server, 2000]

Configuración de la política de auditoría.- Las configuraciones de las políticas de auditoría en un controlador de dominio, son similares a las políticas especificadas para los servidores miembros de un dominio, con la diferencia que *la auditoría de un controlador de dominio asegura que toda la información de auditoría de seguridad correspondiente se registre en los controladores de dominio.* Es recomendable en un ambiente de alta seguridad que sólo se audite las fallas correspondientes a la seguridad.

Configuración de asignación de derechos de usuario.- Esta configuración de derechos de usuarios es una forma de *fortalecer los controladores de dominio*, estas configuraciones difieren a las configuradas para un servidor que es parte de un dominio, en la siguiente tabla se describen las directivas que se deben configurar en un controlador de dominio con Windows Server 2003.

Tabla 2.16. Configuración de asignación de derechos de usuarios recomendada
Fuente: <http://go.microsoft.com/fwlink/?linkid=14846>

Directiva	Configuración empresarial	Alta Seguridad
Access this computer from the network	Not defined	Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS
Add workstations to domain	Not defined	Administrators
Allow log on locally	Administrators, Server Operators, Backup Operators	Administrators
Allow log on through Terminal Services	Administrators	Administrators
Change the system time	Administrators	Administrators
Enable computer and user accounts to be trusted for delegation	Not Defined	Administrators
Load and unload device drivers	Administrators	Administrators
Restore files and directories	Administrators	Administrators
Shutdown the system	Administrators	Administrators

Opciones de Seguridad.- Las opciones de configuración de seguridad en un servidor controlador de dominio, son similares a las configuraciones realizadas para un servidor miembro de un dominio, a continuación en la siguiente tabla se detallan las configuraciones recomendadas que se deben configurar:



Tabla 2.17. Opciones de seguridad recomendadas en un controlador de dominio
Fuente: http://www.microsoft.com/spain/technet/seguridad/recursos/guias/guia_ws2003.msp

Configuraciones para un Controlador de Dominio		
Directiva	Descripción	Configuración de Alta Seguridad
Allow server operators to schedule tasks	Esta política de ajuste, determina si los miembros del grupo de operadores de servidor, están permitidos para enviar trabajos mediante la utilidad AT que permite la programación de tareas.	Disabled
LDAP server signing requirements	Esta política, determina si el servidor LDAP requiere una firma antes de negociar con los clientes LDAP.	Require signing
Refuse machine account password changes	La configuración de esta política determina si los controladores de dominio rechazan las solicitudes computadores miembros que quieren cambiar las contraseñas de sus cuentas.	Disabled
Network Security Settings		
Do not store LAN Manager hash value on next password change	No almacene el valor hash del Administrador LAN en el siguiente cambio de contraseña , determina si el valor hash del Administrador LAN (LM) para la nueva contraseña se almacena cuando se modifica la contraseña. El valor hash de LM es relativamente débil y susceptible a ataques, en comparación con el valor hash criptográficamente más fuerte de Windows NT.	Enabled
Event Log Settings		
	La configuración del registro de eventos en un controlador de dominio, sigue los mismos principios con los que se configura el registro de eventos para servidores miembros. Los administradores deben crear una política de auditoría que defina cuales sucesos se deben reportar como parte de la seguridad del sistema.	
Restricted Groups		
	Las configuraciones de grupos restringidos, se pueden realizar en Windows Server 2003 con SP1 y desde el editor de Objetos de Políticas de Grupo (GPO)	

Todas las configuraciones que se mencionan anteriormente dependen del tipo de equipos que existan en el dominio, tipos de usuarios, criterios de administración y básicamente funcionalidad que se quiere que desempeñe en el entorno donde está operando.

Configuraciones de Seguridad Adicionales.- Las configuraciones de seguridad adicionales son todas aquellas configuraciones que no se las pueden realizar de manera integral en las directivas de seguridad, por lo cual se las debe hacer manualmente, a continuación se detallan las asignaciones de los derechos de los usuarios que deben ser configurados manualmente.

Tabla 2.18. Configuración de derechos de usuarios adheridos manualmente

Fuente: <http://go.microsoft.com/fwlink/?linkid=14845>

Directiva	Descripción	Alta Seguridad
Deny access to this computer from the network	Determina que usuarios tienen impedido el acceso al ordenador desde la red hacia donde se configura esta directiva.	Built-in Administrator; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on as a batch job	Esta directiva determina que cuentas tienen impedido el ingreso al sistema en modo de trabajo en batch.	Support_388945a0 and Guest
Deny log on through Terminal Services	Esta configuración de seguridad determina qué usuarios y grupos se les prohíbe el ingreso al sistema como clientes del Servicio de Terminal Server.	Built-in Administrator; all NON-operating system service accounts



Todas las configuraciones del controlador de dominio, tienen mucha similitud con las configuraciones de un servidor miembro de un dominio, por lo que algunas directivas de seguridad de éstos son aplicables a un controlador de dominio.

Cuando se termina de aplicar las directivas de seguridad en un servidor, se recomienda verificar y validar que los parámetros de seguridad están correctamente configurados, para ello se hace uso de la herramienta provista por Microsoft “Microsoft Security Baseline Analyzer Tool” que es una aplicación que comprueba las seguridades del servidor así como advierte de los problemas de seguridad que puedan existir en el sistema operativo del servidor.

2.3.2 Seguridad de cada función del servidor

Una vez aplicadas las directivas de línea de base, los servidores estarán notablemente más seguros. En este estado, puede que se requiera y deba habilitar parámetros adicionales (canales TSL³⁰, seguridades IPsec, reglas Firewall, etc.) agregando funcionalidad a la línea de base. Dar seguridad de acuerdo a la función que desempeña un servidor permite restringir instalaciones y configuraciones que pueda ser realizada por usuarios sin autorización, en este tipo de aseguramiento está diseñado de manera que un servidor miembro lo único que pueda hacer es comunicarse con el controlador de dominio.

2.3.3 Herramienta Microsoft Security Baseline Analyzer (MBSA) y validación de configuración de puertos

Existe una serie de herramientas para realizar escaneos de vulnerabilidades a un sistema operativo Windows, cada herramienta tiene sus métodos de validación de las configuraciones de seguridad, pero una herramienta que es de mucha utilidad para identificar, analizar y asegurar una intranet es la “Microsoft Security Baseline Analyzer” que es provista por la empresa Microsoft, es de libre distribución y de mucha utilidad en plataformas Windows.

a. Herramienta MBSA

“Esta herramienta de análisis de seguridad da la posibilidad de determinar posibles vulnerabilidades administrativas presentes en uno o más equipos de una intranet. MBSA explorará el equipo o su dirección IP de red. En el caso de una exploración múltiple explorará los equipos en el dominio o el rango de direcciones IP especificado, MBSA luego del análisis devolverá un informe con los detalles del o de los equipo/s que analizó y así se tendrá la posibilidad de ver cómo resolver esos inconvenientes.” [Microsoft TechNet Latinoamérica, 2008]

MBSA, permite analizar configuraciones de seguridad incorrectas en un sistema operativo Windows, también permite examinar actualizaciones de seguridad y además se integra con los servicios de actualización del sistema operativo Windows. A continuación en la tabla, se detalla lo que permite y ayuda a validar MBSA.

³⁰ TSL: Transport Layer Security – Seguridad para Capa de Transporte



Tabla 2.19. Descripción de validaciones de seguridad permitidas con la herramienta MBSA
<http://www.microsoft.com/latam/technet/recursos/howto/MBSA/asegurar.msp>

Actividades que permite realizar MBSA	
Tema	Detalle
Chequeo de vulnerabilidades del sistema operativo Windows	<ul style="list-style-type: none"> ❖ Cantidad de miembros dentro del grupo de administradores locales del equipo. ❖ Sistema de archivos utilizado. ❖ Firewall esta activo o no, etc.
Chequeo de contraseñas	<ul style="list-style-type: none"> ❖ Análisis de la presencia de cuentas con contraseña en blanco y otros inconvenientes.
Chequeo de vulnerabilidades de IIS	<ul style="list-style-type: none"> ❖ Da una idea de los riesgos de seguridad.
Chequeo de vulnerabilidades de SQL	<ul style="list-style-type: none"> ❖ Si SQL se encuentra en una configuración de nodos aparecerán algunas advertencias respecto a los miembros administradores, las cuentas de invitado y el chequeo de las contraseñas de las cuentas.
Chequeo de actualizaciones de seguridad	<ul style="list-style-type: none"> ❖ Configurar los equipos para que realicen ellos mismos el chequeo con los servidores de actualización de Microsoft. ❖ Realizar el chequeo contra los servidores internos de actualización, a través de esta opción solo se instalarán en el equipo las actualizaciones aprobadas por la empresa. ❖ Realizar el chequeo contra los servidores de actualización de Microsoft.

b. Validación de la configuración de puertos

“Es importante que se valide la configuración final de los puertos y que comprenda a qué puertos TCP y UDP "escuchan" los servidores que ejecutan Windows 2003. Después de aplicar las directivas de línea de base, se puede ejecutar el comando netstat para ver a qué puertos sigue escuchando el servidor para cada tarjeta de interfaz de red.” [Microsoft TechNet, WS2000]

A continuación se muestra el resultado esperado de netstat para un servidor miembro con la directiva de línea de base para los servidores miembros aplicada:

Tabla 2.20. Puertos a los que escuchará un servidor miembro después de aplicar la directiva de línea de base para servidores miembros

Fuente: <http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx>

Protocolo	Dirección local	Dirección externa	Estado
TCP	0.0.0.0:135	0.0.0.0:0	ESCUCHANDO
TCP	0.0.0.0:445	0.0.0.0:0	ESCUCHANDO
TCP	<Dirección IP>:139	0.0.0.0:0	ESCUCHANDO
UDP	<Dirección IP>:137	*.*	N/A
UDP	<Dirección IP>:138	*.*	N/A
UDP	0.0.0.0:445	*.*	N/A
UDP	0.0.0.0:1027	*.*	N/A
UDP	0.0.0.0:1045	*.*	N/A

2.4 POLÍTICAS DE UTILIZACIÓN DE WINDOWS UPDATE EN UN SERVIDOR WINDOWS

Contar con unas políticas de actualización de Windows para un servidor que trabaja con Windows Server 2003 es de mucha utilidad, porque protege al equipo contra vulnerabilidades, virus, gusanos y otras amenazas que afectan el rendimiento de un servidor que está en producción.



Para mantener un servidor Windows actualizado con todos los parches de seguridad que garanticen la integridad, confidencialidad y disponibilidad de la información se debe contar con técnicas determinadas que mantengan al servidor actualizado.

Hacer uso de una política de utilización de Windows Update es una manera de comprobar las seguridades de los equipos que operan con Windows, la comprobación se la puede realizar ingresando al sitio Web de Windows Update en donde se compara al equipo conectado con una lista conocida de actualizaciones aplicables y así se determina las actualizaciones por aplicar.

La instalación de actualizaciones para un servidor Windows se las describe en el **manual de políticas y procedimientos**, específicamente se recomienda ver **PL01**.

2.5 RESUMEN Y CHECKLIST DE LAS TÉCNICAS DE CONFIGURACIÓN E INSTALACIÓN DE SEGURIDADES EN LAS PLATAFORMAS WINDOWS



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003
Fuente: <http://www.microsoft.com/spain/technet/recursos/articulos/secmod224.msp>

Configuración del Sistema Operativo	
Información General	
Versión del Sistema Operativo	<input type="checkbox"/> Windows Server 2003 Standard Edition. <input type="checkbox"/> Windows XP. <input type="checkbox"/> Windows Vista. <input type="checkbox"/> Otra versión Windows.
Nivel de Service Pack	<input type="checkbox"/> Servidor Controlador de Dominio Primario. <input type="checkbox"/> Servidor Controlador de Dominio Secundario. <input type="checkbox"/> Servidor Miembro. <input type="checkbox"/> Host.
Pertenencia a la Red	<input type="checkbox"/> SP1 <input type="checkbox"/> SP2 <input type="checkbox"/> SP3 <input type="checkbox"/> Grupo de trabajo. Nombre: _____ <input type="checkbox"/> Dominio. Nombre: _____
Fecha de Instalación	Otros niveles de Service Pack: _____ Revisiones posteriores al Service Pack: _____ _____
Completado y Comprobado	Lista de comprobación de configuraciones de seguridad de Windows Server 2003. Utilizar esta lista para hacer un seguimiento de la configuración de un sistema de manera correcta
<input type="checkbox"/>	Configuración del sistema de archivos: Tipo de sistema de archivos: <input type="checkbox"/> NTFS <input type="checkbox"/> FAT
Directivas de cuenta	Directivas de contraseñas
<input type="checkbox"/>	Enforce password history. - Establecer el límite de la frecuencia de reutilización de las contraseñas. Configuración del equipo: _____ contraseñas recordadas
<input type="checkbox"/>	Maximum password age. - Establecer el período de tiempo que los usuarios podrán mantener la contraseña antes de tener que cambiarla. Configuración del equipo: _____ días
<input type="checkbox"/>	Minimum password age. - Establecer el período de tiempo que los usuarios deben mantener la contraseña antes de poder cambiarla. Configuración del equipo: _____ días
<input type="checkbox"/>	Minimum password length. - Establecer el número mínimo de caracteres necesarios para las contraseñas de usuario. Configuración del equipo: _____ caracteres
<input type="checkbox"/>	Password must meet complexity requirements. - Utilizar necesariamente contraseñas complejas (seguras). Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Store passwords using reversible encryption. - <i>No habilitar.</i> Utilizar un cifrado mínimo para las contraseñas. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
	Directiva de bloqueo de cuentas
<input type="checkbox"/>	Account lockout duration. - Tras varios intentos incorrectos de introducción de contraseña, bloquear la cuenta durante un período de tiempo concreto. Configuración del equipo: _____ minutos
<input type="checkbox"/>	Account lockout threshold. - Establecer el número de intentos de inicio de sesión incorrectos permitidos antes de bloquear la cuenta. Configuración del equipo: _____ intentos de inicio de sesión incorrectos
<input type="checkbox"/>	Reset account lockout counter after. - Establecer la duración del umbral de bloqueos antes de restablecer. Configuración del equipo: _____ minutos



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
	Directiva Kerberos
<input type="checkbox"/>	Enforce user logon restrictions. - Validar las solicitudes de inicio de sesión comprobando la directiva de derechos de usuario. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Maximum lifetime for Service ticket. - Establecer la duración máxima de vigencia de un vale de servicio. Configuración del equipo: _____ minutos
<input type="checkbox"/>	Maximum lifetime for user ticket. - Establecer la duración máxima de vigencia de un vale de usuario. Configuración del equipo: _____ horas
<input type="checkbox"/>	Maximum lifetime for user ticket renewal. - Establecer el período de renovación de vales caducados. Configuración del equipo: _____ días
<input type="checkbox"/>	Maximum tolerance for computer clock synchronization. - Establecer la tolerancia máxima para la sincronización entre los equipos del dominio. Configuración del equipo: _____ minutos
	Directivas Locales
	Directiva de auditoría
<input type="checkbox"/>	Audit account logon events. - Auditar sucesos de inicio o cierre de sesión de la cuenta desde otro equipo en el que se utiliza este equipo para validar la cuenta.
<input type="checkbox"/>	Audit account management. - Auditar las actividades de administración de cuentas.
<input type="checkbox"/>	Audit directory service access. - Auditar el acceso a un objeto de Microsoft Active Directory que tiene especificada su propia lista de control de acceso al sistema.
<input type="checkbox"/>	Audit logon events. - Auditar sucesos de inicio o cierre de sesión de red o local en este equipo. Los "Sucesos de inicio de sesión" se generan en el lugar donde se produce el intento de inicio de sesión.
<input type="checkbox"/>	Audit object Access. - Auditar el acceso a un objeto, por ejemplo, un archivo, carpeta, clave de registro o impresora que tiene especificada su propia lista de control de acceso al sistema.
<input type="checkbox"/>	Audit policy change. - Auditar un cambio en las directivas de asignación de derechos de usuario, directivas de auditoría o directivas de confianza.
<input type="checkbox"/>	Audit privilege use. - Auditar cada instancia en la que un usuario ejerce un derecho de usuario.
<input type="checkbox"/>	Audit process tracking. - Auditar información detallada de seguimiento de sucesos como activación de programas, salida de procesos, duplicación de manipuladores y acceso indirecto a los objetos.
<input type="checkbox"/>	Audit system events. - Auditar el momento en que un usuario reinicia o apaga el equipo o el momento en que se produce un suceso que afecta a la seguridad del sistema o al registro de seguridad.
	Asignación de derechos de usuario
<input type="checkbox"/>	Access this Computer from the network. - Determinar los usuarios que pueden conectarse al equipo a través de la red.
<input type="checkbox"/>	Act as part of the operating system. - Permitir que un usuario ejecute código como el propio sistema operativo y, por lo tanto, como cualquier otro usuario del sistema.
<input type="checkbox"/>	Add Workstation to domain. - Determina cuales grupos o usuarios pueden agregar estaciones de trabajo a un dominio.
<input type="checkbox"/>	Adjust memory quotas for a process. - Determina que puede cambiar el máximo de memoria la cual puede ser consumida por un proceso.
<input type="checkbox"/>	Allow log on locally. - Determina que usuarios pueden iniciar sesión interactivamente en el equipo.
<input type="checkbox"/>	Allow log on through Terminal Services. - Determina que usuarios o grupos tienen permiso para acceder al equipo como un cliente de Terminal Services.
<input type="checkbox"/>	Back up files and directories. - Permitir al usuario ignorar los permisos de archivos y directorios para realizar copias de seguridad del sistema.
<input type="checkbox"/>	Bypass traverse checking. - Permitir que el usuario pase a través de carpetas a las que no tendría acceso de otra manera.
<input type="checkbox"/>	Change the system time. - Permitir que el usuario establezca la hora del reloj interno del equipo.
<input type="checkbox"/>	Create a pagefile. - Permitir al usuario crear y cambiar el tamaño de un archivo de paginación.
<input type="checkbox"/>	Create a token object. - Permitir a un proceso crear un símbolo (token) de acceso.
<input type="checkbox"/>	Create global objects. - Permite crear objetos globales durante las sesiones de servicios de Terminal Services.



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/>	Create permanent shared objects. - Permitir a un proceso crear un objeto de directorio en el administrador de objetos de Windows 2000.
<input type="checkbox"/>	Debug programs. - Permitir al usuario asignar un depurador a un proceso que se ejecute en el contexto de un usuario diferente.
<input type="checkbox"/>	Deny access to this computer from the network. - Prohibir a un usuario o grupo de usuarios la conexión al equipo desde la red.
<input type="checkbox"/>	Deny log on as a batch job. - Prohibir a un usuario o grupo de usuarios iniciar sesión mediante un servicio de cola por lotes.
<input type="checkbox"/>	Deny log on as a service. - Prohibir a un usuario o grupo de usuarios iniciar sesión como servicio.
<input type="checkbox"/>	Deny log on locally. - Prohibir a un usuario o grupo de usuarios iniciar sesión localmente en el teclado.
<input type="checkbox"/>	Deny log on through Terminal Services. - Permite determinar que usuarios y grupos se les prohíbe el inicio de sesión como cliente de Terminal Services.
<input type="checkbox"/>	Enable computer and user accounts to be trusted for delegation. - Permitir que el usuario cambie la configuración de confianza para la delegación de un usuario o equipo en Active Directory.
<input type="checkbox"/>	Force shutdown from a remote system. - Permitir que el usuario apague el equipo desde una ubicación remota de la red.
<input type="checkbox"/>	Generate security audits. - Permitir que un proceso genere entradas en el registro de seguridad.
<input type="checkbox"/>	Impersonate a client after authentication. - Privilegio que impide la suplantación de un usuario no autorizado.
<input type="checkbox"/>	Increase scheduling priority. - Permitir a un proceso con Propiedad de escritura el acceso a otro proceso para cambiar la prioridad de ejecución de dicho proceso.
<input type="checkbox"/>	Load and unload device drivers. - Permitir que un usuario instale y desinstale controladores de dispositivos Plug and Play.
<input type="checkbox"/>	Lock pages in memory. - Permitir que un proceso mantenga datos en la memoria física. Esto evita que el sistema pague los datos en la memoria virtual del disco.
<input type="checkbox"/>	Log on as a batch job. - Permitir que un usuario inicie sesión mediante un servicio de cola por lotes.
<input type="checkbox"/>	Log on as a service. - Permitir que una entidad de seguridad principal inicie sesión como servicio.
<input type="checkbox"/>	Manage auditing and security log. - Permitir que un usuario especifique las opciones de auditoría de acceso a objetos para recursos individuales, como archivos, objetos de Active Directory y claves de registro.
<input type="checkbox"/>	Modify firmware environment values. - Permitir que un proceso, a través de una API, o un usuario, a través del cuadro de diálogo Propiedades del sistema, puedan modificar las variables de entorno del sistema.
<input type="checkbox"/>	Perform volume maintenance tasks. - Determina que usuarios y grupos pueden ejecutar tareas de mantenimiento en un volumen, tales como la desfragmentación remota.
<input type="checkbox"/>	Profile single process. - Permitir que un usuario ejecute las herramientas de supervisión del rendimiento de Microsoft Windows NT y Windows 2000 para supervisar el rendimiento de procesos que no son del sistema.
<input type="checkbox"/>	Profile system performance. - Permitir que un usuario ejecute las herramientas de supervisión del rendimiento de Microsoft Windows NT y Windows 2000 para supervisar el rendimiento de procesos del sistema.
<input type="checkbox"/>	Remove computer from docking station. - Permitir que un usuario de un equipo portátil desbloquee el equipo haciendo clic en "Retirar equipo" en el menú Inicio .
<input type="checkbox"/>	Replace a process level token. - Permitir que un proceso principal reemplace el token de acceso asociado a un proceso secundario.
<input type="checkbox"/>	Restore files and directories. - Permitir al usuario eludir los permisos de archivo y directorio al restaurar archivos o directorios de una copia de seguridad y establecer cualquier entidad principal de seguridad válida como propietaria de un objeto.
<input type="checkbox"/>	Shut down the system. - Permitir al usuario apagar el equipo local.
<input type="checkbox"/>	Synchronize directory service data. - Permitir que un servicio ofrezca servicios de sincronización de directorios.
<input type="checkbox"/>	Take ownership of files or other objects. - Permitir que el usuario sea propietario de cualquier objeto asegurable del sistema.
Opciones de seguridad	
<input type="checkbox"/>	Account: Administrator account status. - Permitir que un equipo cuando se inicia, el estado de la cuenta administrador siempre este habilitada en modo seguro. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Account: Guest account status. - Permite que usuarios de red no autenticados inicien sesión como invitados y accedan de esa manera al equipo. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/>	Account: Limit local account use of blank passwords to console logon only. - Si esta política está configurada en habilitada, cuentas locales con contraseñas en blanco no pueden iniciar sesión desde una red de cliente remoto, y cuentas locales sin contraseña de protección solo puedan iniciar sesión desde el teclado del equipo físico. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Account: Rename administrator account. - Asociar un nombre de cuenta diferente para la cuenta "Administrador".
<input type="checkbox"/>	Account: Rename guest account. - Asociar un nombre de cuenta diferente para la cuenta "Invitado".
<input type="checkbox"/>	Audit: Audit the Access of global System objects. - Permitir el acceso de objetos globales del sistema para su auditoría. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Audit: Audit the use of Backup and Restore privilege. - Permitir la auditoría de los derechos del usuario de copia de seguridad y restauración. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Audit: Shut down system immediately if unable to log security audits. - Determinar si se debe apagar el sistema si no puede registrar sucesos de seguridad. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax. - Política utilizada para controlar el ataque de aplicaciones DCOM al equipo.
<input type="checkbox"/>	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax. - Política que podrían usar usuarios o grupos para iniciar o activar aplicaciones DCOM de manera local o remota. Configuración que controla el ataque de superficie a equipos por parte de aplicaciones DCOM.
<input type="checkbox"/>	Devices: Allow undock without having to log on. - Determina si una computadora portátil puede desacoplarse sin que el usuario tenga que iniciar sesión en la computadora. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Devices: Allowed to format and eject removable media. - Determina quién puede formatear y expulsar medios removibles. En un servidor sería tarea de administradores.
<input type="checkbox"/>	Devices: Prevent users from installing printer drivers. - Determinar que los miembros del grupo de usuarios no puedan instalar controladores de impresora. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Devices: Restrict CD-ROM access to locally logged-on user only. - Si se habilita, esta directiva sólo permite el acceso a los medios de CD-ROM extraíbles a los usuarios que hayan iniciado una sesión de forma interactiva. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Devices: Restrict floppy access to locally logged-on user only. - Determina si los medios floppy removibles son accesibles de manera local como por usuarios remotos de manera simultánea. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Devices: Unsigned driver installation behavior. - Determinar la acción que realizar cuando se intenta instalar un controlador de dispositivo que no ha sido certificado por el laboratorio de calidad de hardware de Windows.
<input type="checkbox"/>	Domain controller: Allow server operators to schedule tasks. - Determinar si los operadores de servidores tienen permiso para enviar trabajos mediante la herramienta de programación AT. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Domain controller: LDAP server signing requirements. - Determina que el servidor LDAP requiere una firma antes de negociar con el cliente LDAP.
<input type="checkbox"/>	Domain controller: Refuse machine account password changes. - Determina si el controlador de dominio rechaza peticiones de cambio de contraseña de cuenta de equipo. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Domain member: Digitally encrypt or sign secure channel data (always). - Si se habilita esta directiva, se deberá firmar o cifrar todo el tráfico saliente de canales seguros. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Domain member: Digitally encrypt secure channel data (when possible). - Si se habilita esta directiva, se deberá cifrar todo el tráfico saliente de canales seguros. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Domain member: Digitally sign secure channel data (when possible). - Si se habilita esta directiva, se deberá firmar todo el tráfico saliente de canales seguros. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/>	Domain member: Disable machine account password changes. - Determinar si se debe impedir que la contraseña de la cuenta del equipo se restablezca semanalmente. Si se habilita esta directiva, el equipo no solicitará un cambio de contraseñas semanal. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Domain member: Maximum machine account password age. - Determina el máximo periodo permitido para una contraseña de una cuenta de equipo.
<input type="checkbox"/>	Domain member: Require strong (Windows 2000 or later) session key. - Si se habilita esta directiva, todo el tráfico saliente de canales seguros requerirá una clave de cifrado segura Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Interactive logon: Display user information when the session is locked. - Muestra información del usuario cuando el período de sesiones está bloqueado
<input type="checkbox"/>	Interactive logon: Do not display last user name. - Determinar si se mostrará en la pantalla de inicio de sesión de Windows el nombre del último usuario que inició una sesión en el equipo. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Interactive logon: Do not require CTRL+ALT+DEL. - Determinar si es necesario presionar CTRL+ALT+SUPR antes de que el usuario pueda iniciar una sesión. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Interactive logon: Message text for users attempting to log on. - Especificar el mensaje de texto que se muestra a los usuarios cuando inician una sesión.
<input type="checkbox"/>	Interactive logon: Message title for users attempting to log on. - Especificar el título de la barra de título de la ventana que contiene el texto del mensaje para los usuarios que intentan iniciar sesión.
<input type="checkbox"/>	Interactive logon: Number of previous logons to cache (in case domain controller is not available). - Determinar el número de veces que un usuario puede iniciar sesión en un dominio de Windows utilizando la información de cuenta almacenada en caché. Configuración del equipo: Caché: _____ inicios de sesión
<input type="checkbox"/>	Interactive logon: Prompt user to change password before expiration. - Determinar con cuánta antelación se debe avisar a los usuarios de Windows 2003 de que su contraseña va a caducar. Configuración del equipo: _____ días
<input type="checkbox"/>	Interactive logon: Require Domain Controller authentication to unlock workstation. - Esta política determina si un controlador de dominio debería ser contactado cuando un equipo se inicia. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Interactive logon: Require smart card. - Política que determina que los usuarios inicien sesión en un equipo con tarjeta inteligente. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Interactive logon: Smart card removal behavior. - Determinar la acción que se debe realizar cuando la tarjeta inteligente de un usuario que ha iniciado sesión se retira del lector de tarjetas inteligentes.
<input type="checkbox"/>	Microsoft network client: Digitally sign communications (always). - Determinar si el equipo siempre firmará digitalmente las comunicaciones con el cliente. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Microsoft network client: Digitally sign communications (if server agrees). - Si se habilita, el cliente SMB firmará los paquetes SMB sólo cuando se comunique con un servidor SMB que tenga habilitada o al que se le solicita la firma de paquetes SMB. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Microsoft network client: Send unencrypted password to third-party SMB servers. - Si se habilita, se permitirá al redirector SMB enviar contraseñas no cifradas a servidores SMB que no sean de Microsoft y no sean compatibles con el cifrado de contraseñas durante la autenticación. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Microsoft network server: Amount of idle time required before suspending session. - Establecer el tiempo de inactividad continuado que debe transcurrir en una sesión de Bloque de mensajes de servidor (SMB) antes de que la sesión se desconecte por inactividad. Configuración del equipo: _____ minutos
<input type="checkbox"/>	Microsoft network server: Digitally sign communications (always). - Si se habilita, solicitar al servidor SMB que realice la firma de paquetes SMB. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/>	Microsoft network server: Digitally sign communications (if client agrees). - Si se habilita, el servidor SMB firmará los paquetes SMB cuando sea necesario. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Microsoft network server: Disconnect clients when logon hours expire. - Desconectar a los usuarios que estén conectados al equipo local fuera de las horas válidas de sesión para sus cuentas de usuario. Sólo se puede establecer en controladores de dominio. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Allow anonymous SID/Name translation. - Si se habilita esta política un usuario con acceso local usaría el SID para obtener el nombre real de un administrador. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Do not allow anonymous enumeration of SAM accounts. - Política que determina que permisos adicionales se concederían para conexiones anónimas a equipos. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Do not allow anonymous enumeration of SAM accounts and shares. - Política para enumeraciones anónimas de cuentas SAM y comparticiones permitidas. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Do not allow storage of credentials or .NET Passports for network authentication. - Configurar para almacenar nombres de usuarios y contraseñas, credenciales o Passports de Microsoft .NET, para luego usarse esa autenticación lograda en el dominio. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Let Everyone permissions apply to anonymous users. - Si se configura, los usuarios Windows son capaces de ejecutar ciertas actividades, tales como enumerar nombres de cuentas de dominio y comparticiones de red. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Named Pipes that can be accessed anonymously. - Determina cuales sesiones de comunicación tendrían atributos y permisos que permitan acceder anónimamente.
<input type="checkbox"/>	Network access: Remotely accessible registry paths. - Determina que caminos del registro pueden accederse desde la red.
<input type="checkbox"/>	Network access: Remotely accessible registry paths and sub-paths. - Detalla cuales es el camino y subcamino para acceder desde la red hasta el registro.
<input type="checkbox"/>	Network access: Restrict anonymous access to Named Pipes and Shares. - Usar esta política para restringir accesos anónimos a compartir y nombrar canalizaciones Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network access: Shares that can be accessed anonymously. - Política que determina que comparticiones de red pueden ser accedidos por usuarios anónimos.
<input type="checkbox"/>	Network access: Sharing and security model for local accounts. - Política para determinar cómo se inicia sesiones en red, que cuentas de usuarios locales son autenticadas.
<input type="checkbox"/>	Network security: Do not store LAN Manager hash value on next password change. - Determina si el valor Hash para nueva contraseña se guarda cuando la contraseña es cambiada. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network security: Force logoff when logon hours expire. - Política útil para desconectar a usuarios que son conectados a un equipo local fuera de las horas de inicio de sesión validas para sus cuentas. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Network security: LAN Manager authentication level. - Determinar qué protocolo de autenticación de desafío/respuesta se utiliza para los inicios de sesión de la red.
<input type="checkbox"/>	Network security: LDAP client signing requirements. - Política que determina el nivel de datos a firmar que son solicitados en nombre de clientes que emiten solicitudes LDAP BIND.
<input type="checkbox"/>	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients. - Esta política establece que un cliente exija la negociación del mensaje de manera confidencial (cifrado), mensaje firmado, cifrado de 128 bits, o seguridad de sesión NTLMv2.
<input type="checkbox"/>	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers. - Esta política establece que un servidor exija la negociación del mensaje de manera confidencial. Integridad del mensaje, cifrado de 128 bits o seguridad de sesión NTLMv2.
<input type="checkbox"/>	Recovery console: Allow automatic administrative logon. - Si se establece, la consola de recuperación no necesitará una contraseña e iniciará una sesión en el sistema de forma automática. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/>	Recovery console: Allow floppy copy and access to all drives and all folders. - Permitir la activación del comando SET de la Consola de recuperación. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Shutdown: Allow system to be shut down without having to log on. - Configurar un equipo para que permita que se apague sin que sea necesario que un usuario inicie la sesión. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	Shutdown: Clear virtual memory pagefile. - Determinar si el archivo de paginación de la memoria virtual debe borrarse cuando se apaga el sistema. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	System cryptography: Force strong key protection for user keys stored on the computer. - Política que determina si las claves privadas de los usuarios (como las claves S-MIME) requieran una contraseña para ser usada.
<input type="checkbox"/>	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing. - Política que determina si la capa de transporte de seguridad (TLS/SSL) Proveedor de Seguridad, solo soporta el sistema de cifrado TLS_RSA_WITH_3DES_EDE_CBC_SHA Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	System objects: Default owner for objects created by members of the Administrators group. - Determina si el grupo Administradores o un objeto creador es el propietario por defecto de cualquier sistema de objetos que se crean.
<input type="checkbox"/>	System objects: Require case insensitivity for non-Windows subsystems. - Política que se aplica o impone para todos los subsistemas no Microsoft Win32. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links). - Si se habilita esta directiva, la DACL predeterminada será más segura y permitirá a los usuarios no administrativos leer objetos compartidos, pero no permitirá modificar objetos compartidos que no hayan creado ellos. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
<input type="checkbox"/>	System settings: Optional subsystems. - Determina cuales subsistemas son usados para soporte de aplicaciones en un entorno.
<input type="checkbox"/>	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies. - Política que determina si los certificados digitales se procesan cuando las políticas de restricción de software están activadas y un usuario o proceso intenta ejecutar un archivo de extensión .exe. Configuración del equipo: <input type="checkbox"/> Habilitada <input type="checkbox"/> Deshabilitada
Registros de sucesos	Configuración para registros de sucesos
<input type="checkbox"/>	Maximum application log size. - Especificar el tamaño máximo del registro de sucesos de la aplicación.
<input type="checkbox"/>	Maximum security log size. - Especificar el tamaño máximo del registro de sucesos de seguridad.
<input type="checkbox"/>	Maximum system log size. - Especificar el tamaño máximo del registro de sucesos del sistema.
<input type="checkbox"/>	Prevent local guests group from accessing application log. - Si se habilita, evitar que los usuarios anónimos tengan acceso al registro de sucesos de la aplicación. Esta opción de directiva no está disponible en los sistemas operativos Windows 2000 Professional y Server independientes.
<input type="checkbox"/>	Prevent local guests group from accessing security log. - Si se habilita, evitar que los usuarios anónimos tengan acceso al registro de sucesos de seguridad. Esta opción de directiva no está disponible en los sistemas operativos Windows 2000 Professional y Server independientes.
<input type="checkbox"/>	Prevent local guests group from accessing system log. - Si se habilita, evitar que los usuarios anónimos tengan acceso al registro de sucesos del sistema. Esta opción de directiva no está disponible en los sistemas operativos Windows 2000 Professional y Server independientes.
<input type="checkbox"/>	Retention method for application log. - Determinar el método de "ajuste" del registro de la aplicación.
<input type="checkbox"/>	Retention method for security log. - Determinar el método de "ajuste" del registro de seguridad.
<input type="checkbox"/>	Retention method for system log. - Determinar el método de "ajuste" del registro del sistema.



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo																																							
Servicios del sistema																																							
<input type="checkbox"/>	<p><i>Servicios habilitados</i></p> <p>Presentar sólo aquellos servicios que sean necesarios.</p> <table border="0"> <tr> <td><input type="checkbox"/> Application Experience Lookup Service</td> <td><input type="checkbox"/> Performance Logs and Alerts</td> </tr> <tr> <td><input type="checkbox"/> Automatic Updates</td> <td><input type="checkbox"/> Plug and Play</td> </tr> <tr> <td><input type="checkbox"/> Background Intelligent Transfer Service</td> <td><input type="checkbox"/> Protected Storage</td> </tr> <tr> <td><input type="checkbox"/> COM+ Event System</td> <td><input type="checkbox"/> Remote Administration Service</td> </tr> <tr> <td><input type="checkbox"/> Computer Browser</td> <td><input type="checkbox"/> Remote Procedure Call (RPC)</td> </tr> <tr> <td><input type="checkbox"/> Cryptographic Services</td> <td><input type="checkbox"/> Remote Registry Service</td> </tr> <tr> <td><input type="checkbox"/> DCOM Server Process Launcher</td> <td><input type="checkbox"/> Removable Storage</td> </tr> <tr> <td><input type="checkbox"/> DHCP Client</td> <td><input type="checkbox"/> Security Accounts Manager</td> </tr> <tr> <td><input type="checkbox"/> DNS Client</td> <td><input type="checkbox"/> Server</td> </tr> <tr> <td><input type="checkbox"/> Event Log</td> <td><input type="checkbox"/> System Event Notification</td> </tr> <tr> <td><input type="checkbox"/> IPsec Policy Agent (IPsec Service)</td> <td><input type="checkbox"/> TCP/IP NetBIOS Helper Service</td> </tr> <tr> <td><input type="checkbox"/> Logical Disk Manager</td> <td><input type="checkbox"/> Terminal Services</td> </tr> <tr> <td><input type="checkbox"/> Logical Disk Manager Administrative Service</td> <td><input type="checkbox"/> Volume Shadow Copy</td> </tr> <tr> <td><input type="checkbox"/> Microsoft Software Shadow Copy Provider</td> <td><input type="checkbox"/> Windows Installer</td> </tr> <tr> <td><input type="checkbox"/> Net Logon</td> <td><input type="checkbox"/> Windows Management Instrumentation</td> </tr> <tr> <td><input type="checkbox"/> Network Connections</td> <td><input type="checkbox"/> Windows Management Instrumentation Driver Extensions</td> </tr> <tr> <td><input type="checkbox"/> Network Location Awareness (NLA)</td> <td><input type="checkbox"/> Windows Time</td> </tr> <tr> <td><input type="checkbox"/> Network Provisioning Service</td> <td><input type="checkbox"/> WMI Performance Adapter</td> </tr> <tr> <td><input type="checkbox"/> NT LM Security Support Provider</td> <td><input type="checkbox"/> Workstation</td> </tr> </table>	<input type="checkbox"/> Application Experience Lookup Service	<input type="checkbox"/> Performance Logs and Alerts	<input type="checkbox"/> Automatic Updates	<input type="checkbox"/> Plug and Play	<input type="checkbox"/> Background Intelligent Transfer Service	<input type="checkbox"/> Protected Storage	<input type="checkbox"/> COM+ Event System	<input type="checkbox"/> Remote Administration Service	<input type="checkbox"/> Computer Browser	<input type="checkbox"/> Remote Procedure Call (RPC)	<input type="checkbox"/> Cryptographic Services	<input type="checkbox"/> Remote Registry Service	<input type="checkbox"/> DCOM Server Process Launcher	<input type="checkbox"/> Removable Storage	<input type="checkbox"/> DHCP Client	<input type="checkbox"/> Security Accounts Manager	<input type="checkbox"/> DNS Client	<input type="checkbox"/> Server	<input type="checkbox"/> Event Log	<input type="checkbox"/> System Event Notification	<input type="checkbox"/> IPsec Policy Agent (IPsec Service)	<input type="checkbox"/> TCP/IP NetBIOS Helper Service	<input type="checkbox"/> Logical Disk Manager	<input type="checkbox"/> Terminal Services	<input type="checkbox"/> Logical Disk Manager Administrative Service	<input type="checkbox"/> Volume Shadow Copy	<input type="checkbox"/> Microsoft Software Shadow Copy Provider	<input type="checkbox"/> Windows Installer	<input type="checkbox"/> Net Logon	<input type="checkbox"/> Windows Management Instrumentation	<input type="checkbox"/> Network Connections	<input type="checkbox"/> Windows Management Instrumentation Driver Extensions	<input type="checkbox"/> Network Location Awareness (NLA)	<input type="checkbox"/> Windows Time	<input type="checkbox"/> Network Provisioning Service	<input type="checkbox"/> WMI Performance Adapter	<input type="checkbox"/> NT LM Security Support Provider	<input type="checkbox"/> Workstation
<input type="checkbox"/> Application Experience Lookup Service	<input type="checkbox"/> Performance Logs and Alerts																																						
<input type="checkbox"/> Automatic Updates	<input type="checkbox"/> Plug and Play																																						
<input type="checkbox"/> Background Intelligent Transfer Service	<input type="checkbox"/> Protected Storage																																						
<input type="checkbox"/> COM+ Event System	<input type="checkbox"/> Remote Administration Service																																						
<input type="checkbox"/> Computer Browser	<input type="checkbox"/> Remote Procedure Call (RPC)																																						
<input type="checkbox"/> Cryptographic Services	<input type="checkbox"/> Remote Registry Service																																						
<input type="checkbox"/> DCOM Server Process Launcher	<input type="checkbox"/> Removable Storage																																						
<input type="checkbox"/> DHCP Client	<input type="checkbox"/> Security Accounts Manager																																						
<input type="checkbox"/> DNS Client	<input type="checkbox"/> Server																																						
<input type="checkbox"/> Event Log	<input type="checkbox"/> System Event Notification																																						
<input type="checkbox"/> IPsec Policy Agent (IPsec Service)	<input type="checkbox"/> TCP/IP NetBIOS Helper Service																																						
<input type="checkbox"/> Logical Disk Manager	<input type="checkbox"/> Terminal Services																																						
<input type="checkbox"/> Logical Disk Manager Administrative Service	<input type="checkbox"/> Volume Shadow Copy																																						
<input type="checkbox"/> Microsoft Software Shadow Copy Provider	<input type="checkbox"/> Windows Installer																																						
<input type="checkbox"/> Net Logon	<input type="checkbox"/> Windows Management Instrumentation																																						
<input type="checkbox"/> Network Connections	<input type="checkbox"/> Windows Management Instrumentation Driver Extensions																																						
<input type="checkbox"/> Network Location Awareness (NLA)	<input type="checkbox"/> Windows Time																																						
<input type="checkbox"/> Network Provisioning Service	<input type="checkbox"/> WMI Performance Adapter																																						
<input type="checkbox"/> NT LM Security Support Provider	<input type="checkbox"/> Workstation																																						
<input type="checkbox"/>	<p><i>Servicios deshabilitados</i></p> <p>Se pueden deshabilitar los servicios predeterminados que se enumeran a continuación.</p> <table border="0"> <tr> <td><input type="checkbox"/> Alerter</td> <td><input type="checkbox"/> Print Server for Macintosh</td> </tr> <tr> <td><input type="checkbox"/> Application Layer Gateway Service</td> <td><input type="checkbox"/> Print Spooler</td> </tr> <tr> <td><input type="checkbox"/> Application Management</td> <td><input type="checkbox"/> Remote Access Auto Connection Manager</td> </tr> <tr> <td><input type="checkbox"/> ASP .NET State Service</td> <td><input type="checkbox"/> Remote Access Connection Manager</td> </tr> <tr> <td><input type="checkbox"/> Certificate Services</td> <td><input type="checkbox"/> Remote Desktop Help Session Manager</td> </tr> <tr> <td><input type="checkbox"/> Client Service for NetWare</td> <td><input type="checkbox"/> Remote Installation</td> </tr> <tr> <td><input type="checkbox"/> ClipBook</td> <td><input type="checkbox"/> Remote Procedure Call (RPC) Locator</td> </tr> <tr> <td><input type="checkbox"/> Cluster Service</td> <td><input type="checkbox"/> Remote Server Manager</td> </tr> <tr> <td><input type="checkbox"/> COM+ System Application</td> <td><input type="checkbox"/> Remote Server Monitor</td> </tr> <tr> <td><input type="checkbox"/> DHCP Server</td> <td><input type="checkbox"/> Remote Storage Notification</td> </tr> <tr> <td><input type="checkbox"/> Distributed File System</td> <td><input type="checkbox"/> Remote Storage Server</td> </tr> <tr> <td><input type="checkbox"/> Distributed Link Tracking Client</td> <td><input type="checkbox"/> Resultant Set of Policy Provider</td> </tr> <tr> <td><input type="checkbox"/> Distributed Link Tracking Server</td> <td><input type="checkbox"/> Routing and Remote Access</td> </tr> </table>	<input type="checkbox"/> Alerter	<input type="checkbox"/> Print Server for Macintosh	<input type="checkbox"/> Application Layer Gateway Service	<input type="checkbox"/> Print Spooler	<input type="checkbox"/> Application Management	<input type="checkbox"/> Remote Access Auto Connection Manager	<input type="checkbox"/> ASP .NET State Service	<input type="checkbox"/> Remote Access Connection Manager	<input type="checkbox"/> Certificate Services	<input type="checkbox"/> Remote Desktop Help Session Manager	<input type="checkbox"/> Client Service for NetWare	<input type="checkbox"/> Remote Installation	<input type="checkbox"/> ClipBook	<input type="checkbox"/> Remote Procedure Call (RPC) Locator	<input type="checkbox"/> Cluster Service	<input type="checkbox"/> Remote Server Manager	<input type="checkbox"/> COM+ System Application	<input type="checkbox"/> Remote Server Monitor	<input type="checkbox"/> DHCP Server	<input type="checkbox"/> Remote Storage Notification	<input type="checkbox"/> Distributed File System	<input type="checkbox"/> Remote Storage Server	<input type="checkbox"/> Distributed Link Tracking Client	<input type="checkbox"/> Resultant Set of Policy Provider	<input type="checkbox"/> Distributed Link Tracking Server	<input type="checkbox"/> Routing and Remote Access												
<input type="checkbox"/> Alerter	<input type="checkbox"/> Print Server for Macintosh																																						
<input type="checkbox"/> Application Layer Gateway Service	<input type="checkbox"/> Print Spooler																																						
<input type="checkbox"/> Application Management	<input type="checkbox"/> Remote Access Auto Connection Manager																																						
<input type="checkbox"/> ASP .NET State Service	<input type="checkbox"/> Remote Access Connection Manager																																						
<input type="checkbox"/> Certificate Services	<input type="checkbox"/> Remote Desktop Help Session Manager																																						
<input type="checkbox"/> Client Service for NetWare	<input type="checkbox"/> Remote Installation																																						
<input type="checkbox"/> ClipBook	<input type="checkbox"/> Remote Procedure Call (RPC) Locator																																						
<input type="checkbox"/> Cluster Service	<input type="checkbox"/> Remote Server Manager																																						
<input type="checkbox"/> COM+ System Application	<input type="checkbox"/> Remote Server Monitor																																						
<input type="checkbox"/> DHCP Server	<input type="checkbox"/> Remote Storage Notification																																						
<input type="checkbox"/> Distributed File System	<input type="checkbox"/> Remote Storage Server																																						
<input type="checkbox"/> Distributed Link Tracking Client	<input type="checkbox"/> Resultant Set of Policy Provider																																						
<input type="checkbox"/> Distributed Link Tracking Server	<input type="checkbox"/> Routing and Remote Access																																						



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
<input type="checkbox"/> Distributed Transaction Coordinator <input type="checkbox"/> DNS Server <input type="checkbox"/> Error Reporting Service <input type="checkbox"/> Fax Service <input type="checkbox"/> File Replication <input type="checkbox"/> File Server for Macintosh <input type="checkbox"/> FTP Publishing Service <input type="checkbox"/> Help and Support <input type="checkbox"/> HTTP SSL <input type="checkbox"/> Human Interface Device Access <input type="checkbox"/> IAS Jet Database Access <input type="checkbox"/> IIS Admin Service <input type="checkbox"/> IMAPI CD-Burning COM Service <input type="checkbox"/> Indexing Service <input type="checkbox"/> Infrared Monitor <input type="checkbox"/> Internet Authentication Service <input type="checkbox"/> Intersite Messaging <input type="checkbox"/> IP Version 6 Helper Service <input type="checkbox"/> Kerberos Key Distribution Center <input type="checkbox"/> License Logging Service <input type="checkbox"/> Message Queuing <input type="checkbox"/> Message Queuing Down Level Clients <input type="checkbox"/> Message Queuing Triggers <input type="checkbox"/> Messenger <input type="checkbox"/> Microsoft POP3 Service <input type="checkbox"/> MSSQL\$UDDI <input type="checkbox"/> MSSQLServerADHelper <input type="checkbox"/> .NET Framework Support Service <input type="checkbox"/> NetMeeting Remote Desktop Sharing <input type="checkbox"/> Network DDE <input type="checkbox"/> Network DDE DSDM <input type="checkbox"/> Network News Transfer Protocol (NNTP) <input type="checkbox"/> Portable Media Serial Number Service	<input type="checkbox"/> SAP Agent <input type="checkbox"/> Secondary Logon <input type="checkbox"/> Shell Hardware Detection <input type="checkbox"/> Simple Mail Transport Protocol (SMTP) <input type="checkbox"/> Simple TCP/IP Services <input type="checkbox"/> Single Instance Storage Groveler <input type="checkbox"/> Smart Card <input type="checkbox"/> SNMP Service <input type="checkbox"/> SNMP Trap Service <input type="checkbox"/> Special Administration Console Helper <input type="checkbox"/> SQLAgent\$* (* UDDI or WebDB) <input type="checkbox"/> Task Scheduler <input type="checkbox"/> TCP/IP Print Server <input type="checkbox"/> Telephony <input type="checkbox"/> Telnet <input type="checkbox"/> Terminal Services Licensing <input type="checkbox"/> Terminal Services Session Directory <input type="checkbox"/> Themes <input type="checkbox"/> Trivial FTP Daemon <input type="checkbox"/> Uninterruptible Power Supply <input type="checkbox"/> Upload Manager <input type="checkbox"/> Virtual Disk Service <input type="checkbox"/> WebClient <input type="checkbox"/> Web Element Manager <input type="checkbox"/> Windows Audio <input type="checkbox"/> Windows Firewall/Internet Connection Sharing (ICS) <input type="checkbox"/> Windows Image Acquisition (WIA) <input type="checkbox"/> Windows Internet Name Service (WINS) <input type="checkbox"/> Windows Media Services <input type="checkbox"/> Windows System Resource Manager <input type="checkbox"/> WinHTTP Web Proxy Auto-Discovery Service <input type="checkbox"/> Wireless Configuration <input type="checkbox"/> World Wide Web Publishing Service
Valores de configuración adicionales del registro	
<input type="checkbox"/>	Fortificar la pila de TCP/IP frente a ataques de denegación de servicio HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\ Clave: Parameters Nombre de valor: DisableIPSourceRouting



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
	<p>Nombre de valor: EnableDeadGWDetect Nombre de valor: EnableICMPRedirect Nombre de valor: EnablePMTUDiscovery Nombre de valor: EnableSecurityFilters Nombre de valor: KeepAliveTime Nombre de valor: PerformRouterDiscovery Nombre de valor: SynAttackProtect Nombre de valor: TcpMaxConnectResponseRetransmissions Nombre de valor: TcpMaxConnectRetransmissions Nombre de valor: TcpMaxDataRetransmissions Nombre de valor: TCPMaxPortsExhausted</p>
<input type="checkbox"/>	<p><i>Configuración de intentos de conexión a las aplicaciones de Windows Sockets</i></p> <p>HKLM\System\CurrentControlSet\Services\AFD\</p> <p>Clave: Parameters Nombre de valor: DynamicBacklogGrowthDelta Nombre de valor: EnableDynamicBacklog Nombre de valor: MinimumDynamicBacklog Nombre de valor: MaximumDynamicBacklog</p>
<input type="checkbox"/>	<p>Otras entradas que se deben configurar en el registro del sistema</p> <p>HKLM\Software\Microsoft\Windows NT\CurrentVersion\ <i>Habilitar inicio de sesión automático (no recomendado)</i> Clave: Winlogon Nombre de valor: AutoAdminLogon</p> <p>HKLM\System\CurrentControlSet\Control\ <i>Permitir que Windows se reinicie automáticamente después de una caída del sistema</i> Clave: CrashControl Nombre de valor: AutoReboot</p> <p>HKLM\System\CurrentControlSet\Services\RasMan\ <i>Habilita acciones administrativas (recomendado a excepción de los entornos de alta seguridad)</i> Clave: Parameters Nombre de valor: AutoShareWks</p> <p>HKLM\System\CurrentControlSet\Services\LanmanServer\ <i>Prevenir el guardado de contraseña por dial-up (recomendado)</i> Clave: Parameters Nombre de valor: DisableSavePassword</p> <p>HKLM\System\CurrentControlSet\Services\ <i>Ocultar la computadora de listas de buscadores de redes vecinas</i> Clave: LanmanServer Nombre de valor: Hidden</p> <p>HKLM\System\CurrentControlSet\Services\ <i>Quitar las excepciones de IPSEC predeterminadas: evitar que un atacante eluda las directivas de IPsec atacando en el puerto de origen</i> Clave: IPSEC Nombre de valor: NoDefaultExempt</p>



Tabla 2.21. Configuraciones de Seguridad en Windows Server 2003 (... continuación)

Configuración del Sistema Operativo	
HKLM\System\CurrentControlSet\Control\ Clave: FileSystem Nombre de valor: NtfsDisable8dot3NameCreation	<i>Activar la PC para detener la generación de nombres de archivo de estilo 8.3</i>
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ Clave: Explorer Nombre de valor: NoDriveTypeAutoRun	<i>Deshabilitar ejecución automática:</i>
HKLM\System\CurrentControlSet\Services\NetBT\ Clave: Parameters Nombre de valor: NoNameReleaseOnDemand	<i>Permite a la PC ignorar las solicitudes de liberación de nombres NetBIOS excepto de los servidores WINS</i>
HKLM\SYSTEM\CurrentControlSet\Control\ Clave: Session Manager Nombre de valor: SafeDllSearchMode	<i>Cambiar el orden de búsqueda de DDL: Evitar la falsificación de DDL del sistema.</i>
HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Clave: Winlogon Nombre de valor: ScreenSaverGracePeriod	<i>El tiempo en segundos antes de que expire el periodo de gracia del protector de pantalla</i>
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\ Clave: Security Nombre de valor: WarningLevel	<i>Generar un suceso de auditoría cuando el registro de auditorías se llene hasta alcanzar un umbral en porcentaje</i>



2.6 PUNTUALIZACIONES

- ✓ Identificar las vulnerabilidades críticas en un sistema operativo Windows de servidor permite instalar y configurar parches y más herramientas complementarias al sistema con la finalidad de dar seguridad al servidor y con ello mantener la consistencia de la información que maneja.
- ✓ Un servidor que haya solucionado el problema de vulnerabilidades, no sufrirá ataques de personas que quieran dañar la información almacenada en él.
- ✓ Configurar de una manera adecuada las directivas de seguridad tanto en un servidor miembro de un dominio como en un servidor controlador de dominio, permite evitar ataques de usuarios internos a una empresa como los usuarios externos a la misma.
- ✓ Fortalecer y configurar de una manera adecuada la pila de protocolos TCP/IP evitan que un servidor que está expuesto o en conexión directa a internet sufra ataques como la denegación de servicio, virus, troyanos, etc.
- ✓ Contar con una manera adecuada de manejar las actualizaciones en un servidor, es una forma de mantener al servidor en un estado confiable y libre de muchos ataques provenientes de la red.

CAPITULO III
IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

Objetivos

- Implementar el esquema de seguridad para los servidores que operan con las plataformas Windows Server 2003
- Evaluar resultados generados de la implementación del esquema de seguridad para los servidores del GDS
- Establecer procesos a seguir cuando se configura seguridad en un servidor Windows



3.1 INTRODUCCIÓN

En una implementación de un esquema de seguridad se deben tener claros los conceptos o procesos que están relacionados y orientados a dar una seguridad a toda la organización, de tal manera que guíen en la implementación del esquema de manera integral, por tanto, un esquema de seguridad comprende la seguridad física, seguridad lógica, medidas o planes de contingencia en caso de ocurrir desastres, etc.

En el presente capítulo se detalla cómo se debe realizar una implementación de un esquema de seguridad a nivel lógico para Windows Server 2003, plataforma en la cual se encuentran corriendo servicios críticos de la UTPL, como son; Sistema de Gestión Académica, Sistema de Digitalización, entre otros. Entonces, es necesario crear y mantener un ambiente de trabajo seguro, que garantice y respalde la consistencia de la información que se maneja.

3.2 DESCRIPCIONES GENERALES QUE COMPRENDE UN ESQUEMA DE SEGURIDAD

La implementación de un esquema de seguridad es una tarea muy subjetiva, debido a que existen muchas formas o maneras para evaluar las necesidades de una organización, por lo que las soluciones de seguridad son variadas y están en función de las políticas de la organización, objetivos que persigue, servicios que presta entre otros.

3.2.1 Consideraciones previas

De manera concreta y específica, antes de realizar una implementación de un esquema de seguridad sobre una red ya constituida, se debe tener presente algunas pautas, es por ello que para el caso de la elaboración de un esquema de seguridad, se debe considerar el **diseño o distribución de los servidores Windows en la red de la organización**, luego se debe proceder a la **implementación del esquema de seguridad**, que involucra todas las configuraciones para el fortalecimiento de los servidores y finalmente se debe considerar la **administración y desempeño**, es decir que el reforzamiento a la seguridad no limite las funcionalidades de los servidores.

3.2.2 Proceso sugerido de implementación

Hablar de un proceso formal o metodología patentada que exista para realizar configuraciones de seguridad en plataforma Windows pues no existe, por ello se debe proponer procesos que sean útiles en el desarrollo de una **implementación de un Esquema de Seguridad** dentro de una organización. Para llevar a cabo una implementación que vaya acorde a las necesidades de **aseguramiento de la información** de cada empresa en particular, se propone basarse en tres conceptos básicos como son el **Conocimiento Organizacional, Diseño, Implementación y finalmente Aplicación de configuraciones**. A continuación en la gráfica se visualiza todo el proceso sugerido.

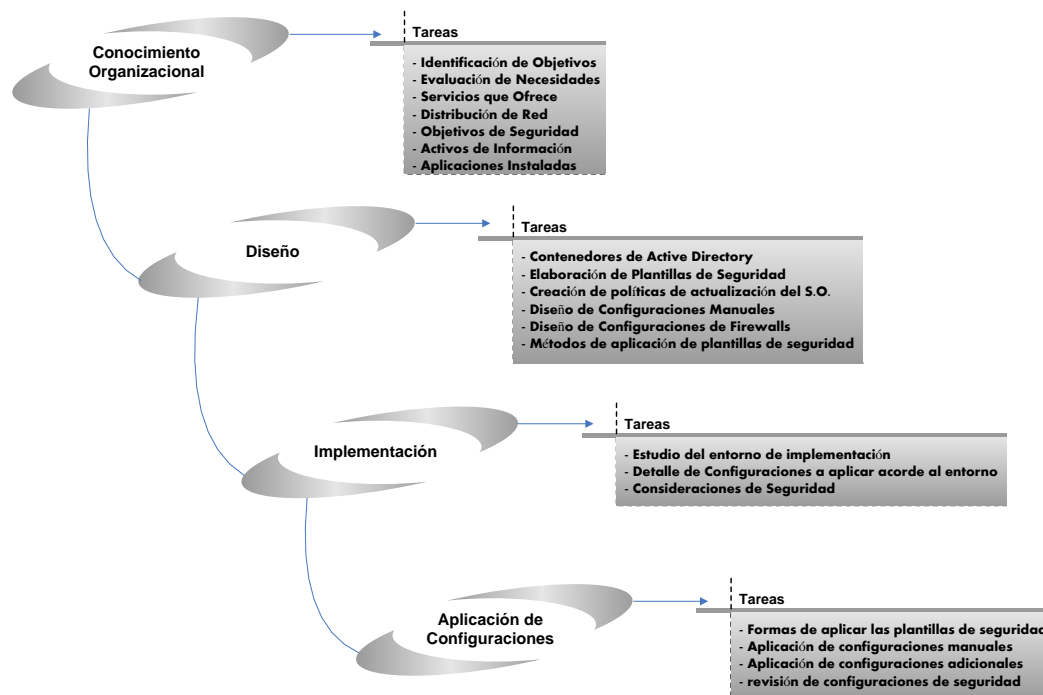


Figura 3.1. Modelo de creación de un Esquema de Seguridad

Conocimiento Organizacional

El conocimiento organizacional engloba la identificación de objetivos de la organización, tipo de organización, evaluación de las necesidades de la organización, servicios que se ofrecen, activos de almacenamiento y administración de información con los que cuenta (servidores, plataformas y hardware), distribución de la red, objetivos de seguridad que se persigue, aplicaciones más críticas, puertos que deberían estar habilitados en los servidores.

Diseño de la Solución

Diseñar la solución de seguridad comprende detallar que servidores van a contener Active Directory, cuales servidores harán de controladores de dominio, elaboración de propuestas de plantillas de seguridad, creación de políticas de actualización del sistema operativo, políticas de administración de cuentas (administradores, usuarios avanzados, usuarios normales, usuarios invitados, etc.), procesos manuales a seguir para configurar seguridades en cada equipo servidor, configuración de firewalls a nivel perimetral que de seguridad al dominio y a nivel local en cada equipo, métodos de aplicación de plantillas de seguridad, roles de los servidores y aplicaciones de acuerdo a su criticidad.

Implementación

La implementación es la materialización de lo mencionado en el diseño de la solución, se hace un estudio del entorno de implementación y en base a eso se elabora plantillas, configuraciones o consideraciones de seguridad apegadas a la realidad organizacional, se puede decir que se elige el mejor proceso de implementación que de la seguridad a los equipos que abarca un Esquema de



Seguridad. En esta etapa se puede utilizar entornos de pruebas (virtuales o bien físicos que sean netamente para pruebas) para las configuraciones que luego serán aplicadas en entornos físicos reales, esto con la finalidad de minimizar errores de funcionalidades en equipos en producción.

Aplicación de Configuraciones

Es la aplicación o instalación ya a nivel de producción, de todas las configuraciones de seguridad elaboradas en la implementación, se hace todo de manera uniforme en todos los equipos servidores que forman parte de un dominio dentro de una organización. Se deja todo listo para empezar a verificar el funcionamiento de todos los procesos, políticas y demás consideraciones de seguridad que se hayan investigado y elaborado, con lo que se puede evaluar que las configuraciones de seguridad son las adecuadas y no afectan el rol que desempeña cada equipo dentro de la organización.

3.2.3 Medidas de seguridad para servidores Windows

Tabla 3.1. Medidas de seguridad Windows

Medida	Descripción	Herramientas	Proceso o Política
Deshabilitar las cuentas de usuario invitado (guest)	Por lo general en la plataforma Windows Server 2003, éstas cuentas están deshabilitadas por defecto, pero se debe cerciorar que en verdad están deshabilitadas.	Para monitoreo: MBSA	PR08
Siempre limitar el número de cuentas de usuario en el servidor	Cuentas innecesarias o en exceso comprometen la seguridad de un servidor Windows y son lo que primero busca un hacker para hacer un ataque. En el caso en concreto para el GDS, se recomienda eliminar usuarios innecesarios, cuentas genéricas o duplicadas. El número de cuentas que se cree en cada servidor es independiente, se deja a criterio del administrador de los servidores y a las necesidades que se tengan.	Para monitoreo: limitlogin.exe	PR09
Limitar y monitorear accesos con la cuenta administrador	Evitar utilizar siempre la cuenta con todos los privilegios como lo es administrador para tareas cotidianas, ésta cuenta debe de tener una configuración rigurosa en cuanto a políticas de contraseñas y auditoría que permita saber quien ha hecho uso de la misma y en qué momento.	Para monitoreo: MMC, MBSA	PL02, PL03
Renombrar y crear una cuenta "tonta" de administrador	Si se renombra la cuenta de administrador se dificulta el ataque de los hackers y si se crea una cuenta "tonta" sin privilegios y con una fuerte contraseña de administrador, se desvía la atención de los atacantes que tratan de acceder a un servidor.	Para monitoreo: MBSA, Computer Management	PR10
Prestar atención a los permisos por omisión para usuarios	Tener configurado de una buena manera los permisos por omisión en un servidor evita pérdida o manipulación de información por parte de terceras partes. Los permisos por omisión dan ingreso a usuarios a carpetas compartidas.	Para monitoreo: MBSA	PR11
Formatear los discos duros de servidor con el sistema de archivos NTFS	Este sistema de archivos posee altos niveles de seguridad.	Para monitoreo: MBSA	
Aplicar políticas de seguridad a nivel de dominio donde están los servidores, en cada servidor y configurar firewalls por cada servidor	Para configurar las seguridades de un servidor Windows se debe emplear las mismas herramientas que trae incorporado el sistema operativo y así evitar la utilización de herramientas de terceros.	Para monitoreo: MMC, SCW, GPMC, AD	PL04, PL05
Deshabilitar o bajar los servicios innecesarios que se están ejecutando en el servidor	Por lo general cuando se instala el sistema operativo por primera vez se instalan por defecto algunos servicios que posteriormente no son necesarios, por lo que constituyen una vulnerabilidad para la integridad del servidor por lo que se los debe deshabilitar.	Para monitoreo: net start	



Tabla 3.1. Medidas de seguridad Windows (... continuación)

Medida	Descripción	Herramientas	Proceso o Política
Cerrar acceso a puertos abiertos que no son utilizados	Evita la mayoría de ataques, ya que son una de las mayores vulnerabilidades tener habilitados puertos innecesarios y que más bien son una invitación y es lo que primero un atacante busca para ingresar a un servidor.	Para monitoreo: netstat -noa	PR12
Habilitar siempre la auditoría de eventos en el servidor	Es una forma de precautelar la seguridad del sistema operativo, pues con la auditoría se puede dar seguimiento a cambios en políticas de seguridad, accesos no autorizados, intentos de modificación de archivos, cambio de privilegios de un usuario en particular, etc., por todo esto es muy importante que se auditen eventos exitosos como fallidos del sistema.	Para monitoreo: Computer Management	
Asegurar o proteger los archivos del registro de eventos	Tienen una gran importancia, se debe dar permisos de lectura y escritura a administradores y usuarios del sistema, esto debido a que por defecto estos archivos no están protegidos y en caso de que un atacante ingrese al sistema del servidor, puede dejarlos borrando si no se aplica políticas de protección.		
Desactivar la opción del último usuario logeado,	Esto evita que cuando otro usuario o administrador vaya a iniciar sesión y presione Ctrl-Alt-Del aparezca el nombre del login del último usuario que ingreso al sistema, esto puede ser utilizado por un atacante para adivinar o crackear la clave de un administrador o usuario en concreto.		PR13
Instalar parches de seguridad que Microsoft libera cada mes	Es muy importante tener un sistema operativo actualizado, con ello se logra no ser víctima por ataques conocidos o ya reparados.	Para monitoreo: Propiedades del sistema	PR14
Deshabilitar carpetas compartidas que son innecesarias	Tener carpetas compartidas por omisión o de manera innecesaria, pone al sistema en un grado de riesgo, debido a que un hacker al tener acceso a una carpeta compartida puede utilizarla para almacenar algún programa malicioso que le permita controlar el sistema del servidor.	Para monitoreo: Command Prompt, digitar el comando net share	PR15
Deshabilitar la opción de creación de archivo dump	Este archivo revela información sensible del sistema como las causas de las populares pantallas azules, así como también información de contraseñas, esta opción suele ser de mucha utilidad cuando se dan fallas en el servidor, pero para ello se la puede habilitar y luego de su uso volver a deshabilitarla sin olvidarse de borrar los archivos que haya generado.		PR16

Las medidas de seguridad aplicables a los servidores Windows, están relacionadas con las necesidades y aplicaciones que cada servidor alberga y presta servicios. Partiendo de estas consideraciones, se realizan plantillas de seguridad personalizadas que están elaboradas según el rol que desempeña cada servidor dentro de un entorno.

Definición de Plantilla de seguridad.- “Una plantilla de seguridad es una colección de valores configurados de seguridad. Las plantillas de seguridad son útiles para elaborar y hacer cumplir las necesidades de seguridad de diferentes Unidades Organizativas dentro de una empresa. Luego de ser elaborada una plantilla de seguridad se la puede usar para configurar la seguridad de un equipo individual o miles de ellos.” [Juansa, 2006]

Una plantilla de seguridad no es más que un archivo, que se guarda con extensión .inf y pueden ser creadas utilizando la Consola de Administración Microsoft (MMC) que es parte del sistema operativo Windows Server 2003.



3.2.4 Consideraciones de seguridad referentes al Sistema Operativo

Las consideraciones realizadas al sistema operativo en la implementación de un esquema de seguridad empieza desde la instalación del sistema operativo en sí, en el caso de los servidores Windows, que es sobre los cuales se implementa el esquema de seguridad y como tales servidores trabajan con la plataforma Windows Server 2003, se debe planificar la seguridad partiendo desde los siguientes conceptos:

- ✓ Proceso Pre-instalación
- ✓ Proceso de instalación
- ✓ Proceso Post-instalación

Proceso Pre-instalación.- En este proceso se obtiene información referente al hardware del equipo donde se va a instalar el sistema operativo, se proporciona un checklist que se emplea para detallar información relacionada con el Hardware de los servidores, consultar **Plantilla 3.1**.

También hay que recalcar que los requerimientos del proceso de pre-instalación dependen en gran medida de la versión del sistema operativo y del número de servicios a instalar en cada servidor.

Proceso de Instalación.- El proceso de instalación de un sistema operativo que es previo a la implementación de un esquema de seguridad, se lo debe de realizar de manera limpia, es decir desde cero, para luego en procesos posteriores empezar con el procedimiento de aseguramiento del sistema y servicios que va a prestar el servidor, el cual debe contemplar las siguientes tareas:

- ✓ Saber cuál es la función del servidor al que se le está instalando el sistema operativo
- ✓ Conocer las configuraciones de Hardware necesarias para instalar el sistema Windows
- ✓ Si el equipo pertenece a un red, se debe chequear las configuraciones de red
- ✓ Chequear los tamaños de las particiones antes de instalar el sistema operativo
- ✓ Contar con documentos de ayuda en caso de que ocurran errores inesperados durante la instalación del sistema operativo

Proceso Post-instalación.- El proceso de post-instalación se da luego de haber instalado el sistema operativo, este proceso engloba algunas actividades las cuales deben cumplirse en un servidor Windows, éstas son:

- ✓ Comprobar que el sistema operativo inicia normalmente, sin errores
- ✓ Comprobar que los servicios requeridos se han instalado
- ✓ Comprobar que el sistema de archivos es consistente
- ✓ Comprobar la existencia de archivos de configuración
- ✓ Comprobar la conectividad de la red
- ✓ Empezar a aplicar las políticas de seguridad acorde a cada servidor e instalar servicios necesarios como adicionales que den una alta seguridad para el servidor Windows
- ✓ Se crean las cuentas de usuario en el servidor para usar el proceso de inicio de sesión
- ✓ Se inicializan los servicios con todas las configuraciones en el server
- ✓ Se realizan estrategias de backup de las configuraciones de seguridad realizadas



Una vez que se ha cumplido con los procesos de Pre-instalación, Instalación y Post-instalación, se procede a asegurar basándose en políticas bien sean empresariales, de grupo de usuarios, clientes, socios, etc., a los cuales cada servidor va a brindar servicios de manera confiable, no permitiendo así el robo de información por intrusos o hackers que intenten apoderarse de los activos de información.

Un **Esquema de Seguridad** de servidores Windows involucra una alta seguridad para todos los servidores, es por eso que se define plantillas de seguridad personalizadas que estén acorde a la función que desempeñan los servidores miembros de un dominio, luego se elaboran otras plantilla de seguridad específicamente para servidores que se configuran como controladores de dominio (PDC ó BDC), además en cada servidor se configura un firewall que cumple políticas específicas de funcionalidad del servidor donde se configura.

Las plantillas de seguridad tanto para los servidores que hacen de controladores de dominio como para los servidores miembros de un dominio en particular, cumplen con políticas específicas y necesarias de seguridad, por ello se definen en la tabla siguiente las políticas que incorpora una plantilla de seguridad de manera estándar.

Tabla 3.2. Configuraciones de seguridad

Fuente: <http://www.microsoft.com/spain/technet/recursos/articulos/secmod48.msp>

DIRECTIVAS DE SEGURIDAD	
Nombre de directiva	Subdirectivas incluidas
Directivas de cuentas	Directivas de contraseñas Directivas de bloqueo de cuentas
Directivas Locales	Directivas de auditoría Asignación de derechos de usuario Opciones de seguridad
Registro de sucesos	Configuración del registro de sucesos de aplicación, sistema y seguridad
Grupos restringidos	Pertenencia a grupos importantes para la seguridad
Configuración de seguridad de servicios del sistema	Inicio y permisos de los servicios del sistema
Configuración de seguridad del registro	Permisos para las claves del registro del sistema
Configuración de seguridad del sistema de archivos	Permisos de archivos y carpetas

Un ambiente de seguridad para servidores Windows, demanda empezar creando la(s) plantilla(s) de seguridad para luego aplicarlas a cada servidor, el proceso de creación se lo describe y se lo puede consultar en **PR17**.

Cuando ya se ha creado la plantilla de seguridad, por lo general las políticas que encierra la plantilla, inicialmente se crean con valores por defecto, es decir sin especificación de ningún tipo de seguridad, en el caso de la personalización de la plantilla de seguridad para los servidores Windows de una organización en particular, se deben empezar las configuraciones de cada una de las directivas acorde al nivel de seguridad que se desee implementar para los servidores.



3.2.5 Conceptos a considerar en la elaboración de un esquema de seguridad

En la elaboración de un Esquema de Seguridad para sistemas operativos de diversa índole, se deben analizar y considerar muchos conceptos concernientes a todo lo relacionado con la seguridad, por lo que no es una excepción para entornos integrados por plataformas Windows Server, por tal motivo en los párrafos seguidos se describen algunas consideraciones útiles en la elaboración de Esquemas de Seguridad para plataformas Windows.

Modelo de seguridad Windows Server

Analizando la plataforma Windows Server 2003, se tiene que ofrece un sólido conjunto de tres características de seguridad sobre las que basa su seguridad. Estas características son la **autenticación**, el **control de acceso** y el **inicio de sesión único**.

La **autenticación** permite al sistema validar la identidad de un usuario cuando inicia sesión, con lo que determina los permisos que el usuario tendrá sobre el sistema. En el ámbito de sistemas operativos Windows existen **permisos o privilegios por omisión**, que es una manera en que un **usuario cualquiera** tiene acceso a todos los datos de la red, lo que no es conveniente y se tiene que cuidar de este tipo de permisos mediante una correcta autenticación y otorgamiento de permisos al usuario. Para evitar este tipo de inconvenientes la autenticación demanda el uso de fuertes políticas de contraseñas (**ver PL02**), y de correctas políticas de bloqueo de cuentas de usuario (**ver PL06**).

El **control de acceso**, es una manera de otorgar derechos a usuarios, grupos de usuarios, equipos de red, etc., que operan dentro de un dominio en particular. Así se puede proteger uno o varios equipos y con ello limitar a usuarios o grupos a realizar solo las tareas permitidas sobre un objeto en particular. Algunas políticas que se deben tener presentes en el control de acceso se describen en **PL07**.

El **inicio de sesión único**, es una forma de mejorar el inicio de sesión en un dominio y que es parte de los sistemas operativos Windows Server, el inicio de sesión único, usa una sola contraseña y luego de haber ingresado se puede autenticar en cualquier equipo del dominio de Windows sin necesidad de volver a escribir la contraseña. Esto reduce la confusión del usuario y mejora la eficiencia laboral, además reduce la cantidad de soporte administrativo, debido a que el administrador solo debe administrar una cuenta por usuario.

Configuración de un Controlador de Dominio Primario (PDC)

Un **Controlador de Dominio** es de mucha importancia, se puede decir que un dominio Windows no puede existir sin estar presente un PDC, por lo que la importancia del PDC es crucial, típicamente un dominio demanda algunos backups, estos suelen llamarse Controladores de Dominio de Backup, los cuales automáticamente se sincronizan con el PDC. Además, los controladores de dominio utilizan **Active Directory** para las tareas administrativas conjuntas de usuarios y servidores, lo que permite brindar una mayor seguridad al grupo de servidores debido al manejo de políticas de seguridad



basadas en roles que se pueden lograr y aplicar gracias al uso de Active Directory, en el **ANEXO 3.1** se explica todo lo relacionado con la configuración de Active Directory en un entorno en particular.

Servicios que se instalan por defecto y que no son necesarios

Existen algunos servicios en Windows Server 2003 que se instalan de manera predeterminada y que muchos de los cuales no son utilizados y que más bien se constituyen en puntos vulnerables para el sistema en general, por lo que se recomienda deshabilitarlos, en la siguiente tabla se detallan los servicios que se instalan por defecto, de los cuales solo son utilizados muy pocos por lo que los restantes se los debe de deshabilitar.

Tabla 3.3. Servicios que se instalan por defecto en Windows Server 2003

Nombre del servicio	Configuración
Alerter	Deshabilitado
Application Layer Gateway Service	Deshabilitado
Application Management	Deshabilitado
Automatic Updates	Habilitado
Background Intelligent Transfer Service	Manual
ClipBook	Deshabilitado
COM+ Event System	Manual
COM+ System Application	Deshabilitado
Computer Browser	Habilitado
Cryptographic Services	Habilitado
DHCP Client	Habilitado
Distributed File System	Deshabilitado
Distributed Link Tracking Client	Deshabilitado
Distributed Link Tracking Server	Deshabilitado
Distributed Transaction Coordinator	Deshabilitado
DNS Client	Habilitado
Error Reporting Service	Deshabilitado
Event Log	Habilitado
File Replication	Deshabilitado
Help and Support	Deshabilitado
HTTP SSL	Deshabilitado
Human Interface Device Access	Deshabilitado
IMAPI CD-Burning COM Service	Deshabilitado
Indexing Service	Deshabilitado
Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Habilitado
Intersite Messaging	Deshabilitado
IPSEC Services	Habilitado
Kerberos Key Distribution Center	Deshabilitado
License Logging	Deshabilitado
Logical Disk Manager	Manual
Logical Disk Manager Administrative Service	Manual



Tabla 3.3. Servicios que se instalan por defecto en Windows Server 2003 (... continuación)

Nombre del servicio	Configuración
Messenger	Deshabilitado
Microsoft Software Shadow Copy Provider	Manual
Net Logon	Habilitado
NetMeeting Remote Desktop Sharing	Deshabilitado
Network Connections	Manual
Network DDE	Deshabilitado
Network DDE DSDM	Deshabilitado
Network Location Awareness (NLA)	Manual
NT LM Security Support Provider	Habilitado
Performance Logs and Alerts	Manual
Plug and Play	Habilitado
Portable Media Serial Number Service	Deshabilitado
Print Spooler	Deshabilitado
Protected Storage	Habilitado
Remote Access Auto Connection Manager	Deshabilitado
Remote Access Connection Manager	Deshabilitado
Remote Desktop Help Session Manager	Deshabilitado
Remote Procedure Call (RPC)	Habilitado
Remote Procedure Call (RPC) Locator	Deshabilitado
Remote Registry	Habilitado
Removable Storage	Manual
Resultant Set of Policy Provider	Deshabilitado
Routing and Remote Access	Deshabilitado
Secondary Logon	Deshabilitado
Security Accounts Manager	Habilitado
Server	Habilitado
Shell Hardware Detection	Deshabilitado
Smart Card	Deshabilitado
Special Administration Console Helper	Deshabilitado
System Event Notification	Habilitado
Task Scheduler	Deshabilitado
TCP/IP NetBIOS Helper	Habilitado
Telephony	Deshabilitado
Telnet	Deshabilitado
Terminal Services	Habilitado
Terminal Services Session Directory	Deshabilitado
Themes	Deshabilitado
Uninterruptible Power Supply	Deshabilitado
Upload Manager	Deshabilitado
Virtual Disk Service	Deshabilitado
Volume Shadow Copy	Manual
WebClient	Deshabilitado
Windows Audio	Deshabilitado

**Tabla 3.3.** Servicios que se instalan por defecto en Windows Server 2003 (... continuación)

Nombre del servicio	Configuración
Windows Image Acquisition (WIA)	Deshabilitado
Windows Installer	Habilitado
Windows Management Instrumentation	Habilitado
Windows Management Instrumentation Driver Extensions	Manual
Windows Time	Habilitado
WinHTTP Web Proxy Auto-Discovery Service	Deshabilitado
Wireless Configuration	Deshabilitado
WMI Performance Adapter	Manual
Workstation	Habilitado

Aspectos a auditar en un servidor Windows Server 2003

En servidores Windows lo que más se debe auditar está en función del rol que desempeña el servidor en si dentro del dominio. Generalizando se tiene que a nivel de sistema operativo lo que se debe auditar tanto de manera satisfactoria como fallida son los **eventos de inicios de sesión de cuenta, administración de cuentas, inicios de sesión y eventos del sistema**, también se auditan aplicaciones que manejen datos críticos para la organización, pero esto está en función las políticas que plantee la organización así como del administrador de los servidores.

Aspectos generales de la creación de una línea base de Seguridad en Windows Server 2003

La configuración de una línea de base de servidores miembros de un dominio, asegura un mismo nivel de seguridad para todo un conjunto de servidores que pertenecen a un dominio en particular. Una línea base enmarca varios aspectos, tales como:

- ✓ Configuración de servicios
- ✓ Configurar puertos
- ✓ Configurar aplicaciones aprobadas por el firewall de Windows
- ✓ Configuración del registro del sistema
- ✓ Configuración de IIS
- ✓ Permite la inclusión de plantillas de seguridad previamente elaboradas

Así la línea de base tiene como objetivo reducir la superficie de ataque a un servidor Windows que esté operando con Windows Server 2003, la creación de línea de base se la realiza con el **Asiste para Configuración de Seguridad (SCW)** que es parte del propio sistema Windows Server 2003.

Configuración de Firewalls en un Servidor Windows 2003

Un firewall se encarga de reforzar las políticas de control de acceso entre dos o más redes que mantienen un intercambio de información de manera constante. En un **Esquema de Seguridad**, es de mucha importancia la configuración de un firewall a nivel de cada equipo, aparte del que se debe configurar a nivel perimetral que permite solo conexiones necesarias tanto de ingreso como de



salida. Sin un firewall individual en cada servidor, se ve comprometida la seguridad e integridad de los demás servidores que forman parte de un dominio o una intranet.

Para configurar un firewall en un servidor Windows Server 2003, se debe considerar lo siguiente:

- ✓ Programas y servicios que se van a permitir
- ✓ Protocolos permitidos
- ✓ Puertos a los que se les permite un tráfico libre

Considerando lo mencionado, se procede a configurar servidor por servidor el firewall.

Evaluación de Resultados obtenidos de un Esquema de Seguridad

Los resultados obtenidos de la **implementación de un Esquema de Seguridad** deben ofrecer un nivel de seguridad aceptable, sin disminuir la funcionalidad operacional de los equipos que están inmiscuidos en el esquema de seguridad. A partir de la seguridad que brinde inicialmente un esquema de seguridad, se continúa un proceso de mantenimiento y mejora de las seguridades tanto a nivel de dominio, a nivel de servidores controladores de dominio, a nivel individual en cada servidor miembro, a nivel de host, etc., lo que permitirá cumplir con un ciclo evolutivo de gestión de seguridades.

3.3 DISEÑO DEL ESQUEMA DE SEGURIDAD

3.3.1 Diseño de la Seguridad de los Servidores Windows

El diseño de la seguridad para los servidores Windows a nivel lógico del GDS y que están operando tanto a nivel interno, así como también brindan servicios a nivel externo (internet) necesitan basarse de forma concreta en los siguientes conceptos de seguridad:

- ✓ Aseguramiento del sistema operativo
- ✓ Seguridad a nivel de red
- ✓ Autenticación
- ✓ Autorización

Asegurar el sistema operativo es el primer objetivo que se ha procedido a configurar y es la primera tarea que se lleva a cabo en la elaboración del esquema de seguridad para los servidores Windows.

El proceso de **aseguramiento del sistema operativo** Windows Server 2003 Enterprise Edition, facilita la utilización de técnicas de seguridad aplicables conforme a la funcionalidad de cada servidor, de esta forma se ha configurado plantillas de seguridad de manera estándar en lo referente a directivas de contraseñas, de dominio y de auditoría, las cuales se pueden aplicar a todos los servidores Windows miembros de un dominio ya que son configuraciones de seguridad comunes dentro de un mismo entorno de seguridad.

La configuración de un servidor Windows que está interactuando de manera directa o indirecta con el internet, **debe tener un alto nivel de seguridad**, debido a que permanece expuesto a cualquier ataque proveniente del exterior como del propio interior de la organización, por tal motivo se debe



realizar una configuración de seguridad avanzada que garantice la integridad de la información que maneja, es por ello que se debe seguir el siguiente orden cronológico de aseguramiento de los servidores Windows:

- ✓ Luego de instalado el sistema operativo **Microsoft Windows Server 2003 Enterprise Edition** por primera vez, se instala: El Release 2 de Windows Server 2003, Windows Defender para que proteja al servidor de spyware y software mal intencionado, y Microsoft Baseline Security Analyzer (MBSA) que es una herramienta que ayuda a verificar la configuración de seguridad de sistemas Windows, por lo que es de mucha utilidad en el aseguramiento de los servidores, también se instalan parches adicionales o aplicaciones de seguridad que permiten mantener el sistema operativo del servidor más seguro y actualizado.
- ✓ Después de haber actualizado el sistema, se empieza a configurar las directivas de seguridad concernientes a cuentas, directivas locales, que permiten la **autenticación y autorización** a usuarios del sistema operativo conforme a sus necesidades, luego se configuran las directivas de registro de sucesos, grupos restringidos, servicios del sistema y sistema de archivos acorde a la funcionalidad que brinda cada servidor dentro de la LAN interna, así como también de aquellos servidores que están en conexión directa a internet brindando sus servicios. Todo el proceso de configuración se detalla en el **ANEXO 3.2**.
- ✓ Los servidores Windows por estar en comunicación directa con la Web, deben asegurar muy bien la pila e implementación TCP/IP (**Ver PR01, PR02, PR03**), pues esto brinda una buena **seguridad a nivel de red**.
- ✓ Una forma de brindar **seguridad a nivel de red** más restrictiva es configurando políticas de seguridad a nivel firewall, con las políticas de firewall se limita de una mejor manera los ingresos indeseados de personas no autorizadas al servidor.

Empezando con la descripción del diseño de la implementación del esquema de seguridad para los servidores Windows de la UTPL, se debe empezar citando que tales servidores son utilizados por el **Grupo de Desarrollo de Software (GDS)** para la realización de software, los servidores en mención están en la actualidad alojando al **Sistema de Gestión Académica (SGA)** y sus diferentes servicios (matrícula en línea, ingreso de notas por parte del profesor, consulta desde los centros universitarios a nivel nacional, etc.), el SGA es uno de los servicios informáticos más críticos de la UTPL, por ésta razón el grupo de servidores se ha dividido en **entorno de Producción, entorno de Desarrollo y entorno de Pruebas**, pues en estos entornos es necesario configurar políticas de seguridad que garanticen la seguridad de la información que manejan.

Para dar seguridad a los servidores Windows se ha planificado configurar el **Esquema de Seguridad** que brinde la mejor seguridad posible a éstos, para ello se ha diseñado un esquema donde exista un servidor que actúe como controlador de dominio primario (PDC) y uno de Backup (BDC), que es desde donde se va a administrar a los demás servidores que en este caso pasan a ser servidores

miembros del dominio **utpl.edu.ec**, vale indicar que todos los servidores Windows están operando bajo éste mismo dominio, aunque los servidores hayan sido ubicados en diferentes **VLAN's** que solo es una forma utilizada para mejorar la seguridad de éstos. Todo la conversión de un servidor miembro a Controlador de Dominio sea Primario o de Respaldo se ha descrito en el **ANEXO 3.3**. A continuación el grafico muestra la manera de operar de un PDC con su servidor de respaldo BDC.

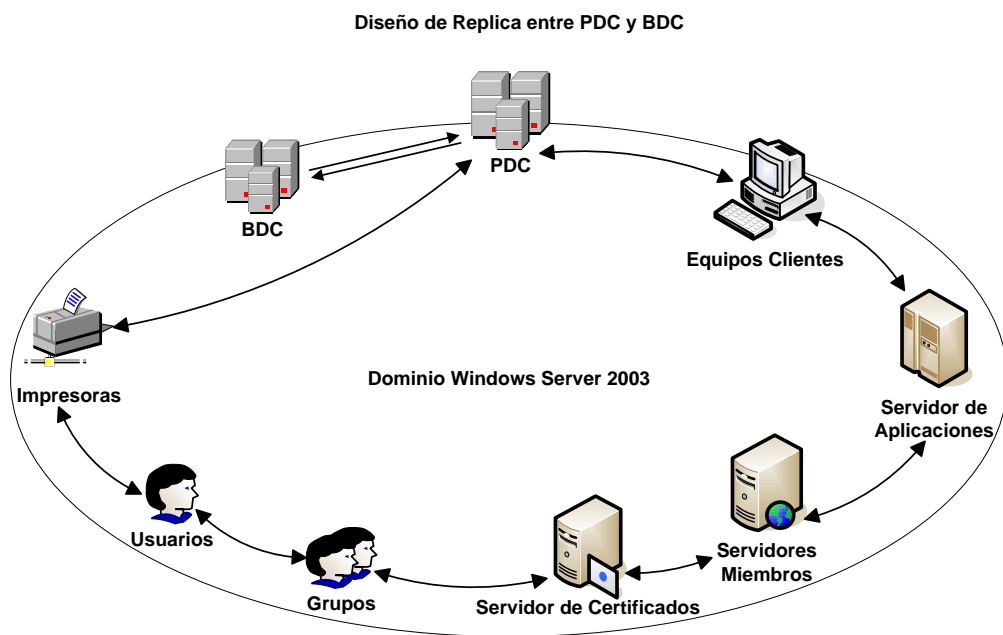


Figura 3.2. Forma en que opera un PDC conjuntamente con el BDC

3.3.2 Esquema de los servidores Windows de la UTPL

Seguidamente se inicia por entender y comprender como es la distribución de todos los servidores Windows dentro de la LAN³¹ de la UTPL, el esquema de red de servidores detalla el nombre, dirección IP y aplicaciones que tienen instaladas.

En la actualidad el Grupo de Desarrollo de Software (GDS) de la UTPL cuenta con **tres entornos de servidores**, uno que está dedicado netamente para la producción y los otros dos están orientados para el desarrollo y pruebas.

³¹ LAN: Local Área Network – Red de área local



PRODUCCIÓN

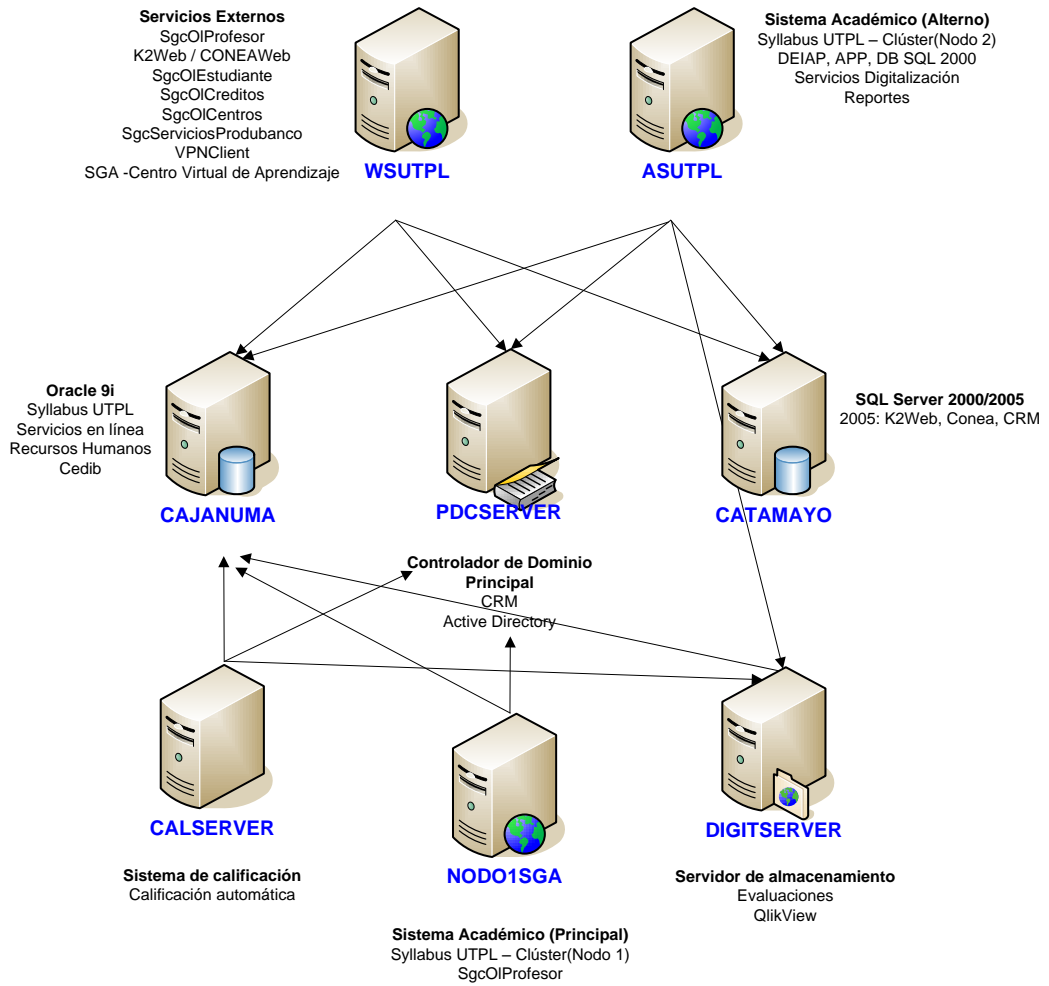


Figura 3.3. Diagrama de red de los servidores Windows que operan en el ambiente de Producción

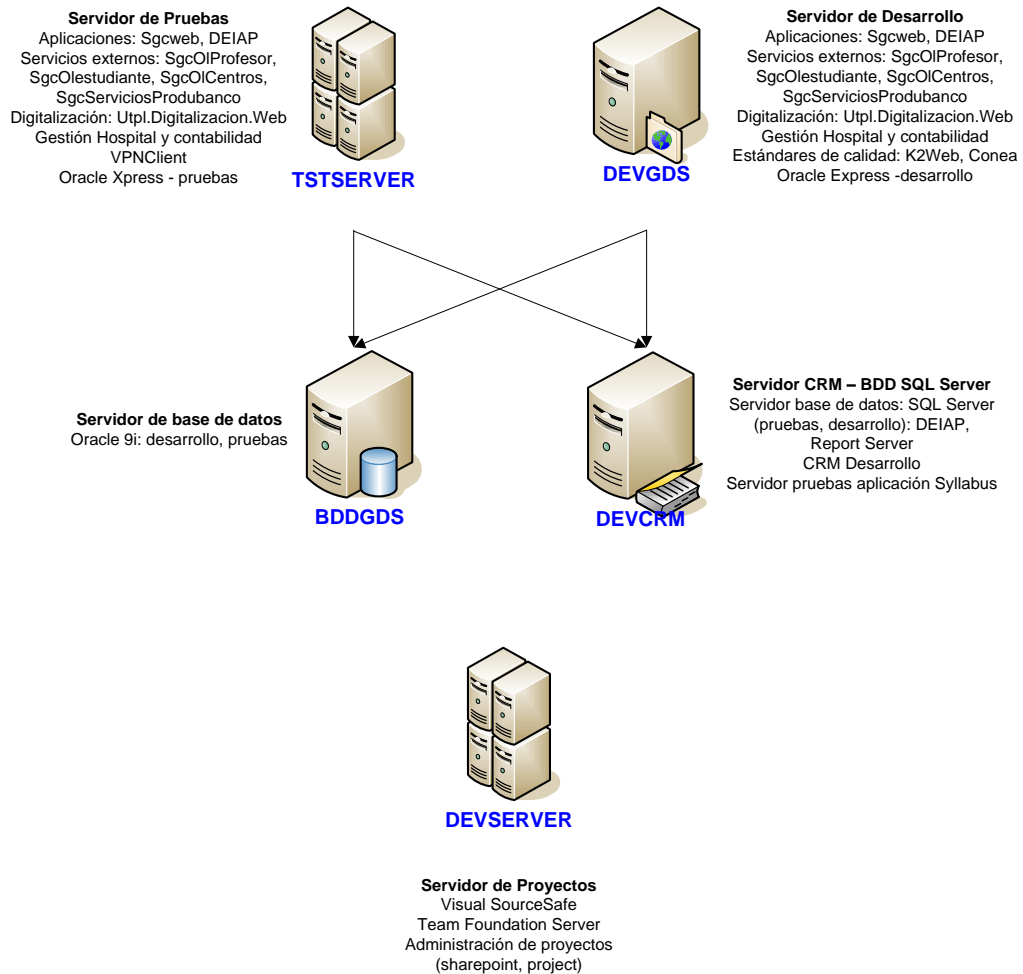
**DESARROLLO - PRUEBAS**

Figura 3.4. Diagrama de red de los servidores Windows del ambiente de Desarrollo y Pruebas

Los tres diagramas de red de los servidores está distribuido de manera correcta, cada entorno de servidores se encuentran ubicados en VLAN's diferentes lo que brinda una mejor administración y manejo cuando se aplican seguridades. Estos diagramas de servidores ya cuentan con una defensa a nivel de perímetro por tal motivo no se designa un servidor para que cumpla con esta actividad en los diagramas, además ello también implica que las seguridades a considerar para cada entorno van desde la protección a nivel de dominio.

Diferenciando y analizando cada servidor según el **rol o servicios que presta, nivel de exposición y criticidad de información o aplicaciones** se tiene la **Tabla 3.5**, que es una tabla clasificatoria bajo los conceptos mencionados.

3.3.3 Rol de los servidores y aplicaciones de acuerdo a su nivel de exposición y criticidad

Para tener conocimiento del **nivel de exposición y criticidad** en un servidor que trabaja con la plataforma Windows Server 2003, es necesario tener presente algunas consideraciones, por lo que



para los servidores Windows del GDS, evaluar el nivel de exposición y la criticidad es una situación que queda a criterio de los administradores tanto del sistema operativo como de los administradores de las aplicaciones.

Factores a considerar para evaluar el nivel de exposición³²

Los factores a considerar en la evaluación del nivel de exposición de los servidores del GDS esta sujeto al entorno donde se ubican los servidores, siendo así que los servers que están mas expuestos son los que pertenecen al entorno de Produccion, por el hecho de estar ofreciendo sus servicios de manera directa a los usuarios e interactuando permanentemente con el internet. En tanto a los servidores que se ubican en el entorno de Desarrollo y Pruebas permanen menos expuestos por el hecho de no necesariamente brindar servicios directamente a los usuarios finales, pues estos servidores son manejados y utilizados por los programadores, administrados y demás personas que pertenecen al GDS y su riesgo de ser atacados es mucho menor en comparación con los servidores que están en Produccion.

Los factores a considerar en el nivel de exposición son:

- ✓ La Disponibilidad y
- ✓ Confiabilidad

Factores a considerar para evaluar la criticidad³³

Evaluar la criticidad demanda conocer primero todas las aplicaciones que se tienen instaladas en los servidores del GDS, luego se evalúa las aplicaciones servidor por servidor para llegar a determinar de esta manera cual de los servidores es el que contiene aplicaciones más críticas que sumadas a las vulnerabilidades del sistema operativo y al nivel de exposición, le dan una criticidad global a todo el servidor.

Existen cuatro factores que se consideran para evaluar la criticidad de servicios o aplicaciones los cuales son:

- ✓ Importancia
- ✓ Características
- ✓ Desarrollo y mantenimiento
- ✓ Extensión y complejidad

La **importancia** de los servicios o aplicaciones que almacenan los servidores del GDS constituyen una de las bases para el desarrollo de los objetivos de la UTPLE como entidad educativa.

³² Información proporcionada por Ing. Janneth Chicaiza, Administradora de los servidores Windows del GDS

³³ Información tomada de la Fase 1 de la tesis "Diseño de un programa de alta disponibilidad para aplicaciones sobre Windows 2003"



En cuanto a las **características** de los servicios que ofrecen los servidores del GDS, se debe seguir o basarse en los siguientes criterios: Edad del servicio o aplicación, interfaces con otros servicios, percepción del usuario y documentación.

En lo referente al **desarrollo y mantenimiento** de aplicaciones o servicios en donde se utiliza los servidores del GDS, se debe considerar si el desarrollo esta basado en una metodología y si se cuenta con las personas indicadas para el uso de la misma.

En lo que se trata a la **extensión y complejidad** de un servicio, es importante su consideración para determinar la cantidad de personas que interactúan directa e indirectamente y así saber si se encuentran en el mismo lugar geográfico en el que reside el servicio o la aplicación. En cuanto a la **complejidad** de una aplicación almacenada en un servidor se evalúa por el número de transacciones que maneja, como por el número de procesos y cálculos que realiza durante un periodo normal de funcionamiento.

Tomando en cuenta los factores que se consideran para evaluar el nivel de exposición como la criticidad de los servidores del GDS se tiene la tabla 3.5 que ha sido consultada y llenada de acuerdo a la ponderación del criterio del administrador de los servidores.

La determinación del riesgo ocasionado por el nivel de exposición y criticidad de los servidores del GDS demanda o involucra la probabilidad de que una amenaza atente a una vulnerabilidad, que en caso de materializarse, conlleva a un impacto. El impacto y la probabilidad de ocurrencia se pueden categorizar a partir de una matriz con diferentes niveles, y dándole valores a cada uno de los niveles definidos según el criterio administrativo se llega a tener el riesgo total que se corre en caso de materializarse una amenaza producto del aprovechamiento de una vulnerabilidad en un servidor. La matriz que sirve para mostrar el nivel de riesgo, la cual se ha considerado para evaluar a los servidores del GDS es la siguiente:

Tabla 3.4. Nivel de medición del riesgo en los servidores del GDS

Impacto \ Probabilidad	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	Bajo ($10 * 1.0 = 10$)	Medio ($50 * 1.0 = 50$)	Alto ($100 * 1.0 = 100$)
Medio (0.5)	Bajo ($10 * 0.5 = 5$)	Medio ($50 * 0.5 = 25$)	Medio ($100 * 0.5 = 50$)
Bajo (0.1)	Bajo ($10 * 0.1 = 1$)	Bajo ($50 * 0.1 = 5$)	Bajo ($100 * 0.1 = 10$)

La escala utilizada para la evaluación del riesgo, nivel de exposición y criticidad esta dado por los valores de la tabla 3.4, en donde **Alto** va desde 51-100, **Medio** va desde 11-50 y **Bajo** va desde 1-10.



Tabla 3.5. Criticidad de los servidores del GDS

CLASIFICACIÓN DE SERVIDORES							
Nombre de Servidor	Rol/Servicios	Nivel de Exposición			Criticidad		
		Alto	Medio	Bajo	Alto	Medio	Bajo
WSUTPL (Web)	Servicios Externos	x			x		
ASUTPL (Web)	Sistema Académico (Alternativo)		x			x	
PDCSERVER (DC)	Controlador de Dominio Principal	x			x		
CATAMAYO (DB)	SQL Server 2000/2005		x				x
CALSERVER	Sistema de Calificación		x		x		
NODO1SGA (Web)	Sistema Académico (Principal)	x				x	
DIGITSERVER	Servidor de Almacenamiento		x		x		
TSTSERVER	Servidor de Pruebas			x		x	
DEVGDS	Servidor de Desarrollo		x			x	
BDDGDS	Servidor de Base de Datos			x		x	
DEVCRM	Servidor CRM – BDD SQL Server			x		x	
DEVSERVER	Servidor de Proyectos			x			x

La tabla 3.5 permite evaluar cual es el riesgo que corren los servidores del GDS tanto por las vulnerabilidades de las plataformas Windows con las que operan así como también por las aplicaciones, datos o servicios que ofrecen y almacenan.

3.3.4 Evaluación de necesidades, objetivos y servicios que presta la UTPL

La UTPL, es una organización orientada a la actividad educacional a nivel superior y por ende como tal, tiene muchas **necesidades**, tales necesidades como organización tienen mucho que ver con temas relacionados con:

- ✓ Educación
- ✓ Administración
- ✓ Investigación
- ✓ Recursos humanos
- ✓ Trámites en línea y
- ✓ Sociedad en general

Tomando en consideración la serie de necesidades que posee la UTPL como organización, se tiene que esas necesidades demandan un conjunto de **objetivos** específicos por cada área, los mismos que se deben satisfacer, para con ello ir dando cumplimiento a los objetivos generales que la universidad tiene planteados.

Partiendo y centrándose en cosas puntuales de las diversas áreas que la UTPL posee, se tiene el GDS, el cual como grupo tiene **objetivos y servicios** que ofrecer para de esa manera proyectar, mejorar y contribuir a que la UTPL logre sus metas. Dentro de los servicios que ofrece la UTPL mediante la cooperación del GDS, se tiene el **Sistema de Gestión Académica (SGA)** que es un sistema de gestión



transaccional que registra desde la creación tanto a estudiantes como a profesores, la creación de materias, la asignación de estudiantes y profesores en las asignaturas correspondientes según el proceso de matriculación en un período académico específico.

Por lo especificado, el GDS debe contar con nivel de seguridad que le permita garantizar la legitimidad de la información que maneja y los servicios que presta, tanto a nivel de la Intranet como en el Internet, por lo que es de mucha importancia esquematizar y contar con un nivel de seguridad aceptable en la manipulación de los datos.

3.3.5 Evaluación de requerimientos de seguridad adecuados para los servidores Windows de la UTPL.

Los requerimientos de seguridad para cada servidor Windows del GDS de la Universidad Técnica Particular de Loja van y están de acuerdo a su roll que desempeñan, es por ello que a continuación se describen los requerimientos que cada servidor necesita de acuerdo al entorno en el que está funcionando.

Entorno de Producción.- En este entorno todos los servidores necesitan tener implementada un excelente nivel de seguridad sin afectar la eficacia ni el rendimiento de cada servidor, los servidores que se encuentran en este entorno albergan aplicaciones realizadas por el grupo de desarrollo que posee la UTPL, así como también aplicaciones útiles para dar servicios al grupo cómo al Sistema de Gestión Académica (SGA), pues en éste entorno es donde esta ejecutándose el SGA y de esta forma brinda sus servicios tanto a estudiantes, profesores, administrativos, entre otros, por lo que se requiere tener un ambiente o entorno que cumpla con políticas de seguridad que permitan asegurar la información manejada, en la **Tabla 3.6** se describen de manera detallada el nombre, dirección IP, puertos y demás información relacionada que cada servidor en éste entorno maneja.

Entorno de Desarrollo y Pruebas.- En el entorno de desarrollo y pruebas de igual forma se debe implementar el nivel de seguridad adecuado para que se trabaje de manera confiable, con la finalidad de que se tenga el máximo provecho de los recursos disponibles, así como la seguridad de todos los datos y programas que se manejan y desarrollan, por lo que es de mucha importancia y relevancia tener asegurado el entorno bajo estrictas políticas de seguridad, a continuación en la **Tabla 3.7**, se detalla información que describe a los servidores como a las aplicaciones instaladas en cada servidor de éste entorno.



Tabla 3.6. Descripción de servidores del ambiente de Producción

DESCRIPCIÓN DE SERVIDORES Y SOFTWARE INSTALADO EN EL ENTORNO DE DESARROLLO Y PRUEBAS				
NOMBRE DEL SERVIDOR	TIPO DE SERVIDOR	DESCRIPCIÓN	APLICACIONES	SOFTWARE INSTALADO
WSUTPL (Web)	Standalone	Servidor WEB – Internet	Servicios en Línea Profesor, estudiante, Interfaz Produbanco	F-Secure Antivirus, Microsoft Visual Studio .NET Enterprise Architect, Microsoft Office Professional, SQL Server, Microsoft Health Monitor 2.1, WinRAR archive, Cliente Oracle, Oracle Data Provider
ASUTPL (Web)	Standalone	Servidor WEB – Intranet (alternativo)	Sistema Académico DANTA, Reporting Server	Microsoft Health Monitor, Antivirus F-Secure, Microsoft Visual SourceSafe 6.0, Microsoft Baseline Security Analyzer, Microsoft SQL Server, Microsoft Reporting Service, Visual Studio .NET Enterprise Architect, WinRAR archive, Cliente Oracle, Oracle Data Provider
PDCSERVER (DC)	Domain Controller	Servidor de servicios de Directorio	Sistema Académico Danta alternativo, Sistema de Evaluaciones Presenciales, Buscador Sistema de Digitalización	F-Secure Antivirus, MS Group Policy Management Console with SP1, Active Directory, WinRAR archive, Cliente Oracle, Oracle9i Database, Cliente de Workflow, Oracle Data Provider
CATAMAYO (DB)	Standalone	Servidor de Base de Datos	Base de Datos y Reportes	SQL Server 2005 y Reportes Services 2005
CALSERVER	Standalone	Servidor de Procesamiento de Pruebas MAD	Sistema de calificación de Pruebas de MAD	F-Secure, Pegasus Imaging's, Oracle9i Client, Oracle Data Provider for .NET
NODO1SGA (Web)	Standalone	Servidor WEB – Intranet (principal)	Sistema de Gestión Académica, Servicios en Línea al Profesor	Antivirus F-Secure, Cliente Oracle, Oracle Data Provider, Microsoft Baseline Security Analyzer, Microsoft Health Monitor, Microsoft Office Professional 2003
DIGITSERVER	Standalone	Servidor de almacenamiento	FTP, Almacenamiento	Antivirus F-Secure, IBM Fast Storage Manager Host Software, Microsoft .NET Framework 2.0, QlickView Publisher, QlickView Server



Tabla 3.7. Descripción de servidores del entorno de Desarrollo y Pruebas

DESCRIPCIÓN DE SERVIDORES Y SOFTWARE INSTALADO EN EL ENTORNO DE DESARROLLO Y PRUEBAS				
NOMBRE DEL SERVIDOR	TIPO DE SERVIDOR	DESCRIPCIÓN	APLICACIONES	SOFTWARE INSTALADO
TSTSERVER	Standalone	Servidor de Pruebas	Sistema Académico DANTA, Servicios en línea al Profesor, Estudiante y Centros. Estándares de Calidad, Sistema del Hospital, Sistema de Contabilidad	Dell OpenManage Array Manager, Cristal Reports Server, F-Secure Antivirus, MS Visual SourceSafe 6.0, MSVisual Studio .NET Enterprise Architect, TOAD Xpert Edition, Microsoft SQL Server 2005, WinRAR archive, SharePoint Services, Cliente Oracle, Oracle9i Database, MS Baseline Security Analyzer, Oracle Data Provider
DEVGDS	Standalone	Servidor de Desarrollo	Servicios externos, Digitalización, Estándares de calidad y aplicaciones de desarrollo.	Dell OpenManage Array Manager, Sgcweb, DEIAP, SgcOIProfesor, SgcOICentros, SgcServiciosProdubanco, UTPL Digitalizacion Web, Gestión Hospitalaria y contabilidad, K2Web, Conea Oracle Express -desarrollo
BDDGDS	Standalone	Servidor de Base de Datos	Bases de datos Oracle 9i	Dell OpenManage Array Manager, Oracle 9i: desarrollo y pruebas
DEVCRM	Standalone	Servidor CRM – BDD SQL Server	Bases de datos SQL Server	Dell OpenManage Array Manager, SQL Server (Pruebas, desarrollo), DEIAP, Report Server, CRM Desarrollo, Servidor pruebas aplicación Syllabus
DEVSERVER	Standalone	Servidor de Proyectos	Sistema Académico DANTA, Servicios en Línea al Profesor, Estudiante y Centros. Estándares de Calidad, Sistema del Hospital, Sistema de Contabilidad	F-Secure Antivirus, Microsoft Visual SourceSafe 6.0, Microsoft Baseline Security Analyzer, Microsoft Office Professional, Microsoft Visual Studio .NET Enterprise Architect, TOAD Xpert Edition, SharePoint Service, Microsoft SQL Server 2005, Microsoft SQL Server 2000, WinRAR archive, Cliente Oracle, Oracle9i Database, Cliente de Workflow, Oracle Data Provider



En los tres entornos de servidores existentes se debe configurar políticas de seguridad que se apeguen a las necesidades y servicios que preste cada servidor, por lo que se debe configurar firewalls y plantillas de seguridad que permitan asegurar los servidores y así mantener un ambiente seguro tanto de producción como de desarrollo y pruebas.

3.3.6 Medidas de seguridad aplicables a los servidores Windows del GDS de la UTPL

Las medidas de seguridad aplicables para los servidores Windows del GDS, son las mismas que se describen en la tabla del **literal 3.2.3**, pues todos los procedimientos y políticas que se detallan y analizan en este punto son de mucha utilidad y aplicables a los servidores del GDS. Se puede decir que es una guía que se debe seguir cuando se configura seguridades para un servidor Windows.

3.4 IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

3.4.1 Detalle de configuraciones que abarca el Esquema de Seguridad

La implementación del esquema de seguridad para los servidores Windows del GDS está sujeta a las siguientes consideraciones:

- ✓ Diseño de la infraestructura de red de los servidores Windows
- ✓ Las necesidades de los servicios de red como: Servicios Web (Internos, Externos), Correo (SMTP³⁴), DNS³⁵, Active Directory, Controlador de dominio, Bases de Datos (Oracle, SQL Server), Sistema de Gestión Académica (SGA), Sistema de calificación, servidor de almacenamiento, pruebas, desarrollo, proyectos y CRM.

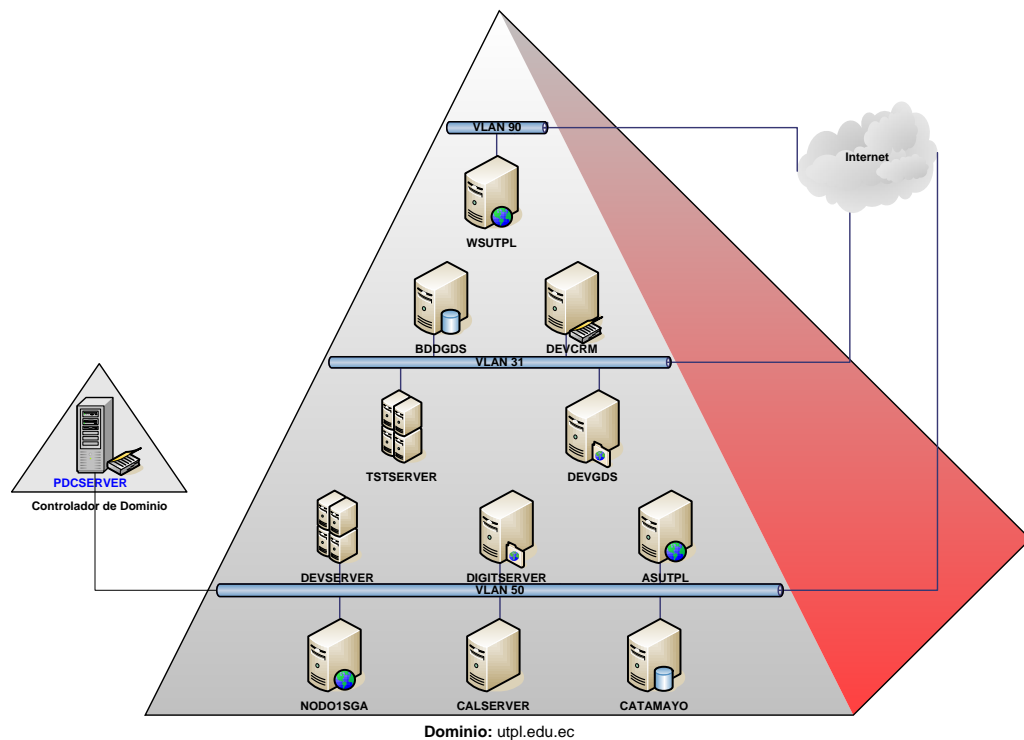
a. Diagrama del Esquema de Seguridad de los servidores Windows Server 2003 del GDS

El diagrama de seguridad de servidores Windows del GDS, distribuye a los servidores de acuerdo a VLAN's. Tener ubicados los servidores en diferentes VLAN's permite garantizar y mantener un mejor nivel de seguridad, cumpliendo los requerimientos operacionales a nivel de servicios de red, y así se obtiene una mejor escalabilidad, disponibilidad, mantenibilidad, manejabilidad y por ende una alta seguridad. Por todo esto, se ha observado que la distribución actual de los servidores del GDS es la adecuada, la cual se la debe mantener y tomarla como punto de partida en la elaboración del esquema de seguridad.

A continuación el diseño físico de la distribución de los servidores considera el número de servidores existentes, la administración y requerimientos de conexión a Internet, pues es un esquema ideado para un alto nivel de seguridad y que está basado en la propuesta actual que tienen los servidores Windows del GDS.

³⁴ SMTP: Simple Mail Transfer Protocol – Protocolo de Simple Transferencia de Correo

³⁵ DNS: Domain Name System – Sistema de Nombres de Dominio

**ESQUEMA DE SEGURIDAD DE LOS SERVIDORES WINDOWS DEL GDS****Figura 3.5.** Diagrama de Seguridad de los Servidores Windows**b. Descripción Física de los Servidores Windows del GDS**

La descripción física o también llamada descripción de Hardware de los servidores sobre los que se va implementar el esquema de seguridad y que tienen instalado el sistema operativo Windows Server 2003, es de importancia debido a que facilita relacionar configuraciones de alta seguridad de acuerdo al hardware del servidor, porque no es lo mismo aplicar configuraciones de alta seguridad a un PC que a un servidor, por lo general un PC pierde cierto porcentaje de funcionalidad, pero un servidor por contar con diferentes características de operación gracias a las altas prestaciones Hardware no se debe notar variación en el nivel de funcionalidad. Además contar con un detalle de Hardware permite ir cumpliendo conceptos iniciales de seguridad, como es saber si los discos duros han sido formateados con el sistema de archivos NTFS, número de particiones creadas, direccionamiento de red, etc. A continuación en la tabla se detalla el hardware de los servidores del GDS:



Tabla 3.8. Descripción Hardware de los Servidores Windows del GDS

DETALLE DEL HARDWARE DE LOS SERVIDORES WINDOWS DE LA UTPL					
Nombre del Servidor	Marca y Modelo	Características Hardware	Particiones de Discos Duros de los Servidores		
			Partición	Tamaño (GB)	Descripción
WSUTPL	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 70 GB en disco, 4 GB RAM	C	70	Partición Primaria NTFS – Sistema Operativo, demás Software y datos
ASUTPL	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 70 GB en disco, 4 GB RAM	C	40	Partición Primaria NTFS – Sistema Operativo y demás Software
			D	30	Partición Primaria NTFS - Datos
PDCSERVER	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 70 GB en disco, 4 GB RAM	C	40	Partición Primaria NTFS – Sistema Operativo y demás Software
			D	30	Partición Primaria NTFS - Datos
CATAMAYO	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 70 GB en disco, 4 GB RAM	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
CALSERVER	IBM System x3650	Intel(R) Xeon(TM) CPU 3.0GHz, 2 HD de 70 GB, 4 GB RAM	C	70	Sistema Operativo
			D	70	Datos
NODO1SGA	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5110 @ 1.60GHz, 70 GB en disco, 3 GB RAM	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
DIGITSERVER	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5110 @ 1.60GHz, 70 GB en disco, 2 GB RAM	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
TSTSERVER	DELL - PowerEdge 1600SC	Intel(R) Xeon(TM) CPU 2.80GHz, 70 GB en disco	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
DEVGDS	DELL - PowerEdge 1600SC	Intel(R) Xeon(TM) CPU 2.80GHz, 70 GB en disco	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software



Tabla 3.8. Descripción Hardware de los Servidores Windows del GDS (... continuación)

DETALLE DEL HARDWARE DE LOS SERVIDORES WINDOWS DE LA UTP					
Nombre del Servidor	Marca y Modelo	Características Hardware	Particiones de Discos Duros de los Servidores		
			Partición	Tamaño (GB)	Descripción
BDDGDS	DELL - PowerEdge 1600SC	Intel(R) Xeon(TM) CPU 2.80GHz, 70 GB en disco	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
DEVCRM	DELL - PowerEdge 1600SC	Intel(R) Xeon(TM) CPU 2.80GHz, 70 GB en disco	C	70	Partición Primaria NTFS – Sistema Operativo y demás Software
DEVSERVER	IBM eServer™ BladeCenter® HS21 (8853L6U)	Intel(R) Xeon(R) CPU 5160 @ 3.00GHz, 70 GB en disco, 4 GB RAM	C	40	Partición Primaria NTFS – Sistema Operativo y demás Software
			D	30	Partición Primaria NTFS - Datos

**Configuración del PDC**

Una vez configurada la seguridad para los servidores miembros del dominio **utpl.edu.ec** (ver **ANEXO 3.2**), se procede a la configuración de seguridad del servidor **Controlador de Dominio Primario**, actualmente ya existe un servidor que actúa de PDC, por lo que se procede a la creación del servidor que va hacer de **Controlador de Dominio de Respaldo** y desde los cuales se va a realizar la administración de todos los servidores miembros del dominio UTPL, éstos servidores al igual que los servidores miembros hacen uso de plantillas para configurar su seguridad, la configuración de la plantilla de seguridad como su forma de aplicación en éstos servidores es similar a la de los servidores miembros. Las diferencias de esta plantilla se tratan a continuación.

La plantilla no incluye lo relacionado con Directivas de cuenta, solo se inicia las configuraciones a partir de las **Políticas Locales**, las cuales no son iguales a las configuraciones que se realizan en las plantillas para un servidor miembro, en la tabla siguiente se detalla las diferencias.

Tabla 3.9. Directivas de Seguridad que difieren entre el DC y un Servidor miembro del GDS

Configuraciones de Seguridad del Controlador de Dominio Primario y Backup		
Configuración de Políticas de Auditoría		
Directiva	Configuración en el DC	
Audit account logon events	Success, Failure	
Audit account management	Success, Failure	
Audit directory service access	Failure	
Audit logon events	Success, Failure	
Audit object access	Failure	
Audit policy change	Success	
Audit privilege use	Failure	
Audit process tracking	No auditing	
Audit system events	Success	
Configuración de Asignación de Derechos de Usuario		
Directiva	Configuración de seguridad Empresarial	Configuración de alta seguridad
Deny access to this computer from the network	ANONYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts	ANONYMOUS LOGON; Guests; Support_388945a0
Deny log on through Terminal Services	Guests; SUPPORT_388945a0	Guests
Configuración de Opciones de Seguridad		
Network access: Named Pipes that can be accessed anonymously	Not defined	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, BROWSER, netlogon, lsarpc, samr
Network security: Force logoff when logon hours expire	Enabled	Not Defined
Shutdown: Clear virtual memory pagefile	Disabled	Disabled



En cuanto a las **Directivas de Registro de Sucesos**, toda la configuración es idéntica entre el DC y el resto de servidores miembros del GDS. En lo que se refiere a **Grupos Restringidos**, pues es de mucha relevancia en un controlador de dominio, así se autoriza a personal administrativo realizar tareas de administración, en el GDS podrán hacer este tipo de actividad los usuarios que pertenecen a los grupos de **Backup Operators** y **Server Operators**.

En cuanto a los **Servicios** que el DC del GDS, debe tener habilitados para su funcionamiento correcto, son los mismos que se indican más adelante en la **Tabla 3.16** de la parte de **aplicación de configuraciones**, más los adicionales que a continuación se describen.

Tabla 3.10. Servicios a habilitarse en el DC del GDS

Servicios básicos a habilitarse en los servidores DC del GDS	
Servicios	Descripción
DCOM Server Process Launcher	Mantiene funcionalidad de lanzamiento para servicios DCOM
Distributed File System	Integra archivos compartidos dispersos en uno solo.
DNS Server	Habilita a clientes DNS a que resuelvan sus nombres DNS, así como también consultas y peticiones dinámicas de actualizaciones DNS. Si se deshabilita este servicio, las actualizaciones DNS no ocurrirán y los servicios dependientes también fallarán.
Error Reporting Service	Registra y reporta daños inesperados en aplicaciones Microsoft. Si se deshabilita, cualquier servicio explícitamente dependiente, no iniciará.
File Replication Service	Permite la copia automática de archivos de manera simultánea sobre múltiples servidores. Si este servicio es detenido, la replicación de archivos no ocurría y los servidores no se sincronizarían.
Kerberos Key Distribution Center	Este servicio habilita a usuarios de los controladores de dominio el inicio de sesión sobre la red usando el protocolo de autenticación Kerberos. Deshabilitado este servicio en un DC, los usuarios no podrán iniciar sesión en la red.

Habilitados los **servicios del sistema** necesarios para que el DC funcione de manera idónea, se procede a asegurar el DC a ataques provenientes desde la red, esto se lo hace desde el **Registro** del sistema (regedit), todo el proceso se lo describe en el **manual de políticas y procedimientos (PR01, PR02, PR03)**.

Configurado y fortalecido el DC frente ataques de la red, se procede a configurar el **Sistema de Archivos** del DC, asegurar estos archivos es de importancia frente a ataques de personas mal intencionadas o por desconocimiento, que dejen fuera de servicio al DC. Los **archivos del sistema**, se encuentran ubicados en la carpeta **%SystemRoot%\System32** (C:\WINDOWS\system32) y son puntos críticos que se deben asegurar para evitar ataques en el DC. Todos los archivos que se describen en la siguiente tabla tienen configurada su seguridad en **Do not allow permissions on this file or folder to be replaced** (No permitir que los permisos de este fichero o carpeta sean sustituidos), lo que garantiza que atacantes no vayan a borrar o dañar estos archivos.

**Tabla 3.11.** Configuración de permisos de archivos ejecutables de Windows

Aseguramiento del sistema de archivos	
❖ %SystemRoot%\System32\regedit.exe	❖ %SystemRoot%\System32\ntbackup.exe
❖ %SystemRoot%\System32\arp.exe	❖ %SystemRoot%\System32\rcp.exe
❖ %SystemRoot%\System32\at.exe	❖ %SystemRoot%\System32\reg.exe
❖ %SystemRoot%\System32\attrib.exe	❖ %SystemRoot%\System32\regedt32.exe
❖ %SystemRoot%\System32\cacls.exe	❖ %SystemRoot%\System32\regini.exe
❖ %SystemRoot%\System32\debug.exe	❖ %SystemRoot%\System32\regsvr32.exe
❖ %SystemRoot%\System32\edlin.exe	❖ %SystemRoot%\System32\rexc.exe
❖ %SystemRoot%\System32\eventcreate.exe	❖ %SystemRoot%\System32\route.exe
❖ %SystemRoot%\System32\eventtriggers.exe	❖ %SystemRoot%\System32\rsh.exe
❖ %SystemRoot%\System32\ftp.exe	❖ %SystemRoot%\System32\sc.exe
❖ %SystemRoot%\System32\nbtstat.exe	❖ %SystemRoot%\System32\secedit.exe
❖ %SystemRoot%\System32\net.exe	❖ %SystemRoot%\System32\subst.exe
❖ %SystemRoot%\System32\net1.exe	❖ %SystemRoot%\System32\systeminfo.exe
❖ %SystemRoot%\System32\netsh.exe	❖ %SystemRoot%\System32\telnet.exe
❖ %SystemRoot%\System32\netstat.exe	❖ %SystemRoot%\System32\tftp.exe
❖ %SystemRoot%\System32\nslookup.exe	❖ %SystemRoot%\System32\tlntsvr.exe

A parte de los archivos descritos en la tabla anterior, también es necesario asegurar otros directorios que almacenan información sensible a ataques en un servidor Controlador de Dominio, los cuales se describen a continuación.

Tabla 3.12. Aseguramiento de carpetas adicionales del DC

Carpetas aseguradas	Permisos aplicados
%systemdrive%	Administradores: Control total Sistema: Control total Usuarios autenticados: Leer y ejecutar, Listar el contenido de la carpeta y Leer
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	Administradores: Control total Creador/Propietario: Control total Sistema: Control total

Haciendo uso de Active Directory y desde el servidor que hace de Controla de Dominio Primario se aplica seguridad a nivel del dominio **utpl.edu.ec**, aplicar seguridades al dominio garantiza que todo usuario estará administrado bajo políticas de seguridad que tengan como objetivo precautelar la información que se maneja en los servidores. Para configurar la seguridad en el dominio utpl.edu.ec igualmente se utiliza plantillas que contienen directivas de seguridad acorde a las necesidades de seguridad que mejor se adapten al dominio de servidores Windows de la UTPL, los valores de configuración de la plantilla de seguridad que se aplica al dominio están detallados en el.

Configuración de Políticas de Aseguramiento del Dominio de Servidores Windows del GDS

Para el aseguramiento de servidores Windows del GDS, se aplica políticas de seguridad a nivel de dominio, específicamente se configura **Directivas de Cuentas** (Políticas de Contraseñas, Políticas de Bloqueo de Cuenta, Políticas Kerberos) complementado con algunas configuraciones de seguridad a nivel de **Directivas Locales** (Opciones de Seguridad).



En cuanto a configuración de las **Políticas de Contraseñas son iguales** a las configuradas para un servidor miembro del GDS, las directivas que si difieren en configuración, se describen en la tabla siguiente:

Tabla 3.13. Configuraciones de Seguridad a nivel de Dominio para el GDS

Directivas de Cuentas		
Directiva	Configuración de Línea de Base	Configuración de Alta Seguridad
<i>Configuración de Políticas de Bloqueo de Cuenta</i>		
Account lockout duration	30 minutes	15 minutes
Account lockout threshold	50 invalid logon attempts	10 invalid logon attempts
Reset account lockout counter after	30 minutes	15 minutes
<i>Configuración de Políticas Kerberos</i>		
Enforce user logon restrictions	Not Defined	Enabled
Maximum lifetime for service ticket	Not Defined	600 minutes
Maximum lifetime for user ticket	Not Defined	10 hours
Maximum lifetime for user ticket renewal	Not Defined	7 days
Maximum tolerance for computer clock synchronization	Not Defined	5 minutes
Directivas Locales		
<i>Configuración de Opciones de Seguridad</i>		
Microsoft network server: Disconnect clients when logon hours expire		Enabled
Network Access: Allow anonymous SID/NAME translation		Disabled
Network Security: Force Logoff when Logon Hours expire		Enabled

Configuración de Firewalls en cada servidor

En la UPL ya existen configurados firewalls a nivel del perímetro que resguardan de conexiones dañinas a los equipos servidores del **Grupo de Desarrollo de Software**, por estas razones en el **Esquema de Seguridad** de los servidores Windows del GDS se configura firewalls servidor por servidor, ya que cada servidor necesita diferente filtrado de tráfico de red, según la función que está desempeñando, todo el proceso a seguir en la configuración del firewall en los servidores Windows del dominio **utpl.edu.ec** esta detallado en **PR12** y en el **ANEXO 3.4**, se describe servidor por servidor la configuración del firewall.

Tabla 3.14. Puertos utilizados por aplicaciones o servicios del GDS

Categoría Software	Aplicación/servicio	Puerto
Base de datos	SQL Server	1433
	Oracle	1521
Aplicaciones	Web, SGA, Sitio online estudiante, profesor, centros, Produbanco	80
	Sharepoint	8081
Administración	Conexión Remota	3389
Servicios de Directorio	Active Directory	389
Repositorios y recursos compartidos	Visual Source Safe	139
	Directorios app	445
Notificaciones	Email	25
Respaldos	FTP	21

**Creación de una línea base de seguridad para un servidor Windows Server 2003**

En el caso de los servidores miembros del dominio **utpl.edu.ec** se realiza la configuración de la línea de base en un solo servidor miembro, luego de probarla en aquel servidor que se ha utilizado para tal propósito, se la aplica a los demás servidores con la finalidad de implementar configuraciones mínimas de seguridad en todos los servidores, la aplicación de la línea de base de seguridad a los servidores restantes, se la puede aplicar desde el PDC o bien de manera manual uno por uno. Todas las tareas llevadas a cabo acerca de la creación de la línea de base de servidores Windows se la describe en el **ANEXO 3.5**. Todo el proceso de línea de base de seguridad de los servidores se lleva a cabo valiéndose del uso de las **herramientas** del propio sistema operativo Windows Server 2003, que proporciona muchas utilidades de aseguramiento para un servidor.

3.4.2 Evaluación de Resultados del Esquema y Herramientas utilizadas

La evaluación de resultados del esquema de seguridad abarca a todos los servidores que tienen instalado Windows Server 2003 cuyo objetivo es proporcionarles una mayor seguridad, para lo cual el esquema hace uso de muchas herramientas propias del sistema operativo Windows Server 2003, lo que da mucha adaptabilidad de todas las seguridades implementadas.

Tabla 3.15. Herramientas de configuración de seguridad de Windows Server 2003
Fuente: <http://www.microsoft.com/latam/technet/seminario/3estrella2.msp>

Herramientas para configurar seguridad	
Nombre	Descripción
Microsoft Management Console (MMC)	Es un componente de Windows Server 2003, que brinda a los administradores y usuarios avanzados una interfaz flexible a través del cual pueden configurar seguridades y supervisar el sistema. Fuente: http://en.wikipedia.org/wiki/Microsoft_Management_Console
Security Configuration Wizard (SCW)	El asistente de configuración de seguridad, permite la configuración rápida y sencilla de las políticas de seguridad de servidores miembros, controladores de dominio, web, etc. Fuente: http://www.microsoft.com/spain/windowsserver2003/technologies/security/configwiz/default.aspx
Group Policy Management Console (GPMC)	La consola de administración de directivas de grupo, integra una serie de interfaces programables para la gestión de Directivas de Grupo, incorpora muchas capacidades para la gestión de políticas de seguridad en los servidores Windows. Fuente: http://geeks.ms/blogs/juansa/archive/2006/08/02/group-policy-management-console-gpmc.aspx
Herramientas de diagnóstico de DC's (Dcdiag, Netdiag, Repadmin, Replmon, portqry, Nslookup, dsastat)	Conjunto de herramientas que sirven para hacer una serie de tareas, tales como: Test a los DC's, Test a nivel de red, Comprobación de replicas entre servidores, Estado de replicas entre las diferentes particiones del AD, Comprobar conectividad entre servidores mediante puertos TCP y UDP, Test de resolución de nombres en servidores DNS, Comparar y detectar diferencias entre las bases de datos de directorio de los DC's que pueda haber. Fuente: http://www.cuencanet.com.ar/how-to/fsmo/Uso_de_herramientas_de%20diagnostico_para_un_DC.pdf



En términos generales el Esquema de Seguridad engloba todas las configuraciones de seguridad básicas como avanzadas que debe tener un servidor implementadas para que protejan los datos, aplicaciones, servicios y funcionalidades, de tal forma que se evita el mal manejo o ataques a los activos de información.

Todas las configuraciones del Esquema de Seguridad son debidamente probadas tanto de manera individual como en conjunto, y los resultados esperados son los correctos, todas las consideraciones que se han tomado para probar y evaluar el Esquema de seguridad están detalladas en el **CAPITULO IV**.

3.5 APLICACIÓN DE CONFIGURACIONES AL GDS

La aplicación de las configuraciones de seguridad elaboradas en pasos anteriores, se inicia aplicando la plantilla de seguridad al **Controlador de Dominio Primario**, que será la que fortalecerá su seguridad así como también la seguridad del **Controlador de Dominio de Backup**. Para aplicar la plantilla que se ha personalizado acorde a las necesidades de seguridad del Controlador de Dominio Primario de los servidores Windows del GDS, se sigue el proceso descrito en **PR18**.

Aplicada la plantilla de seguridad al PDC, se procede a aplicar la plantilla de seguridad al **dominio** de servidores, este proceso se describe en **PR19**, finalmente se aplica la plantilla de seguridad a cada uno de los servidores miembros del dominio del GDS, de igual manera el proceso de aplicación se detalla en **PR20**.

3.5.1 Políticas a activar para el GDS

Para el grupo de servidores que operan y brindan su servicio al GDS, se pueden indicar algunas políticas que permitan una mejor gestión y administración de la seguridad que es un objetivo primordial en un grupo que se dedica al desarrollo de software, complementando a las políticas que ya se mencionan en el **literal 3.2.3 (PL04, PL05)**, se tiene:

- ✓ Los servidores se deben administrar desde un PDC
- ✓ El PDC debe contar con un Controlador de Dominio de Backup
- ✓ Se debe realizar escaneos de comprobación de seguridades de manera periódica en cada servidor (mensualmente sería lo recomendable, utilizando la herramienta MBSA).
- ✓ A todos los usuarios bien sea del sistema operativo o aplicaciones de diversa índole donde tengan que utilizar contraseñas para autenticarse, recomendarles que creen hábitos de utilización de contraseñas fuertes.
- ✓ Servicios o aplicaciones que se crean que poseen vulnerabilidades a ataques de intrusos, es preferible desinstalarlos o no utilizarlos sin las debidas actualizaciones de seguridad que le den la confiabilidad necesaria para su utilización.
- ✓ Contar con planes de contingencia y respaldos en caso de pérdida de información



- ✓ Configurar firewalls servidor por servidor de acuerdo al rol que desempeña cada uno.
- ✓ Dialogar con los programadores del grupo e indicarles que no deshabiliten el firewall de sus equipos por creer que son la causa de determinadas situaciones anómalas de funcionalidad del sistema operativo, pues un firewall bien configurado no impide el trabajo de un programador así como el mal funcionamiento del sistema operativo.
- ✓ No sobrecargar el sistema operativo de los servidores con programas improductivos que pueden comprometer la integridad del sistema.
- ✓ Instalar siempre sólo lo necesario e indispensable para que un servidor realice su trabajo sin ningún inconveniente.

3.5.2 Servicios básicos que se deben ejecutar en los servidores del GDS

A nivel de sistema operativo de los servidores del GDS, se tiene que por defecto se instalan muchos servicios, de los cuales varios no son utilizados y constituyen una vulnerabilidad para el servidor, a parte de las especificaciones de los servicios que se realizan en la parte descriptiva de este capítulo (**literal 3.25**), se debe decir y complementar que para los servidores del GDS servicios como **IIS**, **RAS**³⁶ y **Terminal Services** tienen vulnerabilidades, por lo que deben de ser configurados de manera cuidadosa para evitar ataques, también se tiene que tener cuidado con servicios que se estén ejecutando de manera oculta, para evitar esto se debe auditar y revisar con frecuencia los servicios que se ejecutan en cada servidor. Para los servidores del GDS los **servicios básicos** que se deben revisar y que es esencial su funcionalidad para tareas básicas del servidor son:

Tabla 3.16. Servicios Básicos

Servicios básicos a habilitarse en los servidores miembros del GDS	
Servicios	Descripción
Automatic Updates	Servicio útil para chequear automáticamente si existen actualizaciones o parches, este servicio requiere que se esté ejecutando el servicio de cifrado.
COM+ Event System	COM (Component Object Model) Facilita a los desarrolladores el uso y creación de componentes de software en cualquier lenguaje y con cualquier herramienta.
Computer Browser	Mantiene actualizada la lista de computadoras de la red y da información a los programas que la requieren.
Cryptographic Services	Proporciona tres servicios de administración: <ul style="list-style-type: none"> • Servicio de catalogo de base de datos, que confirma las firmas de archivos de Windows. • Servicio de raíz protegida, que agrega y quita certificados de entidades emisoras. • Servicio de claves, que ayuda a inscribir certificados para un equipo.

³⁶ RAS: Remote Access Server – Servidor de Acceso Remoto



Tabla 3.16. Servicios Básicos (... continuación)

Servicios básicos a habilitarse en los servidores miembros del GDS	
Servicios	Descripción
Distributed Transaction Coordinator	Servicio encargado de coordinar transacciones que están distribuidas en múltiples administradores de recursos. Por ejemplo crear bases de datos, colas de mensajes y sistemas de archivos.
DNS Client	Resuelve y almacena los nombres DNS (Domain Name System) para un equipo. Además no se podrá localizar controladores de dominio Active Directory.
Event Log	Registra eventos producidos por componentes y aplicaciones de Windows para luego ser vistos desde el Visor de Eventos (Event Viewer)
IPSEC Services	Provee autenticación y verificación de paquetes, así como la encriptación de los mismos. Es muy usado en Redes Privadas Virtuales (VPNs)
Logical Disk Manager	Detecta y monitorea los nuevos discos rígidos y envía la información al Servicio del administrador de discos lógicos para su configuración.
Net Logon	Se utiliza para loguearse/autenticarse en un Controlador de Dominio
Network Location Awareness (NLA)	Permite a las aplicaciones identificar a que red lógica se están conectando e identifica las direcciones físicas almacenadas.
NT LM Security Support Provider	Permite a los usuarios conectarse a una red utilizando el protocolo de autenticación NTLM.
Plug and Play	Se encarga de reconocer los dispositivos Plug and Play de un equipo.
Print Spooler	Se encarga de poner los archivos a imprimir en la cola de espera. Este servicio es requerido si se utiliza impresoras locales o de red.
Remote Access Auto Connection Manager	Crea una conexión a una red remota cuando algún programa solicita un nombre o dirección DNS o NetBIOS.
Remote Procedure Call (RPC)	Este servicio es fundamental. La mayoría de las cosas dependen de este servicio para funcionar. Sin este servicio, el equipo no podrá botear.
Remote Procedure Call (RPC) Locator	Administra la base de datos de nombres de servicio de RPC.
Security Accounts Manager	Almacena información de seguridad de cuentas de usuarios locales. El inicio de este servicio, indica a otros servicios que el subsistema SAM (Security Accounts Manager) está listo para recibir peticiones.
Server	Permite compartir a través de una red archivos e impresoras.
Shell Hardware Detection	Se utiliza para detectar dispositivos como ser algunas lectoras de CD o DVD.
System Event Notification	Se utiliza conjuntamente con el servicio de Sistema de sucesos COM+. Detecta y notifica a otros servicios cuando ocurren determinados eventos de sistema.
TCP/IP NetBIOS Helper	Habilita el soporte y resolución de nombres para NetBIOS sobre TCP/IP (NetBT).
Terminal Services	Permite que varios usuarios se conecten de forma interactiva a un equipo y que se muestren los escritorios y aplicaciones de equipos remotos. Servicio requerido para Escritorio Remoto y Asistencia Remota.
Windows Firewall/Internet Connection Sharing (ICS)	Provee traducción de direcciones de red, direccionamiento, resolución de nombres y/o prevención de intrusiones locales o de redes de pequeña oficina.
Windows Management Instrumentation	Proporciona una interfaz común y un modelo de objeto para tener acceso a la información de administración acerca de un sistema operativo, dispositivos, aplicaciones y servicios.
Windows Time	Automáticamente ajusta el reloj de un equipo conectándose a servidores de internet.
workstation	Crea y mantiene conexiones de un equipo con servidores remotos.



3.5.3 Revisiones de recursos compartidos en los servidores del GDS

Complementando a lo que se detalla en el procedimiento **PR15** del manual de políticas y procedimientos, se diría que los recursos compartidos existente en los servidores del GDS se los puede optimizar y dejar solo los necesarios, es recomendable utilizar el comando **net share** desde la línea de comandos para ver los recursos que se están compartiendo, así se podrá contabilizar todos los recursos compartidos de los servidores y así poder deshabilitar los innecesarios. Es recomendable seguir lo que se sugiere en el proceso **PR11** para crear recursos compartidos, además por cuestiones de seguridad contar con un solo directorio de recursos compartidos es lo ideal, donde se compartan solo lo necesario. Nunca se debe compartir carpetas del sistema, el disco duro de manera total o carpetas que contengan información crítica que vayan a comprometer la integridad del sistema operativo. En los recursos que se comparten en los servidores del GDS, se debe manejar políticas de asignación de permisos (**Ver PL08**).

3.5.4 Nivel de seguridad que deben mantener los servidores del GDS que están directamente conectados a Internet

El nivel de seguridad que deben mantener los servidores del GDS depende de varios factores como:

- ✓ Aplicar políticas de contraseñas fuertes.
- ✓ Todos los servidores del grupo y mayormente los que se conectan directo con el internet, deben mantener instalado un buen **antivirus**, (F-Secure, Kaspersky que son con los que cuenta la UTPL, también se puede utilizar otros que están disponibles en el internet).
- ✓ Se debe habilitar el registro de eventos
- ✓ Tener configurado un firewall lo suficientemente restrictivo para evitar ataques

3.5.5 Configuración de Políticas de Seguridad a nivel firewall para los servidores del GDS

Todos los servidores del GDS que están en conexión directa con el internet deben considerar algunas puntualizaciones a nivel firewall, a más de las mencionadas en los conceptos de las **descripciones generales que comprende un esquema de seguridad**, detalladas inicialmente en este capítulo, estas consideraciones son las siguientes:

- ✓ El firewall a configurar es el propio que trae incluido el sistema operativo Windows Server 2003.
- ✓ Incluir permisos para ejecutar antivirus a través del firewall
- ✓ Todos los puertos se deben cerrar para conexiones entrantes, excepto los que se especifiquen.
- ✓ Conexiones de salida a través del firewall deben cumplir reglas que permitan su salida al exterior, esto garantiza que se use puertos indicados y habilitados en el firewall dando así un mejor aislamiento y seguridad.



3.5.6 Recomendaciones sobre el número de cuentas de usuario que se debe tener por servidor en el GDS

Para el GDS se recomienda empezar gestionando las cuentas en cada servidor, así se inicia eliminando usuarios duplicados y cuentas innecesarias como son invitado, guest, pruebas, compartidos, departamentos, etc. Gestionadas las cuentas en cada servidor, se sugiere dejar las siguientes cuentas:

1. **Administrador:** Cuenta que tiene todos los privilegios sobre el sistema, la cual debe visualizarse con un nombre diferente al de "Administrador", se la debe renombrar. **Ver PR10**
2. **Crear Cuenta señuelo:** Es una cuenta que se utiliza de engaño para un atacante, **este tipo de cuenta no es operable y nunca debe de serlo** pues solo se crea por seguridad, igualmente el proceso de creación se describe en **PR10**.
3. **Crear Cuenta del tipo Administrador:** Es un tipo de cuenta que desempeña un papel similar al del administrador, este tipo de cuenta se crea por seguridad y es con la que se debe operar en los servidores del GDS en lugar de la cuenta Administrador.
4. **Crear Cuenta Usuario:** Es una cuenta que se crea para trabajar de manera cotidiana pues es aconsejable trabajar con cuentas que no sean administrativas la mayoría del tiempo, las cuentas tipo Administrador deben ser empleadas solo en casos determinados (crear otras cuentas, administrar cuentas, etc.). Para los servidores del GDS es una buena manera trabajar con cuentas tipo usuario, así se brinda un mayor nivel de seguridad a la integridad del sistema operativo de cada uno de los servidores.

3.5.7 Novedades de diseño en la creación de una línea base de seguridad para los servidores miembros del GDS

En los servidores del GDS las consideraciones que se han enmarcado en la creación de la línea base de seguridad son:

Servicios.- Se habilitan los servicios de Actualización automática, cliente DNS, reportes de cliente DNS, miembros de dominio, cliente FTP y cliente de red Microsoft.

Opciones Administrativas.- Los más básicos como reportes de errores, ayuda y soporte, instalación de aplicaciones locales, administración de escritorio remoto, administración remota de Windows y gestión de Backup.

Puertos.- Se deniegan todos excepto los que utilizan para FTP, Servicio de Correo, Servicios Web, NetBIOS, Bloque de mensajes de servidor (SMB), conexión remota, Active Directory, Base de Datos Oracle, Notificaciones, recursos compartidos y SQL Server 2000/2005.

Auditoría.- En lo concernientes a la auditoría se realiza el registro de eventos de cuenta, administración de cuentas, acceso a servicios de directorio, eventos de inicios de sesión, acceso a objetos, cambio de políticas, uso de privilegios, seguimiento de procesos y eventos del sistema.



Plantillas.- Finalmente se incluye una plantilla de seguridad, donde otorga un mayor nivel de seguridad a cada servidor del GDS y así se llega a constituir la línea base de seguridad, que debe de ser aplicada en todos los servidores del grupo.

Para ver el detalle de cómo se procede a la creación de la línea base de seguridad en un servidor miembro del grupo de servidores del GDS, se puede consultar el **ANEXO 3.5**, donde se describe todo el proceso de configuración.

3.6 PUNTUALIZACIONES

- ✓ Implementar un Esquema de Seguridad en plataformas Windows Server 2003 permite asegurar la información manejada dentro del entorno o ambiente donde se ha implementado el esquema.
- ✓ Un Esquema de Seguridad abarca una serie de consideraciones que se tiene que tener presente cuando se configura, pues una implementación de seguridad comprende todo lo relacionado con el aseguramiento de los sistemas operativos de los Servidores Windows, por ello todo el proceso de aseguramiento corresponde sólo al nivel lógico.
- ✓ Hay que recalcar que para realizar la implementación de un Esquema de Seguridad a nivel de Servidores que operan con la plataforma Windows Server 2003, las medidas de seguridad se deben considerar desde la instalación del sistema operativo en sí, luego se aplica parches, plantillas y demás software que de seguridad a todos los equipos del entorno.
- ✓ Los resultados obtenidos del Esquema de Seguridad determinan el nivel de seguridad de los servidores Windows del GDS, esto permitirá mantener e implantar una mejora continua del esquema.
- ✓ Al diseñar o plantear un Esquema de Seguridad, se debe considerar que un mayor nivel de seguridad afecta la rapidez del sistema por el hecho de que las seguridades elevadas consumen un mayor recurso de los equipos.

CAPITULO IV

EVALUACIÓN DE RESULTADOS DEL ESQUEMA DE

SEGURIDAD PARA EL GDS DE LA UTP

Objetivos

- Evaluar el funcionamiento correcto de todos los servidores virtuales que forman parte del Esquema de Seguridad
- Probar la funcionalidad básica de conexiones de red del Esquema de Seguridad implementado
- Analizar e interpretar los resultados obtenidos de la implementación del Esquema de Seguridad



4.1 INTRODUCCION

Por todos los servicios que presta, desarrolla y mantiene la Universidad Técnica Particular de Loja, los cuales hacen uso de muchos recursos informáticos que están operando bajo plataformas Windows Server 2003, se ha creído necesario implementar un Esquema de Seguridad que refuerce y fortalezca las seguridades de los servidores Windows con la finalidad de que la información que se maneje, mantenga la disponibilidad, integridad y confiabilidad, para de esa manera garantizar los activos de información de la UTPL.

Es por ello que en el presente capítulo con el uso de Máquinas Virtuales se prueba las configuraciones de seguridad que luego se pueden aplicar a los servidores Windows del GDS, otras de las finalidades de usar máquinas virtuales es para evaluar, probar, analizar e interpretar toda la implementación de seguridad realizada en el capítulo anterior y en base a estos análisis poder obtener resultados que permitan concluir y recomendar una serie de puntualizaciones que servirán de guía o referencia cuando se implemente en entornos reales y también sea un punto de apoyo para futuras implementaciones de Esquemas de Seguridad.

4.2 LABORATORIO

4.2.1 Descripciones Generales

Como todo el Esquema de Seguridad ha sido desarrollado sobre un entorno virtual, es importante describir información general tanto de la máquina que hace de host como de las características de la máquina virtual donde se tiene instalado Windows Server 2003 Enterprise Edition que es el sistema con los cuales operan los servidores del GDS.

✓ *Descripción de la máquina Host*

La máquina host o máquina contenedora de las máquinas virtuales, tiene las siguientes características tanto de hardware como de software:



Tabla 4.1. Detalles Hardware y Software de la máquina Host

Componente	Detalles
Procesador	AMD Turion(tm) 64 X2 Mobile Technology TL-56
Memoria (RAM)	1,94 GB
Gráficos	NVIDIA GeForce Go 6150
Disco duro principal	2GB disponible (96GB en total)
Unidad de medios (E:)	CD/DVD
Fabricante	Hewlett-Packard
Modelo	HP Pavilion tx1000 Notebook PC
Tipo de sistema	Windows Vista (TM) Home Premium. Sistema operativo de 32 bits
Número de procesadores principales	2
Compatible con 64 bits	Sí
Adaptador de red	Controladora de red NVIDIA nForce WLAN Broadcom 802.11a/b/g Virtual Machine Network Services Driver

✓ **Requisitos necesarios para instalar la máquina virtual**

La máquina virtual utilizada es Virtual PC 2007, que se puede instalar en cualquier equipo que satisfaga o supere los siguientes requisitos del sistema.

- ❖ Un equipo basado en x64 o en x86 con un procesador a 400 MHz o superior (se recomienda 1 GHz) y caché L2. Virtual PC es compatible con los procesadores AMD Athlon/Duron, Intel Celeron, Intel Pentium II, Intel Pentium III, Intel Pentium 4, Intel Core Duo e Intel Core2 Duo. Puede ejecutar Virtual PC en un equipo con varios procesadores, pero sólo se utilizará un procesador.
- ❖ Unidad de CD-ROM o DVD
- ❖ Se recomienda el uso de un monitor con resolución Super VGA (800 x 600) o superior
- ❖ Sistema operativo host: Windows Vista™ Business; Windows Vista™ Enterprise; Windows Vista™ Ultimate; Windows Server 2003, Standard Edition; Windows Server 2003, Standard x64 Edition; Windows XP Professional; Windows XP Professional x64 Edition o Windows XP Tablet PC Edition

✓ **Requisitos de creación de cada máquina virtual**

La configuración de Virtual PC para poder ejecutar distintos sistemas operativos en un equipo basado en x86 o x64, consta de los siguientes pasos:



- ❖ Los requisitos mínimos que debe satisfacer el sistema para que se pueda implementar correctamente Virtual PC variarán según el número y el tipo de sistemas operativos invitados, y las aplicaciones que desee instalar en los equipos virtuales.
- ❖ Para ejecutar varios equipos virtuales simultáneamente, el equipo físico deberá tener al menos la memoria suficiente para cubrir los requisitos del sistema operativo host y cada sistema operativo invitado que se vaya a ejecutar simultáneamente.

La creación de los equipos virtuales tienen las siguientes características:

Tabla 4.2. Descripción de máquinas virtuales

Nombre del Servidor	Sistema Operativo a Instalar	RAM	Espacio en disco
ASUTPL	Windows Server 2003 Enterprise Edition	256 MB	3 GB
BDDGDS	Windows Server 2003 Enterprise Edition	256 MB	3 GB
CALSERVER	Windows Server 2003 Enterprise Edition	256 MB	3 GB
CATAMAYO	Windows Server 2003 Enterprise Edition	256 MB	3 GB
DEVCRM	Windows Server 2003 Enterprise Edition	256 MB	3 GB
DEVGDS	Windows Server 2003 Enterprise Edition	256 MB	3 GB
DEVSERVER (BDC)	Windows Server 2003 Enterprise Edition	512 MB	8 GB
DIGITSERVER	Windows Server 2003 Enterprise Edition	256 MB	3 GB
NODO1SGA	Windows Server 2003 Enterprise Edition	256 MB	3 GB
PDCSERVER (PDC)	Windows Server 2003 Enterprise Edition	512 MB	8 GB
TSTSERVER	Windows Server 2003 Enterprise Edition	256 MB	3 GB
WSUTPL	Windows Server 2003 Enterprise Edition	256 MB	3 GB

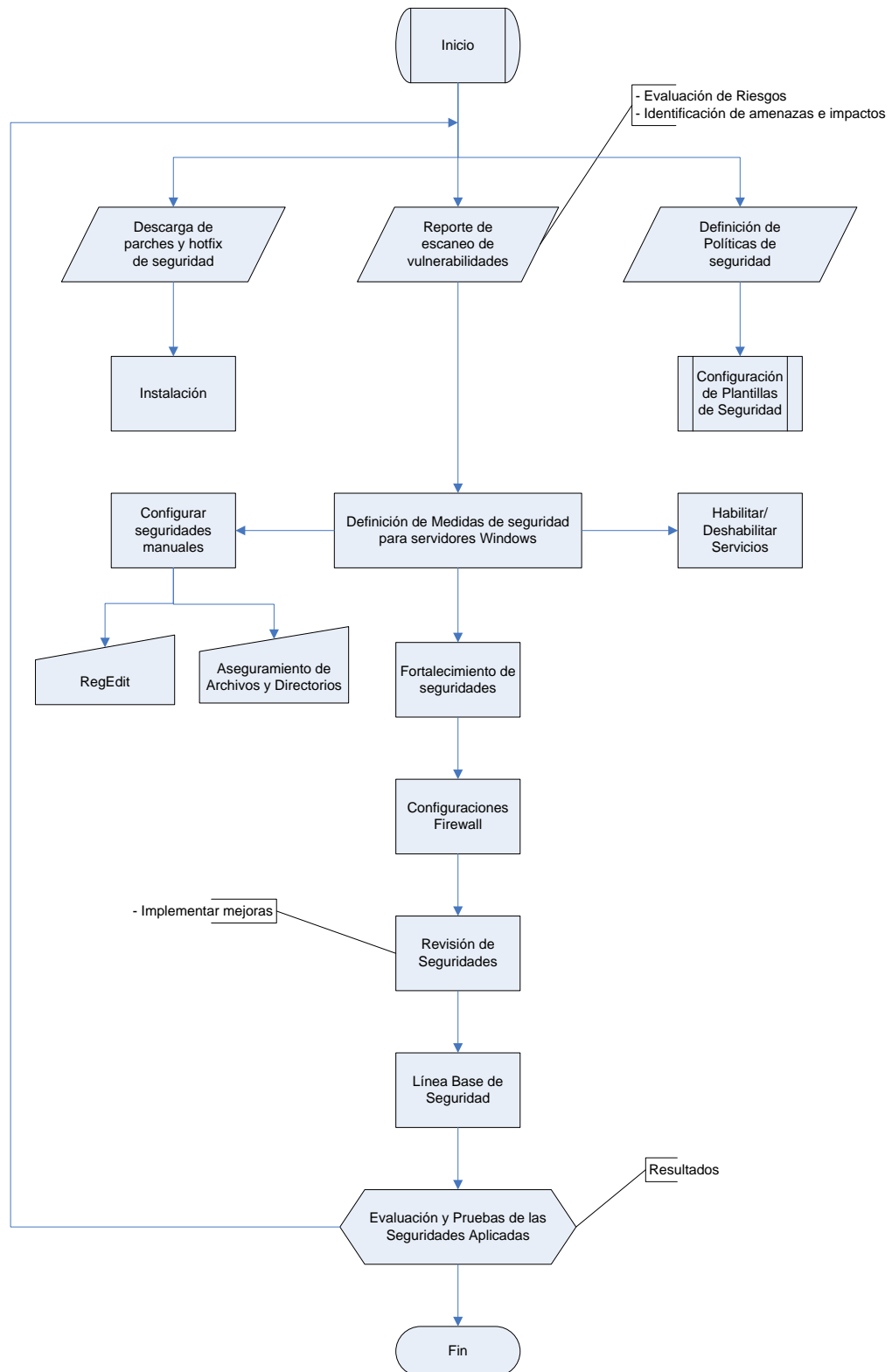
4.2.2 Desarrollo

Se pretende detallar todo el proceso que se debe seguir para esquematizar las seguridades de las plataformas Windows server 2003 Enterprise Edition en un entorno virtual con la finalidad de probar todas las configuraciones antes de ser implementadas en un ambiente real.

Todo el proceso de implementación que se ha seguido desde un inicio hasta la finalización, se describe en el siguiente flujograma.



Figura 4.1. Detalle del proceso de implementación de seguridades en las plataformas Windows





4.2.3 Herramientas Utilizadas

Las herramientas utilizadas para la elaboración del esquema de seguridad son todas las que están disponibles con el sistema operativo Windows Server 2003 y las herramientas que no vienen en el CD de instalación se las puede descargar de manera gratuita desde la Web de la empresa Microsoft. Además también se utilizan herramientas de terceros, para evaluar y escanear las vulnerabilidades del Windows Server 2003 y así poder ir mejorando los niveles de seguridad de un servidor que está inmerso en un esquema de seguridad.

Tabla 4.3. Herramientas utilizadas en la implementación del Esquema de Seguridad

Herramienta	Descripción
Virtual PC 2007	Puede crear y ejecutar uno o más equipos virtuales, cada uno con su propio sistema operativo, en un solo equipo físico
Security Configuration Wizard (SCW)	Esta incorporado en el SP1 de Windows Server 2003, permite configurar de forma rápida y fácil los servidores basados en Microsoft Windows de acuerdo con sus requerimientos funcionales
Editor de configuración de seguridad (ECS)	Se utilizan para definir plantillas de directiva de seguridad que se pueden aplicar a equipos individuales o a grupos de equipos a través de la directiva de grupo de Active Directory
Microsoft Management Console (MMC)	Puede usarse para administrar redes, equipos, servicios, aplicaciones y otros componentes del sistema
Group Policy Management Console (GPMC)	Es un conjunto de interfaces de secuencias de comandos que se pueden utilizar para administrar la directiva de grupo, hacer copias de seguridad y administrar de manera simplificada la seguridad relacionada con la directiva de grupo
Plantillas de Seguridad (.inf)	Son archivos de texto que usan un formato estándar para configurar directivas de seguridad a Windows Server 2003.
RETINA Network Security Scanner	Herramienta utilizada para evaluar las vulnerabilidades de un sistema operativo y de la red.
Microsoft Baseline Security Analyzer (MBSA)	Herramienta examina equipos basados en Windows para buscar configuraciones de seguridad incorrectas
GFI LANguard Network Security Scanner	Herramienta que permite buscar, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de una red.
IIS Lockdown Tool 2.1	Herramienta para deshabilitar características innecesarias reduciendo así el campo de ataque
NetPeeker 3.10	Es una herramienta para monitorear y controlar la red

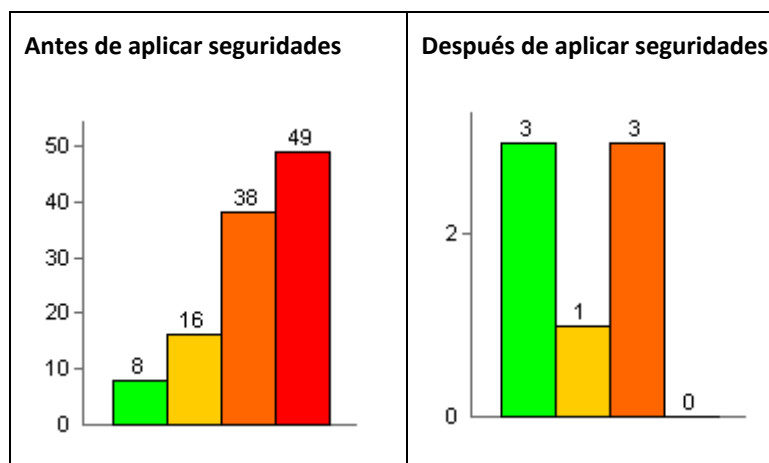
4.2.4 Evaluación

Lo que se evalúa en un esquema de seguridad son todas las configuraciones de seguridad que se han configurado, para así determinar si se ha disminuido la superficie de ataque de un sistema operativo, no existe método formal en particular para evaluar cuán bien configuradas están las seguridades de un servidor, PC o equipo en particular, en su defecto se **utilizan herramientas escáner** que permiten comprobar y alertar acerca de lo que se ha configurado y lo más idóneo a configurar, el Esquema de



seguridad que se implementa en máquinas virtuales, en cierta medida se comprueba mediante el uso de las herramientas del propio Windows Server 2003 y mediante el uso de la herramienta Retina Network Security Scanner que muestra las siguientes vulnerabilidades antes y después de haber aplicado las seguridades.

Tabla 4.4. El antes y después de aplicar seguridades a un Sistema Operativo Windows Server 2003



4.2.5 Resultados

De igual forma y partiendo del apartado de la **evaluación**, se llega a obtener los siguientes resultados:

En cuanto a la configuración de las políticas de contraseñas, se puede observar en figura siguiente que no existen muchos cambios a excepción de la longitud del password esencial para la autenticación de un usuario en Windows Server 2003, el resto de configuraciones tanto las que se configuran por defecto cuando se instala el sistema operativo como las que se aplican son iguales.

Policy	Database Setting	Computer Setting
Enforce password history	24 passwords remembered	24 passwords remembered
Maximum password age	42 days	42 days
Minimum password age	1 days	1 days
Minimum password length	12 characters	7 characters
Password must meet complexity requirements	Enabled	Enabled
Store passwords using reversible encryption	Disabled	Disabled

Figura 4.2. Comparación de políticas configuradas de las aplicadas

En lo que se refiere a las configuraciones de las políticas de auditoría en un servidor, existe una gran variación a las que se configuran por defecto al instalar el sistema, a continuación en la figura se puede constatar tal hecho.



Policy	Database Setting	Computer Setting
Audit account logon events	Success, Failure	Success
Audit account management	Success, Failure	No auditing
Audit directory service access	Success, Failure	No auditing
Audit logon events	Success, Failure	Success
Audit object access	Success, Failure	No auditing
Audit policy change	Success	No auditing
Audit privilege use	Success, Failure	No auditing
Audit process tracking	Not Defined	No auditing
Audit system events	Success	No auditing

Figura 4.3. Cambios en las políticas de auditoría al configurar seguridades en un servidor Windows

Como se puede observar en las figuras anteriores, que realizar configuraciones de seguridad en un servidor que opera con Plataformas Windows Server 2003 Enterprise Edition es relevante por el hecho de que tales seguridades en verdad si fortalecen la seguridad en los servidores, pero hay que recalcar que a mayor nivel de seguridad que se configure en un servidor Windows, existe mayor consumo de recursos y por lo tanto implica mayor coste aunque la seguridad mejore, para explicar gráficamente este hecho se tiene la siguiente figura.

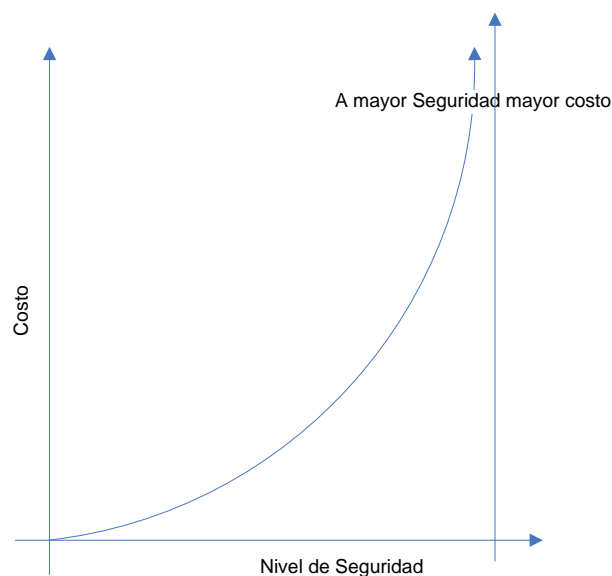


Figura 4.4. Relación Costo grado de seguridad

4.3 PASOS SEGUIDOS EN LA EVALUACIÓN Y PRUEBAS DE FUNCIONALIDAD DEL ESQUEMA DE SEGURIDAD DE LOS SERVIDORES VIRTUALES WINDOWS SIMILARES A LOS DEL GDS

Lo que se pretende con las pruebas del esquema de seguridad de los servidores Windows del GDS, es garantizar que las configuraciones de seguridad de los servidores hayan sido realizadas de manera correcta, sin afectar la funcionalidad de éstos.

Antes de realizar las pruebas es conveniente tomar en cuenta las siguientes consideraciones:



- ✓ Comprobar la conexión de red de todos los servidores Windows Virtuales
- ✓ Ejecutar pruebas básicas de configuraciones de comunicación de los servidores en red, mediante la utilización del comando **ping**.
- ✓ Verificar que los servidores miembros se han integrado correctamente al Controlador de Dominio
- ✓ Verificar que todos los servicios y software necesario está instalado en cada servidor miembro del dominio **utpl.edu.ec**.
- ✓ Comprobar el registro de eventos de todos los servidores Virtuales para cerciorarse de que no existan errores del sistema por configuraciones erróneas.
- ✓ Realizados los pasos anteriores, es recomendable sacar una imagen individual del sistema operativo de cada servidor, con la finalidad de revertir a un estado inicial y funcional el sistema, ocasionado por efecto de malas configuraciones de seguridad, así se retornaría a una línea de configuración base antes de iniciar un ciclo de pruebas nuevo.

Una vez que se ha cumplido con los pasos previos a la realización de las pruebas, se ha procedido a lo siguiente:

- ✓ Aplicar las plantillas de seguridad a nivel de dominio, a nivel de controlador de dominio y finalmente a nivel de servidores miembros del dominio **utpl.edu.ec**.
- ✓ Aplicadas las plantillas de seguridad el paso siguiente es verificar las configuraciones manuales, estas configuraciones se las suele realizar desde la Consola de Administración Microsoft (MMC), lo que se verifica es:
 1. Las cuentas de Administrador local en cada servidor deben tener un password fuerte, (**ver PL02**) que se ha cambiado su nombre y que se le ha quitado la descripción de cuenta predeterminada.
 2. Cambiar el nombre de las cuentas de invitados en todos los servidores miembros y asegurarse de que estén deshabilitadas.
- ✓ Verificar las configuraciones que se hacen en el Registro de Windows, todas esas configuraciones se las hace manualmente y se las debe configurar en todos los servidores.

Una vez que se ha verificado las configuraciones manuales, se procede a comprobar todo en forma individual y conjunta de todos los servidores. El objetivo de realizar pruebas al Esquema de Seguridad es:

- ✓ Asegurarse de que no hayan eventos que afecten a aplicaciones que se ejecutan en cada servidor. Así como también evaluar procesos que refuerzan la seguridad, pero que afectan el rendimiento del servidor.
- ✓ Pérdidas de disponibilidad de información y servicios que dan conexión de red.



Para probar la funcionalidad del Esquema de seguridad se hace uso de **Tablas de Prueba**³⁷, donde se utiliza determinados parámetros que permiten evaluar todas las configuraciones de seguridad realizadas en el Esquema de Seguridad para los servidores Virtuales Windows.

4.4 ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS OBTENIDOS DE LAS PRUEBAS DE FUNCIONALIDAD DEL ESQUEMA DE SEGURIDAD

El Esquema de Seguridad propuesto para los servidores Virtuales Windows 2003, brinda un alto nivel de seguridad en comparación con los test descritos en el **ANEXO 4.2** realizados en un inicio, antes de aplicar las seguridades correspondientes en cada servidor. Para los test de escaneo se hace uso de las herramientas MBSA y RETINA - NETWORK SECURITY SCANNER.

Describiendo de una mejor manera los test realizados con la herramienta RETINA que permite tener un conocimiento a nivel de porcentaje de las vulnerabilidades en los sistemas operativos Windows, se tiene tres tipos de resultados que se han basado en el **escaneo de Windows Server 2003 Enterprise Edition sin configuración de seguridad alguna y sin ningún nivel de Service Pack**, luego se **escanea las vulnerabilidades del sistema operativo Windows del servidor NODO1SGA del entorno de producción del GDS** y finalmente se **escanea al Windows Server 2003 con todas las seguridades, actualizaciones, hotfix y Services Packs instalados y configurados**, lo que permite observar y constatar cómo se maneja la seguridad en Windows Server 2003 Enterprise Edition desde su instalación hasta que aplica las respectivas seguridades. A continuación se analiza e interpreta de manera particular caso por caso, los resultados obtenidos con la herramienta RETINA del Esquema de Seguridad.

Hay que indicar que para obtener los datos de la Figura 4.5 y 4.7, el sistema operativo Windows Server 2003, se instaló en una máquina virtual con la finalidad de evitar contratiempos y agilizar de esa manera los escaneos de las vulnerabilidades.

Análisis de resultados de Windows Server 2003 Enterprise Edition sin aplicar seguridades

Se analiza al Windows Server 2003 recién instalado y sin configurar seguridades de ninguna índole, con la finalidad de darse cuenta de los riesgos que se corre al dejar al sistema tal cual se lo instala, lo que no es aconsejable bajo ningún concepto para entornos donde se está en conexión directa al internet.

³⁷ Testeo de configuraciones de seguridad de los servidores del GDS ver **Anexo 4.1**

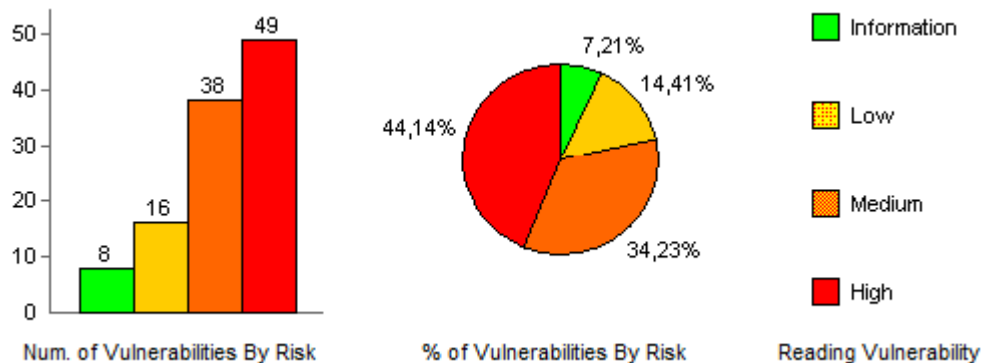


Figura 4.5. Resultados de análisis de Windows Server 2003 sin seguridades configuradas

La figura muestra que existe un gran número de vulnerabilidades altas, medias y bajas que dan de manera conjunta al sistema un riesgo muy elevado, el porcentaje de vulnerabilidades de alto riesgo representa la mayor cantidad de agujeros que pueden ser aprovechados por hackers para perpetrar un ataque al sistema y por medio de ello robar o alterar los datos que se almacene en dicho equipo. Existe de igual manera una cantidad de vulnerabilidades concernientes a datos informativos que en definitiva no comprometen la integridad del sistema, pues solo son alertas de ciertos programas que suelen generar al instalarse en un sistema operativo.

Análisis de resultados de Windows Server 2003 Enterprise Edition en el entorno de producción del GDS de la UTPL

Los resultados que en la figura se muestran, están basados en el escaneo de un servidor físico del entorno de producción del GDS (NODO1SGA).

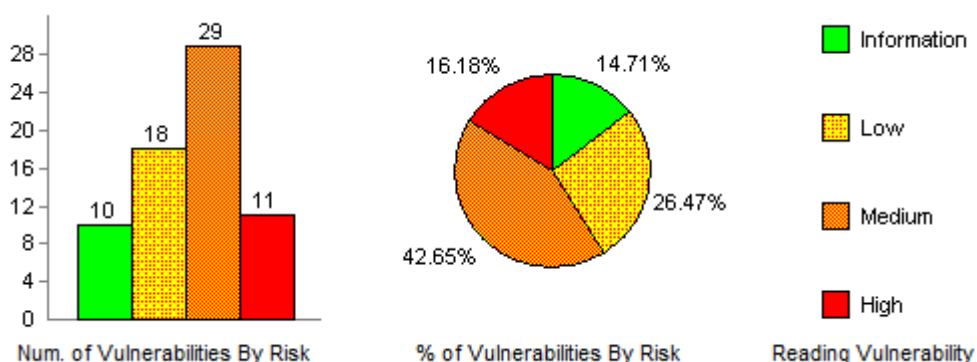


Figura 4.6. Datos informativos de las vulnerabilidades de seguridad del servidor NODO1SGA del entorno de producción del DGS de la UTPL

Analizando la figura, se puede observar que existe un nivel, si bien es cierto no elevadamente alto de vulnerabilidades peligrosas, pero suficientes para que un hacker realice un ataque. De igual forma se puede decir que si existe un alto porcentaje de vulnerabilidades que conllevan un riesgo medio, así



como también se identifican vulnerabilidades de bajo riesgo y vulnerabilidades de información que el sistema operativo posee, generalizando, pues se tiene que tales vulnerabilidades conllevan un riesgo inminente tanto para el sistema operativo como para los datos que se almacenan en los servidores del GDS.

Aplicando seguridades a los servidores del GDS se trata de eliminar las vulnerabilidades de alto medio y bajo riesgo para el sistema operativo, con lo que se evita y protege la información que se almacena en tales servidores y así garantizar la autenticidad, integridad y disponibilidad de la información.

Todas las vulnerabilidades que visualiza el servidor NODO1SGA se mitigan instalando las actualizaciones de seguridad y hotfix que la empresa Microsoft libera cada mes, además se disminuye vulnerabilidades aplicando políticas de seguridad que se describen en el **Manual de Políticas y Procedimientos General** que se adjunta a esta tesis.

Análisis de resultados de Windows Server 2003 Enterprise Edition con todas las seguridades configuradas

Evaluando la aplicación de seguridades al sistema operativo Windows Server 2003 Enterprise Edition, se puede observar un gran cambio y disminución en el número de vulnerabilidades a cuando no se aplicaban o cuando se mantiene el sistema desactualizado.

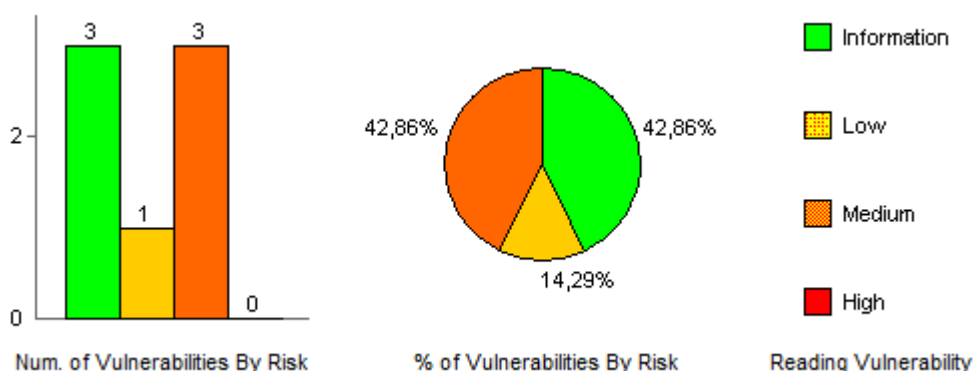


Figura 4.7. Resultado del análisis de Windows Server 2003 con seguridades configuradas

Analizando los datos que muestra la figura se tiene que no existen vulnerabilidades de alto riesgo, lo que existe son tres vulnerabilidades de riesgo medio, y una vulnerabilidad de riesgo bajo, las otras tres vulnerabilidades corresponden a alertas generadas por el mismo escáner de vulnerabilidades, por lo que se puede concluir que las configuraciones de seguridad están en lo correcto, solo que hay



que realizar una revisión e instalar los hotfix complementarios que son utilizados por la maquina virtual como por el mismo escáner.

El Esquema de Seguridad controla y da seguimiento a muchas tareas tales como:

- ✓ Cuando se inicia sesión en los servidores miembros no se presenta el último usuario que inicio sesión en el servidor.



Figura 4.8. No presentación del último usuario logeado en el sistema

- ✓ Cuando se cambia la contraseña se exige que se cumpla las políticas de seguridad que se han configurado.



Figura 4.9. Cumplimiento de políticas fuertes de cambio de contraseñas

- ✓ Se han deshabilitado las cuentas invitado, se ha renombrado la cuenta Administrador y se ha creado una cuenta señuelo de Administrador útil para evitar ataques.

Name	Full Name	Description
Administrator	Administrador señuelo	Built-in account for administering the computer/domain
Asutpldiego	Administrador	Built-in account for administering the computer/domain
Otro		Built-in account for guest access to the computer/domain
SUPPORT_38...	CN=Microsoft Corporat...	This is a vendor's account for the Help and Support Service

Figura 4.10. Cumplimiento de políticas de deshabilitación de cuentas



- ✓ Se habilitan los servicios mínimos en cada servidor para que lleven a cabo sólo tareas específicas, al igual que se deshabilitan servicios innecesarios con lo que se reduce la superficie de ataque y así se evita pérdida de información.
- ✓ Se exige al usuario que utilice contraseñas fuertes cuando inicia sesión en un servidor
- ✓ Se detalla estrategias de configuración de firewalls
- ✓ Se recomienda mantener actualizado el sistema operativo con los últimos parches de seguridad
- ✓ Se mejora la seguridad, utilización de los recursos informáticos, accesibilidad a la información de manera protegida, mayor fiabilidad y estandarización para configurar las seguridades.
- ✓ El Esquema de Seguridad centraliza la administración de los servidores, gracias al uso de Active Directory que trae un conjunto de utilidades para la administración
- ✓ El Esquema de Seguridad consolida a cada servidor de manera individual de acuerdo al rol o escenario de cada servidor.
- ✓ En el Esquema de Seguridad se considera todo lo concerniente a la seguridad lógica de los servidores Windows, sobre los cuales se aplica una serie de políticas de seguridad con la finalidad de cumplir con los conceptos de disponibilidad, autenticidad y fiabilidad de la información.

4.5 CHECKLIST A CONSIDERAR EN LA CONFIGURACIÓN DE SEGURIDAD DE UN SERVIDOR WINDOWS SERVER 2003



CHECKLIST DE LO QUE DEBERÍA TENER INSTALADO Y CONFIGURADO UN SERVIDOR WINDOWS MIEMBRO DE UN DOMINIO			
Concepto	Descripción	Instalado	No Instalado
Parches y actualizaciones de sistema y antivirus	<ul style="list-style-type: none"> ✓ Últimas actualizaciones, parches y hotfix ✓ Antivirus ✓ Suscribirse a las notificaciones de seguridad de Microsoft. Para suscribirse vaya al siguiente enlace: http://www.microsoft.com/technet/security/bulletin/notify.asp. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Servicios	<ul style="list-style-type: none"> ✓ Deshabilitar servicios innecesarios ✓ Servicios que se ejecutan con menos privilegios 	<div style="text-align: center;">Configurado</div> <input type="checkbox"/> <input type="checkbox"/>	<div style="text-align: center;">No Configurado</div> <input type="checkbox"/> <input type="checkbox"/>
Protocolos	<ul style="list-style-type: none"> ✓ Se ha fortificado la pila TCP/IP ✓ Se ha asegurado los puertos utilizados por NetBIOS y SMB 	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Cuentas	<ul style="list-style-type: none"> ✓ Cuentas no utilizadas se han eliminado del servidor ✓ La cuenta de invitado esta deshabilitada en el servidor ✓ Se ha renombrado la cuenta de administrador e invitado ✓ Se ha creado una cuenta denominada "tonta" del administrador, para monitorear futuros ataques ✓ Se han empleado políticas de contraseñas fuertes para la cuenta administrador, como para las de usuario. ✓ Las cuentas no se comparten entre administradores ✓ Sesiones nulas o anónimas están deshabilitadas ✓ Usuarios y administradores no comparten cuentas ✓ No deben existir más de dos cuentas miembros del grupo administrador. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Archivos y Directorios	<ul style="list-style-type: none"> ✓ Los archivos y directorios están contenidos en volúmenes que han sido formateados con el sistema de archivos NTFS. 	<input type="checkbox"/>	<input type="checkbox"/>
Compartir	<ul style="list-style-type: none"> ✓ Todos los recursos compartidos innecesarios se quitan, inclusive los recursos compartidos por defecto. ✓ El acceso a recursos compartidos requeridos debe ser limitado, los usuarios que pertenecen al grupo todos (todo el mundo) no deben tener acceso. ✓ Recursos compartidos administrativos (C\$ y Admin\$) se deben quitar si no se necesitan. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Puertos	<ul style="list-style-type: none"> ✓ Si un servidor esta en conexión directa con Internet, se debe habilitar los puertos 80 y 443. ✓ Encriptar el tráfico o restringirlo si no se cuenta con una infraestructura segura. 	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Registro	<ul style="list-style-type: none"> ✓ El acceso remoto al registro debe de estar restringido. ✓ SAM es asegurado bajo la clave de registro (HKLM\System\CurrentControlSet\Control\LSA\NoLMHas h) 	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Auditar y registrar	<ul style="list-style-type: none"> ✓ Auditar intentos de inicio de sesión fallidos ✓ Asegurar archivos log ✓ Configurar el tamaño apropiado de los archivos log, según los requerimientos de seguridad de las aplicaciones. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Sitios y directorios virtuales	<ul style="list-style-type: none"> ✓ Las particiones que albergan sitios Web se deben configurar en particiones que no estén albergando al sistema operativo. ✓ Los Paths padres se configurar en deshabilitados 	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Código de acceso de seguridad	<ul style="list-style-type: none"> ✓ La seguridad de acceso al servidor debe estar habilitada ✓ Permisos por defecto de la intranet deben ser retirados ✓ Permisos por defecto para usuarios de zonas de Internet deben de ser retirados 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Otros puntos a comprobar	<ul style="list-style-type: none"> ✓ Instalar IISLockdown en cada servidor ✓ Instalar y configurar URLScan ✓ La administración remota del servidor debe de habilitar y configurarse bajo encriptación. ✓ Software detector de vulnerabilidades (MBSA³⁸) ✓ Firewall 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

³⁸ MBSA: Software que permite explorar vulnerabilidades en Sistemas Windows Server



4.6 PUNTUALIZACIONES

- ✓ Se ha probado las conexiones de red, habiendo conexión y comunicación entre todos los servidores del GDS.
- ✓ Todas las políticas y procedimientos del Esquema de Seguridad están detalladas en el **Manual de Políticas y Procedimientos General** donde existen políticas y procedimientos seguidos para el entorno de servidores del GDS.
- ✓ Las políticas, procedimientos y configuraciones de seguridad se pueden aplicar a otros entornos de servidores que estén operando con la plataforma Windows Server 2003, en cambio para otros servidores, se puede utilizar algunos procedimientos, políticas y configuraciones como referencia o con sus debidas modificaciones para que se ajusten a las necesidades de ese server.
- ✓ Se analizó los resultados que el Esquema de Seguridad proporciona, pudiendo constatar que en realidad las configuraciones de seguridad fortalecen la integridad del sistema Windows Server 2003, cabe recalcar que el esquema de seguridad propuesto ha sido probado en un entorno de maquinas virtuales.
- ✓ Un Esquema de Seguridad, debe cumplir con los propósitos para las cuales ha sido elaborado, pero siempre hay que mantener un continuo mantenimiento y actualización ya que la seguridad es un proceso.
- ✓ En la evolución informática cada día se está innovando nuevas herramientas, nuevas aplicaciones, nuevas políticas de seguridad, por lo que la elaboración de un esquema de seguridad a nivel de sistemas operativos de servidor, solo es el inicio de una tarea que se la debe ir realizando conforme evoluciona el internet y tecnología en particular.

CONCLUSIONES Y RECOMENDACIONES



5.1 CONCLUSIONES

- ✓ Esta investigación es un proceso de aseguramiento a nivel lógico de la plataforma Windows Server 2003 Enterprise Edition, y es un punto de referencia o partida para futuras investigaciones en el área de aseguramiento de la información en servidores. Windows Server 2003 es uno de los sistemas con un nivel de seguridad bastante aceptable, aunque su predecesor Windows Server 2008 es un sistema que incorpora e integra muchas más funcionalidades y seguridades que Windows Server 2003 no tiene, pero aun no adquiere la suficiente popularidad por el momento.
- ✓ Este Esquema de Seguridad se puede adaptar a otros entornos de servidores Windows, pero con las debidas modificaciones que se necesiten realizar acorde a la situación empresarial donde se desee implantar, es así que para entornos con Windows Server 2008 se puede adoptar este esquema. Las configuraciones de firewalls, políticas de cuenta, políticas de auditoría, políticas de asignación de derechos de usuario y opciones de seguridad son las cosas que más se adaptan y pueden ser aplicados a otros entornos Windows.
- ✓ La investigación realizada para la elaboración del Esquema de seguridad, permite conocer de una manera más descriptiva como fue la evolución de la seguridad en las plataformas Windows en sus diferentes versiones, de las cuales las versiones para servidores son las que mejor han evolucionado en cuanto a la seguridad, cada vez integran sistemas de autenticación fuertes, gestionan de una mejor manera las cuentas de usuario, facilitan el manejo de políticas de seguridad, incluyen utilidades de encriptación de datos, incorporan protocolos de seguridad a nivel de red y brindan servicios de firewall avanzado.
- ✓ La seguridad en Plataformas Windows de escritorio ha mejorado a un gran nivel, Windows Vista incluye para la seguridad el **Control de Cuenta de Usuario (UAC)**, **Sistema de cifrado de archivos (EFS)**, **Cifrado de Unidad BitLocker**, **Servicios de Módulo de Plataforma Segura (TPM)** y **Windows Defender**, que en comparación con Windows 98 y Windows Millennium no incluyen tales componentes de seguridad mencionados, pero Windows Vista tiene una acogida del **11.30%** que es baja en comparación con Windows XP que es el que mayor acogida tiene con un **74.31%** por parte de los usuarios finales, e igualmente cuenta con seguridades basadas en grupos, sistema de cifrado y control de acceso a nivel de archivos, que hacen que la seguridad del XP sea bastante aceptable, aunque no igual a la de Windows Vista. Las estadísticas de los



sistemas operativos más utilizados hasta el mes de agosto del presente año, están disponibles en <http://www.w3counter.com/globalstats.php>

- ✓ Lo más importante a fortalecer en las plataformas Windows Server 2003 es la pila TCP/IP que es la que posee algunas vulnerabilidades por donde un intruso puede infiltrarse y perpetrar un ataque, otro punto que se debe configurar con valores correctos son los niveles de autenticación de usuarios basados en contraseñas, para así evitar ataques de fuerza bruta y con ello disminuir las vulnerabilidades en el sistema.
- ✓ En las plataformas Windows Server 2003 la mejor manera de aplicar seguridades es mediante la utilización de plantillas de seguridad las cuales permiten configurar una serie de políticas de seguridad a ser aplicadas en un servidor.
- ✓ En este proyecto también se ha utilizado herramientas de escaneo de vulnerabilidades de un sistema operativo Windows, las cuales son: MBSA (Microsoft Baseline Security Analyzer), Retina Network Security Scanner y GFI LANguard Network Security Scanner que han permitido identificar las diferentes vulnerabilidades y configuraciones de seguridad que se deben realizar en un servidor que tiene instalado el sistema operativo Windows Server 2003. Los escaneos con la herramienta Retina dan la cifra de **44.14%** de alto riesgo en Windows Server 2003 sin configurar seguridad alguna, de igual forma se tiene la cifra de **16.18%** de alto riesgo del sistema operativo del servidor NODO1SGA que está en producción y finalmente cuando se aplican seguridades al sistema operativo se tiene un **0%** de alto riesgo del sistema en general.
- ✓ Mediante la elaboración del Esquema de Seguridad, se llega a conocer todo el proceso que se debe seguir desde la instalación del sistema operativo en el servidor hasta aplicar las configuraciones de seguridad de acuerdo al rol y funcionalidad de cada servidor dentro de un entorno empresarial.
- ✓ El objetivo primordial de un Esquema de Seguridad es llegar a tener una línea base de seguridad para un conjunto de servidores o equipos que estén trabajando con la plataforma Windows Server 2003, Windows XP o futuras versiones Windows y sobre esa base seguir un proceso evolutivo de seguridad con la finalidad de mantener una consistencia en el tiempo.
- ✓ El Esquema de Seguridad ha sido implementado y probado en un ambiente de maquinas virtuales, con la finalidad de evitar contratiempos cuando se implemente en entornos de producción. Las pruebas de funcionalidad correctas del DNS, Controladores de Dominio,



conexión de red y aplicación de políticas de seguridad del Esquema de Seguridad permiten confirmar que en verdad las configuraciones se han realizado de manera correcta, inicialmente por lo general se generan errores, pero paulatinamente se va configurando tareas complementarias hasta dejar estabilizada la solución.

- ✓ El Esquema de Seguridad no cubre el aseguramiento de aplicaciones instaladas en un servidor, es un Esquema de Seguridad orientado netamente a fortalecer la seguridad de las plataformas Windows, por tal motivo todas las políticas y algunos procedimientos descritos en el **“Manual de Políticas y Procedimientos General”** son aplicables a otras plataformas Windows.
- ✓ Esta tesis complementada con otros trabajos relacionados a la seguridad puede contribuir al desarrollo de otras investigaciones, porque cubre varios aspectos como es la mejora de la seguridad en conexiones de red, cumplimiento de políticas de autenticación y gestión de usuarios, mejor aseguramiento de archivos del sistema, técnicas de configuración del firewall así como también manejo de actualizaciones del sistema. Con lo que se garantizará que se llegue a obtener proyectos de mejor calidad en temas concernientes a la seguridad de la información.

5.2 RECOMENDACIONES

- ✓ En algún momento futuro, cuando se quiera hacer configuraciones adicionales en el Esquema de Seguridad o se lo quiera actualizar, se recomienda hacer todas las configuraciones que se desee valiéndose de las propias herramientas que ofrece Microsoft.
- ✓ Cuando se aplique seguridades a un servidor Windows utilizando plantillas se lo debe de realizar de manera gradual, con la finalidad de no afectar el sistema o inhabilitarlo y luego no poder volver a un estado funcional.
- ✓ Siempre se recomienda sacar imágenes funcionales del sistema operativo luego que se han instalado los Service Pack y hotfix que contribuyen con actualizaciones para las plataformas Windows. Las imágenes permitirán volver al sistema a un estado funcional en caso de ocurrir errores en las configuraciones de seguridad.



- ✓ Se debe acoger y hacer cumplir las políticas de seguridad que se recomienda en el Esquema de Seguridad, es decir que se debe crear una cultura entre los usuarios para que usasen las recomendaciones básicas de seguridad (políticas de contraseñas fuertes) que ayuden a evitar ataques de hackers o personas que quieran perpetrar algún robo de los activos de información que manejan los servidores Windows del GDS.

- ✓ Vale recordar que **la Seguridad de la Información siempre será un proceso conjunto que involucra a todas las personas que de una u otra manera interactúan con una organización.**

BIBLIOGRAFIA

CONCEPTOS BÁSICOS

- ✓ [Windows 2000 Server – SEGURIDAD, 2007]. Windows 2000 Server – SEGURIDAD, (2007). Facultad de Ciencias Exactas y Naturales y Agrimensura. Windows 2000 Server – SEGURIDAD. [En línea:][Consultado: lunes 29 de octubre de 2007]. Disponible en Internet: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGW01/CENTRAL_INTRO.htm
- ✓ [Descripción general de Windows NT Server, 2002]. Descripción general de Windows NT Server, (2002). Francia. INTRODUCCION A WINDOWS NT SERVER [En línea:] [Consultado: miércoles 31 de octubre de 2007]. Disponible en Internet: <http://cpys.iespana.es/cpys/winnt/2.pdf>
- ✓ [Windows NT, 2002]. Windows NT, (2002). Miguel Pino. La seguridad en Windows NT es una combinación de técnicas que aseguran un nivel de protección consistente contra los accesos no deseados [En línea:] [Consultado: miércoles 31 de octubre de 2007]. Disponible en Internet: <http://www.monografias.com/trabajos10/destem/destem.shtml?relacionados>
- ✓ [Introducción a Windows NT, 2005]. Introducción a Windows NT, (2005). Wikilearning. Introducción a Windows NT - ADMINISTRACIÓN DE CUENTAS: AUTENTIFICACIÓN DE INICIO DE SESIÓN [En línea:] [Consultado: martes 30 de octubre de 2007]. Disponible en Internet: http://www.wikilearning.com/curso_gratis/introduccion_a_windows_nt-administracion_de_cuentas_autenticacion_de_inicio_de_sesion/3789-8
- ✓ [Seguridad en Windows Server 2003, 2003]. Seguridad en Windows Server 2003, (2003). Microsoft Corporation. Paper de Seguridad en Windows Server 2003. [En línea:][Consultado: martes 20 de noviembre de 2007]. Disponible en Internet: <http://download.microsoft.com>
- ✓ [ALEGSA, 1998-2007]. ALEGSA, (1998-2007). ALEGSA. DICCIONARIO DE INFOMÁTICA, INTERNET Y TECNOLOGÍAS - Información y significado de Windows. [En línea:][Consultado: miércoles 23 de enero de 2008]. Disponible en Internet: <http://www.alegsa.com.ar/Dic/windows.php>
- ✓ [Configurar equipos, 2007]. Configurar equipos, (2005). Josito. Diferencias entre versiones de Windows [En línea:] [Consultado: jueves 24 de enero de 2008]. Disponible en Internet: <http://www.configurarequipos.com/doc389.html>

- ✓ [Monografias.com S.A., 1997]. Monografias.com, (1997). Monografias.com. Windows NT. [En línea:][Consultado: viernes 25 de enero de 2008]. Disponible en Internet:
<http://www.monografias.com/trabajos10/destem/destem.shtml?relacionados>
- ✓ [Zona Gratuita .COM, 2002-2007]. Zona Gratuita .COM, (2002-2007). Zona Gratuita .COM. Curso de Seguridad en Windows. [En línea:][Consultado: lunes 28 de enero de 2008]. Disponible en Internet:
<http://www.zonagratis.com/a-cursos/windows/SeguridadWindowsXP.htm>
- ✓ [Abadía DIGITAL, 2007]. Abadía DIGITAL, (2007). José, Windows Vista no es más seguro que Windows XP. [En línea:][Consultado: lunes 28 de enero de 2008]. Disponible en Internet:
<http://www.abadiadigital.com/noticia2378.html>
- ✓ [Microsoft Dynamics, 2007]. Microsoft Dynamics, (2007). Microsoft Business Solutions. Planificación de seguridad. [En línea:][Consultado: martes, 13 de noviembre de 2007]. Disponible en Internet:
<http://mbs.microsoft.com/downloads/public/GP10Docs/ESLA/SecurityPlanning.pdf>
- ✓ [Windows Vista TechCenter, 2007]. Windows Vista TechCenter, (2007). Microsoft Vista TechCenter. Windows User Account Control Step-by-Step Guide. [En línea:][Consultado: lunes 28 de enero de 2008]. Disponible en Internet:
<http://technet2.microsoft.com/WindowsVista/en/library/0d75f774-8514-4c9e-ac08-4c21f5c6c2d91033.msp?mfr=true>
- ✓ [Ciberhabitat, 2008]. Ciberhabitat, (2007). Ciberhábitat CIUDAD DE LA INFORMÁTICA. Seguridad Informática. [En línea:][Consultado: martes 29 de enero de 2008]. Disponible en Internet:
<http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm>
- ✓ [Seguridad Informática, 2001]. Seguridad Informática, (2001). Delitos Informáticos. Seguridad y Protección de la Información [En línea:] [Consultado: viernes 23 de noviembre de 2007]. Disponible en Internet: <http://www.delitosinformaticos.com/>
- ✓ [Soluciones de Seguridad Soluciones de Administración, 2004]. Soluciones de Seguridad Soluciones de Administración, (2004). Microsoft. Guía Microsoft de Gestión de Parches de Seguridad. [En línea:][Consultado: miércoles 07 de noviembre de 2007]. Disponible en Internet:
<http://download.microsoft.com>

- ✓ [Seguridad Windows 2000 Server, 2000]. Seguridad Windows 2000 Server, (2000). Microsoft Corporation. Guía de operaciones de seguridad para Windows 2000 Server [En línea:] [Consultado: viernes 09 de noviembre de 2007]. Disponible en Internet:
<http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx>

- ✓ [Guía de Seguridad de Windows Server 2003, 2005]. Guía de Seguridad de Windows Server 2003, (2005). Microsoft TechNet. Directiva de línea de base de servidores miembro [En línea:] [Consultado: lunes 19 de noviembre de 2007]. Disponible en Internet:
<http://www.microsoft.com/spain/technet/security/prodtech/windowsserver2003/w2003hg/s3sgch04.mspx>

- ✓ [Análisis Vulnerabilidades, 2007]. Análisis Vulnerabilidades, (2007). Armando Carvajal. GLOBALTEKSECURITY: TECNOLOGIAS GLOBALES PARA LA SEGURIDAD DE LA INFORMACION. [En línea:] [Consultado: lunes 19 de noviembre de 2007]. Disponible en Internet:
<http://www.acis.org.co/fileadmin/Articulos/AuditoriaTecnicaSGSI.pdf>

- ✓ [YoREPARO, 2006]. YoREPARO, (2006). El-NoXa. Comunidad de técnicos. [En línea:] [Consultado: miércoles 16 de julio de 2008]. Disponible en Internet:
<http://www.yoreparo.com/foros/windows/117002.html>

- ✓ [Juansa, 2006]. Juansa, (2006). Windows Server Networking. [En línea:] [Consultado: viernes 18 de julio de 2008]. Disponible en Internet:
https://msmvps.com/blogs/juansa/archive/2006/09/23/Implementar-plantillas-administrativas-y-auditor_ED00_as-V.aspx

ANEXOS



ANEXO 1.1 CARACTERÍSTICAS DE SEGURIDAD DE SISTEMAS OPERATIVOS WINDOWS PARA PC'S

La Seguridad de Windows 98

Las plataformas Windows para computadores de escritorio o PC's en las que se considera y se da importancia a la seguridad como parte del sistema operativo de manera integral, aparece con la llegada de Windows 98, este sistema es en el cual se empieza a incluir seguridad para los sistemas Windows de escritorio, se inicia con cosas muy básicas que en versiones posteriores se van a mejorar, las características de seguridad que aparecen en Windows 98 son:

- ✓ Cuando Windows 98 arrancaba se realizaba una copia de seguridad de la base de datos del registro Windows, esto sólo se llevaba a cabo una vez por día.
- ✓ Siempre que Windows 98 arranca se ejecutaba una comprobación del registro, así se comprueba si tiene algún defecto o no que le lleve a fallar en el arranque.

Seguridad de Windows Millennium

Windows Millennium, es un sistema que se caracteriza por no estar construido bajo el núcleo de Windows NT, lo que hace que no comparta características de la seguridad del NT, pero incluye algunas nuevas innovaciones de seguridad, tal es el caso de la **restauración del sistema** a un estado anterior que es una manera útil para la reparación de fallas bien sea del sistema o por programas instalados por el usuario, esta opción de restaurar sistema si bien es cierto es una característica de seguridad, también puede comprometer la estabilidad del sistema en general porque puede retornar el sistema a un estado en que estuvo aun más comprometida la seguridad.

Windows ME, también incluye otra importante característica de seguridad que es la **Protección del fichero del sistema**. “La protección del fichero del sistema está pensado para proteger archivos del sistema contra la modificación y los daños de una manera silenciosa y transparente al usuario. Cuando la protección de archivo está actuando, si se reemplaza un fichero del sistema de una manera insegura (acción de virus, troyanos o malware) Windows Me restaura inmediatamente y silenciosamente la copia original. Esta copia se toma de una carpeta de reserva del disco duro o directamente del CD de instalación de Windows Me, si no se encuentra dicha copia en ninguna de las opciones buscadas por defecto por Windows. Si no hay tal CD en la unidad, un cuadro de diálogo alerta al usuario sobre el problema y solicita que el CD esté insertado. Los mismos procedimientos ocurren si se suprime un fichero del sistema. La protección del fichero del sistema es una tecnología distinta de Restaurar Sistema y no se debe confundir con ésta. Restaurar Sistema mantiene un amplio sistema de archivos cambiantes incluyendo usos agregados y datos de la configuración del usuario almacenados en varias ocasiones en los puntos específicos creados por el usuario, mientras que la protección de archivo de Windows protege archivos del sistema operativo sin actuación del usuario.”[WIKIPEDIA, 2008].



Otras características de seguridad que incluye Windows ME, es las **nuevas opciones del TCP/IP** que se han mejorado para dar una mayor confiabilidad y estabilidad al sistema, y el uso de **actualizaciones automáticas** que necesitan de muy poca intervención del usuario para su instalación.



PLANTILLA 3.1 CHECKLIST HARDWARE DE SERVIDORES WINDOWS PREVIO A INSTALAR WINDOWS SERVER 2003

A continuación la tabla checklist describe la compatibilidad hardware que deben tener los servidores Windows de una organización determinada.

Tabla 3.a. Checklist de Hardware de los servidores Windows

COMPATIBILIDAD HARWARE DE LOS SERVIDORES WINDOWS															
INFORMACIÓN GENERAL	DESCRIPCIÓN														
	Tipo de CPU														
	Mother board chip set														
	Tipo de Bus de datos														
	Velocidad del procesador (MHZ)														
	Tamaño de RAM														
	Interfaz de usuario gráfica														
	Número de puertos seriales que posee el servidor														
	Número de puertos COM que tiene el servidor														
	Número de puertos USB que tiene el servidor														
INFORMACIÓN ESPECÍFICA	UNIDADES			DETALLE											
Mouse:				Tipo			Nro. de botones								
				PS2	Serial	Otro									
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>										
CD-ROM:				Dispositivo booteable		Dispositivo CD-Writer									
				Si	No	Si	No								
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
Floppy drives:				Driver booteable		Tipo									
				Si	<input type="checkbox"/>	3½	<input type="checkbox"/>	5¼	<input type="checkbox"/>						
				No	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
Tape drives:				Tiene		<input type="checkbox"/>									
				No tiene		<input type="checkbox"/>									
Disco Duro:				Tipo			Nro. Particiones								
				IDE	<input type="checkbox"/>	SCSI	<input type="checkbox"/>	1	<input type="checkbox"/>	2	<input type="checkbox"/>	más	<input type="checkbox"/>		
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Monitor:				Tipo			Tamaño (plg)								
				EGA	<input type="checkbox"/>	VGA	<input type="checkbox"/>	CGA	<input type="checkbox"/>	15"	<input type="checkbox"/>	17"	<input type="checkbox"/>	19"	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
				Resolución del monitor											
				600x480		<input type="checkbox"/>		800x600		<input type="checkbox"/>		1024x768		<input type="checkbox"/>	
Dispositivo de red:				Velocidad de la tarjeta Ethernet											
				10Base2		<input type="checkbox"/>		100Base2		<input type="checkbox"/>		1000Base2		<input type="checkbox"/>	
				<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>			
				Tipo de direccionamiento											
				Estático			<input type="checkbox"/>			Dinámico			<input type="checkbox"/>		
				<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>		
Impresoras:				Uso del Servidor											
				Internet			<input type="checkbox"/>			Intranet			<input type="checkbox"/>		
				<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>					
				Puertos usados para impresora											
				Paralelo			<input type="checkbox"/>			USB			<input type="checkbox"/>		
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						



REQUERIMIENTOS MÍNIMOS HARDWARE PARA INSTALAR WINDOWS SERVER 2003 ENTERPRISE EDITION

La versión **Windows Server 2003 Enterprise Edition**, necesita de los siguientes requerimientos mínimos hardware para su instalación, los mismos que se describen a continuación en la tabla:

Tabla 3.b. Requerimientos mínimos hardware para instalar Windows Server 2003 Enterprise Edition
Fuente: <http://www.microsoft.com/latam/windowsserver2003/evaluation/sysreqs/default.mspx>

Microsoft Windows server 2003 Enterprise Edition	
Componente	Requerimiento
Computadora y procesador	Procesador de 133 MHz o superior para PCs x86; 733-MHz para PCs Itanium; hasta ocho procesadores para versiones de 32 o 64 bits.
Memoria	Mínimo: 128 MB de RAM; máximo: 32 GB para PCs x86 con versión de 32 bits y 64 GB para PCs Itanium con versión de 64 bits.
Disco duro	1.5 GB de espacio disponible en el disco rígido para PCs x86; 2 GB para PCs Itanium; se necesita espacio suplementario si la instalación se realiza en red.
Lector	Lector de CD-ROM o DVD-ROM.
Monitor	VGA o hardware que admita la redirección de consola.
Otros	Windows Server 2003 Enterprise Edition. La versión de 64 bits es solamente compatible con sistemas Intel de 64 bits, y no puede instalarse en versiones de 32 bits.

Para consultar todos los requisitos mínimos que necesitan las diferentes Ediciones de Windows Server 2003, puede consultar la dirección web fuente de donde se ha citado la **Tabla 3.b.** En aquel enlace Web encontrará información de manera detallada relacionada con la instalación de Windows Server 2003.



ANEXO 3.1 CONFIGURACIÓN DE ACTIVE DIRECTORY

1. Luego de creado el Controlador de Dominio Primario, se procede a crear las unidades organizativas y grupos de usuarios de los servidores Windows de la UTPL que se lo debe realizar en el PDC. Para llevara a cabo estas tareas se empieza haciendo clic en el botón **Start**, luego se selecciona **All Programs, Administrative Tools y Active Directory Users and Computers**.

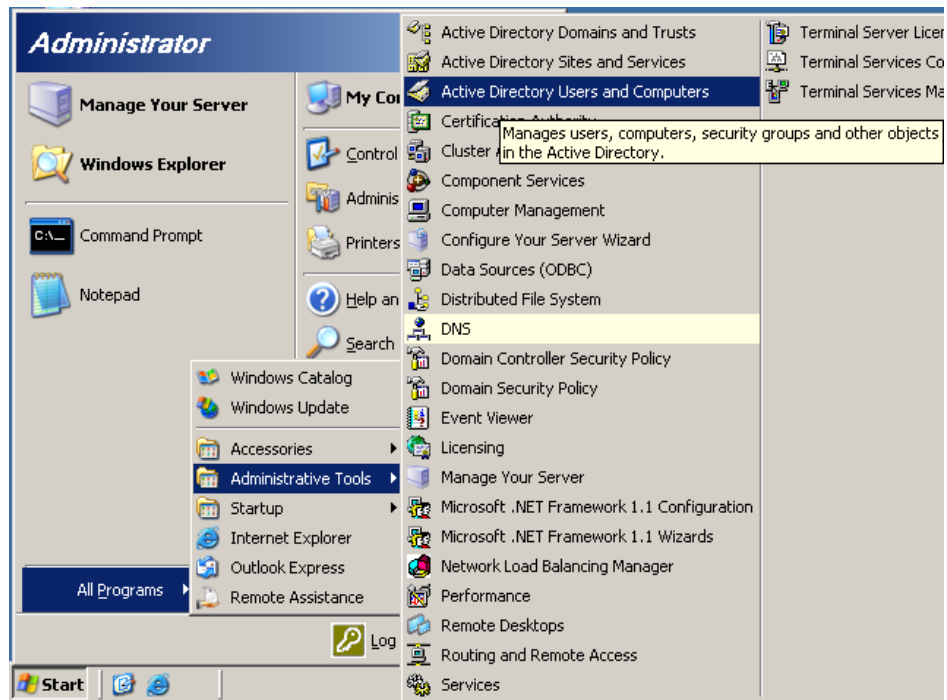


Figura 3.1.1. Proceso previo a la creación de unidades organizativas y grupos en Active Directory

2. En la pantalla que se presenta debe dar clic en el signo + que está situado junto a **utpl.edu.ec** el cual se debe expandir. Dando clic en **utpl.edu.ec**, se presenta en el panel derecho el contenido de Active Directory que trae por defecto.

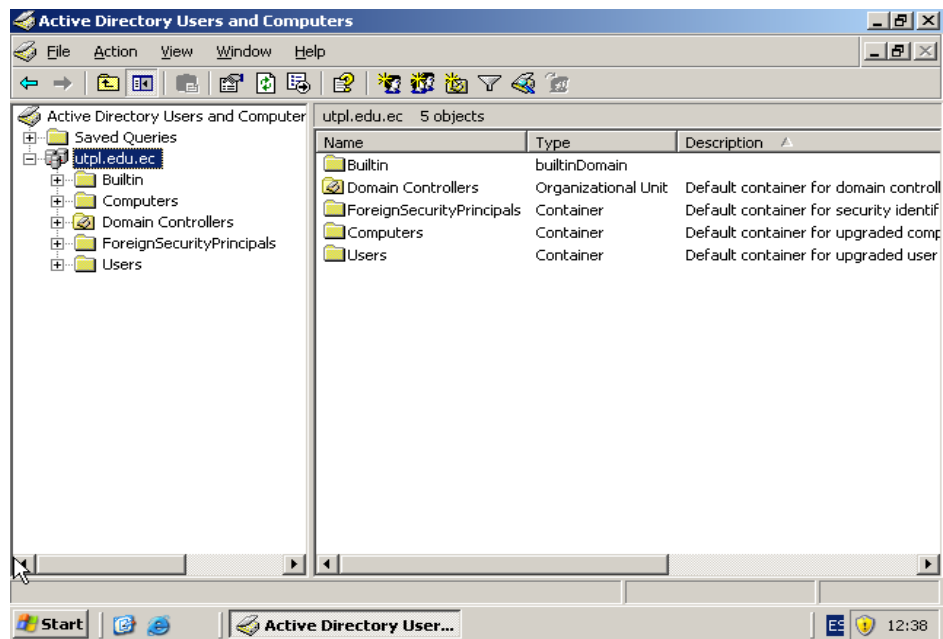


Figura 3.1.2. Creación de Usuarios y equipos de Active Directory

3. En el panel de la izquierda, se hace clic sobre **utpl.edu.ec** con el botón secundario del mouse y se escoge **New** y luego **Organizational Unit**.

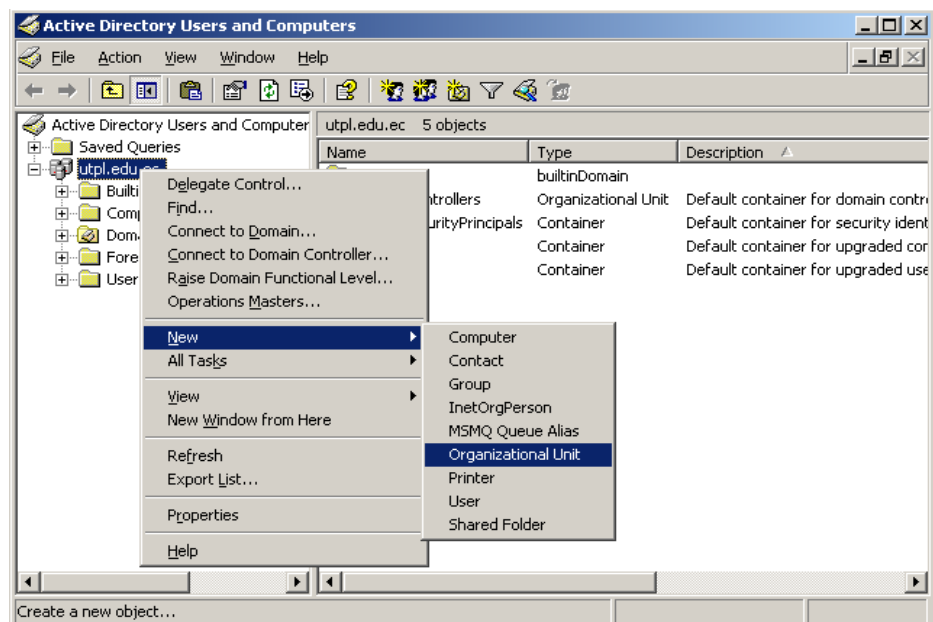


Figura 3.1.3. Creación de Unidades Organizativas

4. En la pantalla de creación de la Unidad Organizativa, en el cuadro de texto **Name**, se ingresa **Grupos** como nombre que va a identificar a la Unidad Organizativa, luego se pulsa el botón **Ok**.

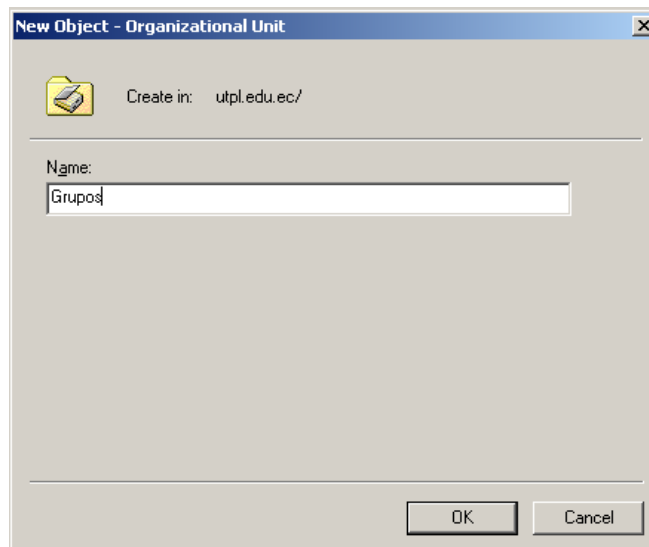


Figura 3.1.4. Ingreso del Nombre de la Unidad Organizativa Servidores

5. Para crear más Unidades Organizativas, se sigue el mismo proceso de los literales 3 y 4, y de esa manera completa un sin número de unidades organizativas conforme lo requiera la empresa o administrador de los recursos organizacionales. A continuación se describe el siguiente esquema de Active Directory para los servidores Windows de la UTP.

ESQUEMA DE ADMINISTRACIÓN DE SERVIDORES MEDIANTE ACTIVE DIRECTORY

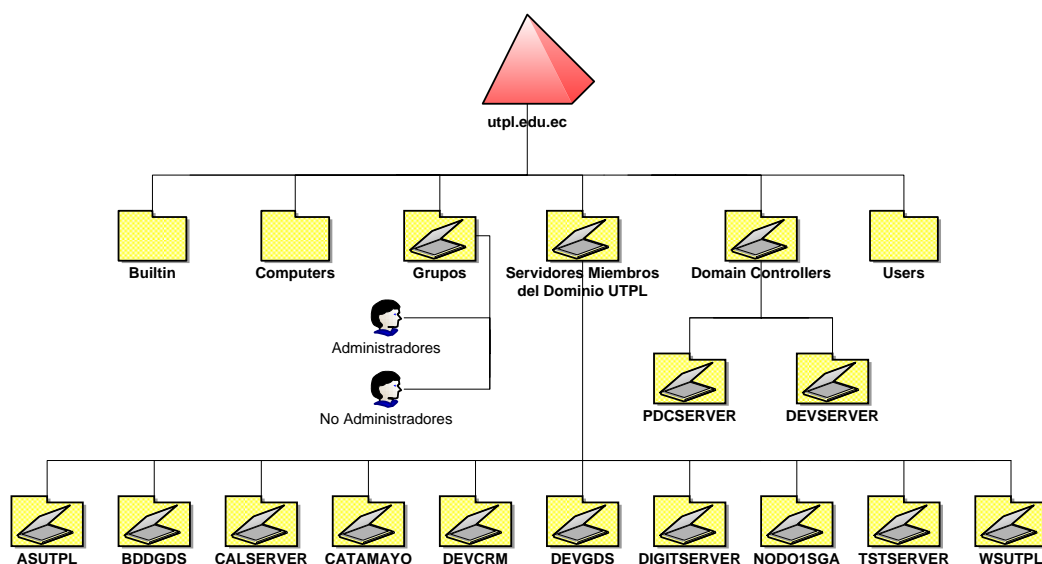


Figura 3.1.5. Estructura de Active Directory para los Servidores Windows de la UTP

6. Haciendo clic en **Domain Controllers** que se ha creado, muestra inicialmente en el panel de la derecha el contenido, en ocasiones esta vacío, pero como se muestra en el esquema de la



Figura 3.46, los controladores de dominio tanto el **Primario** como el de **Respaldo** (**PDCSERVER**, **DEVSERVER**) se han reconocido automáticamente en la **Unidad Organizativa** de Controladores de Dominio, esto debido a que se los ha configurado de servidor miembro a Controlador de Dominio, por lo que no es necesario su creación manual.

De no darse la creación automática de un servidor de dominio a Controlador de Dominio, se procede a agregarlos dentro de la Unidad Organizativa correspondiente. El proceso de creación se inicia dando clic con el botón secundario del mouse en **Domain Controllers**, seleccionando luego **New** y seguidamente clic en **Computer**.

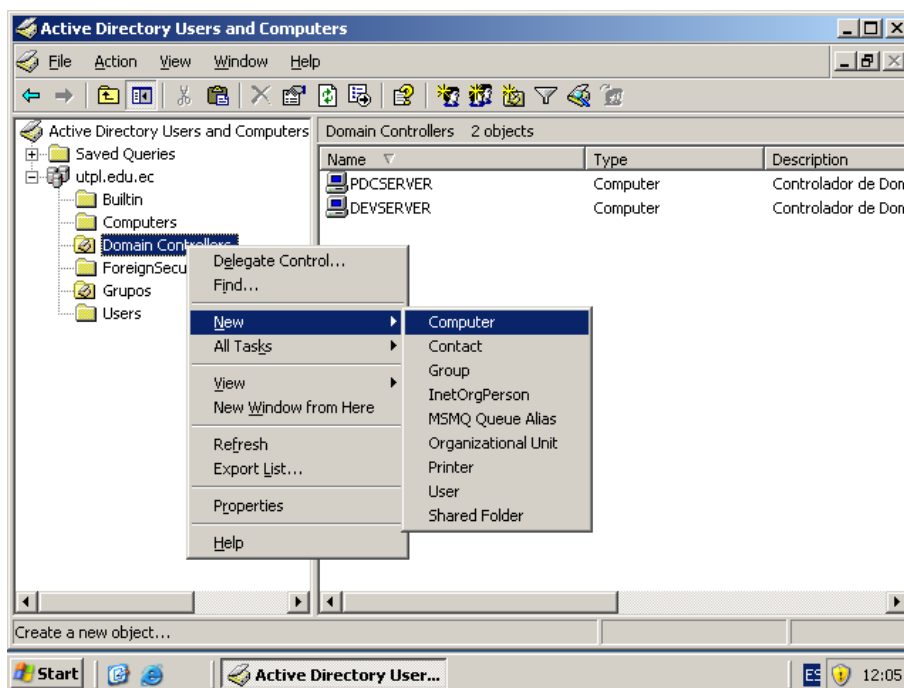


Figura 3.1.6. Agregación manual del PDC dentro la Unidad Organizativa Controladores de Dominio

7. En la ventana de diálogo que se presenta, se ingresa el nombre, **PDCSERVER** en el cuadro de texto **Computer name**, y luego se pulsa el botón **Next**.

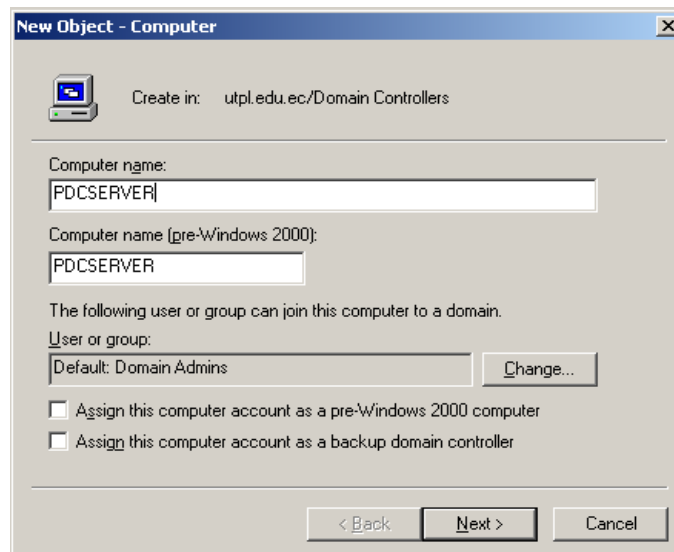


Figura 3.1.7. Ingreso manualmente del nombre del PDC dentro del Dominio utpl.edu.ec bajo Windows

8. En la siguiente pantalla que se presenta se da clic en el botón **Next**, y en la otra pantalla siguiente se pulsa el botón **Finish**, y tiene agregados los servidores a una **Unidad Organizativa** perteneciente a un dominio

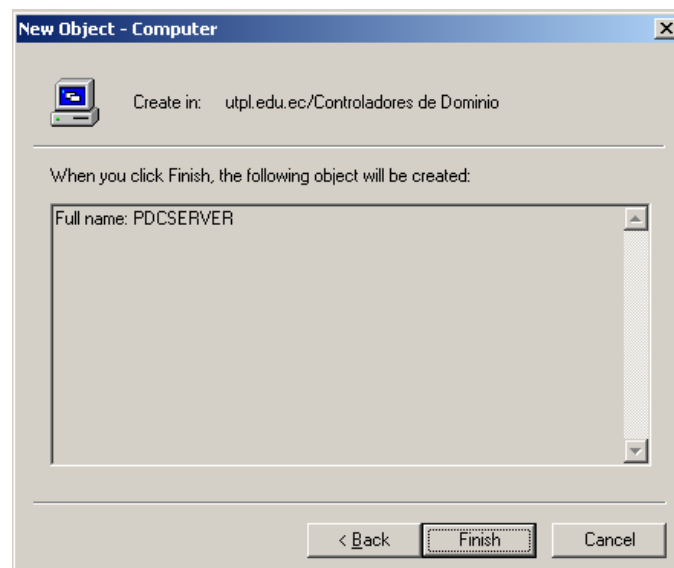


Figura 3.1.8. Finalización de la creación del PDC en la UO Controladores de Dominio

9. Luego se sigue el mismo proceso desde el paso 6 al 8 para la creación de nuevos objetos sean servidores, equipos PC's o portátiles y que de igual manera serán creados como **Computer name**, todo esto se hace cuando no se han reconocido los equipos de manera automática, aunque por lo general si se inicia sesión especificando el dominio de servidores Windows **utpl.edu.ec**, se reconocerán los equipos automáticamente en Active Directory, como se muestra en la siguiente figura, donde están todos los servidores reconocidos.

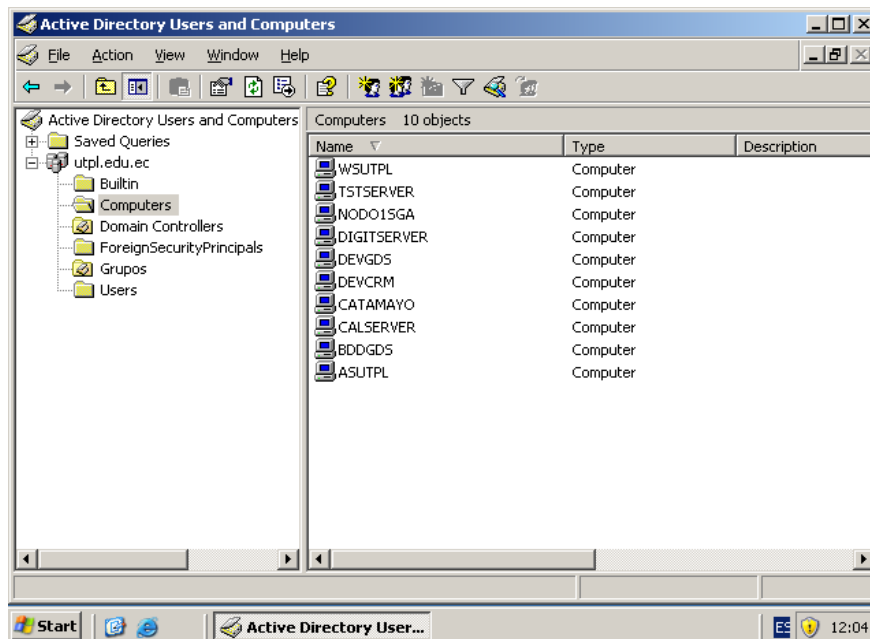


Figura 3.1.9. Servidores Windows que son miembros del dominio utpl.edu.ec

10. Reconocidos los servidores Windows dentro de la **Unidad Organizativa Computers** de Active Directory, se procede a crear primeramente los usuarios y luego los grupos de seguridad que administran los servidores Windows de la UTPL, para llevar a cabo esta tarea, debe dar clic con el botón secundario del mouse en la **Unidad Organizativa Domain Controllers**, luego selecciona **New y User**.

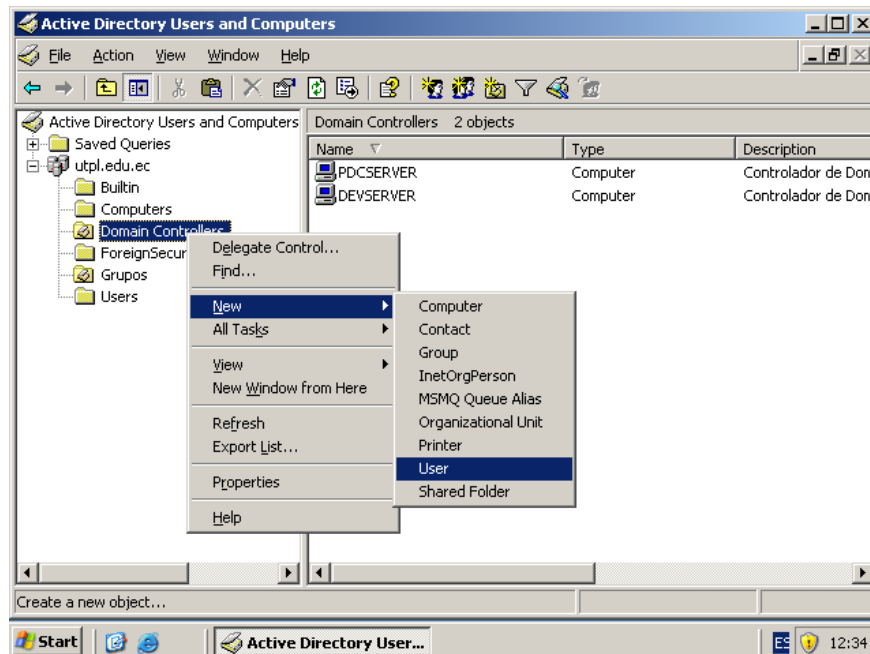


Figura 3.1.10. Creación de usuarios de las unidades organizativas

11. En la pantalla que se presenta se ingresa la información que pide del usuario que se está creando y se da clic en **Next**.

Figura 3.1.11. Ingreso de información de creación de usuario

12. Luego se presenta una pantalla donde debe ingresar un **Password** y escoger algunas políticas de manejo del password, se debe ingresar contraseñas fuertes ya que así lo exige Windows Server 2003 y además es una forma de dar protección al entorno organizacional.

Figura 3.1.12. Ingreso del password del usuario

13. En la pantalla que se presenta luego es para finalizar la creación del usuario de manera satisfactoria.
14. El proceso del 10 al 13 lo debe repetir para la creación de usuarios sobre la Unidad Organizativa **Computers** o sobre cualquier otra Unidad Organizativa que lo necesite, o también lo puede hacer directamente sobre el dominio **utpl.edu.ec**, en este caso serían usuarios del dominio y dispondrían del acceso a todo el dominio en sí.



15. Una vez que se ha creado los usuarios de las unidades Organizacionales, se procede a crear los grupos de seguridad, para ello debe ubicarse en el panel de la izquierda y dar clic derecho sobre la **Unidad Organizativa Grupos**, luego selecciona **New y Group**, como se ilustra en la figura.

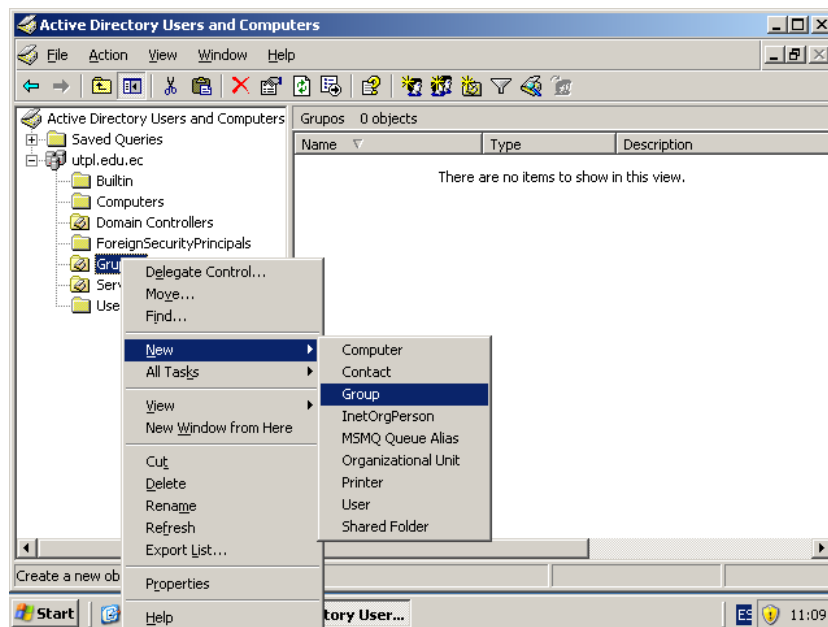


Figura 3.1.13. Pasos de creación de los grupos de Administración de los servidores

16. En la pantalla donde se ingresa el nombre del grupo, se digita **Administradores** con la configuración de seguridad **Global** y **Security** respectivamente seleccionados de **Group scope** y **Group type**. Luego hacer clic en **Ok**.

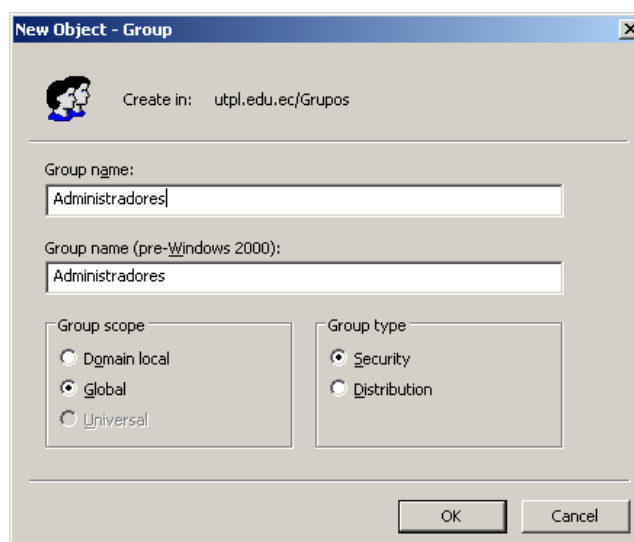


Figura 3.1.14. Ingreso del nombre del grupo con su respectiva configuración de seguridad

17. Para crear más grupos, siga el mismo procedimiento del paso 15, escogiendo la configuración de seguridad deseada. Una vez creados los grupos se tendría la siguiente estructura:

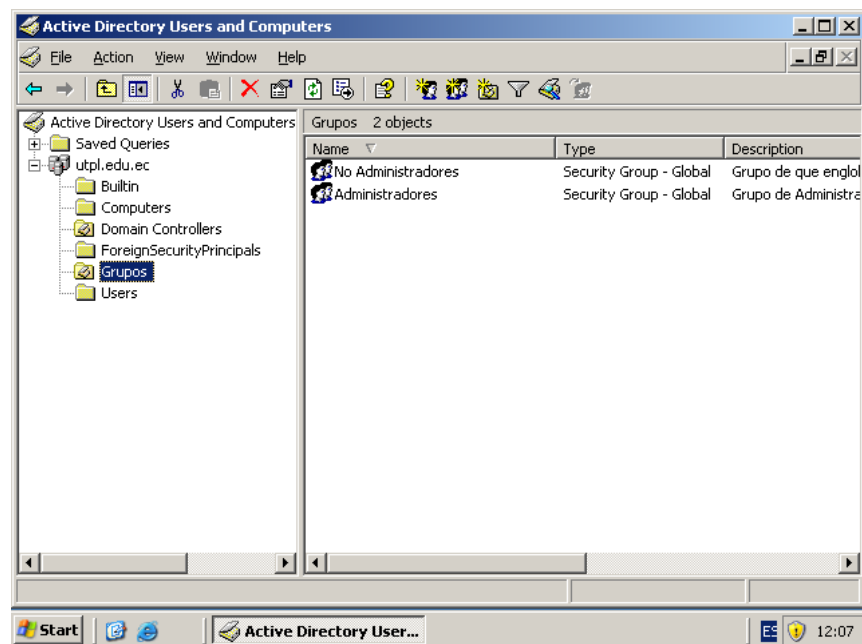


Figura 3.1.15. Estructura de grupos creados

18. Creados los grupos que **administran** como los que **no administran** los servidores Windows de la UTP, se procede a crear o asociar usuarios que van a pertenecer a dichos grupos de seguridad, para llevar a cabo este proceso, en el panel de la izquierda dar clic en **Grupos**, luego en el panel de la derecha dar doble clic en **Administradores** y en la pantalla de propiedades que se presenta, seleccione la pestaña **Members** y de manera consecutiva vaya haciendo clic en **Add**, **Advanced** y **Find Now**, en la parte inferior donde se presentan los resultados de la búsqueda, seleccione pulsando **Ctrl** de ser varios los usuarios que van a administrar a los servidores y que formarán parte del grupo de **seguridad Administradores**, luego hacer clic en **Ok** en todas las pantallas que se presentan, finalizando con la pantalla de **Propiedades de Administradores**.

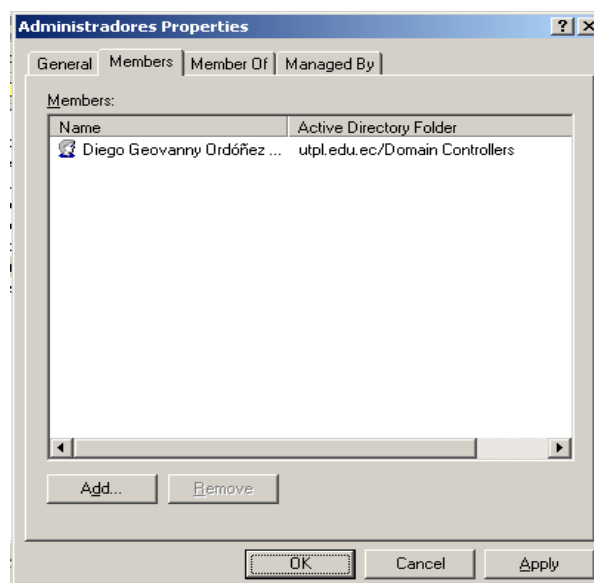


Figura 3.1.16. Agregación de miembros al grupo Administradores de los servidores



ANEXO 3.2 DETALLE PERSONALIZADO DE CONFIGURACIÓN DE LA PLANTILLA DE SEGURIDAD PARA UN SERVIDOR MIEMBRO DE UN DOMINIO

La personalización de la plantilla de seguridad se empieza desde la definición de las políticas de cuentas, estas políticas van de acuerdo a los objetivos que persigue la organización.

1. Políticas de cuentas

1.1 Personalización de seguridad de las políticas de contraseñas

1. Empiece a configurar las seguridades de la plantilla creada **SecurityServers** para ello vaya al árbol de la plantilla mencionada y expanda **SecurityServers** y luego despliegue **Account Policies** y desde aquí empiece a configurar cada directiva de acuerdo a las políticas de seguridad que desee aplicar.

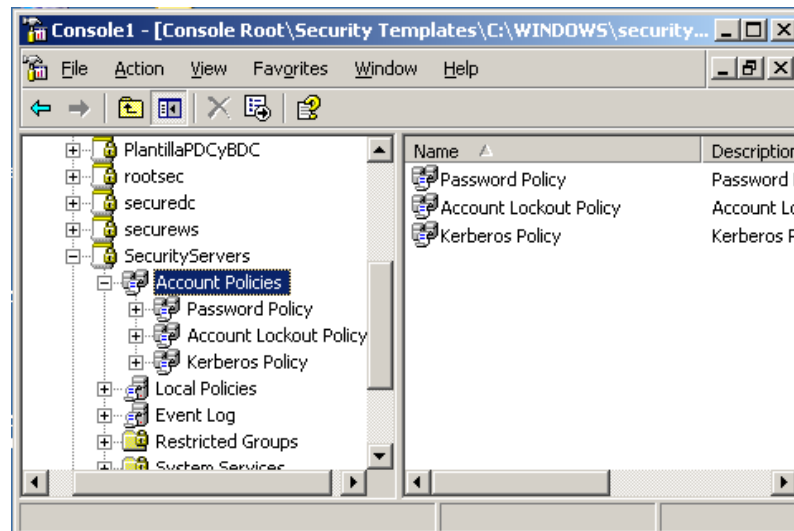


Figura 3.2.1. Despliegue de la directiva de políticas de cuentas

2. Luego de desplegar **Account Policies**, haga clic en la directiva **Password Policy**, que le permitirá en la parte derecha **Policy** configurar las políticas de contraseñas que desee aplicar al servidor

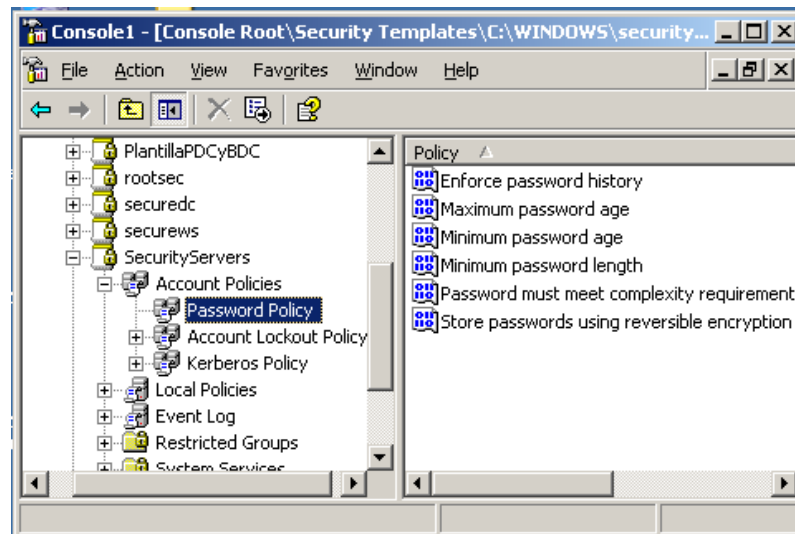


Figura 3.2.2. Directivas de contraseñas

3. Haga doble clic en **Enforce password history**, que está ubicado en **Policy**, luego le aparece un diálogo que le permite configurar las políticas de seguridad de la plantilla, debe habilitar el checkbox de **Enforce password history** (Forzar el historial de contraseñas) la configuración mínima recomendada es dejarle en 24 contraseñas recordadas, después debe dar clic en **Apply** y **OK**, se detalla a continuación en la figura.

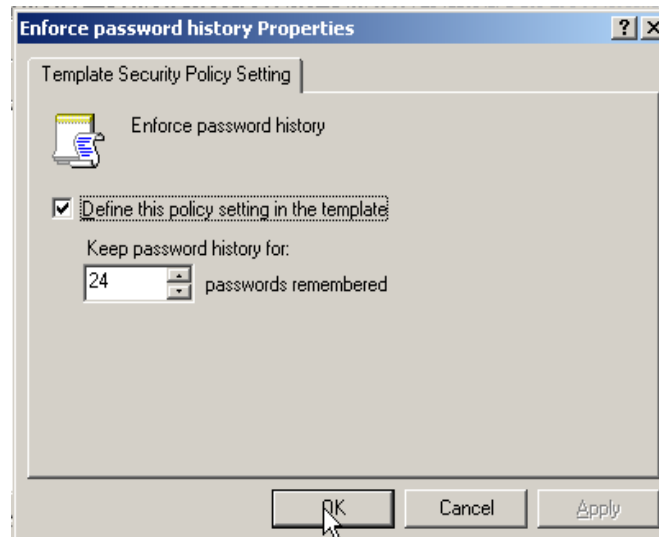


Figura 3.2.3. Dialogo donde se configura la política de seguridad de Forzar el historial de contraseñas

4. De igual manera que el paso anterior, se continúa con las configuraciones de las demás directivas de seguridad de acuerdo a la siguiente tabla de configuraciones recomendadas para las directivas de contraseñas.



Tabla 3.2.1. Valores de configuración recomendados para las distintas políticas de contraseñas que deben aplicarse al servidor

Directiva	Configuración recomendada
Enforce password history (Forzar el historial de contraseñas)	24 passwords remembered (24 contraseñas recordadas)
Maximum password age (Vigencia máxima de la contraseña)	42 days (42 días)
Minimum password age (Vigencia mínima de la contraseña)	1 day (1 día)
Minimum password length (Longitud mínima de la contraseña)	12 characters (12 caracteres)
Password must meet complexity requirements (Las contraseñas deben cumplir los requisitos de complejidad)	Enabled (Habilitado)
Store passwords using reversible encryption (Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio)	Disabled (Deshabilitado)

1.2 Personalización de las políticas de bloqueo de cuentas

1. Configurada la directiva de políticas de contraseñas, haga clic en **Account Lockout Policy**, en la parte derecha del cuadro **Policy**, se mostrarán tres directivas las cuales debe configurarlas, vea la figura a continuación.

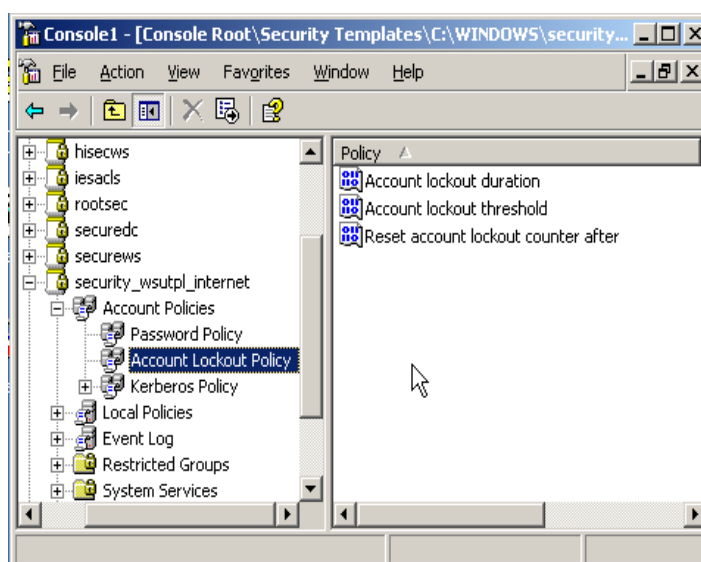


Figura 3.2.4. Configuración de la directiva de bloqueo de cuentas

2. Haga doble clic en **Account lockout duration** de la parte derecha, habilite el checkbox que aparece, por defecto no sabe estar definido, pero debe configurarlo con 15 minutos (15 minutes), luego pulse **Apply**, y **OK**.

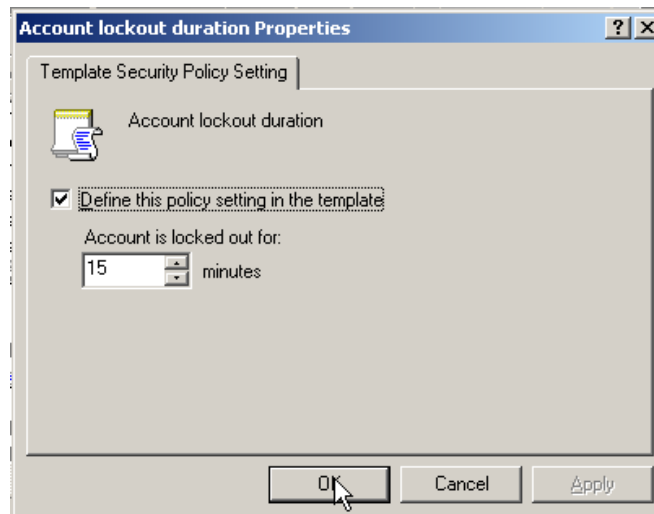


Figura 3.2.5. Configuración de la duración del Bloqueo de cuenta

3. Ahora haga doble clic en **Account lockout threshold** para que configure el umbral de bloqueo de cuenta, asigne **5 invalid logon attempts** (5 intentos incorrectos de inicio de sesión), y a continuación pulse **Apply** y **OK**. vea la figura.

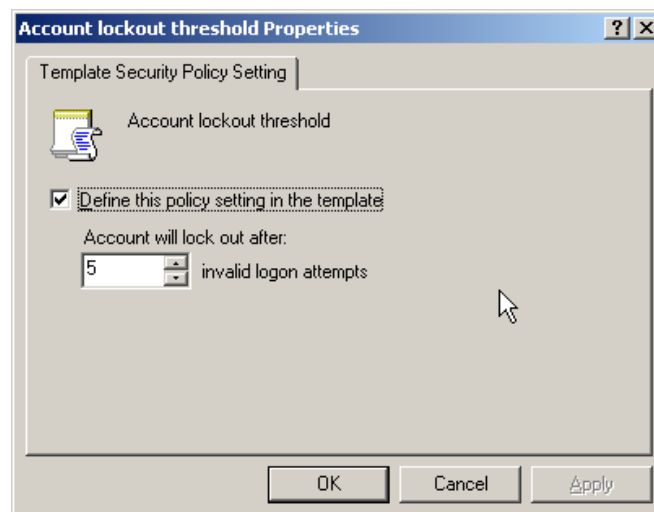


Figura 3.2.6. Configuración del umbral de bloqueo de cuenta

4. Haga doble clic en **Reset account lockout counter after**, asigne 15 minutos que es una configuración recomendada y luego pulse **Apply** y **OK**.

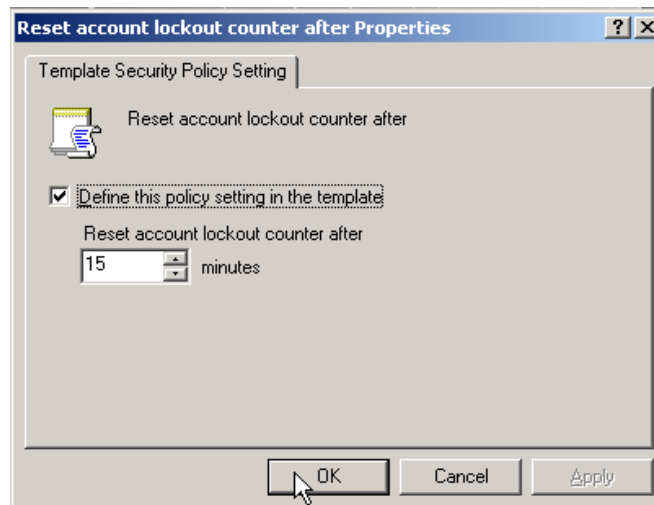


Figura 3.2.7. Configuración del restablecimiento del bloqueo de cuenta

2. Políticas locales

2.1 Personalización de políticas de Auditoría

1. En el árbol de la consola **mmc**, despliegue la plantilla personalizada que está creando, luego expanda **Local Policies**, y haga clic en **Audit Policy**, en el cuadro de la derecha tendrá las directivas de auditoría que debe configurar, para empezar a configurar la primera directiva de doble clic en **Audit account logon events** y en el diálogo que aparece habilite los dos checkbox de **Success** y **Failure** (Acierto y error), vea la figura.



Figura 3.2.8. Habilitación de la Auditoría de sucesos de inicio de sesión de cuenta

2. De doble clic en **Audit account management**, y habilite de igual manera **Success** y **Failure**, a continuación se muestra la figura.

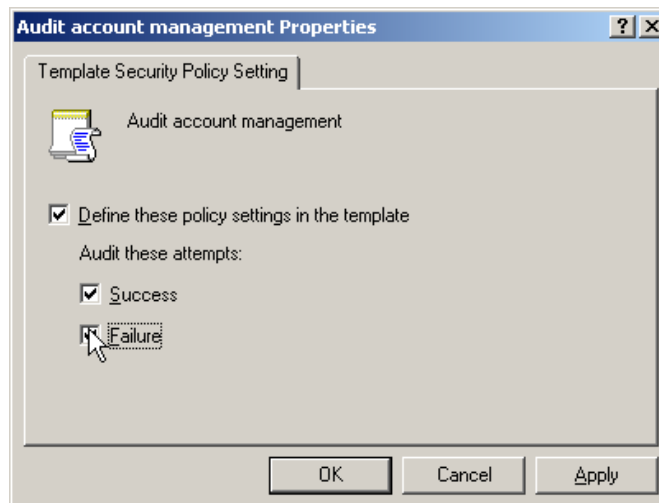


Figura 3.2.9. Configuración de la administración de cuentas de auditoría

3. De doble clic en **Audit directory service access**, habilite **Success** y **Failure**, luego de manera consecutiva pulse en **Apply** y **OK**, así estará auditando el acceso al servicio de directorios, a continuación se muestra la figura.

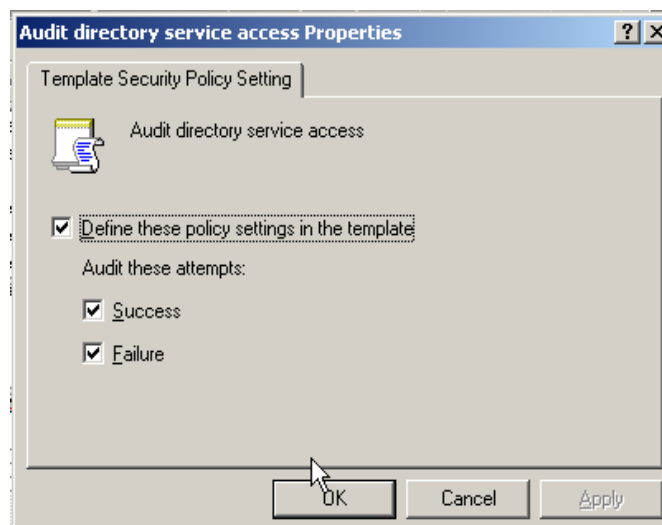


Figura 3.2.10. Configuración de la directiva de auditoría de acceso al servicio de directorios

4. Continúe configurando las siguientes directivas de políticas de auditoría de igual manera que en los pasos anteriores, pero aplicando los valores de configuración conforme se muestran en la siguiente tabla.



Tabla 3.2.2. Valores de configuración de directivas de auditoría

Directiva	Configuración del equipo
Audit logon events (Auditar sucesos de inicio de sesión)	Success, Failure (Acierto, error)
Audit object Access (Auditar el acceso a objetos)	Success, Failure (Acierto, error)
Audit policy change (Auditar el cambio de directivas)	Success (Acierto)
Audit privilege use (Auditar el uso de privilegios)	Success, Failure (Acierto, Error)
Audit process tracking (Auditar el seguimiento de procesos)	No Defined (No Definido)
Audit system events (Auditar sucesos del sistema)	Success (Acierto)

5. Una vez que haya configurado todas las directivas de políticas de auditoría, tendrá un resultado similar al que se muestra a continuación en la siguiente figura.

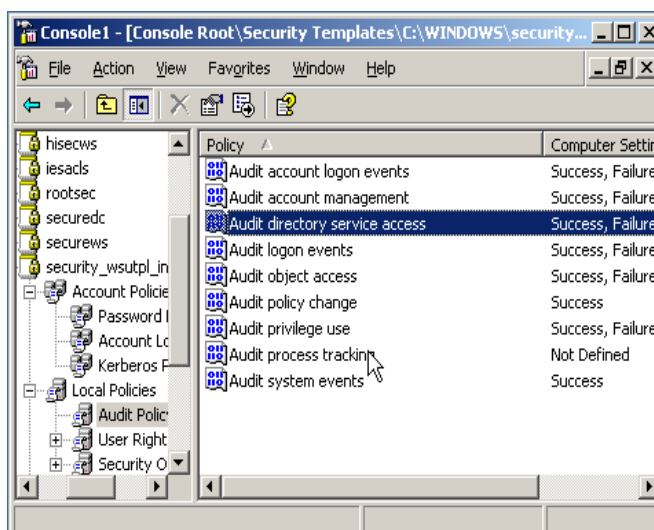


Figura 3.2.11. Configuración de todas las directivas de políticas de auditoría

2.2 Personalización de asignación de derechos de usuario

1. Siguiendo en la personalización de la plantilla de seguridad, ahora de clic en **User Rights Assignment** (Asignación de derechos de usuario) y en la parte derecha, en el cuadro de **Policy**, de doble clic en **Access this Computer from the network**, y habilite el checkbox **Define these policy settings in the template**, luego pulse el botón **Add User or Group**, (vea Figura 3.2.12.) en la nueva ventana de diálogo que aparece pulse el botón **Browse**, (vea Figura 3.2.13.) después se muestra otra ventana de diálogo de selección de usuarios o grupos, pulse el botón **Advanced** y se abrirá otra ventana de diálogo donde debe pulsar el botón **Find now** para que se muestren todos los usuarios o grupos del equipo y a los cuales debe seleccionar pulsando **Ctrl+clic**, según al criterio de configuración de seguridad, en éste caso **Administrators**, **Authenticated Users** y **ENTERPRISE DOMAIN CONTROLLERS**, luego de manera consecutiva debe ir pulsando en **OK** en las ventanas de diálogo que están abiertas, (vea Figura 3.2.14.)

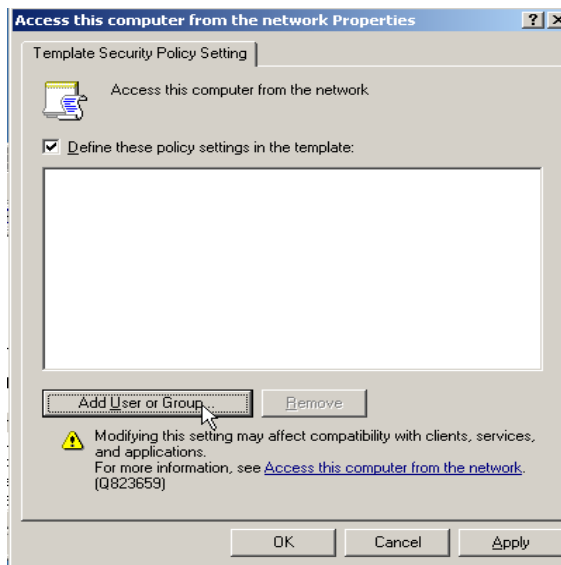


Figura 3.2.12. Diálogo de agregación de usuarios o grupos

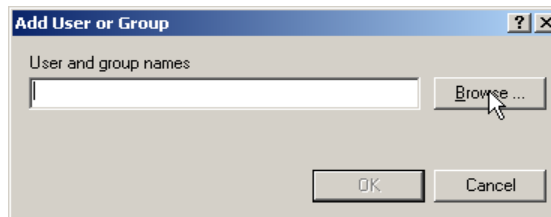


Figura 3.2.13. Búsqueda de usuarios o grupos

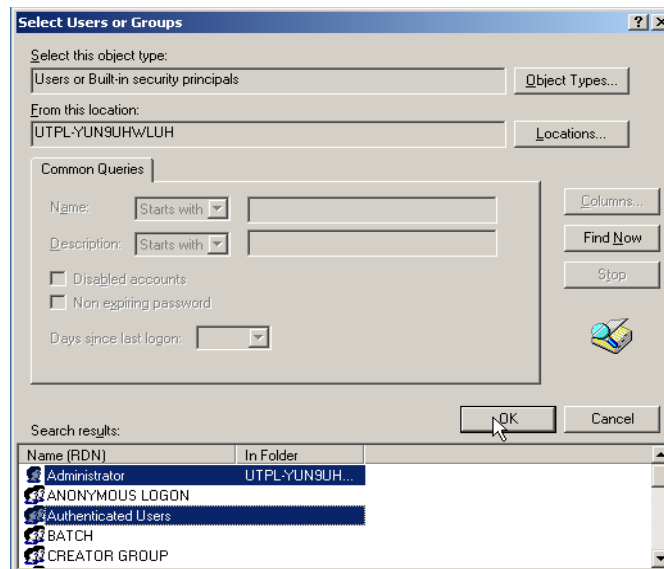


Figura 3.2.14. Selección de usuarios o grupos

2. Conforme procedió en el paso anterior, siga configurando las demás políticas de seguridad correspondientes a la directiva de asignación de derechos de usuario, a continuación se detalla la tabla con los valores que deben asignarse a cada directiva de seguridad, las cuales brindan un alto nivel de seguridad en servidores que ejecutan Windows Server 2003.



Tabla 3.2.3. Configuración de derechos de usuario

Directiva	Configuración de seguridad empresarial	Configuración de alta seguridad
Act as part of the operating system	Not Defined	No one
Add workstations to domain	Not Defined	Administrators
Adjust memory quotas for a process	Not Defined	Administrators, NETWORK SERVICE, LOCAL SERVICE
Allow log on locally	Administrators, Power Users, Backup Operators	Administrators
Allow log on through Terminal Services	Administrators, Remote Desktop Users	Administrators
Back up files and directories	Not Defined	Administrators
Bypass traverse checking	Not Defined	Authenticated Users
Change the system time	Not Defined	Administrators, LOCAL SERVICE
Create a pagefile	Not Defined	Administrators
Create a token object	Not Defined	No one
Create global objects	Not Defined	Administrators, SERVICE
Create permanent shared objects	Not Defined	No one
Debug programs	Administrators	No one
Deny access to this computer from the network	ANONYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts	ANONYMOUS LOGON; Guests; Support_388945a0; all NON-Operating System service accounts
Deny log on as a batch job	Guests;Support_388945a0	Guests; Support_388945a0
Deny log on as a service	Not Defined	No one
Deny log on locally	Not Defined	Guests; Support_388945a0;
Deny log on through Terminal Services	Guests; SUPPORT_388945a0	Guests; SUPPORT_388945a0
Enable computer and user accounts to be trusted for delegation	Not Defined	Administrators
Force shutdown from a remote system	Not Defined	Administrators
Generate security audits	Not Defined	NETWORK SERVICE, LOCAL SERVICE
Impersonate a client after authentication	Not Defined	Administrators, SERVICE
Increase scheduling priority	Not Defined	Administrators
Load and unload device drivers	Not Defined	Administrators
Lock pages in memory	Not Defined	No one
Log on as a batch job	Not Defined	No one
Log on as a service	Not Defined	NETWORK SERVICE
Manage auditing and security log	Not Defined	Administrators
Modify firmware environment values	Not Defined	Administrators
Perform volume maintenance tasks	Not Defined	Administrators
Profile single process	Not Defined	Administrators
Profile system performance	Not Defined	Administrators
Remove computer from docking station	Not Defined	Administrators
Replace a process level token	Not Defined	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Administrators	Administrators
Shut down the system	Administrators, Power Users, Backup Operators, Users	Administrators
Synchronize directory service data	Not Defined	No one
Take ownership of files or other objects	Not Defined	Administrators

2.3 Personalización de opciones de seguridad

1. Para configurar las opciones de seguridad, de una plantilla de seguridad, expanda la plantilla, y ubíquese en **Local Policies**, luego de clic en **Security Options** y proceda a configurar todas las directivas de seguridad ubicadas en el cuadro de **Policy**. Para iniciar las configuraciones debe ubicarse en **Accounts: Administrator account status**, de doble clic sobre la directiva, luego se le aparecerá una ventana de diálogo, donde debe habilitar el checkbox de definición de la política de seguridad y luego escoger la opción de **Enable**, y de manera consecutiva pulse **Apply** y **OK**, a continuación se ilustra en la figura.

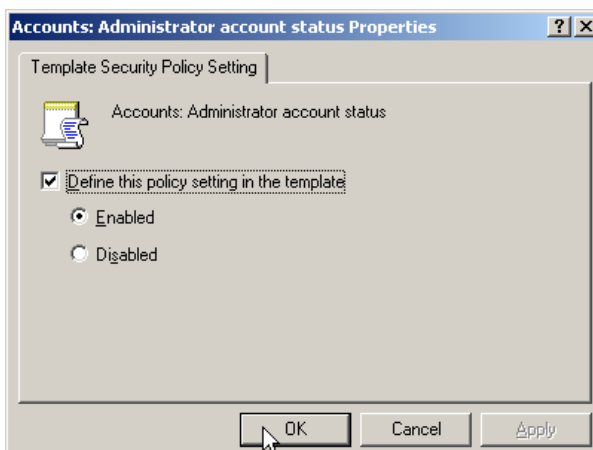


Figura 3.2.15. Configuración del estado de cuenta del administrador

2. A continuación se detallan los diferentes valores de una alta configuración que se debe realizar con las demás directivas de seguridad, prosiga de manera similar al paso anterior, en la siguiente figura se muestra los valores mencionados.

Tabla 3.2.4. Valores de configuración de las directivas opciones de seguridad

Directiva	Configuración de seguridad empresarial	Configuración de alta seguridad
Accounts: Guest account status	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled
Accounts: Rename administrator account	Not Defined	Not Defined
Accounts: Rename guest account	Not Defined	Not Defined
Audit: Audit the access of global system objects	Disabled	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled	Enabled
Audit: Shut down system immediately if unable to log security audits	Disabled	Enabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	Not Defined
Devices: Allow undock without having to log on	Disabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Administrators
Devices: Prevent users from installing printer drivers	Enabled	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Not defined	Disabled
Devices: Restrict floppy access to locally logged-on user only	Not defined	Disabled
Devices: Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Disabled	Disabled
Domain controller: LDAP server signing requirements	Not Defined	Require Signing
Domain controller: Refuse machine account password changes	Disabled	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled



Tabla 3.2.4. Valores de configuración de las directivas opciones de seguridad (... continuación)

Directiva	Configuración de seguridad empresarial	Configuración de alta seguridad
Domain member: Disable machine account password changes	Disabled	Disabled
Domain member: Maximum machine account password age	30 days	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabled
Interactive logon: Display user information when the session is locked	Not defined	User display name, domain and user names
Interactive logon: Do not display last user name	Enabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled
Interactive logon: Message text for users attempting to log on	Este sistema está limitado solo para usuarios autorizados. Individuos no autorizados que intenten acceder, serán enjuiciados. Si no está autorizado, termine el acceso ahora. Haga clic en OK indicando su aceptación de la información y condiciones mencionadas, caso contrario absténgase a las consecuencias	Este sistema está limitado solo para usuarios autorizados. Individuos no autorizados que intenten acceder, serán enjuiciados. Si no está autorizado, termine el acceso ahora. Haga clic en OK indicando su aceptación de la información y condiciones mencionadas, caso contrario absténgase a las consecuencias
Interactive logon: Message title for users attempting to log on	ESTO ES UN DELITO SI CONTINUA INGRESANDO SIN AUTORIZACIÓN	ESTO ES UN DELITO SI CONTINUA INGRESANDO SIN AUTORIZACIÓN
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0	0
Interactive logon: Prompt user to change password before expiration	14 days	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled	Enabled
Interactive logon: Require smart card	Not Defined	Disabled
Interactive logon: Smart card removal behavior	Lock Workstation	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled
Network access: Allow anonymous SID/Name translation	Not Defined	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled
Network access: Named Pipes that can be accessed anonymously	Not defined	COMNAP, COMNODE, SQL\QUERY, SPOOLSS, LLSRPC, netlogon, lsarpc, samr, browser
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\Product Options; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\Product Options; System\CurrentControlSet\Control\Server Applications; Software\Microsoft\Windows NT\Current Version



Tabla 3.2.4. Valores de configuración de las directivas opciones de seguridad (... continuación)

Directiva	Configuración de seguridad empresarial	Configuración de alta seguridad
Network access: Remotely accessible registry paths and sub-paths	Software\Microsoft\Windows NT\CurrentVersion\Print; Software\Microsoft\Windows NT\CurrentVersion\Windows; System\CurrentControlSet\Control\Print\Printers; System\CurrentControlSet\Services\Eventlog; Software\Microsoft\OLAP Server; System\CurrentControlSet\Control\ContentIndex; System\CurrentControlSet\Control\Terminal Server; System\CurrentControlSet\Control\Terminal Server\UserConfig; System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration; Software\Microsoft\Windows NT\CurrentVersion\Perflib; System\CurrentControlSet\Services\SysmonLog	Software\Microsoft\Windows NT\CurrentVersion\Print; Software\Microsoft\Windows NT\CurrentVersion\Windows; System\CurrentControlSet\Control\Print\Printers; System\CurrentControlSet\Services\Eventlog; Software\Microsoft\OLAP Server; System\CurrentControlSet\Control\ContentIndex; System\CurrentControlSet\Control\Terminal Server; System\CurrentControlSet\Control\Terminal Server\UserConfig; System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration; Software\Microsoft\Windows NT\CurrentVersion\Perflib; System\CurrentControlSet\Services\SysmonLog
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled
Network access: Shares that can be accessed anonymously	Not Defined	None
Network access: Sharing and security model for local accounts	Disabled	Classic – local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled
Network security: Force logoff when logon hours expire	Enabled	Enabled
Network security: LAN Manager authentication level	Send NTLMv2response only\refuse LM	Send NTLMv2 response only\refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate Signing	Negotiate Signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled all settings	Enabled all settings
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled all settings	Enabled all settings
Recovery console: Allow automatic administrative logon	Disabled	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Enabled	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled
Shutdown: Clear virtual memory pagefile	Disabled	Enabled
System cryptography: Force strong key protection for user keys stored on the computer	User is prompted when the key is first used	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	Enabled
System objects: Default owner for objects created by members of the Administrators group	Object creator	Object creator
System objects: Require case insensitivity for non-Windows subsystems	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled
System settings: Optional subsystems	None	None
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	Enabled



3. Sucesos Log

1. Estando en la plantilla de seguridad creada, de clic en **Event Log**, en el cuadro de **Policy** se detallan todas las directivas de seguridad que se deben configurar, para ello de doble clic en la primera directiva que es **Maximum application log size**, luego le aparecerá una ventana de diálogo en donde debe habilitar el checkbox de definición de la política y luego ingresar el valor en **kilobytes** que desea darle como máximo a los logs de aplicaciones, vea la figura.

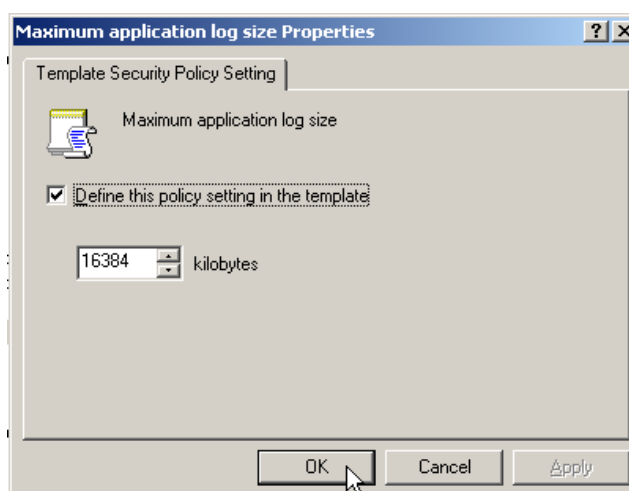


Figura 3.2.16. Configuración del tamaño de logs para aplicaciones

2. Las demás configuraciones de las directivas de sucesos log, debe realizarlo de acuerdo a las especificaciones que a continuación se detallan en la siguiente tabla.

Tabla 3.2.5. Configuraciones recomendadas para los sucesos log

Directiva	Configuración de seguridad empresarial	Configuración de alta seguridad
Maximum security log size	81920 KB	81920 KB
Maximum system log size	16384 KB	16384 KB
Prevent local guests group from accessing application log	Enabled	Enabled
Prevent local guests group from accessing security log	Enabled	Enabled
Prevent local guests group from accessing system log	Enabled	Enabled
Retain application log	Not Defined	Not Defined
Retain security log	Not Defined	Not Defined
Retain system log	Not Defined	Not Defined
Retention method for application log	Overwrite events as needed	Overwrite events as needed
Retention method for security log	Overwrite events as needed	Overwrite events as needed
Retention method for system log	Overwrite events as needed	Overwrite events as needed

3. Luego de haber configurados las directivas de sucesos log, debería aparecer el cuadro de **Policy** de la siguiente manera como se muestra a continuación.

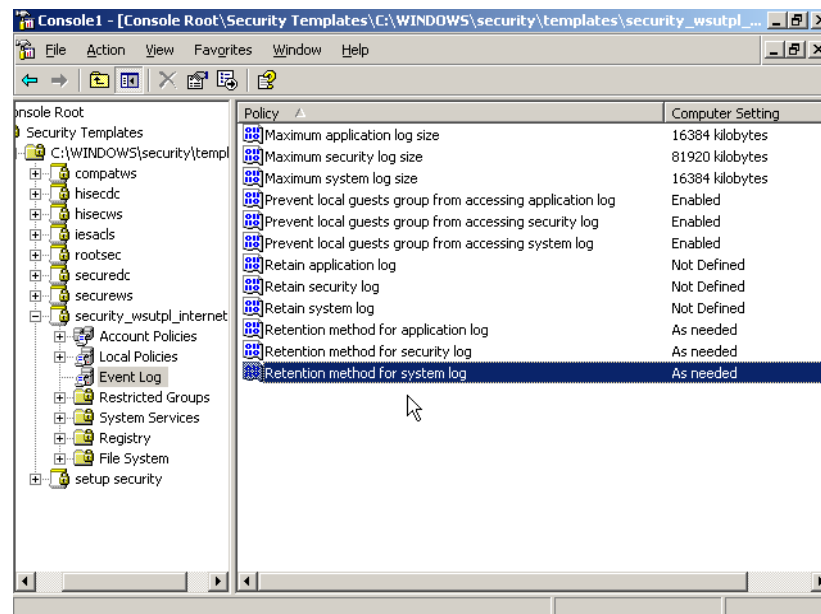


Figura 3.2.17. Apariencia de las directivas de sucesos log configuradas

4. Grupos restringidos

En una plantilla de alta seguridad se debe delimitar el grupo de usuarios que tengan el acceso a un servidor en específico, por tal motivo, en esta plantilla personalizada que se está configurando para un servidor miembro de un dominio, se considera dos tipos de usuarios: Administradores y Usuarios con poder para hacer cualquier tipo de cambio en el servidor.

1. Expanda el árbol de la plantilla personalizada creada, ubíquese y de clic derecho en **Restricted Groups**, luego en el menú que se le presenta seleccione **Add Group** (vea Figura 3.2.18) y a continuación en el diálogo que se le presenta pulse en **Browse**, esto le lleva a otra ventana de diálogo en donde debe pulsar en **Advanced**, la misma que le presentará otra ventana de diálogo, allí debe pulsar en **Find Now**, para que se visualicen los usuarios y grupos a los cuales va a seleccionar, en éste caso pulsando **ctrl+clic**, escoja Administrators y Power Users, y luego pulse de manera consecutiva en **OK**, en las ventanas de diálogo abiertas (vea Figura 3.2.19)

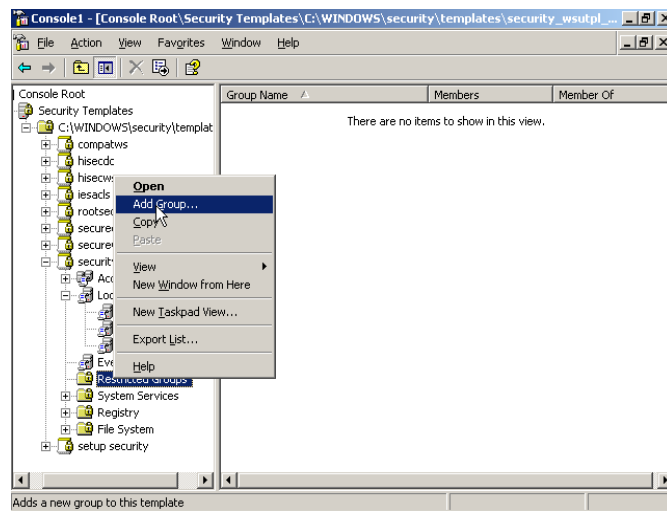


Figura 3.2.18. Agregando usuarios al grupo restringidos

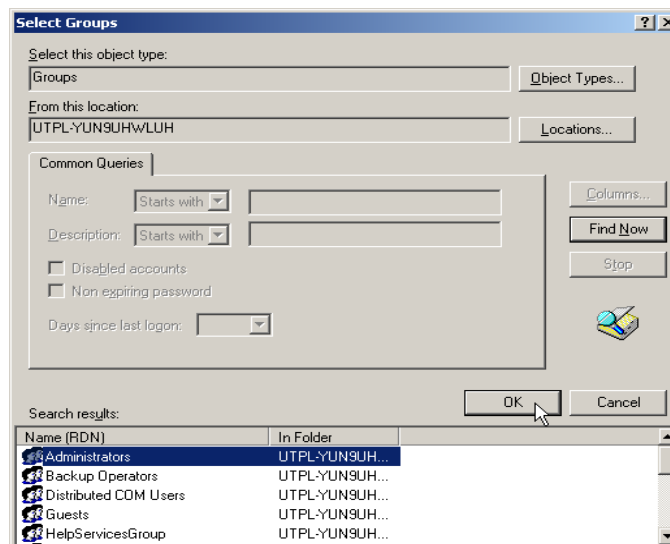


Figura 3.2.19. Selección de usuarios para el grupo restringidos

5. Servicios del sistema

En la configuración de una plantilla se debe considerar los servicios del sistema, estos servicios por lo general se crean por defecto cuando se instala el sistema operativo por primera vez, para ello es aconsejable configurar los servicios que estén acorde a las necesidades del propio sistema y así deshabilitar los servicios que no utilice o que son innecesarios, a continuación se detalla los valores de configuración óptimos y recomendados en un sistema operativo Windows Server 2003.



Tabla 3.2.6. Configuraciones de los servicios del sistema que deben habilitarse

Nombre completo del servicio	Nombre del Servicio	Tipo de Inicio del Servicio
Alerter	Alerter	Disabled
Application Experience Lookup Service	AELookupSvc	Automatic
Application Layer Gateway Service	ALG	Disabled
Application Management	AppMgmt	Disabled
ASP .NET State Service	aspnet state	Disabled
Automatic Updates	wuauerv	Automatic
Background Intelligent Transfer Service	BITS	Manual
Certificate Services	CertSvc	Disabled
Client Service for NetWare	NWCWorkstation	Disabled
ClipBook	ClipSrv	Disabled
Cluster Service	ClusSvc	Disabled
COM+ Event System	COMSysApp	Manual
COM+ System Application	EventSystem	Disabled
Computer Browser	Browser	Automatic
Cryptographic Services	CryptSvc	Automatic
DCOM Server Process Launcher	DcomLaunch	Automatic
DHCP Client	Dhcp	Automatic
DHCP Server	DHCPServer	Disabled
Distributed File System	Dfs	Disabled
Distributed Link Tracking Client	TrkWks	Disabled
Distributed Link Tracking Server	TrkSvr	Disabled
Distributed Transaction Coordinator	MSDTC	Disabled
DNS Client	Dnscache	Automatic
DNS Server	DNS	Disabled
Error Reporting Service	ERSvc	Disabled
Event Log	Eventlog	Automatic
Fax Service	Fax	Disabled
File Replication	NtFrs	Disabled
File Server for Macintosh	MacFile	Disabled
FTP Publishing Service	MSFtpsvc	Disabled
Help and Support	Helpsvc	Disabled
HTTP SSL	HTTPFilter	Disabled
Human Interface Device Access	HidServ	Disabled
IAS Jet Database Access	IASJet	Disabled
IIS Admin Service	IISADMIN	Disabled
IMAPI CD-Burning COM Service	ImapiService	Disabled
Indexing Service	Cisvc	Disabled
Infrared Monitor	Irmon	Disabled
Internet Authentication Service	IAS	Disabled
Intersite Messaging	IsmServ	Disabled
IP Version 6 Helper Service	6to4	Disabled
IPSec Policy Agent (IPSec Service)	PolicyAgent	Automatic
Kerberos Key Distribution Center	Kdc	Disabled
License Logging Service	LicenseService	Disabled
Logical Disk Manager	dmserver	Manual
Logical Disk Manager Administrative Service	dmadmin	Manual
Machine Debug Manager	MDM	Not installed
Message Queuing	Msmq	Disabled
Message Queuing Down Level Clients	Mqds	Disabled
Message Queuing Triggers	Mqtgsvc	Disabled
Messenger	Messenger	Disabled
Microsoft POP3 Service	POP3SVC	Disabled
Microsoft Software Shadow Copy Provider	SwPrv	Manual
MSSQL\$UDDI	MSSQL\$UDDI	Disabled
MSSQLServerADHelper	MSSQLServerADHelper	Disabled
.NET Framework Support Service	CORRTSvc	Disabled
Net Logon	Netlogon	Automatic
NetMeeting Remote Desktop Sharing	mnmsrvc	Disabled
Network Connections	Netman	Manual
Network DDE	NetDDE	Disabled
Network DDE DSDM	NetDDEdsdm	Disabled
Network Location Awareness (NLA)	NLA	Manual
Network Provisioning Service	xmlprov	Manual



Tabla 3.2.6. Configuraciones de los servicios del sistema que deben habilitarse (... continuación)

Nombre completo del servicio	Nombre del Servicio	Tipo de Inicio del Servicio
Network News Transfer Protocol (NNTP)	NntpSvc	Disabled
NT LM Security Support Provider	NtLmSsp	Automatic
Performance Logs and Alerts	SysmonLog	Manual
Plug and Play	PlugPlay	Automatic
Portable Media Serial Number Service	WmdmPmSN	Disabled
Print Server for Macintosh	MacPrint	Disabled
Print Spooler	Spooler	Disabled
Protected Storage	ProtectedStorage	Automatic
QoS RSVP Service	RSVP	Not installed
Remote Access Auto Connection Manager	RasAuto	Disabled
Remote Access Connection Manager	RasMan	Disabled
Remote Administration Service	SrvcSurg	Manual
Remote Desktop Help Session Manager	RDsessMgr	Disabled
Remote Installation	BINLSVC	Disabled
Remote Procedure Call (RPC)	RpcSs	Automatic
Remote Procedure Call (RPC) Locator	RpcLocator	Disabled
Remote Registry Service	RemoteRegistry	Automatic
Remote Server Manager	AppMgr	Disabled
Remote Server Monitor	Appmon	Disabled
Remote Storage Notification	Remote_Storage_User_Link	Disabled
Remote Storage Server	Remote_Storage_Server	Disabled
Removable Storage	NtmsSvc	Manual
Resultant Set of Policy Provider	RSOPProv	Disabled
Routing and Remote Access	RemoteAccess	Disabled
SAP Agent	nwsapagent	Disabled
Secondary Logon	Seclogon	Disabled
Security Accounts Manager	SamSs	Automatic
Server	Lanmanserver	Automatic
Shell Hardware Detection	ShellHWDetection	Disabled
Simple Mail Transport Protocol (SMTP)	SMTPSVC	Disabled
Simple TCP/IP Services	SimpTcp	Disabled
Single Instance Storage Groveler	Groveler	Disabled
Smart Card	SCardSvr	Disabled
SNMP Service	SNMP	Disabled
SNMP Trap Service	SNMPTRAP	Disabled
Special Administration Console Helper	Sacsvr	Disabled
SQLAgent\$* (* UDDI or WebDB)	SQLAgent\$WEBDB	Disabled
System Event Notification	SENS	Automatic
Task Scheduler	Schedule	Disabled
TCP/IP NetBIOS Helper Service	LMHosts	Automatic
TCP/IP Print Server	LPDSVC	Disabled
Telephony	TapiSrv	Disabled
Telnet	TlntSvr	Disabled
Terminal Services	TermService	Automatic
Terminal Services Licensing	TermServLicensing	Disabled
Terminal Services Session Directory	Tssdis	Disabled
Themes	Themes	Disabled
Trivial FTP Daemon	Tftpd	Disabled
Uninterruptible Power Supply	UPS	Disabled
Upload Manager	Uploadmgr	Disabled
Virtual Disk Service	VDS	Disabled
Volume Shadow Copy	VSS	Manual
WebClient	WebClient	Disabled
Web Element Manager	elementmgr	Disabled
Windows Audio	AudioSrv	Disabled
Windows Firewall/Internet Connection Sharing (ICS)	SharedAccess	Disabled
Windows Image Acquisition (WIA)	StiSvc	Disabled
Windows Installer	MSIServer	Automatic
Windows Internet Name Service (WINS)	WINS	Disabled
Windows Management Instrumentation	winmgmt	Automatic
Windows Management Instrumentation Driver Extensions	Wmi	Manual
Windows Media Services	WMServer	Disabled



Tabla 3.2.6. Configuraciones de los servicios del sistema que deben habilitarse (... continuación)

Nombre completo del servicio	Nombre del Servicio	Tipo de Inicio del Servicio
Windows System Resource Manager	WindowsSystemResourceManager	Disabled
Windows Time	W32Time	Automatic
WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Disabled
Wireless Configuration	WZCSVC	Disabled
WMI Performance Adapter	WmiApSrv	Manual
Workstation	Lanmanworkstation	Automatic
World Wide Web Publishing Service	W3SVC	Disabled

6. Registro y sistema de archivos

6.1. Aseguramiento del sistema de archivos

Si bien es cierto que los permisos predeterminados de archivos en Windows Server 2003 son suficientemente seguros en las diferentes situaciones. Sin embargo, en entornos de configuraciones de servidores se debe considerar un mayor nivel de seguridad de ciertos archivos que pueden ser manipulados por usuarios malintencionados, para evitar esto se debe dar privilegios elevados a determinados archivos del sistema que impidan la mala manipulación y con ello lleven a la inestabilidad del sistema en general. Los archivos que se deben asegurar están ubicados en la carpeta **%SystemRoot%\System32** y a todos estos archivos que se detallan a continuación se les debe dar los siguientes permisos: **Administradores: Control total, Sistema: Control total.**

Tabla 3.2.7. Aseguramiento de ejecutables del sistema operativo

Asegurando archivos ejecutables de Windows Server 2003	
❖ regedit.exe	❖ ntbackup.exe
❖ arp.exe	❖ rcp.exe
❖ at.exe	❖ reg.exe
❖ attrib.exe	❖ regedt32.exe
❖ cacls.exe	❖ regini.exe
❖ debug.exe	❖ regsvr32.exe
❖ edlin.exe	❖ rexec.exe
❖ eventcreate.exe	❖ route.exe
❖ eventtriggers.exe	❖ rsh.exe
❖ ftp.exe	❖ sc.exe
❖ nbtstat.exe	❖ secdedit.exe
❖ net.exe	❖ subst.exe
❖ net1.exe	❖ systeminfo.exe
❖ netsh.exe	❖ telnet.exe
❖ netstat.exe	❖ tftp.exe
❖ nslookup.exe	❖ tlntsvr.exe

Para configurar estos permisos sobre estos archivos, lo puede realizar desde la ubicación del Group Policy Object Editor (Editor de objetos de directiva de grupo):

Computer Configuration\Windows Settings\Security Settings\File System También puede configurar los permisos de los archivos citados desde la plantilla de seguridad que se está creando, para ello debe expandir la plantilla y ubicarse en **File System** y luego ir buscando los archivos en el panel **Object Name** que está ubicado en la parte derecha y se encuentran bajo la carpeta **%SystemRoot%\System32**. Debe ubicar el archivo y luego dar doble clic sobre él, seguidamente se



le presentará una ventana de diálogo donde debe pulsar el botón **Edit Security**, esto le llevará a otra ventana de diálogo donde puede dar los permisos que se recomiendan para estos archivos y luego de manera consecutiva pulsar el botón **OK** que aparecen en las ventanas de diálogo, de esta manera estará dando una mayor seguridad al sistema operativo contra ataques malintencionados.

A parte de los permisos sobre determinados archivos que se deben configurar en un servidor miembro de un dominio, también se debe considerar la configuración de permisos sobre algunos directorios, estos permisos deben ser más restrictivos para así proteger directorios que almacenan información sensible a ataques. A continuación se muestran en la tabla, las carpetas o directorios que deben estar aseguradas o incluirse en la configuración de seguridad básica de un servidor miembro de un dominio.

Tabla 3.2.8. Configuración de permisos sobre directorios claves que deben considerarse en el aseguramiento básico de servidores miembros de un dominio

Carpetas aseguradas	Permisos aplicados
%systemdrive%\	Administradores: Control total Sistema: Control total Usuarios autenticados: Leer y ejecutar, Listar el contenido de la carpeta y Leer
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	Administradores: Control total Creador/Propietario: Control total Sistema: Control total
%systemdrive%\inetpub	Administradores: Control total Sistema: Control total Todos: Leer y ejecutar, Listar el contenido de la carpeta y Leer



ANEXO 3.3 CONVERSIÓN DE SERVIDORES MIEMBROS EN CONTROLADOR DE DOMINIO PRIMARIO Y DE BACKUP

CONFIGURACIÓN DEL CONTROLADOR DE DOMINIO PRIMARIO

En el esquema de seguridad para los servidores Windows del GDS, se ha configurado un servidor que actúa como **Controlador de Dominio Primario** y desde el cual se controla al resto de servidores miembros que son parte del dominio, para lograr este trabajo conjunto se debe instalar a Windows Server 2003 para que funcione como un Controlador de Dominio.

Detalles del servidor a Configurar

El servidor que se ha configurado como **Controlador de Dominio Primario** (PDC) de entre el conjunto de servidores Windows que tiene la UTPL es el servidor que tiene por nombre (hostname) **PDCSERVER** con la dirección IP **172.16.50.42** el cual está ejecutando Windows Server 2003 Enterprise Edition, éste servidor cuenta con una tarjeta de red de alta velocidad y un solo disco duro de 70 GB, el cual esta particionado en particiones de 40 y 30 GB respectivamente, en la partición de 40 GB se ha instalado el sistema operativo y en la partición de 30 GB se deja para datos y archivos de registro de Active Directory, para de esta forma cumplir como el PDC del grupo de servidores.

Configuración del Servidor PDCSERVER como Controlador de Dominio Primario

Para configurar el servidor PDCSERVER como Controlador de Dominio, se hace uso de las propias herramientas que trae incluidas el propio sistema operativo Windows Server 2003 Enterprise Edition, dentro del sistema operativo existen dos formas de configuración, una mediante el uso del Asistente para configuración y otra mediante la utilización de herramientas manuales o línea de comandos.

Del servidor PDCSERVER es de donde se va a administrar al grupo de los demás servidores Windows, por tal razón se debe configurar DNS y Active Directory, para llevar a cabo esta tarea, se procede de la siguiente manera:

1. Clic en **Start**, luego en **Run**, en la ventana de diálogo que se presenta se debe escribir **DCPROMO** y hacer clic en **OK**, la figura ilustra lo mencionado.

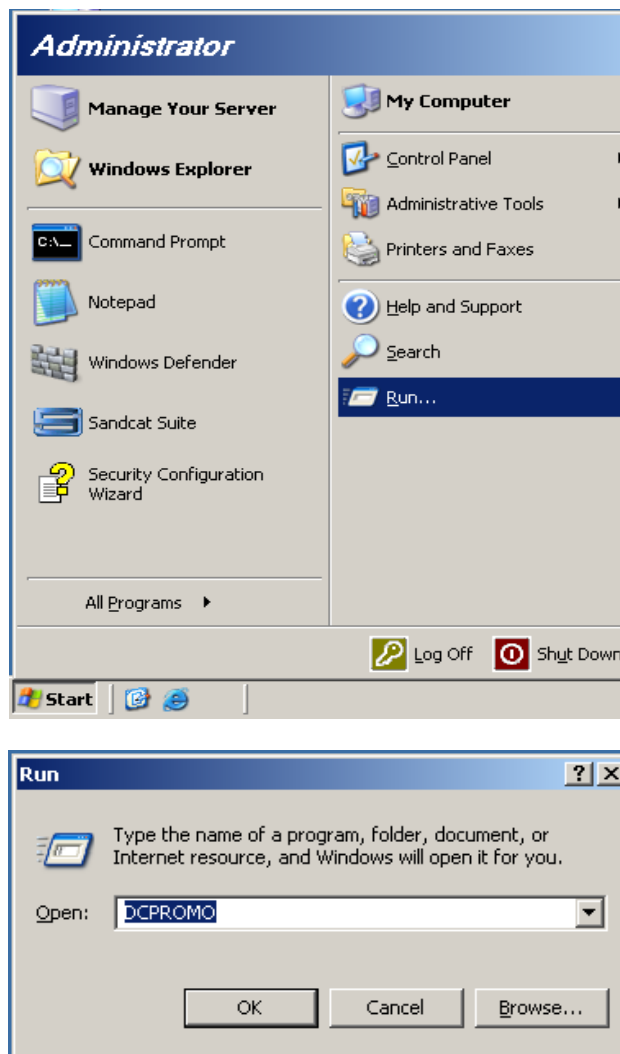


Figura 3.3.1. Pasos iniciales del PDC

2. Digitado **DCPROMO** en la ventana de diálogo **Run**, aparecerá el **Active Directory Installation Wizard**, (Asistente de configuración de Active Directory), en el que se debe hacer clic en **Next**, para comenzar con la instalación.



Figura 3.3.2. Wizard de instalación del PDC

3. El asistente de configuración de Active Directory presenta una ventana de diálogo de Compatibilidad del sistema operativo (Operating System Compatibility), el cual se debe revisar y luego pulsar en **Next**.

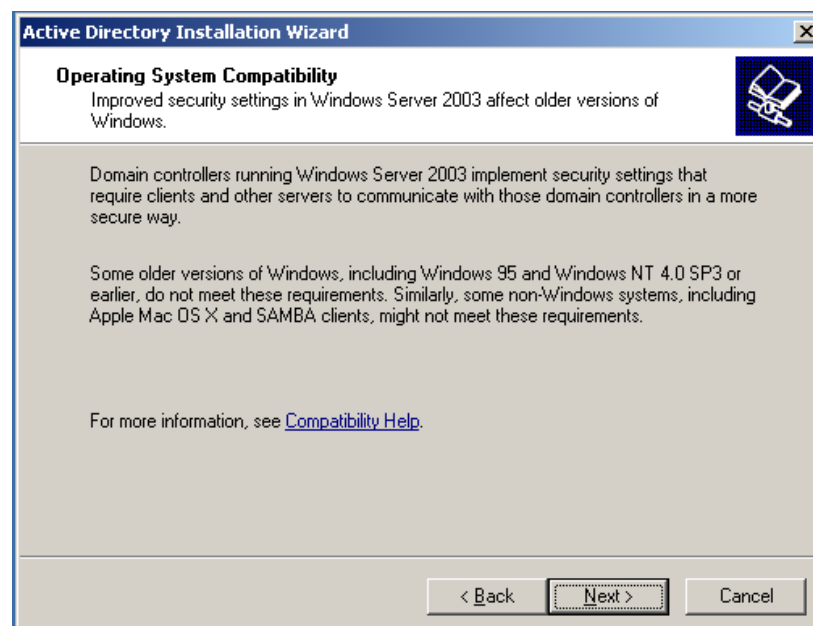


Figura 3.3.3. Diálogo de revisión de compatibilidad del sistema operativo

4. En el diálogo siguiente se debe escoger el **Tipo de Controlador de Domino** (Domain Controller Type), en este caso se selecciona **Controlador de Dominio para un Dominio Nuevo** (Domain Controller for a new domain) y pulsar en el botón **Next**.

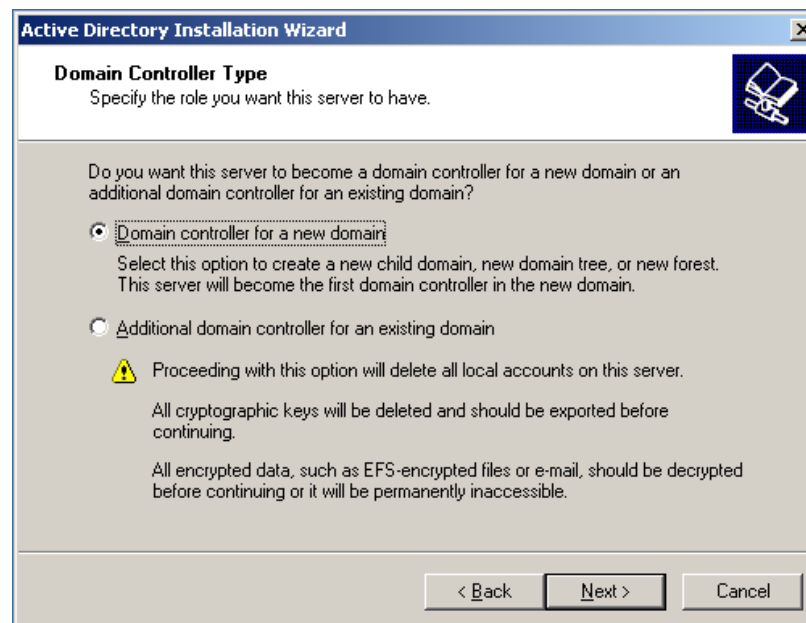


Figura 3.3.4. Selección del tipo de Controlador de Dominio que va a ser el server

5. Seleccionado el tipo de controlador de dominio, se debe **Crear el Nuevo Dominio**, para ello se debe escoger la opción predeterminada de **Dominio en un Nuevo Bosque** (Domain in a new forest) y pulsar en **Next**.

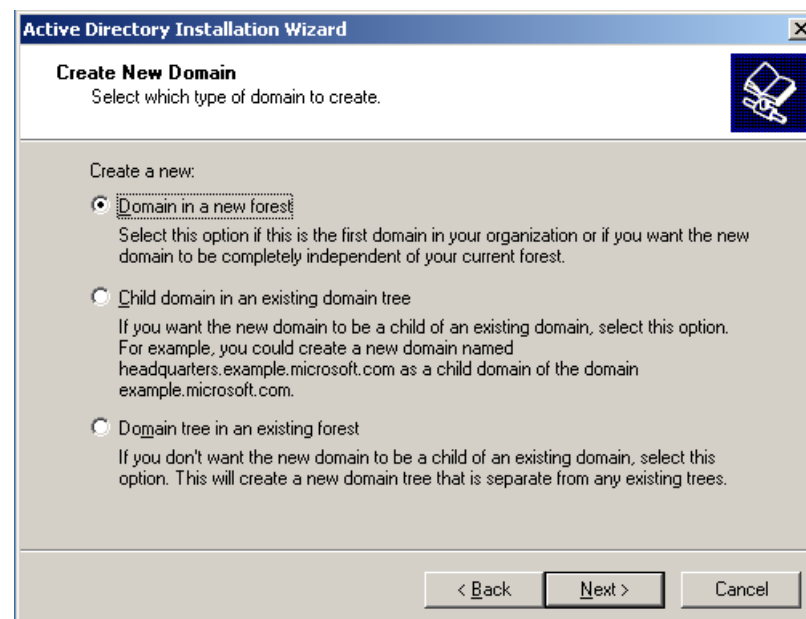


Figura 3.3.5. Selección del Dominio en el nuevo bosque

6. En la ventana de diálogo que pide el **Nombre del Nuevo Dominio**, en el cuadro de diálogo de **Nombre de DNS Completo para el nuevo Dominio** (Full DNS name for new domain), se escribe **utpl.edu.ec** y luego se pulsa el botón **Next**.

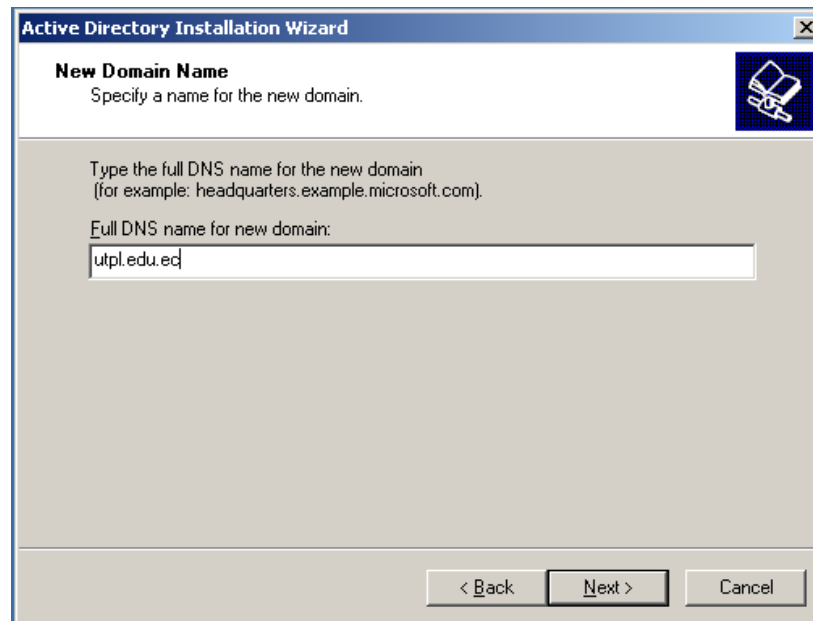


Figura 3.3.6. Ingreso del nombre de Dominio

7. En la asignación de **Nombre NetBIOS del Dominio** (Domain NetBIOS name) se acepta la opción predeterminada en este caso **UTPL** y se pulsa en el botón **Next**.

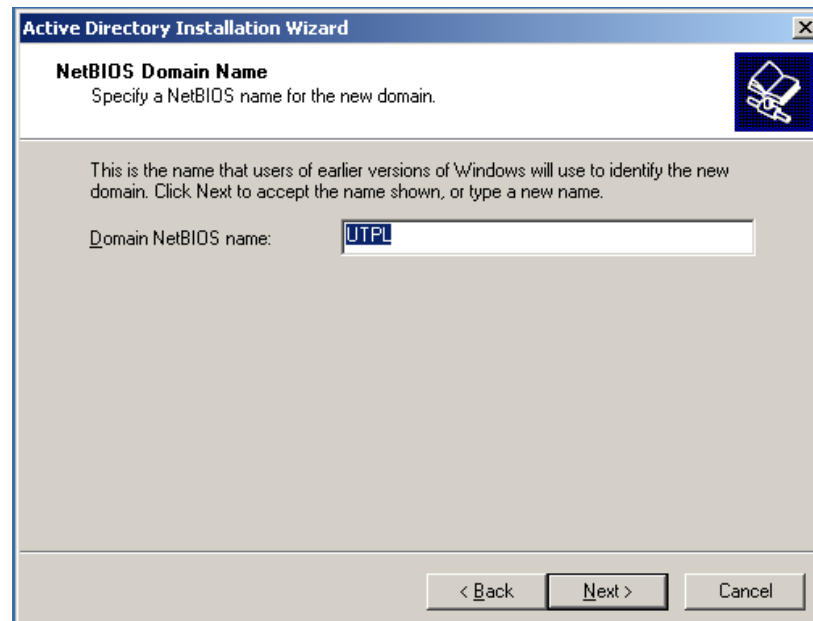


Figura 3.3.7. Opción predeterminada de Nombre NetBIOS del Dominio

8. Una vez que se ha predeterminado el Nombre NetBIOS del Dominio, se debe establecer las carpetas de la **Base de Datos** y del **registro** para Active Directory, pues la carpeta de **base de datos** (Database folder) va a estar direccionada a la primera partición en este caso **C:\Windows\NTDS** y la **carpeta de registro** (Log folder) debe apuntar a **D:\Windows\NTDS** y a continuación se debe pulsar en el botón **Next**.

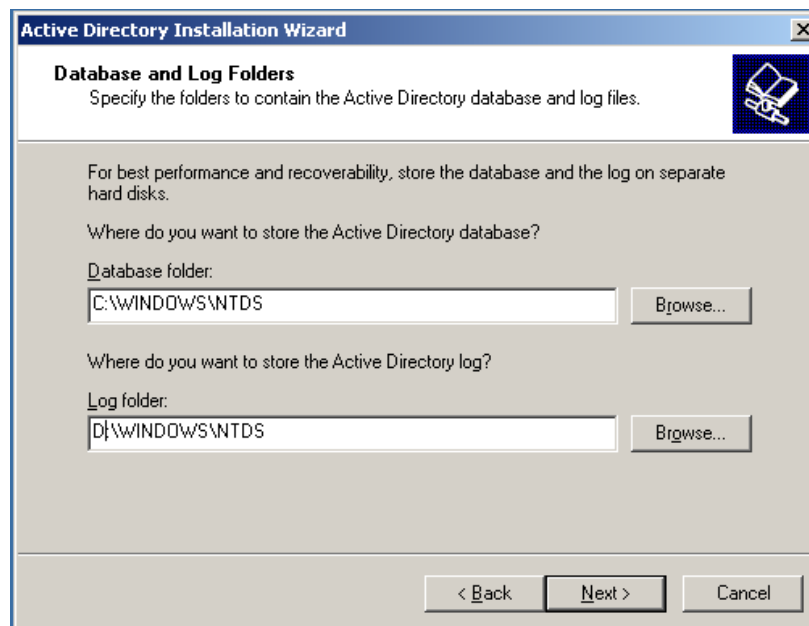


Figura 3.3.8. Selección de carpetas de base de datos y registro para Active Directory

9. En la ventana de diálogo **Volumen del Sistema Compartido** (Shared System Volume), se debe dejar la **localización de la carpeta** predeterminada (Folder location) y después pulsar el botón **Next**.

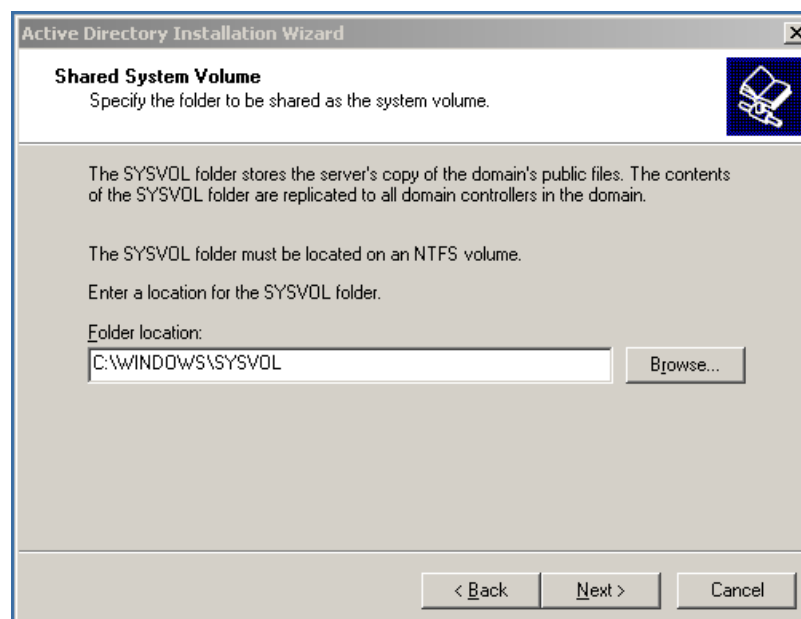


Figura 3.3.9. Especificación de la carpeta para el volumen del sistema compartido

10. En la pantalla de **Diagnóstico de registro de DNS**, se selecciona la opción **Instalar y configurar el servidor DNS en este equipo, y utilizar este equipo como servidor DNS predefinido** (Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server), luego pulsar en el botón Next.

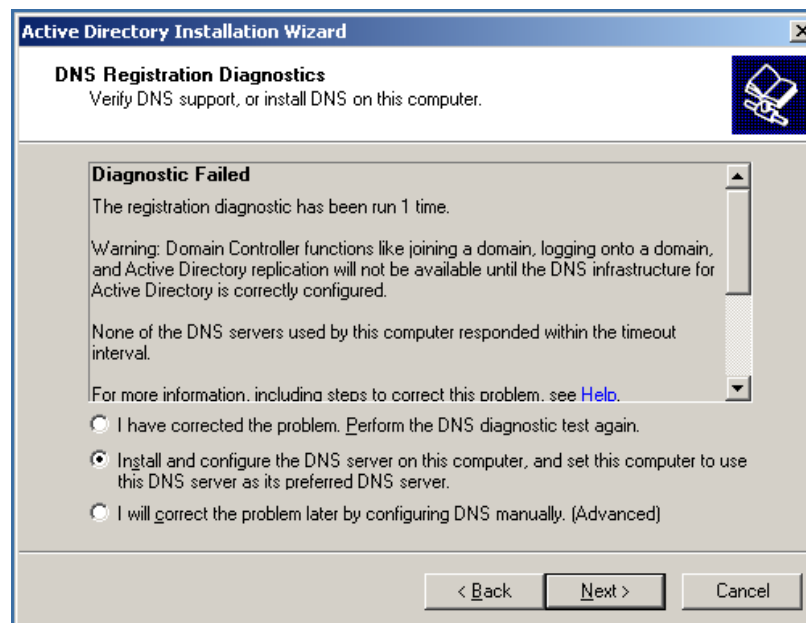


Figura 3.3.10. Verificación del soporte DNS o instalación del DNS en el servidor

11. En la pantalla Permisos, se escoge la opción **Permisos compatibles sólo con sistemas operativos de servidor Windows 2000 o Windows Server 2003** (Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems), y pulsar el botón Next.

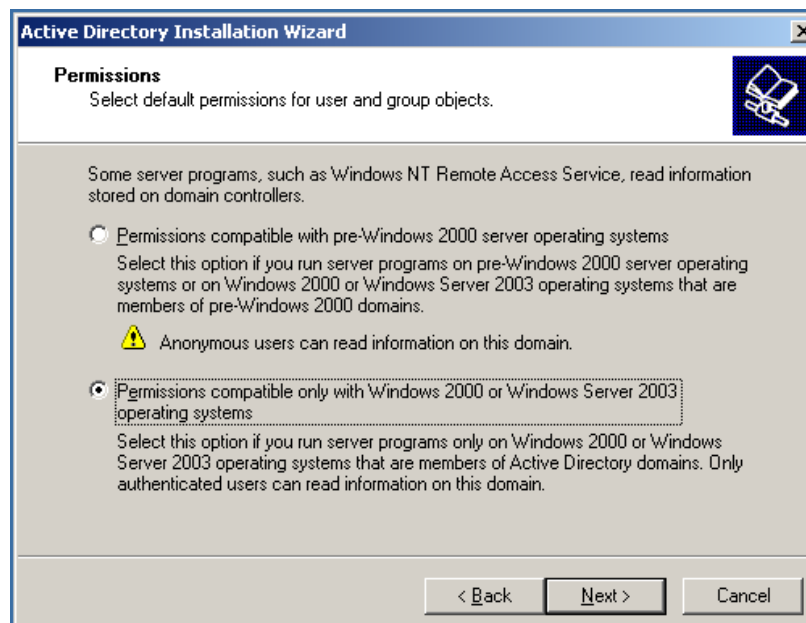


Figura 3.3.11. Selección de permisos por defecto para usuarios y grupos de objetos

12. En la ventana de diálogo que solicita contraseña, debe ingresar una **Contraseña de modo de restauración y Confirmar contraseña** (Restore Mode Password, Confirm password), las contraseñas ingresadas deben ser de un alto nivel de complejidad, luego debe pulsar sobre el botón **Next**.

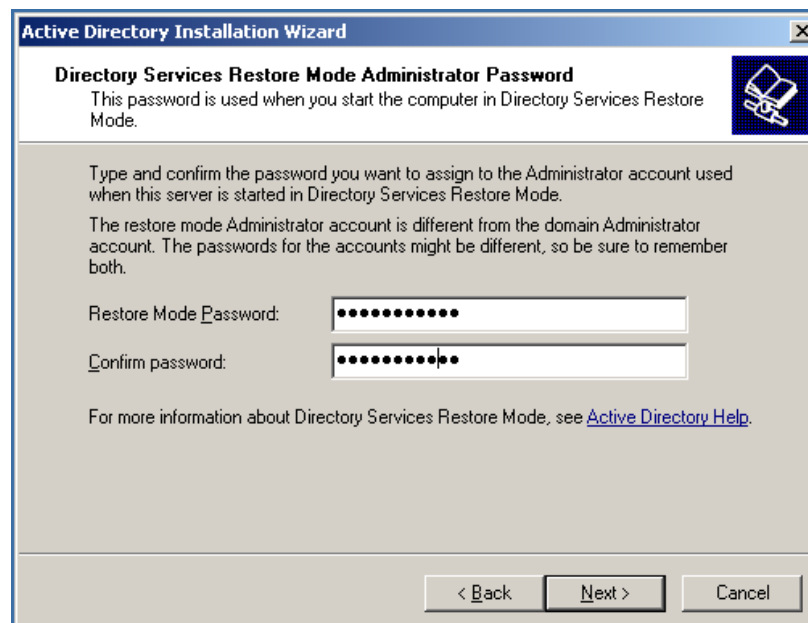


Figura 3.3.12. Ingreso de contraseñas del modo de restauración

13. En la pantalla de **resumen** (Summary), se presenta algunas de las opciones de instalación de Active Directory, la cual se debe revisar y pulsar en el botón **Next**, si está de acuerdo con lo seleccionado y empezar la instalación de Active Directory, en este paso pide que se ingrese el CD de instalación de Windows Server 2003 Enterprise Edition.

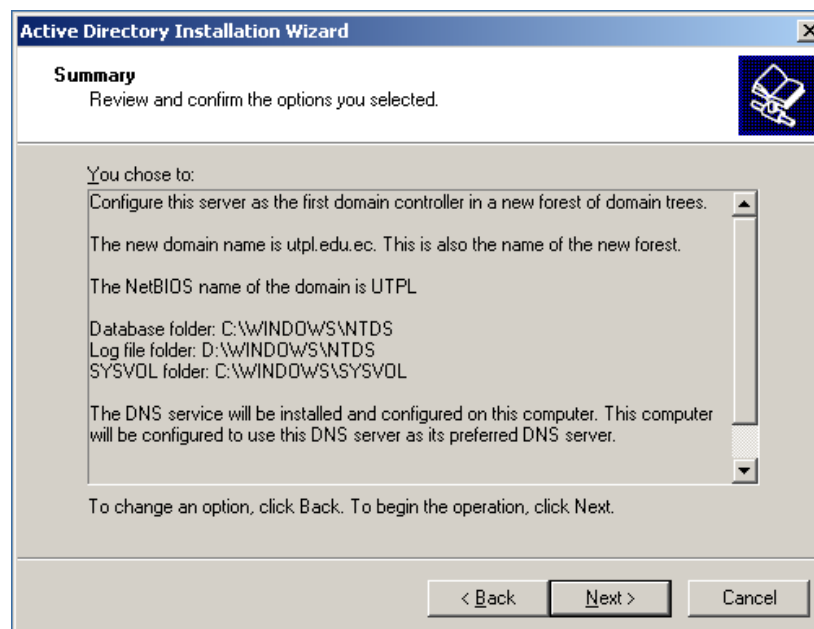


Figura 3.3.13. Revisión y confirmación de las opciones seleccionadas para instalar Active Directory

14. Una vez que se ha completado la instalación de Active Directory, aparece la siguiente ventana de diálogo, en donde se debe pulsar en **Finish**, luego se le presentará una pantalla donde se debe pulsar en el botón **Restart Now** y al siguiente inicio de sesión el servidor estará actuando como PDC.



Figura 3.3.14. Finalizando la instalación de Active Directory en el servidor PDCSERVER

15. Durante la conversión del servidor a Controlador de Dominio, es necesario realizar la configuración de la interfaz de red, para lo cual debe ir a **Control Panel**, seleccionar **Network Connections** y luego dar clic en **Local Area Connection**, luego se presentará una ventana de diálogo donde debe dar clic en el botón de **Properties** ubicado en la pestaña **General** y en la siguiente sección, se presenta una pestaña de nombre **General** donde se debe hacer clic en **Internet Protocol (TCP/IP)** y nuevamente dar clic en **Properties** y seleccionar **Use the following IP address**, a continuación, en **IP address** se escribe **172.16.50.42** y como **Subnet mask 255.255.0.0**, como **Default Gateway** se deja vacío. Seguidamente, se selecciona **Use the following DNS server address** e ingresar la dirección **127.0.0.1** como **Preferred DNS server** y luego pulsar el botón **OK**, y cerrar las demás ventanas consecutivas que se presenten.

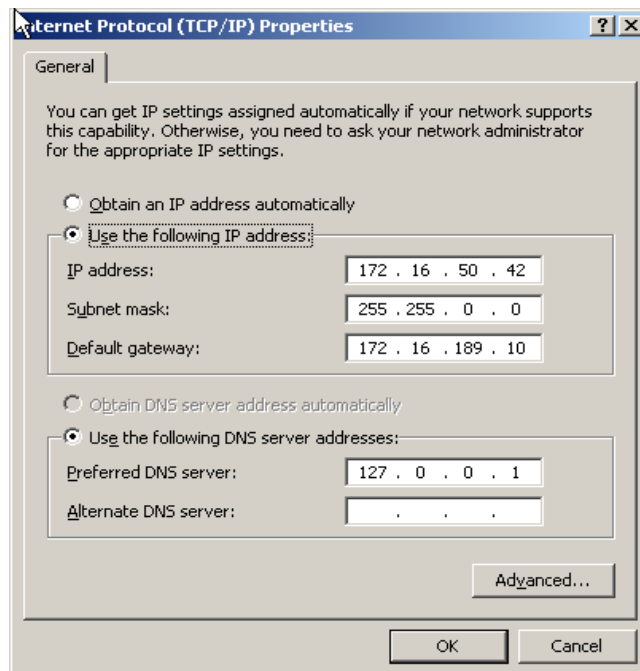


Figura 3.3.15. Asignación de dirección IP al servidor PDCSERVER



CREACIÓN DE UN CONTRLADOR DE DOMINIO SECUNDARIO

En todo dominio de red que se desee mejorar la administración y seguridad, es necesario configurar un **Controlador de Dominio de Respaldo** (BDC), tal es el caso en la implementación del esquema de seguridad para los servidores Windows de la UTPL, se es necesario tener un Controlador de Dominio Primario y uno de Backup que sirva de respaldo cuando el Controlador de Dominio Primario falle por cualquier circunstancia, el servidor que se ha considerado para estos propósitos es **DEVSERVER** y que tiene la dirección **IP 172.16.50.62**, a continuación se detalla el proceso de creación del **Controlador de dominio de Respaldo**.

1. Se empieza iniciando sesión como administrador en el servidor que se baya a configurar como Controlador de Dominio de Respaldo.
2. Se hace clic en **Start, Run** y en la ventana que aparece se escribe **DCPROMO /ADV**, esto presentará el Asistente para instalación de Active con la opción de crear un controlador de dominio adicional.

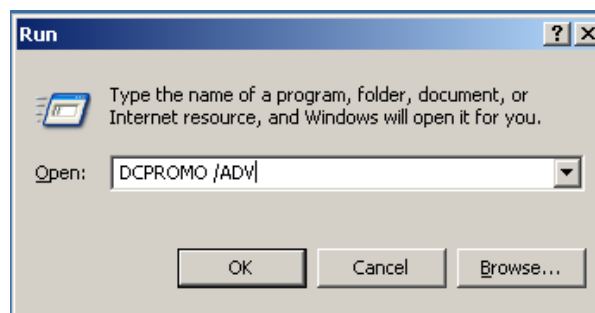


Figura 3.3.16. Comandos para crear el BDC

3. En la pantalla de Compatibilidad de Sistema Operativo lea la información y haga clic en **Next**.
4. En la pantalla de **Domain Controller Type** (Tipo de Controlador de Dominio), escoja la opción **Additional domain controller for an existing domain** (Controlador de Dominio Adicional para un Dominio Existente), luego haga clic en **Next**.

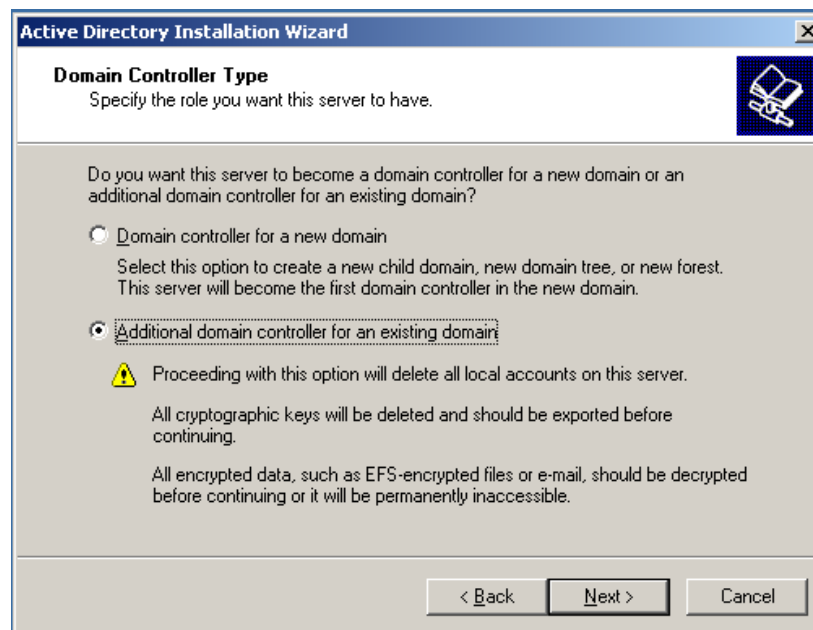


Figura 3.3.17. Selección del tipo de Controlador de Dominio

5. En la ventana de diálogo **Copying Domain Information** (Copiar Información del Dominio), seleccione **Over the network from a domain controller** y luego haga clic en **Next**.

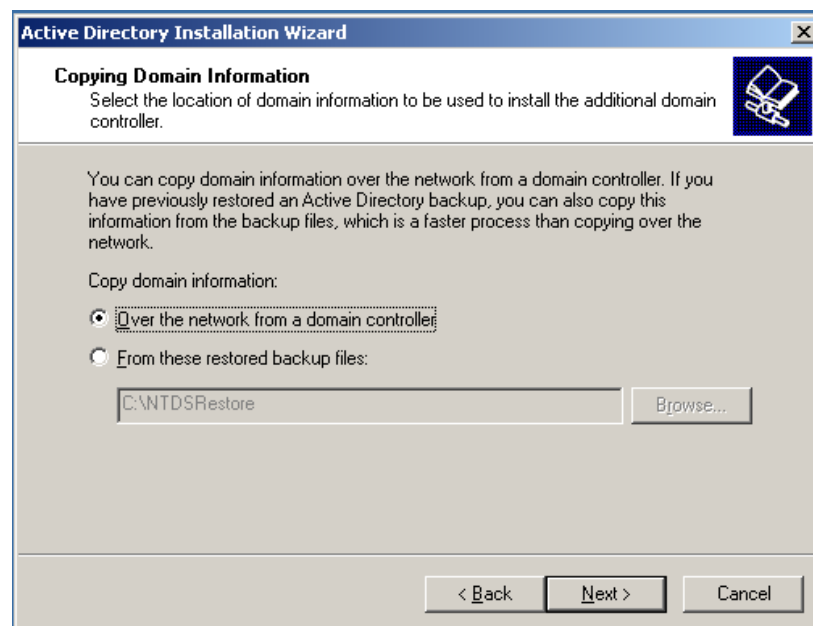


Figura 3.3.18. Selección de información del dominio local

6. En la pantalla de **Network Credentials**, se especifica el **User name**, **Password** y **Domain** de la cuenta de un usuario que se va a utilizar para operar el servidor. La cuenta debe pertenecer al grupo Administradores de Dominio del dominio destino.

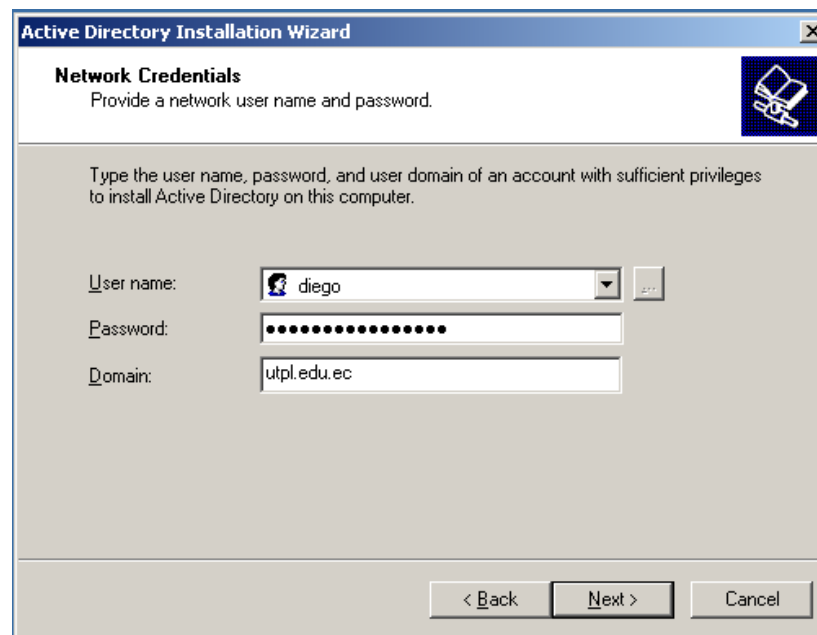


Figura 3.3.19. Ingreso de credenciales de red

7. En el diálogo siguiente se debe especificar el nombre del dominio para el cual el servidor que está siendo configurado va hacer de **Controlador de Dominio Adicional**.

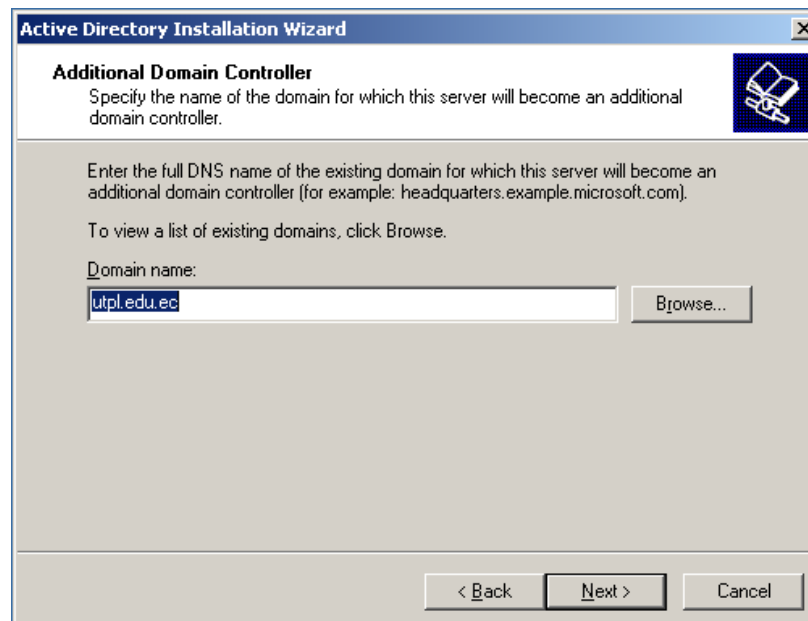


Figura 3.3.20. Ingreso del nombre del dominio

8. A continuación en la siguiente pantalla se debe escoger la ruta de almacenamiento para la Base de Datos (C:\WINDOWS\NTDS) y para los registros (E:\WINDOWS\NTDS) de Active Directory, y luego dar clic en **Next**.
9. En la siguiente pantalla de **Shared System Volume** se debe ingresar la ubicación en donde se desea instalar la carpeta SYSVOL, se deja la predeterminada (C:\WINDOWS\SYSVOL) y se da clic en **Next**.



10. En la pantalla de Directory **Services Restore Mode Administrator Password**, se debe escribir la contraseña que se utiliza al iniciar el equipo en el modo de restauración de servicios de directorio. Luego haga clic en **Next**.
11. Finalmente se visualiza una pantalla de **Summary** la cual contiene información que se ha seleccionado en los pasos previos, cerciórese que sea información correcta y pulse en **Next**. Luego se inicia el proceso de configuración y creación del **Controlador de Dominio de Respaldo**, al finalizar este proceso, se debe reiniciar el Servidor, para que las configuraciones tengan efecto.



ANEXO 3.4 CONFIGURACIÓN DE FIREWALLS EN CADA SERVIDOR MIEMBRO DEL GDS DEL DOMINIO UTPL

Aplicando y siguiendo el proceso descrito en el manual de políticas y procedimientos (**PR12**) para configurar el firewall en cada equipo servidor que forma parte del dominio Windows del GDS, se tiene lo siguiente:

PDCSERVER

Para el servidor PDCSERVER que es el **Controlador de Dominio Primario** se hace las siguientes configuraciones desde el **panel de control** y escogiendo la opción **Windows Firewall**, en la pestaña de Excepciones y Avanzado se permite o deniega los servicios, aplicaciones o puertos de manera particular, para el caso del servidor PDCSERVER, se realiza las siguientes configuraciones.

Configuración Firewall del PDCSERVER	
Servicio/Programa	Puerto
Active Directory	389
Base de Datos ARPA	1521
Domain Name System (DNS)	53
FTP Server	21
Recursos Compartidos	445
Remote Desktop	3389
Servicio de sesiones	139
Internet Explorer, Web Server (HTTP)	80

Todas las demás configuraciones firewall sobre los demás servidores tendrán y utilizarán el mismo proceso de configuración seguido para el PDCSERVER, solo difieren en las aplicaciones y servicios que se permitirán de manera individual en cada uno.

DEVSERVER

Es el servidor que opera como **Controlador de Dominio de Respaldo**, por lo que incluye las configuraciones del PDCSERVER, más las propias de las aplicaciones que almacena.

Configuración Firewall del DEVSERVER	
Servicio/Programa	Puerto
SharePoint	8080

WSUTPL

Es el servidor del GDS que está en conexión directa con el internet, y de igual forma ofrece los servicios que presta la UTPL a los usuarios. Por el hecho de ser un servidor crítico, se debe configurar el firewall de buena manera.



Configuración Firewall de WSUTPL	
Servicio/Programa	Puerto
Active Directory	389
FTP Server	21
Recursos Compartidos	445
Remote Desktop	3389
Servicios de Sesiones	139
Web Server (HTTP)	80

ASUTPL

Es el servidor que brinda servicios alternos del Sistema Académico del GDS, además contiene otras aplicaciones como los servicios de digitalización, por esto la configuración firewall es igual a la del servidor WSUTPL, más el permiso en el firewall de servicio de mail y Base de Datos SQL Server.

Configuración Firewall de ASUTPL	
Servicio/Programa	Puerto
Internet Mail Server (SMTP)	25
SQL Server 2000	1433

CATAMAYO

Es el servidor que contiene Bases de Datos SQL Server 2000/2005, por lo que a más de las configuraciones que se hacen en el servidor WSUTPL, debe permitirse en el firewall los puertos en que trabajan las Bases de Datos.

Configuración Firewall de CATAMAYO	
Servicio/Programa	Puerto
SQL Server	1433

CALSERVER

Es el servidor que mantiene el sistema de calificaciones automáticas, por lo que debe configurar el firewall de la siguiente manera.

Configuración Firewall de CALSERVER	
Servicio/Programa	Puerto
Active Directory	389
Base de Datos Oracle BAAN	1521
Base de Datos Oracle SGA	
FTP Server	21
Recursos Compartidos	445
Servicios de Sesiones	139

NODO1SGA

Es el servidor donde está instalado todo el Sistema Académico Principal con todas sus aplicaciones complementarias, el firewall se configura de manera idéntica al servidor CALSERVER.

DIGITSERVER

Es el servidor que almacena las evaluaciones a los estudiantes de modalidad abierta, por lo que el firewall debe estar configurado de la siguiente manera.



Configuración Firewall de DIGITSERVER	
Servicio/Programa	Puerto
Active Directory	389
FTP Server	21
Recursos Compartidos	445
Servicios de Sesiones	139

TSTSERVER

Es un servidor de pruebas y por ello contiene varias aplicaciones que deben ser habilitadas en el firewall.

Configuración Firewall de TSTSERVER	
Servicio/Programa	Puerto
Active Directory	389
Bases de Datos de pruebas	1521
Base de Datos Oracle SGA	
Base de Datos Oracle, BAAN	
FTP Server	21
Recursos Compartidos	445
Remote Desktop	3389
Servicios de Sesiones	139
Web Server (HTTP)	80

DEVGDS

Es un servidor de desarrollo, y de igual forma deben habilitarse en el firewall todas las aplicaciones que contiene para un buen funcionamiento. Se configura el firewall de igual forma que el firewall del servidor TSTSERVER.

BDDGDS

Es el servidor que contiene netamente bases de datos, por lo que debe de fortalecerse dichas aplicaciones tras una buena configuración del firewall.

Configuración Firewall de BDDGDS	
Servicio/Programa	Puerto
Active Directory	389
Bases de Datos Oracle 9i, desarrollo y pruebas	1521
Recursos Compartidos	445
Servicios de Sesiones	139

DEVCRM

Es un servidor de pruebas y desarrollo, por lo que el firewall debe configurarse de acuerdo a las necesidades.

Configuración Firewall de DEVCRM	
Servicio/Programa	Puerto
Active Directory	389
Recursos Compartidos	445
Servicios de Sesiones	139
SQL Server	1433
Web Server (HTTP)	80

ANEXO 3.5 CREACIÓN DE UNA LÍNEA BASE DE SEGURIDAD DE SERVIDORES MIEMBRO

Para crear la línea base de seguridad de servidores miembro, se utiliza la **Security Configuration Wizard (SCW)**, ésta guía de configuración de Seguridad permite crear la línea base en un servidor miembro estándar, para que luego esta línea de seguridad base se la convierta en un objeto de directiva de grupo (GPO) y se la aplique al resto de servidores miembros que conforman el dominio **utpl.edu.ec** de servidores Windows. Mediante SCW es posible incluir la plantilla de seguridad de línea de base de servidores miembro que se ha elaborado acorde a las necesidades de seguridad de los servidores Windows del GDS de la UTPL.

El servidor **ASUTPL** se ha escogido para crear la directiva de seguridad mediante SCW, esta directiva es un archivo de tipo XML que está almacenado en **%systemdir%\security\msscw\Policies** y puede ser aplicada al resto de servidores miembros mediante las Unidades Organizacionales de Active Directory.

El Proceso de creación de la directiva SCW es el siguiente:

1. Se inicia sesión como administrador en **ASUTPL**
2. Ir a **Start, Run** y digitar **scw.exe** y luego **OK**.

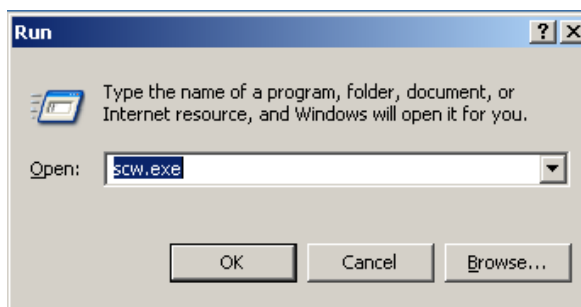


Figura 3.5.1. Iniciar la herramienta SCW

3. En la pantalla siguiente se presenta el inicio de la herramienta SCW, donde proporciona información de seguridad que se puede configurar con esta herramienta, ahí se debe dar clic en **Next**.
4. En la pantalla de la acción a configurar se debe seleccionar **Create a new security policy**, y luego dar clic en **Next**.

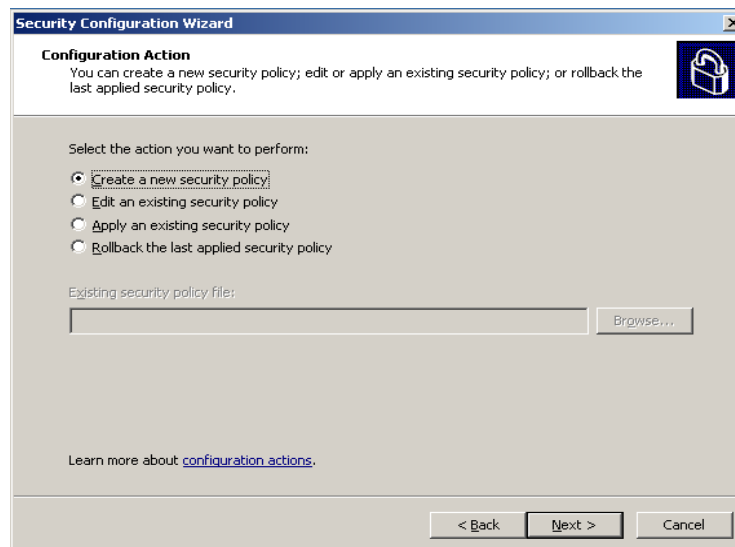


Figura 3.5.2. Selección de la acción que se quiere configurar

5. En la siguiente pantalla de diálogo se ingresa o deja el propio nombre del server que esta por defecto, en este caso **ASUTPL**, y se pulsa luego el botón **Next**.
6. En la pantalla que se presenta se puede consultar o ver la configuración de la base de seguridad y lo que es posible configurar con la herramienta SCW, luego se pulsa en botón **Next**.

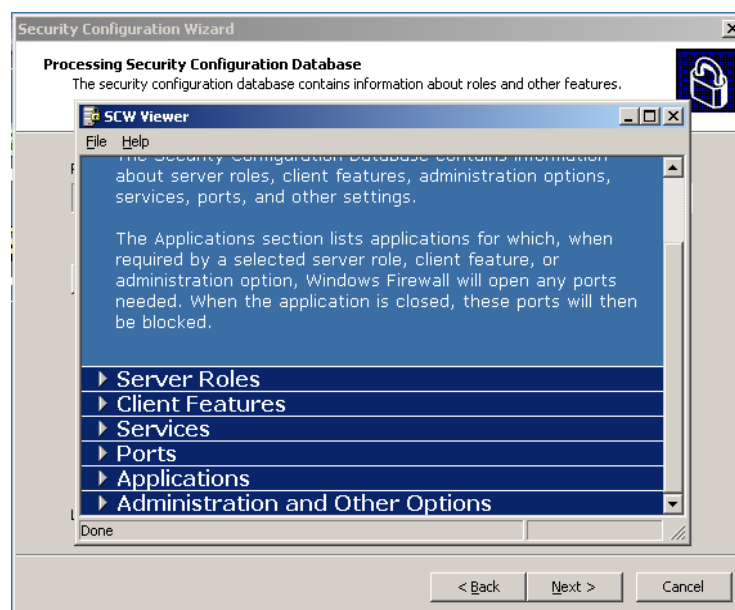


Figura 3.5.3. Visualización de la Base de Datos de Configuración de Seguridad

7. Luego aparece la pantalla de **Role-Based Service Configuration**, la cual visualiza información de configuración de servicios, lo cual se lee y se pulsa en **Next**.
8. En la pantalla de selección de roles para el servidor se empieza a seleccionar los roles instalados o los que se desea instalar para el servidor **ASUTPL**, luego de seleccionados se pulsa en **Next**.

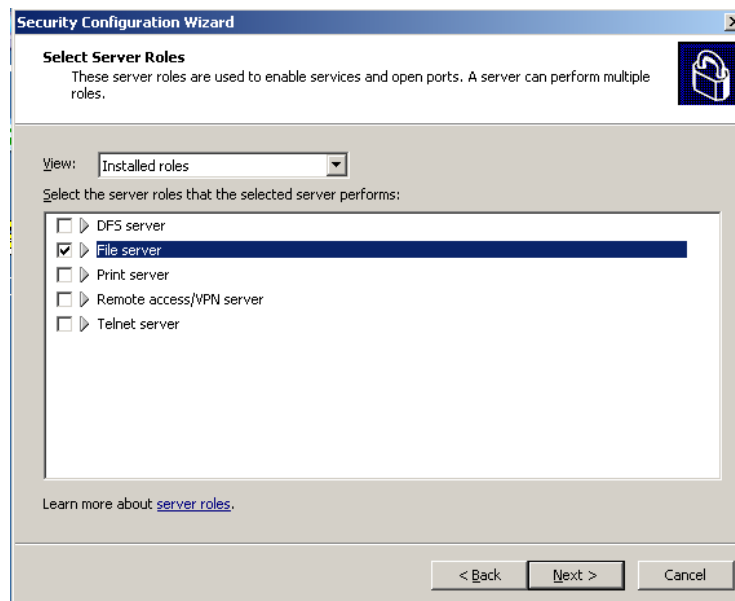


Figura 3.5.4. Selección de roles del servidor ASUTPL

9. En la pantalla de selección de características cliente, se selecciona solo las necesarias para que el servidor interactúe en el dominio con el resto de equipos y así no quede aislado, luego de seleccionar las necesarias para el server **ASUTPL**, se da clic en el botón **Next**.

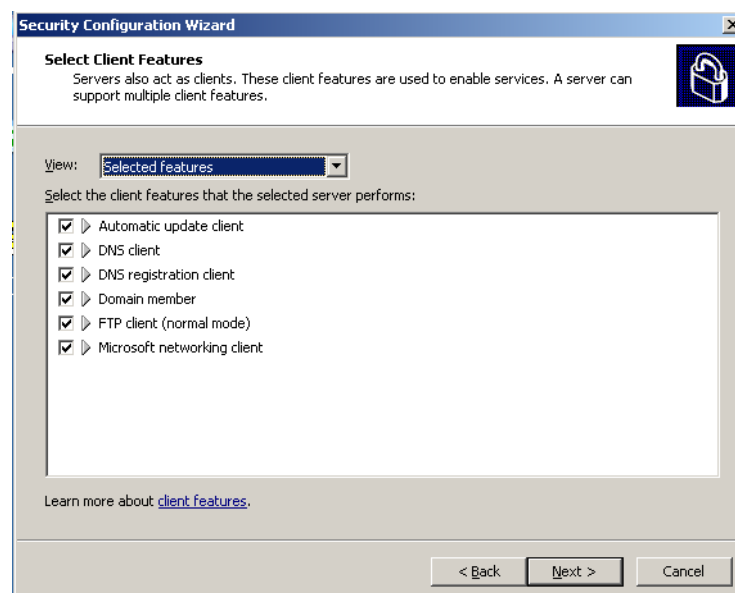


Figura 3.5.5. Características a ser habilitadas en ASUTPL

10. En la pantalla de selección de otras opciones de Administración se escoge las necesarias y a continuación se pulsa en **Next**.

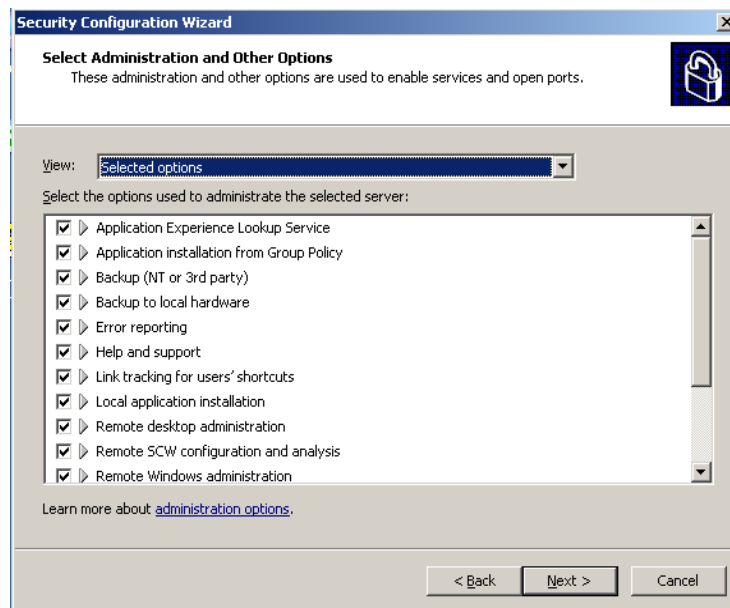


Figura 3.5.6. Selección de Opciones de Administración

11. Luego se presenta una pantalla de Selección de servicios adicionales, no debe haber inconveniente en esta selección, por lo que debe dar clic en **Next**, y de igual forma en la pantalla de **Handling Unspecified Services**. Luego se presenta otra pantalla donde se debe confirmar el cambio de servicios según la directiva que está configurando, se revisa y luego se da clic en **Next**.

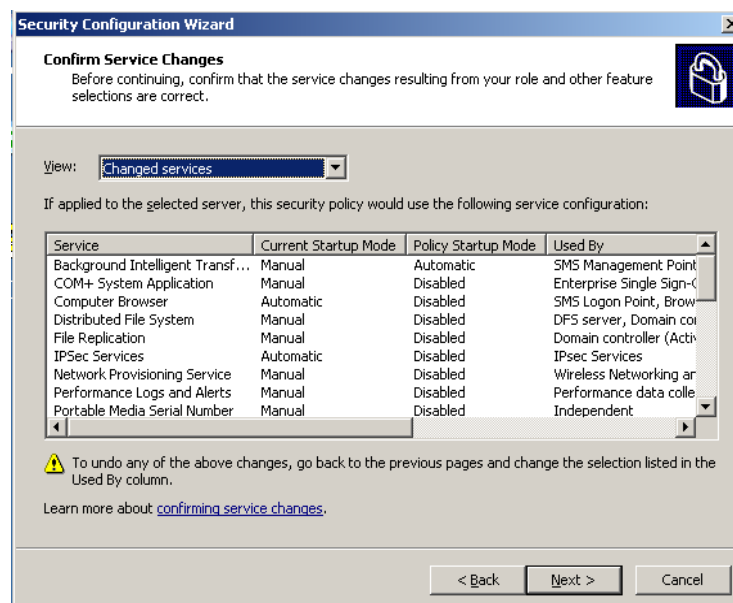


Figura 3.5.7. Confirmación de cambios de servicios en el servidor

12. Luego aparece una pantalla donde se describe información previa a la **configuración de la seguridad de la red**, la cual la puede saltar, pero en este caso se procede a configurar.



Figura 3.5.8. Configuración de la seguridad de la red

13. Se presenta la ventana de diálogo **Open Ports and Approve Applications**, es aquí donde se especifican los puertos que van a estar habilitados en el servidor y van hacer utilizados por las aplicaciones que se instalen en el servidor, por lo que se pueden agregar puertos adicionales de no estar habilitados, luego de habilitar los puertos necesarios se da clic en **Next**.

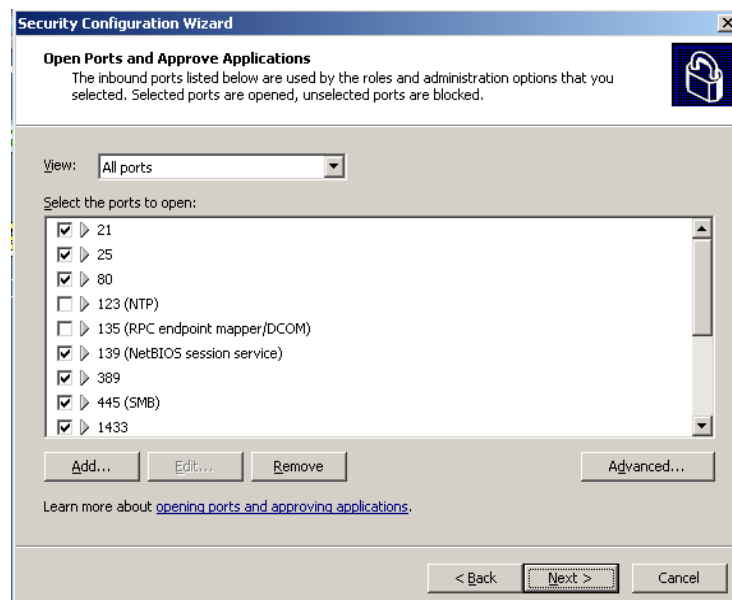


Figura 3.5.9. Abriendo puertos y confirmando los puertos habilitados

14. Luego aparece una pantalla donde se debe confirmar las tareas del paso anterior y de igual forma pulsar luego el botón **Next**.

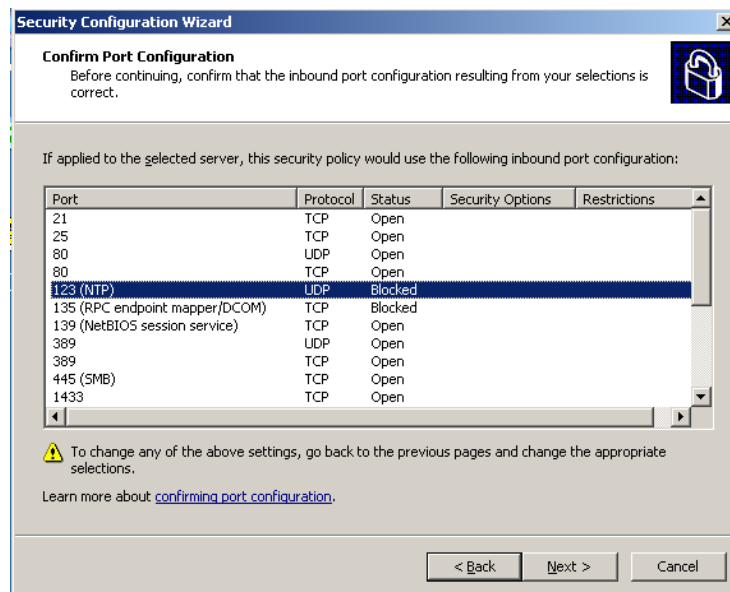


Figura 3.5.10. Confirmación de puertos

15. Configurada la **seguridad de red**, se empieza seguidamente la **configuración del registro**, lo puede obviar, pero el objetivo de la configuración mediante SCW es reducir lo mayor posible la superficie de exposición de un servidor a ataques a su sistema. Es por ello que debe pulsar el botón **Next** para proceder a la **configuración de seguridad del registro**.
16. En la pantalla de **Require SMB Security Signatures**, se selecciona los dos atributos disponibles y luego se da clic en **Next**.

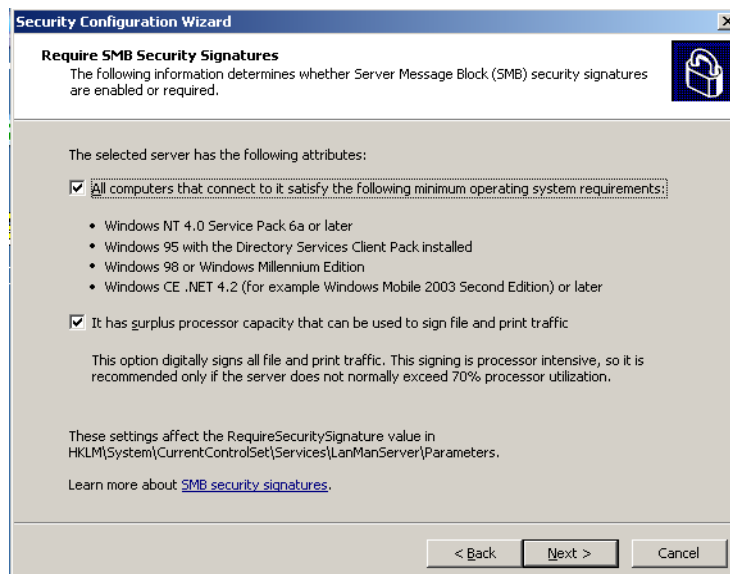


Figura 3.5.11. Aseguramiento del Bloque de Mensajes de servidor (SMB)

17. En la pantalla **Outbound Authentication Methods**, se deja seleccionado la opción por defecto (Domain Accounts), pues esto le utilizar métodos de autenticación para conexiones salientes del servidor. Luego se hace clic en **Next**.

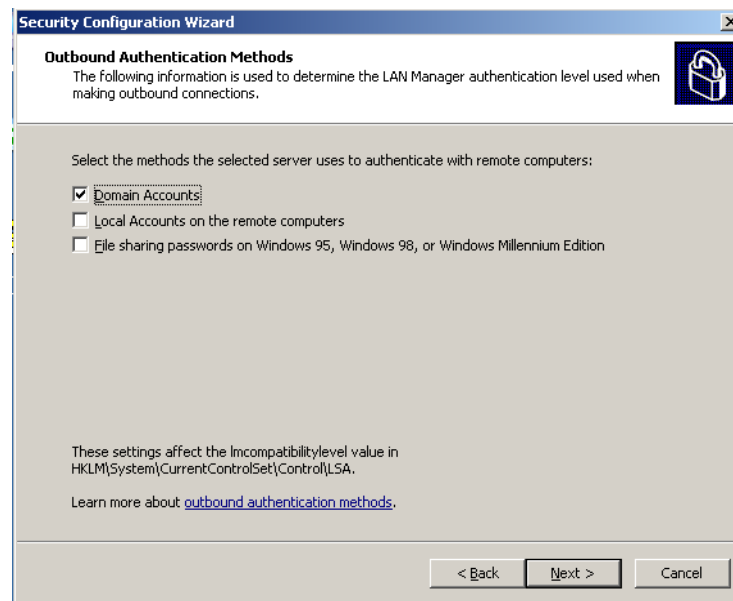


Figura 3.5.12. Autenticación de las conexiones salientes

18. Luego en la pantalla **Outbound Authentication using Domain Accounts**, se deja los valores seleccionados por defecto y se pulsa en **Next**.
19. Finalmente se presenta una pantalla donde se resume las configuraciones de seguridad sobre el registro, se las revisa y se pulsa luego el botón **Next**.

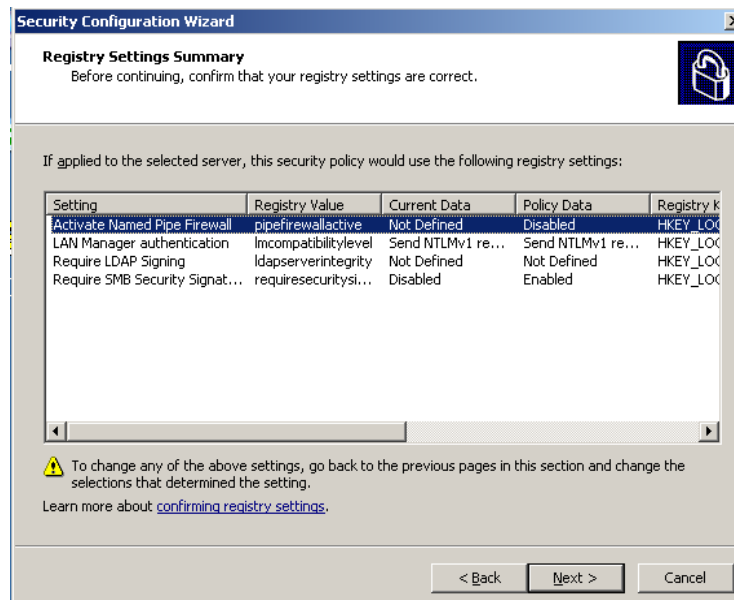


Figura 3.5.13. Resumen de Configuración del registro

20. Una vez que se ha configurado el registro, se procede a **configurar las directivas de auditoría**, de igual manera el SCW permite obviar esta configuración, pero para crear la línea de base de seguridad, se debe proceder a su configuración, para ello debe pulsar en el botón **Next**.
21. En la pantalla **System Audit Policy**, escoger la opción **Audit successful activities**, y luego pulsar en **Next**.

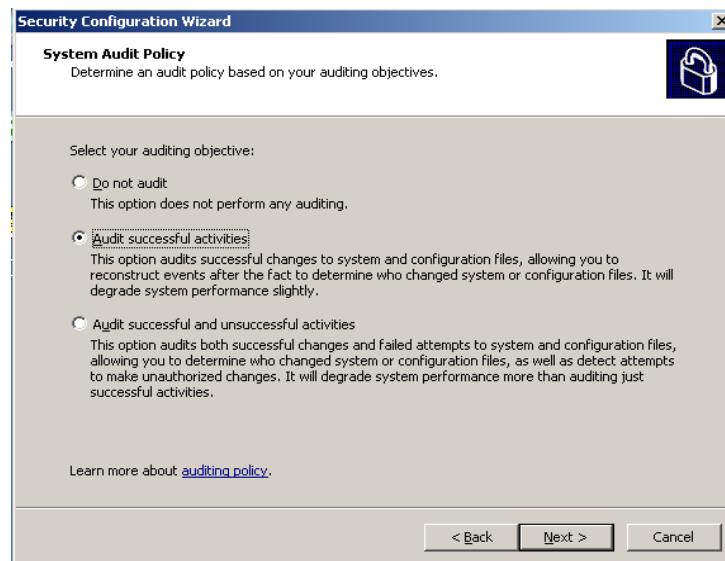


Figura 3.5.14. Políticas de auditoría del sistema

22. En la pantalla **Audit Policy Summary**, se presentan las configuraciones actuales y las que se habilitan en el servidor, revisadas las configuraciones se pulsa el botón **Next**.

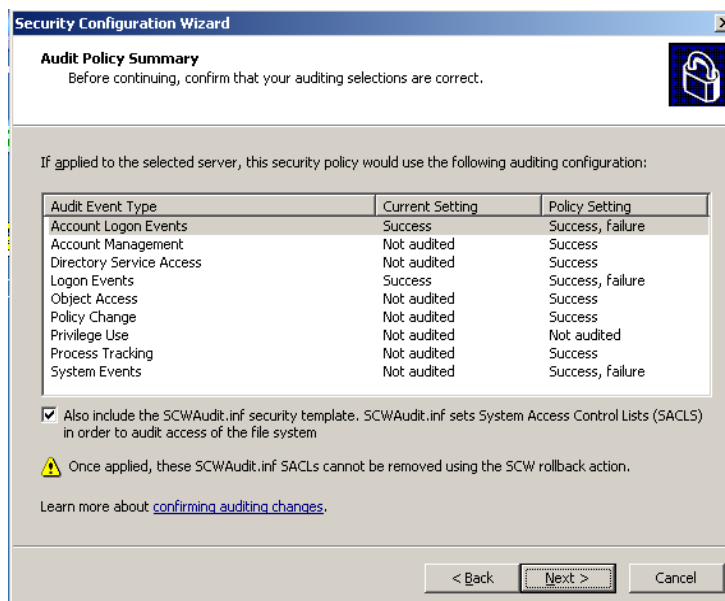


Figura 3.5.15. Resumen de políticas de auditoría

23. Configuradas las directivas de auditoría, se presenta una pantalla que proporciona información relacionada con las configuraciones realizadas por el SCW las cuales se deben guardar para continuar, para ello debe pulsar el botón **Next**.

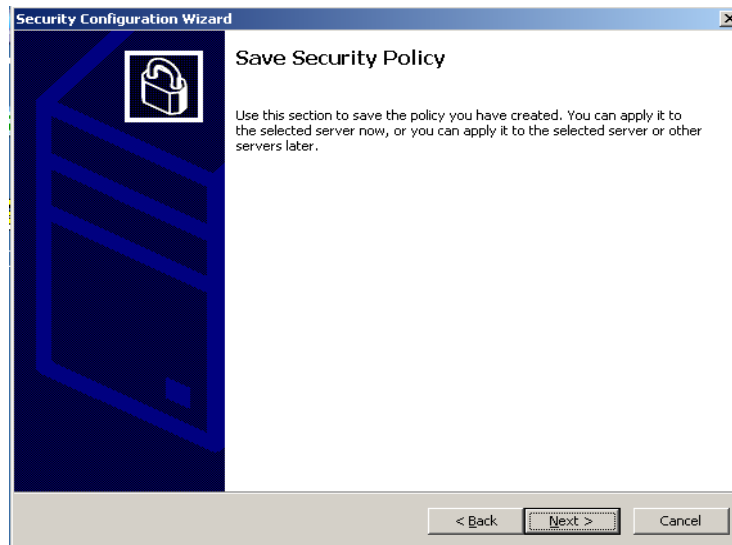


Figura 3.5.16. Guardando las Directivas de seguridad configuradas

24. Luego se presenta la pantalla **Security Policy File Name**, ahí se debe ingresar un nombre para la Directiva elaborada con SCW. También se especifica la ruta donde se va a guardar, es recomendable dejar la ruta de guardado por defecto, **C:\WINDOWS\security\msscw\Policies\Línea Base de Seguridad**. Se puede ingresar una descripción para la Directiva creada, así como también visualizar las políticas de seguridad, configuradas y también permite incluir la plantilla de seguridad elaborada específicamente para servidores miembros, en este caso para incluirla se pulsa el botón **Include Security Templates**.

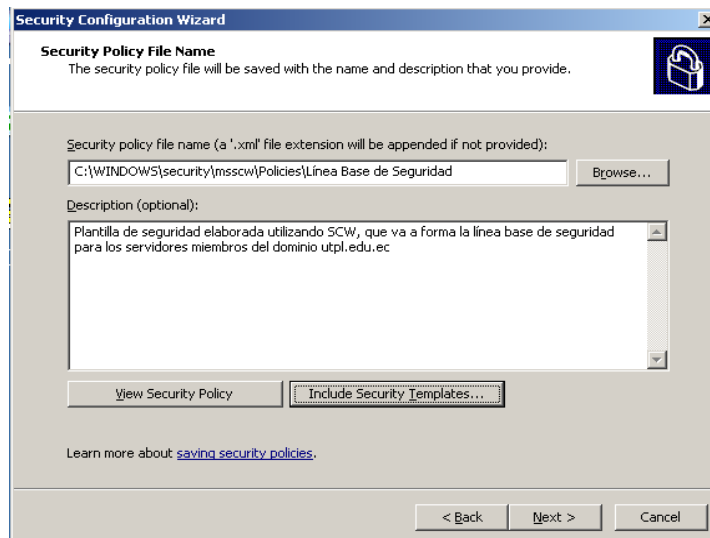


Figura 3.5.17. Ingreso de nombre y descripción de las Directivas configuradas

25. Para incluir la plantilla de seguridad a la Línea de Seguridad Base, luego de pulsar en **Include Security Templates**, en la ventana de diálogo que se presenta se debe dar clic en el botón **Add** y luego ir a la ubicación donde está la plantilla de seguridad en este caso la ruta es:



C:\WINDOWS\security\templates y se selecciona **Plantilla Servidores Miembros.inf**, luego se pulsa en el botón **Ok** y luego en el botón **Next**.

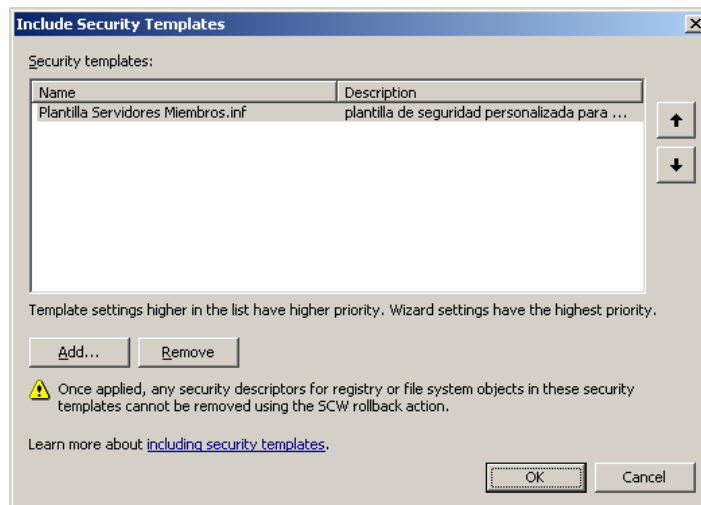


Figura 3.5.18. Inclusión de la plantilla de seguridad para servidores miembros

26. La siguiente pantalla luego del paso anterior, es **Apply Security Policy** que presenta dos opciones **Apply later** y **Apply now**, se escoge esta última y luego se da clic en **Next**, y las configuraciones se empiezan a aplicar de manera inmediata.

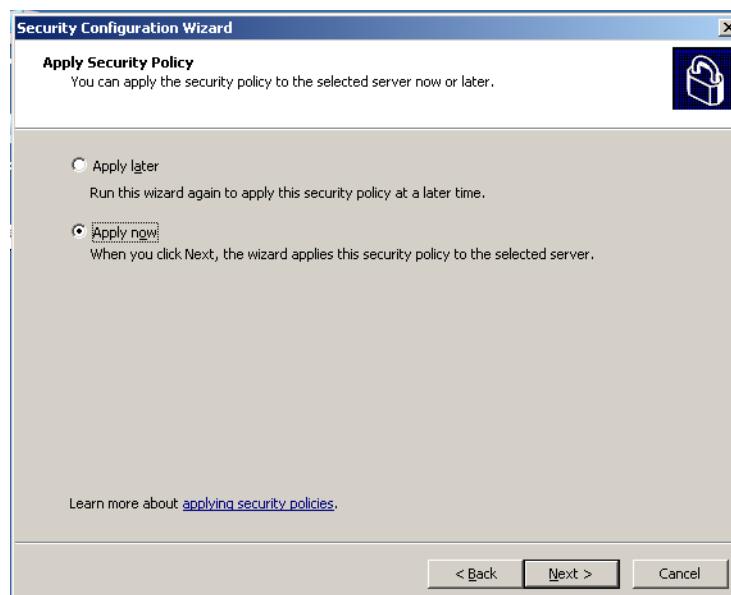


Figura 3.5.19. Aplicando las directivas de seguridad



ANEXO 4.1 PRUEBAS DE SEGURIDAD DE LOS SERVIDORES WINDOWS DEL GDS

Tabla 4.1.1. Caso de Prueba a los Controladores de Dominio

Entorno de seguridad Personalizado para el GDS						
Tipo de Maquina						
Sistema Operativo						
Usuarios de Dominio						
Servidores						
Dirección IP						
				MV PC 2007		MV PC 2007
				Win Server		Win Server
				2003		2003
				Administrator		Administrator
				DEVSERVER		PDCSERVER
				172.16.50.62		172.16.50.42
Nro. De Prueba	Condiciones a ser probadas	Detalles de Prueba	Resultados Esperados	Herramientas Requeridas	Pasa/Error	Pasa/Error
1	Comprobar el registro de sucesos de errores críticos que se deben considerar	<ol style="list-style-type: none"> 1. Inicie sesión en el Controlador de Dominio (PDC , BDC) 2. Haga clic en Start -> Run -> eventvwr y pulse enter 3. Navegar a través de Aplicación, Seguridad y Sistema de registro de carpetas 	No debería haber nada crítico o funcionalidad fallida o errores en el registro de eventos		Pasa	Pasa
2	Verificar que el controlador de dominio este funcionando	<ol style="list-style-type: none"> 1. Inicie sesión en los controladores de dominio PDC y BDC 2. Abra el command prompt 3. Ejecute DCDIAG.exe 	DCDIAG ejecuta una serie de pruebas. Todas las pruebas deben pasar.	DCDIAG.EXE	Pasa	Pasa
3	Verifique que los controladores de dominio pueden ser detectados por los servidores miembros y demás equipos	<ol style="list-style-type: none"> 1. Inicie sesión en cada servidor miembro del dominio 2. Abra el command prompt 3. Digite el comando "ipconfig / flushdns" 4. Compruebe que los equipos clientes pueden acceder al PDC y BDC (Usando ping y nslookup) 	Ping y nslookup debería detectar al PDC y BDC	ipconfig	Pasa	Pasa
4	Verificar la replicación mediante Active Directory entre PDC y BDC	<ol style="list-style-type: none"> 1. Inicie sesión en los controladores de dominio (PDC y BDC) 2. Desde el Command Prompt, ejecute repadmin / showreps 3. Desde el Command Prompt, ejecute repadmin / showconn 4. Ejecute replmon desde el Command Prompt. Agregue un controlador de dominio para ser monitoreado y revise el estado. 	La correcta verificación de los enlaces de entrada y salida así como todas las conexiones de entrada. Todos deben ser detectados con éxito	repadmin, replmon	Pasa	Pasa
5	Verificar la replicación mediante Active Directory entre el PDC y BDC utilizando replmon	<ol style="list-style-type: none"> 1. Inicie sesión en los controladores de dominio (PDC y BDC) 2. Desde el Command Prompt, ejecute repadmin / showreps 3. Desde el Command Prompt, ejecute repadmin / showconn 4. Ejecutar replmon en el Command Prompt. Agregue un controlador de dominio para ser monitoreado y controle su estado. 	La verificación correcta de entrada y salida de todos los enlaces y conexiones de entrada, deben ser detectados con éxito.	repadmin, replmon		
6	Verificar el trabajo FRS en el sitio interno así como la replicación de archivos entre sitios	Ejecutar DCDIAG para testear la replicación FRS. Abra el Command Prompt y ejecute DCDIAG /test:frssysvol	Verificar que la prueba pasa	DCDIAG.EXE		

Tabla 4.1.1. Caso de Prueba a los Controladores de Dominio (... continuación)



Nro. De Prueba	Condiciones a ser probadas	Detalles de Prueba	Resultados Esperados	Herramientas Requeridas	Pasa/Error	Pasa/Error
7	Un Administrador puede hacer copias de seguridad del sistema y datos	Ejecutar la utilidad ntbakup desde el Command Prompt. Se invoca 'El asistente para Restaurar o hacer copias de seguridad'. Siga el asistente para tomar el estado del sistema y hacer una copia de seguridad del PDC	El usuario debe ser capaz de hacer copias de seguridad satisfactoriamente y restaurar los archivos y carpetas en el host	ntbackup	Pasa	Pasa
8	Verifique que BDC puede replicarse con éxito con los demás BDC o con el PDC	<ol style="list-style-type: none"> 1. Inicie sesión en los controladores de dominio PDC y BDC 2. Desde el Command Prompt, ejecute repadmin / showreps. Esto le dará una lista de nombres de los contextos. 3. Utilice el comando "repadmin / replicate <PDC> <BDC> <Nombrar Contexto> / full" 	La replicación de AD debe trabajar sin ningún tipo de error	repadmin		
9	Verifique que el PDC y el BDC puede replicarse con éxito uno al otro	<ol style="list-style-type: none"> 1. Inicie sesión en el controlador de dominio raíz (PDC) y el de respaldo (BDC) 2. Desde el Command Prompt, ejecute repadmin / showreps. Esto le dará una lista de nombres de los contextos. 3. Utilice comando 'repadmin / replicate <PDC 1> <BDC > <Nombre del Contexto> / full' 	La replicación de AD debe trabajar sin ningún tipo de error	repadmin		
10	Compruebe que RPC end-point mappers está disponible en el BDC después de que los puertos del Firewall de Windows están habilitados por la aplicación de las directivas de seguridad	<ol style="list-style-type: none"> 1. Inicie sesión en el controlador de dominio BDC 2. Desde el Command Prompt, ejecutar 'portqry -n < PDC hostname> -e 135' 3. Revise la salida 4. Ejecute los pasos 1 hasta el 3 intercambiando los DCs 	la lista de RPC end-point mapper deben ser visualizados y la disponibilidad del objetivo DC	portqry		
11	Verificar que RPC end-point mappers está disponible en el PDC después que los puertos del Firewall de Windows son habilitados por aplicación de las directivas de seguridad	<ol style="list-style-type: none"> 1. Inicie sesión en el controlador de dominio de respaldo 2. Desde el Command shell, ejecute 'portqry -n <root DC hostname> -e 135' 3. Revise la salida 	la lista de RPC end-point mapper deben ser visualizados y la disponibilidad del objetivo DC	portqry		
12	Separe y entonces replique un servidor miembro (por ejemplo ASUTPL) a un dominio	<ol style="list-style-type: none"> 1. Inicie sesión en el servidor (ASUTPL) 2. Vaya a Start-Click derecho en My Computer- Properties-Computer Name-Change 3. Remueva el servidor desde el dominio y después de reiniciado vuelva a unirse al dominio 	El Desasociado y re-asociado debería ser satisfactorio	Pass	Pasa	Pasa



Tabla 4.1.2. Caso de Pruebas al servidor DNS

Entorno de seguridad Personalizado para el GDS

Tipo de Maquina

Sistema Operativo

Usuarios de Dominio

Servidores

Dirección IP

MV PC 2007

Win Server 2003

Administrator

PDCSERVER

172.16.50.42

Nro. De Prueba	Condiciones a ser probadas	Detalles de Prueba	Resultados Esperados	Herramientas Requeridas	Pasa/Error
1	Verificar que el servidor DNS este operando en el controlador de dominio	<ol style="list-style-type: none"> 1. Iniciar sesión en el servidor DNS 2. Click en Start-All Programs-Administrative Tools-Services 3. Verificar que el servicio de DNS se ha iniciado 	El servicio de DNS debería estar iniciado		Pasa
2	Event Logs	<ol style="list-style-type: none"> 1. Iniciar sesión en el servidor DNS 2. Click en Start-Run-eventvwr y pulse enter 3. Navegue a través de las aplicaciones, Seguridad y carpetas del sistema de registros log 	No debería haber nada crítico o funcionalidad fallida o errores en el registro de eventos		Existen registros de alerta
3	Verificar que el servicio de nombres trabaja desde el Controlador de Dominio	<ol style="list-style-type: none"> 1. Abrir el Command Prompt en el host 2. Usar el comando nslookup para chequear si la propiedad del servicio de nombres trabaja: nslookup <hostname o dirección IP> 	El usuario debería ser capaz de resolver el hostname para esa IP usando el servicio de DNS		Pasa
4	Verificar que el servicio de nombres trabaja probando desde todos los servidores miembros	<ol style="list-style-type: none"> 1. Inicie sesión en los servidores miembros 2. Abra Command Prompt en los servidores 3. Use el comando nslookup para chequear la propiedad del servicio de nombres para los DCs y otros servidores miembros del dominio: nslookup <hostname o dirección IP> 	El usuario debería ser capaz de resolver el hostname para esa IP usando el servicio de DNS		Pasa
5	El administrador puede hacer datos de Backup tanto del sistema como de los datos	Ejecute la utilidad ntbacup desde Command Prompt. Esto invocará a la 'Guía de copia de seguridad o de respaldo'.	El usuario debería ser capaz de hacer copias de seguridad o respaldo de datos de manera satisfactoria en el host		Pasa



Tabla 4.1.3. Caso de Pruebas desde una maquina Cliente a los servidores

Entorno de seguridad Personalizado para el GDS														
				Tipo de Maquina	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007	MV PC 2007
				Sistema Operativo	Win Server	Win Server	Win Server	Win Server	Win Server	Win Server	Win Server	Win Server	Win Server	Win Server
				Usuarios de Dominio	2003	2003	2003	2003	2003	2003	2003	2003	2003	2003
				Servidores	ASUTPL	BDDGDS	CALSERVER	CATAMAYO	DEVCRM	DEVGDS	DIGITSERVER	NODO1SGA	TSTSERVER	WSUTPL
				Dirección IP	172.16.50.43	172.16.31.18	172.16.50.64	172.16.50.60	172.16.31.17	172.16.31.50	172.16.50.46	172.16.50.41	172.16.31.1	172.16.90.12
Nro. De Prueba	Componente	Detalles de Prueba	Pasos de Ejecución	Resultados Esperados	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error
1	Event Viewer	Consulta de los eventos del sistema	1. Ir a Start-Run-eventvwr	No debería haber ningún error en los archivos logs	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
2	Group Policy	Ejecutar gpupdate /force, Reiniciar el servidor y chequear los logs de eventos	1. Abrir el Command Prompt. 2. Digitar gpupdate /force	El comando debe correr con éxito	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
3	DNS	Ejecutar nslookup al dominio utpl.edu.ec, y a los servidores integrantes del dominio	1. Abrir el Command Prompt. 2. Ejecutar el comando: nslookup por dirección IP y por nombre para todos los servidores miembros	El usuario debe ser capaz de llevar a cabo con éxito nslookup	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
4	PING	Hacer ping entre todos los servidores miembros del dominio	1. Abrir el Command Prompt. 2. Ejecutar el comando ping a todos los servidores tanto con dirección IP como por Nombre	El usuario debe poder hacer ping a todos los servidores y demás equipos clientes que estén dentro del entorno de seguridad	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
5	Password	Los usuarios pueden cambiar su password	1. Presione CTRL+ALT+DEL. 2. Click sobre 'Change Password' 3. Ingrese el Password a Cambiar y a continuación digite el nuevo password.	El usuario debe obtener una pop-up diciendo su contraseña se ha cambiado	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa



Tabla 4.1.3. Caso de Pruebas desde una maquina Cliente a los servidores (... continuación)

Nro. De Prueba	Componente	Detalles de Prueba	Pasos de Ejecución	Resultados Esperados	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error	Pasa/Error
6	PRINT	Un usuario puede agregar una impresora al dominio	1. Ir a Start-Impresoras y Faxes o Ir al panel de control-Printers and Faxes. 2. Start "Add Printer Wizard" y adherir una impresora al dominio	Un usuario debería ser capaz de añadir una impresora al dominio	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
7	PRINT	Los usuarios pueden imprimir documentos en la impresora del dominio	Imprimir un documento desde un equipo cliente y utilizar la impresora del dominio o la que este en la red local	Un usuario debería ser capaz de imprimir un documento	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
8	FTP	Usuarios pueden compartir archivos por ftp	1. Abrir el Internet Explorer. 2. Probar el acceso vía ftp, por ejem. 'ftp://ASUTPL'	Un usuario debería ser capaz de acceder por FTP	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa
9	Change Domain	Un usuario del Dominio no pueden cambiarse a menos que tengan derechos de administrador local Los administradores de Dominio pueden cambiarse de Dominio	1. Iniciar sesión con alguna cuenta que tenga privilegios de Administrador Local. 2. Click derecho en My Computer y luego en propiedades. 3. Sobre la ficha de identificación de red haga click en propiedades. 4. Click en Domain e ingrese el nombre de dominio utpl.edu.ec Siga los pasos anteriores en el dominio y con Admin login	Un usuario con derechos de Admin. Local debería ser capaz de cambiar el Dominio Un Administrador debería ser capaz de cambiar de Dominio	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa	Pasa

**ANEXO 4.2 TEST DE ESCANEO Y FUNCIONALIDAD DE LOS SERVIDORES WINDOWS DEL GDS****Tabla 4.2.1.** Testeo de Funcionalidad de los Controladores de Dominio

Comando	Resultado
dcdiag	<p>Domain Controller Diagnosis</p> <p>Performing initial setup: Done gathering initial info.</p> <p>Doing initial required tests</p> <p>Testing server: Default-First-Site-Name\PDCCSERVER Starting test: Connectivity PDCCSERVER passed test Connectivity</p> <p>Doing primary tests</p> <p>Testing server: Default-First-Site-Name\PDCCSERVER Starting test: Replications PDCCSERVER passed test Replications Starting test: NCSecDesc PDCCSERVER passed test NCSecDesc Starting test: NetLogons PDCCSERVER passed test NetLogons Starting test: Advertising PDCCSERVER passed test Advertising Starting test: KnowsOfRoleHolders PDCCSERVER passed test KnowsOfRoleHolders Starting test: RidManager PDCCSERVER passed test RidManager Starting test: MachineAccount PDCCSERVER passed test MachineAccount Starting test: Services PDCCSERVER passed test Services Starting test: ObjectsReplicated PDCCSERVER passed test ObjectsReplicated Starting test: frssysvol PDCCSERVER passed test frssysvol Starting test: frsevent PDCCSERVER passed test frsevent Starting test: kccevent PDCCSERVER passed test kccevent Starting test: systemlog PDCCSERVER passed test systemlog Starting test: VerifyReferences PDCCSERVER passed test VerifyReferences</p> <p>Running partition tests on : ForestDnsZones Starting test: CrossRefValidation ForestDnsZones passed test CrossRefValidation Starting test: CheckSDRefDom ForestDnsZones passed test CheckSDRefDom</p> <p>Running partition tests on : DomainDnsZones Starting test: CrossRefValidation DomainDnsZones passed test CrossRefValidation Starting test: CheckSDRefDom DomainDnsZones passed test CheckSDRefDom</p> <p>Running partition tests on : Schema Starting test: CrossRefValidation Schema passed test CrossRefValidation Starting test: CheckSDRefDom Schema passed test CheckSDRefDom</p> <p>Running partition tests on : Configuration Starting test: CrossRefValidation Configuration passed test CrossRefValidation Starting test: CheckSDRefDom Configuration passed test CheckSDRefDom</p>



Tabla 4.2.1. Testeo de Funcionalidad de los Controladores de Dominio (... continuación)

Comando	Resultado
	<p>Running partition tests on : utpl Starting test: CrossRefValidation utpl passed test CrossRefValidation Starting test: CheckSDRefDom utpl passed test CheckSDRefDom</p> <p>Running enterprise tests on : utpl.edu.ec Starting test: Intersite utpl.edu.ec passed test Intersite Starting test: FsmoCheck utpl.edu.ec passed test FsmoCheck</p>
<pre>dcdiag /test:registerindns /dnsdomain:utpl.edu.ec /v</pre>	<p>Starting test: RegisterInDNS DNS configuration is sufficient to allow this domain controller to dynamically register the domain controller Locator records in DNS. The DNS configuration is sufficient to allow this computer to dynamically register the A record corresponding to its DNS name. pdcserver passed test RegisterInDNS</p>
<pre>netdiag</pre>	<p>Computer Name: PDCSERVER DNS Host Name: pdcserver.utpl.edu.ec System info : Windows 2000 Server (Build 3790) Processor : x86 Family 15 Model 104 Stepping 1, AuthenticAMD List of installed hotfixes : Q147222</p> <p>Netcard queries test : Passed</p> <p>Per interface results: Adapter : Local Area Connection Netcard queries test . . . : Passed Host Name. : pdcserver IP Address : 172.16.50.42 Subnet Mask. : 255.255.0.0 Default Gateway. : Dns Servers. : 172.16.50.42</p> <p>AutoConfiguration results. : Passed Default gateway test . . . : Skipped [WARNING] No gateways defined for this adapter. NetBT name test. : Passed [WARNING] At least one of the <00> 'WorkStation Service', <03> 'Messenger Service', <20> 'WINS' names is missing. WINS service test. : Skipped There are no WINS servers configured for this interface.</p> <p>Global results: Domain membership test : Passed NetBT transports test. : Passed List of NetBt transports currently configured: NetBT_Tcpip_{7C9DDEFD-A196-4E70-B37F-2ECC690E5AC5} 1 NetBt transport currently configured.</p> <p>Autonet address test : Passed IP loopback ping test. : Passed Default gateway test : Failed [FATAL] NO GATEWAYS ARE REACHABLE. You have no connectivity to other network segments. If you configured the IP protocol manually then you need to add at least one valid gateway. NetBT name test. : Passed [WARNING] You don't have a single interface with the <00> 'WorkStation Service', <03> 'Messenger Service', <20> 'WINS' names defined.</p> <p>Winsock test : Passed DNS test : Passed PASS - All the DNS entries for DC are registered on DNS server '172.16.50.42' and other DCs also have some of the names registered.</p>



Tabla 4.2.1. Testeo de Funcionalidad de los Controladores de Dominio (... continuación)


Comando	Resultado
	<p>Redir and Browser test : Passed List of NetBt transports currently bound to the Redir NetBT_Tcpip_{7C9DDEFD-A196-4E70-B37F-2ECC690E5AC5} The redir is bound to 1 NetBt transport. List of NetBt transports currently bound to the browser NetBT_Tcpip_{7C9DDEFD-A196-4E70-B37F-2ECC690E5AC5} The browser is bound to 1 NetBt transport.</p> <p>DC discovery test. : Passed DC list test : Passed Trust relationship test. : Skipped Kerberos test. : Passed LDAP test. : Passed Bindings test. : Passed WAN configuration test : Skipped No active remote access connections. Modem diagnostics test : Passed IP Security test : Skipped Note: run "netsh ipsec dynamic show /?" for more detailed information The command completed successfully</p>
<pre>repadmin /showrepl pdcserver.utpl.edu.ec</pre>	<p>Default-First-Site-Name\PDCCSERVER</p> <p>DC Options: IS_GC</p> <p>Site Options: (none)</p> <p>DC object GUID: 68fb4da4-5e72-4e86-9bdf-c7d3e29623e3 DC invocationID: 68fb4da4-5e72-4e86-9bdf-c7d3e29623e3</p> <p>==== INBOUND NEIGHBORS =====</p> <p>DC=utpl,DC=edu,DC=ec Default-First-Site-Name\DEVSERVER via RPC DC object GUID: f7b68d6d-0362-4fb6-9377-11d2ca747c98 Last attempt @ 2008-09-05 18:34:50 was successful.</p> <p>CN=Configuration,DC=utpl,DC=edu,DC=ec Default-First-Site-Name\DEVSERVER via RPC DC object GUID: f7b68d6d-0362-4fb6-9377-11d2ca747c98 Last attempt @ 2008-09-05 18:34:57 was successful.</p> <p>CN=Schema,CN=Configuration,DC=utpl,DC=edu,DC=ec Default-First-Site-Name\DEVSERVER via RPC DC object GUID: f7b68d6d-0362-4fb6-9377-11d2ca747c98 Last attempt @ 2008-09-05 12:53:05 was successful.</p>
<pre>Replmon</pre>	
<pre>portqry -n pdcserver.utpl.edu.ec -e 25</pre>	<p>Querying target system called:</p> <p>172.16.50.42 UDP port 53 (domain service): LISTENING</p>



Tabla 4.2.1. Testeo de Funcionalidad de los Controladores de Dominio (... continuación)

Comando	Resultado
portqry -n pdcserver.utpl.edu.ec - r 21:445	<p>Querying target system called: pdcserver.utpl.edu.ec</p> <p>Attempting to resolve name to IP address... Name resolved to 172.16.50.42</p> <p>TCP port 53 (domain service): LISTENING TCP port 88 (kerberos service): LISTENING TCP port 135 (epmap service): LISTENING TCP port 139 (netbios-ssn service): LISTENING TCP port 389 (ldap service): LISTENING Sending LDAP query to TCP port 389... LDAP query response: currentdate: 09/08/2008 20:25:54 (unadjusted GMT) subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=utpl,DC=edu,DC=ec dsServiceName: CN=NTDS Settings,CN=PDCSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=utpl,DC=edu,DC=ec namingContexts: DC=utpl,DC=edu,DC=ec defaultNamingContext: DC=utpl,DC=edu,DC=ec schemaNamingContext: CN=Schema,CN=Configuration,DC=utpl,DC=edu,DC=ec configurationNamingContext: CN=Configuration,DC=utpl,DC=edu,DC=ec rootDomainNamingContext: DC=utpl,DC=edu,DC=ec supportedControl: 1.2.840.113556.1.4.319 supportedLDAPVersion: 3 supportedLDAPPolicies: MaxPoolThreads highestCommittedUSN: 24777 supportedSASLMechanisms: GSSAPI dnsHostName: pdcserver.utpl.edu.ec ldapServiceName: utpl.edu.ec:pdcserver\$@UTPL.EDU.EC serverName: CN=PDCSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=utpl,DC=edu,DC=ec supportedCapabilities: 1.2.840.113556.1.4.800 isSynchronized: TRUE isGlobalCatalogReady: TRUE domainFunctionality: 0 forestFunctionality: 0 domainControllerFunctionality: 2</p> <p>===== End of LDAP query response =====</p> <p>TCP port 445 (microsoft-ds service): LISTENING</p>
portqry -n pdcserver.utpl.edu.ec - e 389 -p udp	<p>Querying target system called: pdcserver.utpl.edu.ec</p> <p>Attempting to resolve name to IP address... Name resolved to 172.16.50.42 UDP port 389 (unknown service): LISTENING or FILTERED</p> <p>Sending LDAP query to UDP port 389... LDAP query response: currentdate: 09/08/2008 20:36:29 (unadjusted GMT) subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=utpl,DC=edu,DC=ec dsServiceName: CN=NTDS Settings,CN=PDCSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=utpl,DC=edu,DC=ec namingContexts: DC=utpl,DC=edu,DC=ec defaultNamingContext: DC=utpl,DC=edu,DC=ec schemaNamingContext: CN=Schema,CN=Configuration,DC=utpl,DC=edu,DC=ec configurationNamingContext: CN=Configuration,DC=utpl,DC=edu,DC=ec rootDomainNamingContext: DC=utpl,DC=edu,DC=ec supportedControl: 1.2.840.113556.1.4.319 supportedLDAPVersion: 3 supportedLDAPPolicies: MaxPoolThreads highestCommittedUSN: 24782 supportedSASLMechanisms: GSSAPI</p>



Tabla 4.2.1. Testeo de Funcionalidad de los Controladores de Dominio (... continuación)

Comando	Resultado
	<pre> dnsHostName: pdcserver.utpl.edu.ec ldapServiceName: utpl.edu.ec:pdcserver\$@UTPL.EDU.EC serverName: CN=PDCSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=utpl,DC=edu,DC=ec supportedCapabilities: 1.2.840.113556.1.4.800 isSynchronized: TRUE isGlobalCatalogReady: TRUE domainFunctionality: 0 forestFunctionality: 0 domainControllerFunctionality: 2 ===== End of LDAP query response ===== UDP port 389 is LISTENING </pre>
<pre> portqry -n pdcserver.utpl.edu.ec - p udp -e 135 </pre>	<pre> Querying target system called: pdcserver.utpl.edu.ec Attempting to resolve name to IP address... Name resolved to 172.16.50.42 UDP port 135 (epmap service): NOT LISTENING </pre>
nslookup	<pre> C:\Documents and Settings\Administrator>nslookup Default Server: pdcserver.utpl.edu.ec Address: 172.16.50.42 > set type=srv > _ldap._tcp.dc._msdcs.utpl.edu.ec Server: pdcserver.utpl.edu.ec Address: 172.16.50.42 DNS request timed out. timeout was 2 seconds. _ldap._tcp.dc._msdcs.utpl.edu.ec SRV service location: priority = 0 weight = 100 port = 389 svr hostname = devserver.utpl.edu.ec _ldap._tcp.dc._msdcs.utpl.edu.ec SRV service location: priority = 0 weight = 100 port = 389 svr hostname = pdcserver.utpl.edu.ec devserver.utpl.edu.ec internet address = 172.16.50.62 pdcserver.utpl.edu.ec internet address = 172.16.50.42 > exit </pre>
<pre> dsastat - s:pdcserver;devserver - b:dc=utpl.edu,dc=ec </pre>	<pre> Stat-Only mode. Unsorted mode. Opening connections... pdcserver...success. Connecting to pdcserver... reading... **> ntMixedDomain = 1 reading... **> Options = Setting server as [pdcserver] as server to read Config Info... devserver...success. Connecting to devserver... reading... **> Options = ignored attrType = 0x3, blsRepl 2.5.4.3 ignored attrType = 0xb, blsRepl 2.5.4.11 BEGIN: Getting all special metadata attr info ... --> Adding special meta attrs, (3, cn) --> Adding special meta attrs, (6, c) --> Adding special meta attrs, (1376281, dc) --> Adding special meta attrs, (7, l) --> Adding special meta attrs, (591522, msTAPI-uid) --> Adding special meta attrs, (10, o) --> Adding special meta attrs, (11, ou) </pre>



Tabla 4.2.1. Testeo de Funcionalidad de los Controladores de Dominio (... continuación)

Comando	Resultado
	<pre> reading... **> ntMixedDomain = 1 END: Getting all special metadata attr info ... No. attributes in schema = 1070 No. attributes in replicated = 1015 No. attributes in PAS = 150 Generation Domain List on server pdcserver... > Searching server for GC attribute partial set on property attributeld. > Searching server for GC attribute partial set on property ldapDisplayName. Retrieving statistics... Paged result search... Paged result search... ...(Terminated query to pdcserver. <No result present in message>) ...(Terminated query to devserver. <No result present in message>) --> *** DSA Diagnostics *** <<-- Objects per server: Obj/Svr Bytes per object: Object Bytes Bytes per server: Server Bytes Checking for missing replies... No missing replies!INFO: Server sizes are equal. *** Identical Directory Information Trees *** -->> PASS <<-- closing connections... pdcserver; devserver; </pre>

Tabla 4.2.2. Test de Análisis de Seguridades con la herramienta MBSA

Información General		
Computer name:	DESARROLLO\NODO1SGA	
IP address:	172.16.50.41	
Security report name:	DESARROLLO – NODO1SGA (9-9-2008 4:31 PM)	
Scan date:	9/9/2008 4:31 PM	
Scanned with MBSA version:	2.0.6706.0	
Catalog synchronization date:		
Security update catalog:	Microsoft Update	
Security assessment:	Severe Risk (One or more critical checks failed.)	
Security Update Scan Results		
Score	Issue	Result
X	Windows Security Updates	28 security updates are missing. 5 service packs or update rollups are missing.
X	Office Security Updates	1 service packs or update rollups are missing.
Windows Scan Results		
Administrative Vulnerabilities		
Score	Issue	Result
X	Automatic Updates	Updates are automatically downloaded, but not automatically installed on this computer.
X	Administrators	More than 2 Administrators were found on this computer.
X	Password Expiration	Some user accounts (7 of 12) have non-expiring passwords.
*	Incomplete Updates	No incomplete software update installations were found.
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. 2 of 2 network connections either do not have Windows Firewall enabled, or they are enabled with exceptions.
✓	Local Account Password Test	Some user accounts (1 of 12) have blank or simple passwords, or could not be analyzed.
✓	File System	All hard drives (2) are using the NTFS file system
✓	Autologon	Autologon is not configured on this computer.
✓	Guest Account	The Guest account is disabled on this computer
✓	Restrict Anonymous	Computer is properly restricting anonymous access.



Tabla 4.2.2. Test de Análisis de Seguridades con la herramienta MBSA (... continuación)

Additional System Information		
Score	Issue	Result
*	Auditing	Logon Success auditing is enabled, however Logon Failure auditing should also be enabled.
*	Services	Some potentially unnecessary services are installed.
i	Shares	3 share(s) are present on your computer.
i	Windows Version	Computer is running Windows 2000 or greater.
Internet Information Services (IIS) Scan Results		
Administrative active Vulnerabilities		
Score	Issue	Result
✓	IIS Lockdown Tool	The IIS Lockdown tool was developed for IIS 4.0, 5.0, and 5.1, and is not needed for new Windows Server 2003 installations running IIS 6.0.
✓	Sample Applications	IIS sample applications are not installed.
✓	IISAdmin Virtual Directory	IISADMIN virtual directory is not present.
✓	Parent Paths	Parent paths are not enabled.
✓	MSADC and Scripts Virtual Directories	The MSADC and Scripts virtual directories are not present.
Additional System Information		
Score	Issue	Result
*	Domain Controller Test	IIS is not running on a domain controller.
*	IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options.
SQL Server Scan Result		
Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Tabla 4.2.3. Test de Análisis de Seguridades con la herramienta RETINA - NETWORK SECURITY SCANNER

NETWORK ANALYSIS RESULTS			
Report Summary			
Scanner Name	Retina	Machines Scanned	1
Scanner Version	5.6.0.1558	Vulnerabilities Total	58
Scan Start Date	9/12/2008	High Risk Vulnerabilities	11
Scan Start Time	4:29:28 PM	Medium Risk Vulnerabilities	29
Scan Duration	0h 1m 19s	Low Risk Vulnerabilities	18
Scan Name	Untitled	Information Only Audits	10
Scan Status	Completed	Credential Used	- Null Session -
Vulnerabilities on your network			
Vulnerability Name			Count
Password Does Not Expire			9
Cannot Change Password			7
User Never Logged On			3
WebDAV enabled			2
Account Lockout Threshold			1
Last Username			1
Min Password Age			1
Min Password Length			1
Password History			1
Anonymous FTP			1
IIS FTP Bounce Attack			1
ICMP Timestamp Request			1
ISAKMP Server detected			1
TCP IP Security			1
SMTP Relaying			1
SMTP Service Potential Security Hazard			1
Microsoft Office 2003 Service Pack 2 Not Installed			1
Microsoft Office Filters Remote Code Execution (915384) - Gifimp32.fl			1
Microsoft Office Filters Remote Code Execution (915384) - Png32.fl			1
Microsoft PowerPoint Remote Code Execution (922968) - PowerPoint 2003			1



Tabla 4.2.3. Test de Análisis de Seguridades con la herramienta RETINA - NETWORK SECURITY SCANNER (... continuación)

Microsoft Windows Malicious Software Removal Tool	1	
Microsoft WordPerfect Converter Command Execution	1	
Windows Legal Notice Not Enabled	1	
Windows USB Storage Device Interface Enabled	1	
Open ports on your network		
Port Number	Description	Count
TCP:21	FTP - File Transfer Protocol [Control]	1
TCP:25	SMTP - Simple Mail Transfer Protocol	1
TCP:80	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)	1
TCP:135	RPC-LOCATOR - RPC (Remote Procedure Call) Location Service	1
TCP:139	NETBIOS-SSN - NETBIOS Session Service	1
TCP:445	MICROSOFT-DS - Microsoft-DS	1
TCP:1036	Nebula Secure Segment Transfer Protocol	1
TCP:1411	AF - AudioFile	1
TCP:1412	INNOSYS - InnoSys	1
TCP:1413	INNOSYS-ACL - InnoSys-ACL	1
TCP:2000	CALLBOOK -	1
TCP:2030	DEVICE2 -	1
TCP:2265	Audio Precision Apx500 API Port 2	1
TCP:3389	MS RDP (Remote Desktop Protocol) / Terminal Services	1
TCP:5444		1
TCP:18181	OPSEC CVP	1
TCP:18182	OPSEC UFP	1
UDP:123	NTP - Network Time Protocol	1
UDP:137	NETBIOS-NS - NETBIOS Name Service	1
UDP:138	NETBIOS-DGM - NETBIOS Datagram Service	1
User accounts on your network		
Account Name	Count	
ACC_NODO1SGA	1	
Administrator	1	
ASPNET	1	
cargaeva	1	
floja	1	
Guest	1	
IUSER_RETINA	1	
IUSR_NODO1SGA	1	
IWAM_NODO1SGA	1	
Jchicaiza	1	
SUPPORT_388945a0	1	
vrmontano	1	
Network shares on your network		
Share Name	Count	
ADMIN\$	1	
C\$	1	
D\$	1	
IPC\$	1	

**MANUAL DE POLÍTICAS Y PROCEDIMIENTOS
PARA CONFIGURAR SEGURIDADES EN
WINDOWS SERVER 2003**



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD – DETALLE																																							
PR01	<p align="center">CONFIGURACIÓN DE SEGURIDADES DESDE EL REGISTRO DEL SISTEMA (REGEDIT)</p> <p>Configurar el registro del sistema ayuda a aumentar la resistencia de la pila TCP/IP ante los ataques de servicios denegados.</p> <p>Se debe configurar el registro con los valores de la tabla que a continuación se detalla, cuyos valores se ubican bajo la subclave:</p> <p>HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\</p> <table border="1" data-bbox="624 645 1270 1137"> <thead> <tr> <th>Clave</th> <th>Formato</th> <th>Alta Seguridad</th> </tr> </thead> <tbody> <tr> <td>DisableIPSourceRouting</td> <td>DWORD</td> <td>2</td> </tr> <tr> <td>EnableDeadGWDetect</td> <td>DWORD</td> <td>0</td> </tr> <tr> <td>EnableCMPRedirect</td> <td>DWORD</td> <td>0</td> </tr> <tr> <td>EnablePMTUDiscovery</td> <td>DWORD</td> <td>0</td> </tr> <tr> <td>EnableSecurityFilters</td> <td>DWORD</td> <td>1</td> </tr> <tr> <td>KeepAliveTime</td> <td>DWORD</td> <td>300000</td> </tr> <tr> <td>PerformRouterDiscovery</td> <td>DWORD</td> <td>0</td> </tr> <tr> <td>SynAttackProtect</td> <td>DWORD</td> <td>2</td> </tr> <tr> <td>TcpMaxConnectResponseRetransmissions</td> <td>DWORD</td> <td>2</td> </tr> <tr> <td>TcpMaxConnectRetransmissions</td> <td>DWORD</td> <td>2</td> </tr> <tr> <td>TcpMaxDataRetransmissions</td> <td>DWORD</td> <td>3</td> </tr> <tr> <td>TCPMaxPortsExhausted</td> <td>DWORD</td> <td>5</td> </tr> </tbody> </table> <p>OBS: Todas estas claves se deben modificar o crear de no existir bajo la ruta que se indica, con esto estará fortaleciendo de una manera más adecuada las conexiones desde y hacia la red y así se evita los ataques de denegación de servicio.</p>	Clave	Formato	Alta Seguridad	DisableIPSourceRouting	DWORD	2	EnableDeadGWDetect	DWORD	0	EnableCMPRedirect	DWORD	0	EnablePMTUDiscovery	DWORD	0	EnableSecurityFilters	DWORD	1	KeepAliveTime	DWORD	300000	PerformRouterDiscovery	DWORD	0	SynAttackProtect	DWORD	2	TcpMaxConnectResponseRetransmissions	DWORD	2	TcpMaxConnectRetransmissions	DWORD	2	TcpMaxDataRetransmissions	DWORD	3	TCPMaxPortsExhausted	DWORD	5
Clave	Formato	Alta Seguridad																																						
DisableIPSourceRouting	DWORD	2																																						
EnableDeadGWDetect	DWORD	0																																						
EnableCMPRedirect	DWORD	0																																						
EnablePMTUDiscovery	DWORD	0																																						
EnableSecurityFilters	DWORD	1																																						
KeepAliveTime	DWORD	300000																																						
PerformRouterDiscovery	DWORD	0																																						
SynAttackProtect	DWORD	2																																						
TcpMaxConnectResponseRetransmissions	DWORD	2																																						
TcpMaxConnectRetransmissions	DWORD	2																																						
TcpMaxDataRetransmissions	DWORD	3																																						
TCPMaxPortsExhausted	DWORD	5																																						
PR02	<p align="center">CONFIGURACIÓN DE AFD DESDE EL REGEDIT</p> <p>Los valores que se agregan al registro para configurar el Afd.sys se describen en la tabla siguiente y todos los valores se ubican bajo la subclave:</p> <p>HKLM\System\CurrentControlSet\Services\AFD\Parameters\</p> <table border="1" data-bbox="624 1509 1270 1700"> <thead> <tr> <th>Clave</th> <th>Formato</th> <th>Alta Seguridad</th> </tr> </thead> <tbody> <tr> <td>DynamicBacklogGrowthDelta</td> <td>DWORD</td> <td>10</td> </tr> <tr> <td>EnableDynamicBacklog</td> <td>DWORD</td> <td>1</td> </tr> <tr> <td>MinimumDynamicBacklog</td> <td>DWORD</td> <td>20</td> </tr> <tr> <td>MaximumDynamicBacklog</td> <td>DWORD</td> <td>20000</td> </tr> </tbody> </table> <p>OBS: De no existir o tener otros valores las claves descritas, se las debe modificar o crear con los valores indicados.</p>	Clave	Formato	Alta Seguridad	DynamicBacklogGrowthDelta	DWORD	10	EnableDynamicBacklog	DWORD	1	MinimumDynamicBacklog	DWORD	20	MaximumDynamicBacklog	DWORD	20000																								
Clave	Formato	Alta Seguridad																																						
DynamicBacklogGrowthDelta	DWORD	10																																						
EnableDynamicBacklog	DWORD	1																																						
MinimumDynamicBacklog	DWORD	20																																						
MaximumDynamicBacklog	DWORD	20000																																						
PR03	<p align="center">CONFIGURACIONES RECOMENDADAS DEL REGISTRO PARA FORTALECER LA PILA TCP/IP</p> <p>Todas las entradas que se detallan en la tabla siguiente, es de mucha importancia su configuración en la subclave correspondiente para que den la seguridad que se requiere en un servidor.</p>																																							



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE		
	Clave	Formato	Alta Seguridad
	AutoAdminLogon	DWORD	0
	Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\		
	AutoReboot	DWORD	0
	Subclave: HKLM\System\CurrentControlSet\Control\CrashControl\		
	AutoShareWks	DWORD	0
	Subclave: HKLM\System\CurrentControlSet\Services\RasMan\Parameters\		
	DisableSavePassword	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\		
	Hidden	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Services\LanmanServer\		
	NoDefaultExempt	DWORD	3
	Subclave: HKLM\System\CurrentControlSet\Services\IPSEC\		
	NtfsDisable8dot3NameCreation	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Control\FileSystem\		
	NoDriveTypeAutoRun	DWORD	0xFF
	Subclave: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\		
	NoNameReleaseOnDemand	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Services\NetBT\Parameters\		
	SafeDllSearchMode	DWORD	1
	Subclave: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\		
	ScreenSaverGracePeriod	String	0
	Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\		
	WarningLevel	DWORD	90
	Subclave: HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\		
	AllocateCDRoms	String	1
	Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon		
	AllocateFloppies	String	1
	Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon		
	AutoShareServer	DWORD	0
	Subclave: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters		
	AutoShareWks	DWORD	0
	Subclave: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters		
	Autorun	DWORD	0
	Subclave: HKLM\System\CurrentControlSet\Services\Cdrom		
	ForceEncryptedData	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Services\RasMan\PPP		
	DisableSavePassword	DWORD	1
	Subclave: HKLM\System\CurrentControlSet\Services\RasMan\Parameters		
	ForceEncryptedPassword	DWORD	2
	Subclave: HKLM\System\CurrentControlSet\Services\RasMan\PPP		
	Start	DWORD	4
	Subclave: HKLM\SYSTEM\CurrentControlSet\Services\Schedule		



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE															
	<table border="1" data-bbox="539 383 1361 734"> <thead> <tr> <th>Clave</th> <th>Formato</th> <th>Alta Seguridad</th> </tr> </thead> <tbody> <tr> <td>SecureVPN Subclave: HKLM\System\CurrentControlSet\Services\RasMan\PPP</td> <td>DWORD</td> <td>1</td> </tr> <tr> <td>Logging Subclave: HKLM\System\CurrentControlSet\Services\Rasman\Parameters</td> <td>DWORD</td> <td>1</td> </tr> <tr> <td>ClearPageFileAtShutdown Subclave: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management</td> <td>DWORD</td> <td>1</td> </tr> <tr> <td>DontDisplayLastUserName Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon</td> <td>DWORD</td> <td>1</td> </tr> </tbody> </table> <p data-bbox="539 734 1155 871">Eliminar la siguiente subclave del registro: Nombre del Valor: Posix Tipo de Dato: REG_EXPAND_SZ Valor del Dato: %SystemRoot%\system32\psxs.exe Ruta: HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems</p> <p data-bbox="507 913 1393 976">OBS: De no existir cualquier subclave mencionada, se debe crearla y si existe y tiene otros valores, se la configura con los valores recomendados.</p>	Clave	Formato	Alta Seguridad	SecureVPN Subclave: HKLM\System\CurrentControlSet\Services\RasMan\PPP	DWORD	1	Logging Subclave: HKLM\System\CurrentControlSet\Services\Rasman\Parameters	DWORD	1	ClearPageFileAtShutdown Subclave: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	DWORD	1	DontDisplayLastUserName Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	DWORD	1
Clave	Formato	Alta Seguridad														
SecureVPN Subclave: HKLM\System\CurrentControlSet\Services\RasMan\PPP	DWORD	1														
Logging Subclave: HKLM\System\CurrentControlSet\Services\Rasman\Parameters	DWORD	1														
ClearPageFileAtShutdown Subclave: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management	DWORD	1														
DontDisplayLastUserName Subclave: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	DWORD	1														
PR04	<p data-bbox="544 1032 1353 1055">PARA AGREGAR GRUPOS DE SEGURIDAD A LAS ASIGNACIONES DE DERECHOS DE USUARIO</p> <ul style="list-style-type: none"> ✓ En Usuarios y equipos de Active Directory, hacer click con el botón secundario en la UO Servidores miembro y, a continuación, seleccionar Propiedades. ✓ En la ficha Directiva de grupo, seleccionar Enterprise Client Member Server Baseline Policy (directiva de línea de base de servidores miembros de Cliente de empresa) para editar el GPO vinculado. ✓ Seleccionar Enterprise Client – Member Server Baseline Policy y, a continuación, hacer click en Editar. ✓ En la ventana Directiva de grupo, hacer click en Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Asignación de derechos de usuario para agregar los grupos de seguridad únicos de la tabla anterior para cada derecho. ✓ Cerrar la directiva de grupo que se ha modificado. ✓ Cerrar la ventana Propiedades de la UO Servidores miembro. ✓ Forzar la replicación entre los controladores de dominio para que la directiva se aplique a todos; para ello, proceder del siguiente modo: <ul style="list-style-type: none"> ❖ Abrir una ventana del símbolo del sistema, escriba gpupdate /Force y presione ENTRAR para forzar al servidor a actualizar la directiva. ❖ Reiniciar el servidor. <p data-bbox="507 1619 1393 1677">Compruebe en el registro de eventos que la directiva de grupo se ha descargado correctamente y que el servidor puede comunicarse con los otros controladores de dominio en el dominio.</p>															
PR05	<p data-bbox="539 1733 1361 1794">CONSIDERACIONES A SEGUIR EN EL ASEGURAMIENTO DE LAS CUENTAS MÁS CONOCIDAS EN WINDOWS SERVER 2003</p> <p data-bbox="507 1809 1326 1832">Complete los siguientes pasos para asegurar las cuentas más conocidas en los dominios y servidores</p> <ul style="list-style-type: none"> ✓ Cambiar el nombre de las cuentas del Administrador y el Invitado, y cambie sus contraseñas por un valor largo y complejo en cada dominio Usar nombres y contraseñas distintas en cada servidor. Si se usan los mismos nombres de cuenta y contraseñas en todos los dominios y servidores, un agresor que logre el acceso a un servidor miembro podrá tener acceso a todos los demás con el mismo nombre de cuenta y contraseña. Ver PL02 															



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE
	<ul style="list-style-type: none">✓ Cambiar las descripciones de cuenta a algo distinto a los valores predeterminados para ayudar a evitar una identificación fácil de las cuentas.✓ Registrar estos cambios en una ubicación segura.✓ y servidor.
PR06	<p style="text-align: center;">CONFIGURACIÓN DE TERMINAL SERVER</p> <p>Para realizar la configuración de Terminal Server se debe seguir los siguientes pasos:</p> <ol style="list-style-type: none">1. Start -> Control Panel -> Administrative Tools -> Terminal Services Configuration.2. En el panel derecho que se presenta al pulsar en Connections del árbol de Terminal Services Configuration. Dar doble click en la conexión que se quiere configurar o también dar click derecho en la conexión y luego escoger Properties.3. Cuando se presente la ventana de diálogo de Properties, se procede a configurar las opciones de seguridad, ubicadas en la pestaña General.4. Para Security Layer se escoge RDP Security Layer5. Para Encryption level se asigna High, que es lo recomendable.
PR07	<p style="text-align: center;">CONFIGURACIÓN DE INFORME DE ERRORES</p> <p>Para configurar el reporte de errores en equipos que operan con Windows server 2003, se debe seguir los siguientes pasos:</p> <ol style="list-style-type: none">1. Ir a Start -> Control Panel -> System.2. En el diálogo de System Properties, ir a la pestaña de Advanced.3. Click en el botón Error Reporting.4. Seleccionar Enable error reporting.5. Si se quiere reportar errores de programas de manera específica, pulsar el botón Choose Programs y luego adherir el programa que se desee.6. Pulsar Ok. si se está de acuerdo con los reportes de errores a generar en un futuro.
PR08	<p style="text-align: center;">DESHABILITANDO Y RENOMBRANDO LA CUENTA DE USUARIO INVITADO</p> <p>El proceso que se debe seguir para deshabilitar o renombrar la cuenta de invitado en Windows Server 2003, es el siguiente:</p> <ol style="list-style-type: none">1. Ir al Control Panel -> Administrative Tools -> Computer Management.2. En Computer Management, ir a Local Users and Groups -> Users.3. En el panel derecho, click derecho en Guest -> Properties.4. En el diálogo Guest Properties -> General -> click en Account is disabled -> OK.5. En el panel Details -> click derecho en Guest -> Rename.6. De un nuevo nombre y presionar ENTER. <p>Fuente: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/16727f91-87c4-4c06-8875-4b0bd3d97134.mspx?mfr=true</p>



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE
PR09	<p style="text-align: center;">LIMITAR EL NÚMERO DE USUARIOS QUE ACCEDEN SIMULTÁNEAMENTE A UN SERVIDOR</p> <ol style="list-style-type: none">1. Ir a Start -> Run, digitar regedit e ir a la clave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters2. Crear una nueva clave llamada Users de tipo DWORD y asignarle un valor decimal que se desee <p>Fuente: http://www.publispain.com/trucos-windows/trucos/Win_NT/limitar_usuarios_servidor.html</p> <p style="text-align: center;">COMO MONITOREAR Y LIMITAR CONEXIONES EN UN DOMINIO SERVER 2003</p> <p>Fuente: http://jelperu.spaces.live.com/Blog/cns!ECE299A619F24CBE!843.entry</p> <p>Fuente de donde se puede descargar la herramienta de monitoreo: http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-5c359cc0842/limitlogin.exe</p>
PR10	<p style="text-align: center;">RENOMBRANDO LA CUENTA DEL USUARIO ADMINISTRADOR</p> <ol style="list-style-type: none">1. Ir al Control Panel -> Administrative Tools -> Computer Management.2. En la consola Computer Management, expandir Local Users and Groups -> Users.3. En el panel derecho, click derecho en Administrator -> Rename.4. Ingrese un nuevo nombre y presionar ENTER. <p style="text-align: center;">CREACIÓN DE UNA CUENTA “TONTA ó SEÑUELO” DE ADMINISTRADOR</p> <ol style="list-style-type: none">5. Una vez renombrada la cuenta de administrador principal, se crea una cuenta de administrador denominada “tonta”6. En el panel derecho de la consola Computer Management -> click derecho en la parte vacía, click en New User7. Llenar el campo User name con el nombre Administrator, en el campo Description ingrese el texto “Built-in account for administering the computer/domain” para que se describa que es una cuenta Administrador, ingresar un password muy fuerte en el campo Password, tiene que cumplir con las políticas de contraseñas recomendadas.8. Asegurarse que no esté el checkbox User must change password at next logon seleccionado y comprobar que este seleccionada la opción Password never expires9. Ir a la pestaña Member Of y remover todos los grupos que aparezcan hay que tener presente que se está configurando una cuenta “tonta” que se utilizará de engaño ante los atacantes. <p>Fuente: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/16727f91-87c4-4c06-8875-4b0bd3d97134.mspx?mfr=true</p>
PR11	<p style="text-align: center;">SEGURIDADES EN CARPETAS Y ARCHIVOS</p> <p>El proceso a seguir para asegurar carpetas y archivos en Windows Server 2003 es el que a continuación se detalla:</p> <ol style="list-style-type: none">1. Ir a Start -> Administrative Tools -> Computer Management.2. En la ventana de Computer Management, seleccionar y expandir Shared Folders, luego dar click en Shares.3. En el panel de la derecha dar click derecho en una parte vacía, en el menú que se presenta seleccionar New Share, lo que le muestra un asistente



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE
	<ol style="list-style-type: none"> 4. Pulsar en el botón Next para ir a la siguiente etapa donde se debe escoger la ruta de la carpeta a compartir, Folder path, luego se pulsa el botón Next. 5. En la siguiente etapa se confirma el nombre de la carpeta a compartir, la ruta que permite ubicar la carpeta compartida, se agrega una descripción si se desea, se puede hacer configuraciones de comportamiento de usuarios desconectados, luego se pulsa el botón Next. 6. En la etapa de Permissions, se escoge la configuración que se desea permitir para la carpeta que se está compartiendo. También se puede personalizar los permisos sobre la carpeta compartida y luego finalizar el proceso pulsando en el botón Finish. 7. Finalmente aparece una etapa que describe el estado de la compartición como satisfactoria.
PR12	<p style="text-align: center;">CONFIGURACIÓN DEL FIREWALL EN WINDOWS SERVER 2003</p> <p>El proceso que se debe seguir para configurar el firewall en Windows Server 2003, es el siguiente:</p> <p>ALTERNATIVA 1</p> <ol style="list-style-type: none"> 1. Ir a Start -> Control Panel -> Network Connections. 2. Seleccionar Local Area Connection. 3. En la ventana de diálogo Local Area Connection Status pulsar Properties -> Internet Protocol (TCP/IP) -> Properties. 4. En la ventana de diálogo Internet Protocol (TCP/IP) Properties, dar click en Advanced. 5. En el diálogo Advanced TCP/IP Settings pulsar en la pestaña Options -> TCP/IP filtering y luego dar click en Properties. 6. En el diálogo TCP/IP Filtering seleccionar Enable TCP/IP Filtering (All adapters), a continuación debe seleccionar Permit Only para cualquier categoría de puertos sean TCP, UDP o IP y luego pulsar el botón Add e ingresar el puerto en concreto y pulsar OK, así ingresar todos los puertos que se desea habilitar en el servidor y luego pulsar en OK para aceptar el filtrado de puertos TCP/IP de manera total. Luego se debe ir aceptando o cerrando las ventanas de diálogo abiertas y se debe reiniciar el servidor y con ello se habilitará solo los puertos necesarios en cada servidor. <p>ALTERNATIVA 2</p> <ol style="list-style-type: none"> 1. Ir a Start->Control Panel y seleccionar Windows Firewall, éste firewall suele estar deshabilitado, para habilitarlo debe seleccionar la opción On, en la pestaña General. 2. Cuando habilita el firewall puede también habilitar la opción Don't allow exceptions, o también configurar excepciones para el servidor de acuerdo a la funcionalidad que vaya a prestar el servidor, para llevar a cabo la configuración de excepciones, se debe seleccionar la pestaña Exceptions e ir agregando Programas o puertos que se quiera permitir que estén habilitados en el servidor. 3. Existe también una pestaña Advanced donde se puede configurar conexiones de Área Local, archivos de registro del firewall y además la propagación de los paquetes ICMP a través de la red. 4. Configurando las conexiones de área local debe pulsar el botón Settings que está ubicado junto a Local Area Connection, luego se presenta una ventana de diálogo de Advanced Settings que presenta dos pestañas denominadas Services e ICMP, en éstas pestañas se agrega los servicios de red que permite a usuarios del internet acceder a tales servicios. 5. Para configurar la seguridad de logs del firewall, debe pulsar en el botón Settings del panel Security Logging y luego seleccionar las opciones Logging Options, de igual forma se determina el nombre y la ruta donde se va a guardar el archivo log del firewall y también se especifica el tamaño límite en KB que puede tener el archivo log. <p>Para configurar ICMP debe pulsar el botón Settings del panel ICMP, el cual lleva a una ventana donde se puede habilitar o deshabilitar las peticiones que se desea para el equipo donde se está configurando éste tipo de políticas.</p>



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE																																				
PR13	<p style="text-align: center;">CONFIGURACIÓN DE INICIO DE SESIÓN INTERACTIVO NO VISUALIZAR EL NOMBRE DEL ÚLTIMO USUARIO LOGEADO</p> <p>Es una tarea de seguridad, no mostrar el nombre del último usuario que ha iniciado sesión en un equipo, para realizar esta tarea existen varias maneras:</p> <p>ALTERNATIVA 1</p> <ol style="list-style-type: none"> 1. Se lo puede realizar desde la plantilla de seguridad que se van a aplicar a un equipo, esta directiva es parte del grupo de Directivas locales (Local Policies), y específicamente se la ubica en Security Options como Interactive logon: Do not display last user name. 2. La directiva que se menciona en el paso anterior se la debe configurar en Enable, la misma que tendrá su efectividad cuando se aplique la plantilla de seguridad en el equipo. <p>ALTERNATIVA 2</p> <ol style="list-style-type: none"> 1. Ir a Start -> Administrative Tools -> Domain Security Policy. 2. En la ventana Default Domain Security Settings, ubicarse en Local Policies y expandirlo, luego seleccionar Security Options, en el panel Directivas de la derecha buscar Interactive logon: Do not display last user name y dar doble click sobre ella y luego seleccionar Enable. 3. Cerrar la ventana de Default Domain Security Settings, y reiniciar el equipo. <p>ALTERNATIVA 3</p> <p style="text-align: center;">DESACTIVAR NOMBRE DEL ULTIMO USUARIO LOGEADO DESDE EL REGEDIT</p> <ol style="list-style-type: none"> 1. Ir a Start -> Run -> escribir regedit. 2. Ubicarse en la ruta: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system. 3. Buscar la clave: DontDisplayLastUserName e ingresar el valor decimal 1. 4. Cerrar el editor de registro del sistema y reiniciar el equipo. 																																				
PR14	<p style="text-align: center;">PROCESO DE ACTUALIZACIÓN DEL SISTEMA OPERATIVO WINDOWS SERVER 2003</p> <ol style="list-style-type: none"> 1. El servidor debe de estar conectado al internet de manera ininterrumpida durante el proceso de actualización. La opción de actualización que se debería elegir para los servidores del GDS sería de manera automática, con ello evita sobrecargar el trabajo de los administradores de los servidores. 2. La actualización realizarla los días sábados o domingos. 3. El horario en que se actualice el sistema de los servidores es de preferencia que se realice luego de las 6 pm. 4. Para iniciar la configuración, dar click derecho en My Computer -> Properties, también se puede hacerlo desde el Control Panel -> System. 5. En System Properties ubicar Automatic Updates -> seleccionar Automatic 6. Escoger la frecuencia con que se desea actualizar el equipo, así como la hora que se desea que se instalen las actualizaciones. <table border="1" data-bbox="746 1760 1152 1989"> <thead> <tr> <th>Frecuencia</th> <th colspan="3">Hora</th> </tr> </thead> <tbody> <tr> <td>Every day</td> <td>0:00</td> <td>8:00</td> <td>16:00</td> </tr> <tr> <td>Every Sunday</td> <td>1:00</td> <td>9:00</td> <td>17:00</td> </tr> <tr> <td>Every Monday</td> <td>2:00</td> <td>10:00</td> <td>18:00</td> </tr> <tr> <td>Every Tuesday</td> <td>3:00</td> <td>11:00</td> <td>19:00</td> </tr> <tr> <td>Every Wednesday</td> <td>4:00</td> <td>12:00</td> <td>20:00</td> </tr> <tr> <td>Every Thursday</td> <td>5:00</td> <td>13:00</td> <td>21:00</td> </tr> <tr> <td>Every Friday</td> <td>6:00</td> <td>14:00</td> <td>22:00</td> </tr> <tr> <td>Every Saturday</td> <td>7:00</td> <td>15:00</td> <td>23:00</td> </tr> </tbody> </table>	Frecuencia	Hora			Every day	0:00	8:00	16:00	Every Sunday	1:00	9:00	17:00	Every Monday	2:00	10:00	18:00	Every Tuesday	3:00	11:00	19:00	Every Wednesday	4:00	12:00	20:00	Every Thursday	5:00	13:00	21:00	Every Friday	6:00	14:00	22:00	Every Saturday	7:00	15:00	23:00
Frecuencia	Hora																																				
Every day	0:00	8:00	16:00																																		
Every Sunday	1:00	9:00	17:00																																		
Every Monday	2:00	10:00	18:00																																		
Every Tuesday	3:00	11:00	19:00																																		
Every Wednesday	4:00	12:00	20:00																																		
Every Thursday	5:00	13:00	21:00																																		
Every Friday	6:00	14:00	22:00																																		
Every Saturday	7:00	15:00	23:00																																		



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD – DETALLE
	7. Aplicar las configuraciones realizadas y pulsar OK .
PR15	<p style="text-align: center;">PARANDO O QUITANDO RECURSOS COMPARTIDOS</p> <p>Quitar recursos compartidos innecesarios es una forma de dar seguridad a la información que se comparte. El proceso que se debe seguir para quitar recursos innecesarios es el siguiente:</p> <ol style="list-style-type: none"> 1. Ir a Start -> Administrative Tools -> Computer Management. 2. En la ventana de Computer Management, seleccionar y expandir Shared Folders, luego dar click en Shares. 3. En el panel de la derecha dar click derecho en una parte vacía, en el menú que se presenta seleccionar New Share, lo que le muestra un asistente 4. En el panel de la derecha click derecho sobre el recurso que desea quitar de entre el conjunto de recursos compartidos y luego seleccionar Stop Sharing del menú que se presenta. <p>OBS: Hay que tener presente que en Windows Server 2003 existen recursos compartidos ocultos, por lo que no aparecen en la lista de recursos compartidos normales, a estos recursos solo puede acceder el administrador y son los siguientes:</p> <ul style="list-style-type: none"> ✓ C\$: Acceso a la partición o volumen raíz. También se puede acceder a las demás particiones por su letra seguida del carácter "S". ✓ ADMIN\$: El acceso al directorio %systemroot% (raíz del sistema), que permite administrar el equipo en la red. ✓ IPC\$: Permite la comunicación entre los procesos de red. ✓ PRINT\$: Acceso remoto a las impresoras. <p>Fuente: http://es.kioskea.net/configuration-reseau/partage-fichiers.php3</p>
PR16	<p style="text-align: center;">DESHABILITAR LA OPCIÓN DE CREACIÓN DE ARCHIVO DUMP</p> <p>Esta opción puede proveer información a un atacante ya que este archivo almacena información de las aplicaciones que se ejecutan en un equipo</p> <ol style="list-style-type: none"> 1. Ir a Control Panel->System->Advanced->Startup and Recovery->Settings. 2. Deshabilitar la opción Write debugging Information a none.
PR17	<p style="text-align: center;">PROCESO DE CREACIÓN DE UNA PLANTILLA DE SEGURIDAD EN WINDOWS SERVER 2003 ENTERPRISE EDITION</p> <p>A continuación, se describen todos los pasos que se deben seguir para la creación de una plantilla de seguridad para servidores que trabajan bajo la plataforma Windows Server 2003 Enterprise Edition.</p> <ol style="list-style-type: none"> 1. Click en Start -> Run. 2. En la ventana de diálogo Run y específicamente en el campo Open, digitar mmc y luego pulsar el botón OK. 3. En la ventana de consola que se aparece ir a File -> Add/Remove Snap-in. 4. En la ventana de diálogo Add/Remove Snap-in, pulsar en el botón Add, luego buscar y seleccionar Security Templates, pulsar el botón Add, de esa ventana de diálogo y luego el botón Close, y finalmente Ok. 5. En el árbol de Console, expanda Security Templates y, a continuación, expanda unidad: \WINDOWS\security\templates, donde unidad es la unidad en la que se ha instalado Windows. 6. Para crear la plantilla de seguridad nueva, haga clic con el botón secundario en unidad: \WINDOWS\security\templates y, a continuación, haga clic en New Template.



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE
	<p>7. Escriba un nombre para la plantilla en el cuadro Template name y haga clic en OK.</p> <p>8. Con todos los pasos del 1 al 7 creará una plantilla de seguridad, obviamente sin configuraciones previas, pues éstas se las debe configurar luego.</p>
PR18	<p style="text-align: center;">PROCESO DE APLICACIÓN DE LA PLANTILLA DE SEGURIDAD AL PDC DEL GDS</p> <p>El proceso a seguir es estándar para cualquier PDC de un dominio Windows en particular.</p> <ol style="list-style-type: none"> 1. Se utiliza la Directiva de grupo para aplicar la plantilla de seguridad en el PDC, esto es posible debido a que Active Directory para la administración de la configuración y cambios hace uso de la Directiva de grupo. 2. Se debe iniciar sesión como administrador o como miembro del grupo administradores en el Controlador de Dominio Primario y de Backup, ya que las configuraciones que se hacen en el PDC se replican al BDC. 3. La plantilla de seguridad (Plantilla Controladores de Dominio.inf) que se va a aplicar al PDC debe estar copiada en %SystemRoot%\Security\Templates. 4. Para iniciar el proceso de aplicación de la plantilla de seguridad, primero debe iniciar el Active Directory (Start -> All Programs -> Administrative Tools -> Active Directory Users and Computers). 5. Dentro de Active Directory, expanda el dominio utpl.edu.ec, luego ubíquese en la Unidad Organizativa Domain Controllers y de clic derecho sobre ésta, seleccionando ahí Properties. 6. En el cuadro de diálogo de las propiedades, seleccione la ficha Group Policy y pulse el botón New para crear el nuevo objeto de directiva de grupo (GPO). Se ingresa un nombre para la directiva de línea de base de controladores de dominio, y luego se hace clic en Close. 7. Creada la Directiva de línea de base de controladores de dominio y estando en la ventana de diálogo de propiedades de la unidad organizativa Domain Controllers, de doble clic o clic simplemente en el botón Edit una vez que haya seleccionado "Línea de Seguridad Base" que se ha creado. Tenga mucho cuidado de no modificar Default Domain Controllers Policy porque en caso de querer revertir, por algún inconveniente o error, la configuración de seguridad que se está creando a la que se crea por defecto cuando se promueve el servidor a PDC, le es de utilidad absoluta Default Domain Controllers Policy. 8. Realizado el paso anterior aparecerá la ventana de Group Policy Object Editor, que es, desde donde se va a importar la plantilla de seguridad, para ello debe expandir Windows Settings, dar clic derecho sobre Security Settings y seleccionar Import Policy. 9. En el cuadro de diálogo Import Policy From, escoja la plantilla a ser aplicada al PDC, en este caso para el PDCSERVER seleccione Plantilla Controladores de Dominio.inf y pulse el botón Open. 10. Cierre el Group Policy Object Editor, luego pulse el botón Ok de Domain Controllers Properties y cierre la ventana de Active Directory Users and Computers. Reinicie el servidor PDCSERVER o el servidor que se esté utilizando de PDC, cuando existen varios servidores que están configurados de PDC debe irlos reiniciando uno a uno. Para el caso de este esquema, primero se reinicia el PDCSERVER, luego el servidor que hace de Controlador de Dominio de Backup, para este caso DEVSERVER. 11. Para comprobar que la plantilla de seguridad se aplicado de manera correcta al PDCSERVER, vaya al Control Panel, haga clic en Administrative Tools y luego seleccione Event Viewer, donde puede elegir ver los sucesos de Aplicaciones, Seguridad, Sistema, etc., elija algunos de ellos y luego de doble clic en el panel de la derecha sobre el suceso seleccionado y podrá verificar información que indica que las configuraciones de seguridad son satisfactorias.



CÓDIGO DE PROCEDIMIENTO	ACTIVIDAD - DETALLE
PR19	<p data-bbox="507 387 1385 409">PROCESO DE APLICACIÓN DE LA PLANTILLA DE SEGURIDAD AL DOMINIO DE SERVIDORES DEL GDS</p> <p data-bbox="507 427 1394 595">Para aplicar la plantilla de seguridad al dominio de servidores Windows utpl.edu.ec, se debe estar ubicado en el servidor PDCSERVER y haber iniciado sesión como Administrador, también se debe instalar el Group Policy Management, si no se tiene disponible, se lo debe descargar de la Web de Microsoft, el administrador de políticas de grupo facilita la aplicación de la plantilla de seguridad al dominio. El proceso de aplicación en sí de la plantilla de seguridad al dominio es el siguiente:</p> <ol data-bbox="507 645 1394 1211" style="list-style-type: none">1. Se abre Active Directory Users and Computers, una vez ahí, se da clic derecho sobre utpl.edu.ec y se selecciona en Properties, luego aparecerá una pantalla de diálogo de las propiedades, en ella se debe pulsar sobre la pestaña Group Policy y clic sobre el botón Open para que se abra el Group Policy Management.2. En la pantalla de Group Policy Management, hay que desplegar los ítems hasta llegar a Group Policy Objects, una vez ahí, clic derecho sobre ésta y luego en New, se ingresa un nombre en New GPO y luego pulsa el botón Ok.3. Creado el nuevo objeto de directiva de grupo (GPO), clic derecho sobre la GPO creada y luego en Edit, donde llevará a la ventana Group Policy Object Editor allí se debe pulsar consecutivamente en Windows Settings y Security Settings, para importar la plantilla que se aplica al dominio, se debe dar clic derecho sobre Security Settings y seleccionar luego Import Policy.4. Luego aparece una pantalla Import Policy From, para este caso se selecciona Plantilla Dominio utpl.edu.ec, que es la que contiene las configuraciones a ser aplicadas al dominio en general, luego se pulsa el botón Open.5. Luego se cierra el editor de objeto de directiva de grupo y el administrador de Políticas de Grupo, luego se reinicia el Servidor PDCSERVER para que las configuraciones tengan efecto.
PR20	<p data-bbox="507 1270 1385 1328">PROCESO DE APLICACIÓN DE LAS PLANTILLAS DE SEGURIDAD A LOS SERVIDORES MIEMBROS DEL GDS</p> <p data-bbox="507 1346 1394 1404">El proceso de aplicación de una plantilla de seguridad a un servidor miembro de cualquier dominio, es el siguiente:</p> <ol data-bbox="507 1422 1394 1989" style="list-style-type: none">1. Ir a Start -> Run2. En el campo Open de la ventana de diálogo Run, digitar mmc, acción que le llevará a una Consola.3. En la ventana de la consola ir a File -> Add/Remove Snap-in.4. En la ventana de diálogo Add/Remove Snap-in pulsar el botón Add y escoger de la lista Available Standalone Snap-ins -> Security Configuration and Analysis y pulsar el botón Add luego el botón Close y OK de manera sucesiva.5. En la consola aparecerá Security Configuration and Analysis sobre la que se da click derecho y se escoge Open Database, lo cual abre una ventana de diálogo donde se debe ingresar un nombre para la base de datos de seguridad y se pulsa el botón Open, lo que conduce a otra ventana de diálogo donde se escoge "Plantilla Servidores Miembros.inf" e igualmente se pulsa el botón Open.6. Con click derecho en Security Configuration and Analysis escoger Analyze Computer Now para verificar y comprobar el tipo de seguridades que ha tenido el servidor configurado y así poder observar los cambios que se realizarán.7. Igualmente desde Security Configuration and Analysis dar click derecho y seleccionar Configure Computer Now con lo que aplicará las configuraciones contenidas en la plantilla de seguridad.8. Luego reinicie el equipo para que las configuraciones de seguridad tengan efecto.



POLÍTICAS A CONSIDERAR AL CONFIGURAR SEGURIDADES EN WINDOWS SERVER 2003



CÓDIGO DE POLÍTICA	ACTIVIDAD
PL01	<p style="text-align: center;">POLÍTICAS DE ACTUALIZACIÓN DE LAS PLATAFORMAS WINDOWS</p> <ol style="list-style-type: none">1. El sistema operativo debe actualizarse dependiendo de la exposición en que se encuentre, así es recomendable que se actualice cada semana.2. Escoger el día que exista menos tráfico de red para que las actualizaciones se instalen de manera adecuada. Es recomendable realizar las actualizaciones por las noches, porque la carga de trabajo de un equipo es baja.3. El administrador del equipo es quien debe configurar la forma en que las actualizaciones se deben instalar, pudiendo ser:<ul style="list-style-type: none">❖ Automáticas que es lo recomendado.- Se instalan directamente desde el propio sitio Web de Microsoft, se debe contar con una conexión a internet de manera permanente y haber iniciado sesión en el equipo donde se va a actualizar como administrador.❖ Descargar las actualizaciones por cuenta propia y elegir cuando instalarlas.- Involucra que en cualquier momento el administrador del equipo puede ir al sitio Web de Microsoft (Windows Update) y descargar actualizaciones de seguridad, hotfix, archivos de ayuda recientes, controladores y demás productos que garanticen y ayuden a la integridad del sistema operativo.❖ Que el sistema notifique que hay actualizaciones disponibles, pero no descargar ni instalarlas.- Opción que deja a criterio del administrador la decisión de instalar o no las actualizaciones de seguridad en un equipo.❖ Optar por la opción de apagar el servicio de actualizaciones automáticas.- No se recomienda parar el servicio que notifica la disponibilidad de nuevas actualizaciones de seguridad, pero es un criterio que debe decidir el administrador del equipo.4. Cuando se hace una actualización, al finalizar la misma, se pide reiniciar el equipo, este tipo de acción debe de ser afirmado o cancelado, el administrador del equipo debe decidir cuándo reiniciar, pero por lo general todas las actualizaciones en sistemas Windows demandan reiniciar el equipo para que surtan efecto.5. Toda actualización que se haga mediante la utilización de Windows Update o de manera manual, debe pasar su tráfico por un firewall, con la finalidad de filtrar las descargas de actualización y con ello evitar descargar software malicioso que vaya afectar el rendimiento del equipo, así como a la información que se almacena en el mismo.6. Contar con un servidor actualizado, permite resolver problemas desconocidos y protege al equipo contra vulnerabilidades de seguridad
PL02	<p style="text-align: center;">POLÍTICAS DE CONTRASEÑAS</p> <p>CONSIDERACIONES GENERALES</p> <ol style="list-style-type: none">1. Todas las contraseñas de los sistemas de información, por ejemplo cuentas de sistema operativo, cuentas de aplicación, etc. deben de cambiarse con una periodicidad trimestral.2. Todas las contraseñas de de inicio de sesión para los usuarios, deben de cambiarse con una periodicidad de 45 días.3. Todas las contraseñas en los sistemas en producción deben ser parte de un sistema de autenticación global de administración (Active Directory – Domain Controller).4. Las cuentas administrativas no pueden ser compartidas, en caso de requerirse que varios usuarios tengan acceso a privilegios administrativos a nivel del sistema, estos serán otorgados a través de un grupo de usuarios administrativos de sistemas.5. Las contraseñas no pueden ser comunicadas a otras personas ya que son intransferibles y personales.



CÓDIGO DE POLÍTICA	ACTIVIDAD										
	<p>6. Todas las contraseñas que se manejen dentro de una entidad, ya sea a nivel de usuario o a nivel de administración de sistemas deben de conformarse con base a los lineamientos descritos a continuación.</p> <p style="text-align: center;">CONSIDERACIONES ESPECIFICAS EN LA CONSTRUCCIÓN DE CONTRASEÑAS</p> <p>1. Utilizar al menos 13 caracteres para crear una contraseña (15 para seguridad completa).</p> <p>2. Utilizar en una misma contraseña tres tipos de caracteres de los cuatro grupos descritos en la tabla siguiente, eligiendo SIEMPRE QUE UNO DE ELLOS SEA EL DE SÍMBOLOS.</p> <p style="text-align: center;">Caracteres utilizables para una contraseña segura</p> <table border="1" data-bbox="639 728 1257 920"> <thead> <tr> <th>Grupo</th> <th>Carácter</th> </tr> </thead> <tbody> <tr> <td>Letras mayúsculas</td> <td>A, B, C, D,.....Z</td> </tr> <tr> <td>Letras minúsculas</td> <td>a, b, c, d,.....z</td> </tr> <tr> <td>Números</td> <td>0, 1, 2,.....9</td> </tr> <tr> <td>Símbolos</td> <td>~@#\$\$%&/()[]\`{}-.*+_= ?!\`";<>.</td> </tr> </tbody> </table> <p>3. Alternar aleatoriamente letras mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.</p> <p>4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.</p> <p>5. Cambiar las contraseñas con una cierta regularidad. La duración máxima de una contraseña no debe ser más de 60 días, después del día 60 “máxima duración de la contraseña”, la contraseña debe expirar.</p> <p>6. Procurar no generar reglas secuenciales de cambio de contraseñas. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. Por ejemplo pasar de “01Juitnx” a “02Juitnx”.</p> <p>7. Utilizar signos de puntuación si el sistema lo permite. Por ejemplo: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos.</p> <p>8. Emplear algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, y combinar esas palabras con números o letras e introducir alguna letra mayúscula. Otro método sencillo de crear contraseñas consiste es elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante este artificio es más sencillo recordarla. Por ejemplo, de la frase “comí mucho Chocolate el Domingo 3, por La tarde”, resultaría la contraseña: “cmCeD3xLt”.</p> <p style="text-align: center;">ESTÁNDARES PARA LA GESTIÓN DE CONTRASEÑAS SEGURAS</p> <p>1. Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas.</p> <p>2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el código de identificación personal o número de teléfono.</p> <p>3. Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)</p>	Grupo	Carácter	Letras mayúsculas	A, B, C, D,.....Z	Letras minúsculas	a, b, c, d,.....z	Números	0, 1, 2,.....9	Símbolos	~@#\$\$%&/()[]\`{}-.*+_= ?!\`";<>.
Grupo	Carácter										
Letras mayúsculas	A, B, C, D,.....Z										
Letras minúsculas	a, b, c, d,.....z										
Números	0, 1, 2,.....9										
Símbolos	~@#\$\$%&/()[]\`{}-.*+_= ?!\`";<>.										



CÓDIGO DE POLÍTICA	ACTIVIDAD
	<ol style="list-style-type: none"> 4. No repetir los mismos caracteres en la misma contraseña. (ejemplo: "111222"). 5. Evitar utilizar solamente números, letras mayúsculas o minúsculas en la contraseña. 6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña. 7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ejemplo: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.). 8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ejemplo: no guardar las contraseñas de las tarjetas de débito/crédito en el celular o las contraseñas de los correos en documentos de texto dentro del ordenador). 9. No se debe utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como "ataque por diccionario". 10. No enviar nunca la contraseña por correo electrónico o en un mensaje. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo. 11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o "vuelta atrás". 12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas. 13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.). 14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes. <p>Fuente: http://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenenas.pdf</p>
PL03	<p style="text-align: center;">POLÍTICAS DE AUDITORÍA EN WINDOWS SERVER 2003</p> <p>Las políticas de auditoría en un sistema operativo son de mucha importancia ya que es un medio para dar seguimiento a errores del propio sistema, aplicaciones, usuarios, etc. A continuación se detallan algunas políticas que son necesarias su consideración en entornos de seguridad.</p> <ol style="list-style-type: none"> 1. Auditar cada instancia de un usuario que inicie o cierre una sesión desde otro equipo, en la que el equipo que registra el suceso de auditoría se utiliza para validar la cuenta. 2. Auditar todos los sucesos de administración de cuentas de un equipo. 3. Auditar el suceso de un usuario que tiene acceso a un objeto de Microsoft Active Directory que tiene su propia lista de control de acceso al sistema (SACL) especificada. 4. Auditar cada instancia de un usuario que inicie, cierre una sesión o realice una conexión de red al equipo que registra el suceso de auditoría. 5. Auditar el suceso de un usuario que obtiene acceso a un objeto como, por ejemplo, un archivo, una carpeta, una clave de Registro, una impresora, etc., que tiene su propia lista de control de acceso al sistema especificada. 6. Auditar cada caso de cambio de las directivas de asignación de derechos de usuario, de auditoría o de confianza. 7. Auditar cada caso en el que un usuario ejecute un derecho de usuario.



CÓDIGO DE POLÍTICA	ACTIVIDAD																																				
	<p>8. Auditar información de seguimiento detallada de sucesos como la activación de programas, la salida de procesos, la duplicación de identificadores y el acceso indirecto a objetos.</p> <p>9. Auditar el reinicio o cierre de un equipo realizado por un usuario o un suceso que afecte a la seguridad del sistema o al registro de seguridad.</p> <p>Fuente: http://www.microsoft.com/spain/technet/recursos/articulos/secmod50.mspx</p>																																				
<p>PL04</p>	<p style="text-align: center;">POLÍTICAS QUE SE DEBEN ACTIVAR PARA LOS SERVIDORES DEL GDS</p> <p>Las políticas que se deben configurar para los servidores del GDS se elaboran de acuerdo al rol, nivel de exposición y criticidad de cada servidor es por ello que se describen las siguientes políticas:</p> <ol style="list-style-type: none"> 1. Configurar un firewall a nivel perimetral que de protección al dominio utpl.edu.ec 2. Aplicar políticas de cuenta a nivel de dominio, las cuales deben tener los siguientes valores de configuración: <table border="1" data-bbox="568 790 1329 1473"> <thead> <tr> <th data-bbox="568 790 1062 824">Directiva</th> <th data-bbox="1062 790 1329 824">Configuración recomendada</th> </tr> </thead> <tbody> <tr> <td colspan="2" data-bbox="568 824 1329 857" style="text-align: center;">Políticas de Contraseña</td> </tr> <tr> <td data-bbox="568 857 1062 898">Enforce password history</td> <td data-bbox="1062 857 1329 898">24 passwords remembered</td> </tr> <tr> <td data-bbox="568 898 1062 938">Maximum password age</td> <td data-bbox="1062 898 1329 938">42 days</td> </tr> <tr> <td data-bbox="568 938 1062 978">Minimum password age</td> <td data-bbox="1062 938 1329 978">1 day</td> </tr> <tr> <td data-bbox="568 978 1062 1019">Minimum password length</td> <td data-bbox="1062 978 1329 1019">13 characters</td> </tr> <tr> <td data-bbox="568 1019 1062 1059">Password must meet complexity requirements</td> <td data-bbox="1062 1019 1329 1059">Enabled</td> </tr> <tr> <td data-bbox="568 1059 1062 1099">Store passwords using reversible encryption</td> <td data-bbox="1062 1059 1329 1099">Disabled</td> </tr> <tr> <td colspan="2" data-bbox="568 1099 1329 1133" style="text-align: center;">Políticas de Bloqueo de Cuenta</td> </tr> <tr> <td data-bbox="568 1133 1062 1173">Account lockout duration</td> <td data-bbox="1062 1133 1329 1173">15 minutes</td> </tr> <tr> <td data-bbox="568 1173 1062 1214">Account lockout threshold</td> <td data-bbox="1062 1173 1329 1214">10 invalid logon attempts</td> </tr> <tr> <td data-bbox="568 1214 1062 1254">Reset account lockout counter after</td> <td data-bbox="1062 1214 1329 1254">15 minutes</td> </tr> <tr> <td colspan="2" data-bbox="568 1254 1329 1288" style="text-align: center;">Políticas Kerberos</td> </tr> <tr> <td data-bbox="568 1288 1062 1328">Enforce user logon restrictions</td> <td data-bbox="1062 1288 1329 1328">Enabled</td> </tr> <tr> <td data-bbox="568 1328 1062 1368">Maximum lifetime for Service ticket</td> <td data-bbox="1062 1328 1329 1368">600 minutes</td> </tr> <tr> <td data-bbox="568 1368 1062 1408">Maximum lifetime for user ticket</td> <td data-bbox="1062 1368 1329 1408">10 hours</td> </tr> <tr> <td data-bbox="568 1408 1062 1449">Maximum lifetime for user ticket renewal</td> <td data-bbox="1062 1408 1329 1449">7 days</td> </tr> <tr> <td data-bbox="568 1449 1062 1489">Maximum tolerance for computer clock synchronization</td> <td data-bbox="1062 1449 1329 1489">5 minutes</td> </tr> </tbody> </table> 3. Administrar los servidores a través de Active Directory 4. Aplicar plantillas de seguridad a los servidores que trabajan como Controladores de Dominio, Servidores miembros, tomando en consideración el rol que desempeñan dentro del GDS. 5. Manejar contraseñas fuertes por parte de los administradores como de los usuarios normales 6. Configurar firewalls personalizados de acuerdo a la funcionalidad que cada servidor debe ofrecer 7. Habilitar auditorias de sucesos de eventos en cada servidor, para detectar fallas en caso de darse por parte de aplicaciones instaladas y del propio sistema en sí. 8. Concientizar a que todos los miembros del GDS sigan técnicas de seguridad en cuentas de inicio de sesión de aplicaciones, bases de datos y del propio sistema operativo. De igual forma exigir que los usuarios de sistemas de información utilicen contraseñas fuertes para inicio de sesión en sus cuentas. 	Directiva	Configuración recomendada	Políticas de Contraseña		Enforce password history	24 passwords remembered	Maximum password age	42 days	Minimum password age	1 day	Minimum password length	13 characters	Password must meet complexity requirements	Enabled	Store passwords using reversible encryption	Disabled	Políticas de Bloqueo de Cuenta		Account lockout duration	15 minutes	Account lockout threshold	10 invalid logon attempts	Reset account lockout counter after	15 minutes	Políticas Kerberos		Enforce user logon restrictions	Enabled	Maximum lifetime for Service ticket	600 minutes	Maximum lifetime for user ticket	10 hours	Maximum lifetime for user ticket renewal	7 days	Maximum tolerance for computer clock synchronization	5 minutes
Directiva	Configuración recomendada																																				
Políticas de Contraseña																																					
Enforce password history	24 passwords remembered																																				
Maximum password age	42 days																																				
Minimum password age	1 day																																				
Minimum password length	13 characters																																				
Password must meet complexity requirements	Enabled																																				
Store passwords using reversible encryption	Disabled																																				
Políticas de Bloqueo de Cuenta																																					
Account lockout duration	15 minutes																																				
Account lockout threshold	10 invalid logon attempts																																				
Reset account lockout counter after	15 minutes																																				
Políticas Kerberos																																					
Enforce user logon restrictions	Enabled																																				
Maximum lifetime for Service ticket	600 minutes																																				
Maximum lifetime for user ticket	10 hours																																				
Maximum lifetime for user ticket renewal	7 days																																				
Maximum tolerance for computer clock synchronization	5 minutes																																				
<p>PL05</p>	<p style="text-align: center;">POLÍTICAS DE CONFIGURACIÓN DEL FIREWALL DE WINDOWS</p> <p>Antes de especificar las políticas a seguir en la configuración de un firewall ya sea en sistemas operativos Windows o en cualquier otro, se debe tener presente algunas puntualizaciones previas:</p>																																				



CÓDIGO DE POLÍTICA	ACTIVIDAD
	<p>CARACTERÍSTICAS GENERALES DEL FIREWALL</p> <ol style="list-style-type: none"> 1. Para que un firewall sea efectivo, todo el tráfico de información entre redes debe pasar a través de él. 2. Una vez que un agresor pasa la línea firewall, pues éste no ofrece protección 3. Un firewall es una parte de una política de seguridad global dentro de una organización 4. Un firewall sin seguir una política de seguridad bien definida es poco eficiente 5. Un firewall permite a un administrador de red definir una especie de embudo por donde pase el tráfico de red, manteniendo así controlados a usuarios no autorizados (hackers, crackers, espías, etc.) 6. Simplifica los trabajos administrativos 7. Permite monitorear actividades sospechosas <p><u>Lo que un firewall no protege</u></p> <ol style="list-style-type: none"> 1. Ataques que se dan fuera de su punto de operación (conexiones punto a punto, dial-up, etc.) 2. Amenazas internas (empleados, usuarios empresariales, administradores mal intencionado, etc.) 3. Ataques de ingeniería social 4. Ataques de virus a través de archivos y software que se almacena en medios extraíbles (CD, DVD, Memory flash, etc.) 5. Ataques posibles en transferencia de datos, suelen ocurrir cuando se envían o copian datos infectados a un servidor interno y luego son ejecutados, desencadenando así un ataque. <p>POLÍTICAS</p> <ol style="list-style-type: none"> 1. El firewall puede obstruir todo el tráfico de red, servicios y aplicaciones que se desee, por tal motivo se debe analizar caso por caso lo que se desea permitir y así denegar todo lo demás. Se debe dar prioridad a la seguridad y con ello permitir lo que demanda únicamente la organización. 2. El firewall puede permitir todo el tráfico de red y luego ir aislando servicio por servicio que se considere potencialmente peligroso hasta depurar de manera total lo permitido de lo denegado. Es decir se da un mayor ámbito de operación de servicios para los usuarios. <p>Fuente: http://www.redes-linux.com/manuales/seguridad/firewalls1.pdf</p>
PL06	<p>POLÍTICAS DE BLOQUEO DE CUENTAS DE USUARIO</p> <p>La correcta definición de las políticas de bloqueo de cuentas evita la pérdida de trabajo por parte de los empleados dentro de una organización, por tal motivo se deben considerar algunas políticas antes de ser aplicado un bloqueo de cuenta:</p> <ol style="list-style-type: none"> 1. Se tiene que tener saber que un bloqueo de cuenta es una deshabilitación temporal de una cuenta de usuario (10 min, 20 min, 30 min, etc.). 2. Es verdad que al habilitar el bloqueo de cuentas de usuario se reduce la posibilidad de ser atacados por individuos mal intencionados, pero también existe el riesgo que se bloquee de manera involuntaria a usuarios autorizados, por eso la importancia de fijar de manera correcta esta política. 3. Conociendo lo positivo y negativo que podría generar el establecer este tipo de política, se aconseja configurar el umbral de bloqueo a un número lo suficientemente alto, con la finalidad de evitar que usuarios autorizados queden bloqueados, por haber escrito u olvidado la contraseña de manera temporal. 4. No permitir que sean los usuarios los que establezcan este tipo de política en su equipo, porque quedarían bloqueados esto en el caso que se esté usando un controlador de dominio, por lo general este tipo de política debe fijarla un administrador del sistema o su encargado desde el equipo que controla a



CÓDIGO DE POLÍTICA	ACTIVIDAD
	<p>todos los equipos de un dominio, puede ser un PDC por ejemplo.</p>
<p>PL07</p>	<p style="text-align: center;">POLÍTICAS DE CONTROL DE ACCESO</p> <p>Algunas políticas de control de acceso se recomiendan poner en práctica en esquemas de seguridad, bien sea para denegar como para conceder acceso a un sistema operativo.</p> <ol style="list-style-type: none"> 1. Asignar permisos a grupos en lugar de a usuarios. No resulta eficaz mantener cuentas de usuario directamente, la asignación de permisos por usuario debe realizarse con mucha excepción. 2. Utilizar los permisos Denegar para determinados casos especiales. Se puede utilizar Denegar para excluir un subconjunto de un grupo que tiene permisos permitidos. Utilice Denegar para excluir un permiso en particular cuando ya ha concedido control total a un usuario o grupo. 3. Nunca denegar al grupo Todo el acceso a un objeto. Si deniega el permiso a todos respecto de un objeto, se incluye a los administradores. Una mejor solución sería quitar el grupo Todos, siempre que conceda a otros usuarios, grupos o equipos permisos para ese objeto. 4. Asignar permisos a un objeto en el nivel más alto posible del árbol y, luego, aplicar la herencia para propagar la configuración de seguridad en todo el árbol. Puede aplicar de forma rápida y eficaz la configuración de control de acceso a todos los objetos secundarios o a un subárbol de un objeto principal. De esta manera, se obtiene la mayor extensión del efecto con el esfuerzo mínimo. La configuración de permisos que especifique debe ser adecuada para la mayoría de los usuarios, grupos y equipos. 5. Los permisos explícitos pueden a veces reemplazar los permisos heredados. Los permisos Denegar heredados no impiden el acceso a un objeto si el objeto tiene una entrada explícita de permiso explícito Permitir. Los permisos explícitos prevalecen sobre los permisos heredados, incluso los permisos Denegar heredados. 6. Para los permisos en objetos de Active Directory, asegúrese de comprender las prácticas recomendadas concernientes a objetos de Active Directory.
<p>PL08</p>	<p style="text-align: center;">POLÍTICAS DE PRIVILEGIOS O ASIGNACIÓN DE PERMISOS EN WINDOWS SERVER 2003</p> <p>La asignación de permisos en Windows server 2003 está sujeta a algunas políticas a considerar:</p> <ol style="list-style-type: none"> 1. Antes de aplicar permisos a un recurso, objeto, archivo o directorio que se vaya a compartir primero se debe hacer una planificación de lo que se les permitirá y lo que se denegará. 2. Otorgar permisos a nivel de grupo es una buena práctica de administración, de lo contrario dar permisos usuario por usuario es un trabajo arduo. 3. De acuerdo a los grupo de usuarios se dan privilegios sobre los recursos compartidos de un servidor 4. Optar por denegar siempre excepto en los siguientes casos: <ul style="list-style-type: none"> ✓ Denegar permisos de uso para tratar de excluir un subconjunto de usuarios de un grupo al cual se ha permitido permisos determinados. ✓ Tratar de denegar para excluir un permiso especial si ya se ha concedido el control completo a un usuario o grupo en particular. 5. Si se da permisos de manera individual a usuarios sobre recursos compartidos, se lo debe de realizar de una manera cautelosa. 6. Evitar utilizar la opción de denegar permisos a nivel de grupo, porque puede denegarse a todo el mundo inclusive a usuarios administradores. 7. Los permisos que se pueden asignar sobre los recursos compartidos se detallan en la siguiente tabla:



CÓDIGO DE POLÍTICA	ACTIVIDAD														
	<table border="1"> <thead> <tr> <th data-bbox="536 387 724 421">Permisos</th> <th data-bbox="724 387 1362 421">Descripción</th> </tr> </thead> <tbody> <tr> <td data-bbox="536 421 724 499">Full Control</td> <td data-bbox="724 421 1362 499">Permite a los usuarios crear, borrar, modificar, compartir y conceder permisos</td> </tr> <tr> <td data-bbox="536 499 724 577">Modify</td> <td data-bbox="724 499 1362 577">Permite a los usuarios crear, borrar y modificar el contenido de una carpeta. Esto incluye la creación de documentos y subcarpetas.</td> </tr> <tr> <td data-bbox="536 577 724 689">Read & Execute</td> <td data-bbox="724 577 1362 689">Ofrece la capacidad de leer y ejecutar archivos y recorrer carpetas hijas. En efecto, ejecuta acciones permitidas por el permiso de lectura y el permiso de listar contenido de carpetas.</td> </tr> <tr> <td data-bbox="536 689 724 801">Read</td> <td data-bbox="724 689 1362 801">Permite al usuario leer el contenido de una carpeta, pero no modificar ni escribir cualquier contenido. Los usuarios tampoco pueden crear archivos, ni directorios.</td> </tr> <tr> <td data-bbox="536 801 724 869">Write</td> <td data-bbox="724 801 1362 869">Permite crear nuevos archivos y subcarpetas, además deja cambiar los atributos del sistema de archivos.</td> </tr> <tr> <td data-bbox="536 869 724 943">Special Permissions</td> <td data-bbox="724 869 1362 943">Proporciona los medios para editar permisos existentes para hacerlos más granulares.</td> </tr> </tbody> </table>	Permisos	Descripción	Full Control	Permite a los usuarios crear, borrar, modificar, compartir y conceder permisos	Modify	Permite a los usuarios crear, borrar y modificar el contenido de una carpeta. Esto incluye la creación de documentos y subcarpetas.	Read & Execute	Ofrece la capacidad de leer y ejecutar archivos y recorrer carpetas hijas. En efecto, ejecuta acciones permitidas por el permiso de lectura y el permiso de listar contenido de carpetas.	Read	Permite al usuario leer el contenido de una carpeta, pero no modificar ni escribir cualquier contenido. Los usuarios tampoco pueden crear archivos, ni directorios.	Write	Permite crear nuevos archivos y subcarpetas, además deja cambiar los atributos del sistema de archivos.	Special Permissions	Proporciona los medios para editar permisos existentes para hacerlos más granulares.
Permisos	Descripción														
Full Control	Permite a los usuarios crear, borrar, modificar, compartir y conceder permisos														
Modify	Permite a los usuarios crear, borrar y modificar el contenido de una carpeta. Esto incluye la creación de documentos y subcarpetas.														
Read & Execute	Ofrece la capacidad de leer y ejecutar archivos y recorrer carpetas hijas. En efecto, ejecuta acciones permitidas por el permiso de lectura y el permiso de listar contenido de carpetas.														
Read	Permite al usuario leer el contenido de una carpeta, pero no modificar ni escribir cualquier contenido. Los usuarios tampoco pueden crear archivos, ni directorios.														
Write	Permite crear nuevos archivos y subcarpetas, además deja cambiar los atributos del sistema de archivos.														
Special Permissions	Proporciona los medios para editar permisos existentes para hacerlos más granulares.														
PL09	<p align="center">POLÍTICAS CONSIDERADAS EN LA ELABORACIÓN DEL ESQUEMA DE SEGURIDAD PARA EL GDS DE LA UTPL</p> <p>Las políticas que se deben considerar al llevar a cabo la implementación de un Esquema de Seguridad, están de acuerdo a muchos conceptos dependiendo de donde se vaya a implementar dicho esquema, en la implementación del Esquema de seguridad para los servidores del GDS de la UTPL que trabajan con plataformas Windows Server 2003, se ha considerado las siguientes políticas:</p> <ol style="list-style-type: none"> Identificar el propósito de los servidores que forma parte del Esquema de Seguridad <ul style="list-style-type: none"> ❖ Categoría de información que va a ser almacenada en los servidores ❖ Que información va a ser procesada o transmitida a través de los servidores ❖ Que requerimientos de seguridad se necesita para la información que maneja ❖ Toda la información será recuperada o almacenada en otros servidores (servidores de Base de Datos, servidores de Directorio, servidores Web, etc.) ❖ Cuáles son los requerimientos de seguridad para los demás servidores involucrados ❖ Que otros servicios serán proporcionados por los servidores ❖ Que requerimientos de seguridad son necesarios para los servicios adicionales ❖ Requisitos para la continuidad de los servicios prestados por los servidores en caso de que falle alguno de ellos (continuidad de operaciones, planes de recuperación de desastres, etc.) ❖ En que parte de la red los servidores están ubicados Identificar los servicios de red que serán proporcionados por los servidores que van a conformar el Esquema de Seguridad. Identificar todo software de servicio de red, tanto del lado del cliente como del servidor que será instalado en el servidor, así como software de soporte para los servidores. Identificar los usuarios o categorías de usuarios de los servidores, así como también los servidores de soporte. Determinar los privilegios que cada categoría de usuarios tendrá en cada servidor, así como en los servidores de soporte Determinar la forma en que los servidores serán administrados (localmente, remotamente desde la red interna, remotamente desde redes externas, etc.) 														



CÓDIGO DE POLÍTICA	ACTIVIDAD
	<p>7. Definir como serán los usuarios autenticados y como serán protegidos los datos de autenticación.</p> <p>8. Determinar el acceso apropiado a ser aplicado para los recursos de información</p> <p>9. Determinar cuáles aplicaciones de servidor son requeridas y esenciales para satisfacer las necesidades de la organización. Considere los servidores que pueden ofrecer una gran seguridad aunque con menos funcionalidad en muchos casos. Algunos puntos a considerar son:</p> <ul style="list-style-type: none">❖ Costo❖ Compatibilidad con la infraestructura existente❖ Conocimiento de los trabajadores de la entidad❖ Historial de vulnerabilidades❖ Funcionalidad <p>10. Descripciones detalladas del hardware de los servidores, ésta información se la consigue o es proporcionada por el fabricante de los servers, contar con un detalle de hardware en la etapa de planificación es relevante para la construcción de un Esquema de Seguridad.</p>