

---

# Políticas de Grupo Definidas

---



## Tabla de Contenido

<b>Objetivo</b> _____	<b>3</b>
<b>Introducción</b> _____	<b>4</b>
<b>Políticas de Grupo a nivel Unidades Organizacionales</b> _____	<b>6</b>
<b>Políticas de Grupo en OU CCDAdministrators</b> _____	<b>6</b>
<b>Políticas de Grupo en OU CCDUsers</b> _____	<b>10</b>
<b>Políticas de Grupo en OU CCDComputers</b> _____	<b>16</b>
<b>Políticas Aplicadas a clientes Windows 95/98</b> _____	<b>17</b>
<b>Definición de Políticas en Poledit</b> _____	<b>17</b>

## Objetivo

El documento tiene como objetivo el resumir la definición de Políticas de Grupo definidas y configuradas en el Directorio Activo de Windows 2000 del Ambiente de Pruebas, para clientes 2000/XP y 98.

La información contenida en este documento permitirá comprender la definición de las políticas aplicadas, su configuración dentro del Directorio Activo y su efecto sobre computadoras y usuarios.

## Introducción

Las políticas de grupo de Directorio Activo de Windows 2000, nos permiten controlar y limitar el comportamiento de los usuarios al acceder los recursos los equipos y la red.

Las políticas de grupo se definen en dos secciones: la primera que modifica la configuración de clientes o servidores y la segunda que configura el ambiente para los usuarios.

La sección "Computer Configuration" permite configurar entre otras cosas los "security settings" de los equipos, esto incluye: Account policies (password policy y account lockout policy), Local Policies (audit policy, user rights y security options), Event Log, System Services, configuración del registry y File System, etc. Adicionalmente permite la configuración de ciertas funciones de diferentes productos, así como el poder el poder publicar aplicaciones para su instalación. Esta parte de la política se aplica por equipo en el momento que este inicia e inicia su sesión de red (Netlogon).

La sección de "User Configuration" permite configurar diferentes aspectos del ambiente de Windows, tales como acceso al control panel, o la configuración de red, instalación de software, configuración del escritorio (fondo, protector de pantalla, etc.), configuración del Internet Explorer, las opciones disponibles en los menús, etc. Esta parte de la política se aplica por usuario, al momento en que este se firma en una computadora con su cuenta y contraseña del dominio.

Las políticas de grupo pueden definirse a nivel Sitio (Site), a nivel Dominio y a nivel Unidad Organizacional (OU). Las políticas a nivel dominio afectan a todos objetos (usuarios y/o equipos) dentro de un dominio. Las políticas a nivel OU afectan solo a los usuarios y/o equipos que se encuentren contenidos en dicha OU. Las OU's pueden estar anidadas, las políticas se heredan hacia los niveles inferiores de OU's. En estos casos si existe la misma política definida en múltiples niveles se aplica la política más cercana a los objetos, a menos de que explícitamente especifique lo contrario. No se recomienda utilizar políticas a nivel de sitios, a menos de que sea totalmente indispensable, ya que en un sitio donde existan múltiples dominios puede degradar el proceso de firma (logon) del usuario.

Al definir políticas a diferentes niveles hay que tener en cuenta que a un usuario o equipo le son aplicadas todas estas políticas. Un numero grande de políticas de grupo, que apliquen a un usuario, pueden degradar de forma significativa el proceso de firma (logon) del usuario a la red.

Es posible filtrar las políticas de grupo por Grupo de Seguridad de Windows 2000/XP, aplicando la política solo al grupo de usuarios definido y evitando el tiempo de proceso a los otros usuarios.

**PAG. 5**

También es posible deshabilitar una de las dos secciones de una política de grupo, en caso de que no existan políticas definidas en la sección. Esto ahorra tiempo de proceso de la política al "saltarse" la sección, mejorando el tiempo de firma a la red de los usuarios o equipos.

Para el caso de clientes con Windows 98, las políticas no las aplica el directorio activo, así como tampoco se tienen las mismas restricciones; en este caso el alcance de las restricciones con las que se cuenta es más limitado, pero de igual forma contamos con la configuración para los usuarios y para los equipos.

Para habilitar estas restricciones es necesario la instalación de un software que permita poner estas políticas. Aparte de los programas comerciales que puedan haber para este propósito, existe un programa llamado "Poedit" (Editor de políticas de sistema) que viene en el CD original de Windows y que sirve para esta tarea.

## Políticas de Grupo a nivel Unidades Organizacionales

Las políticas que se definieron reflejan el uso que se pudiera tener en un CCD, considerando para ello que existe un administrador de toda la red, el administrador del CCD, y un usuario de aplicaciones.

En el Directorio Activo se definió la siguiente Arquitectura de OU's:



A continuación se detallan la configuración de los perfiles que se definieron. Para el caso del administrador del dominio, este no cuenta con alguna restricción.

### Políticas de Grupo en OU CCDAdministrators

En la OU CCDAdministrators se creó la política de grupo "CCD Administrators GPO". Esta política se definió considerando que un administrador de un CCD no cuenta con suficientes conocimientos técnicos para resolver un problema, por ello se le restringen algunas acciones, pero si puede ayudar en el diagnóstico de un problema.

Algunas de las restricciones presentes para este perfil, es el no poder cambiar el fondo de la pantalla, ya que este se considera institucional y se define por el administrador global y no por el del ccd, cuenta con restricciones de contenido en Internet, y algunas restricciones de configuración del equipo, entre otros.

A continuación se muestran los valores configurados:

### Sección User Configuration

Windows Settings/Internet Explorer Maintenance

Policy	Setting
Security	Security Zones and Content Rating: Language: Moderate Expletives Nudity: Revealing Attire Sex: Passionate Kissing

	Violence: Fighting
--	--------------------

Administrative Templates/Windows Components/Internet Explorer

Policy	Setting
Search: Disable Search Customization	Enabled
Disable external branding of Internet Explorer	Enabled
Disable importing and exporting of favorites	Enabled
Disable changing home page settings	Enabled
Use Automatic Detection for dial-up connections	Enabled
Disable caching of Auto-Proxy scripts	Enabled
Display error message on proxy script download failure	Enabled
Disable changing Temporary Internet files settings	Enabled
Disable changing history settings	Enabled
Disable changing color settings	Enabled
Disable changing link color settings	Enabled
Disable changing font settings	Enabled
Disable changing accessibility settings	Enabled
Disable Internet Connection wizard	Enabled
Disable changing Automatic Configuration settings	Enabled
Disable changing ratings settings	Enabled
Disable changing certificate settings	Enabled
Disable changing Profile Assistant settings	Enabled
Disable AutoComplete for forms	Enabled
Do not allow AutoComplete to save passwords	Enabled
Disable changing Messaging settings	Enabled
Disable the Reset Web Settings feature	Enabled
Disable changing default browser check	Enabled
Identity Manager: Prevent users from using Identities	Enabled

Administrative Templates/Windows Components/Internet Explorer/Offline Pages

Policy	Setting
Disable adding channels	Enabled
Disable removing channels	Enabled
Disable adding schedules for offline pages	Enabled
Disable editing schedules for offline pages	Enabled
Disable removing schedules for offline pages	Enabled
Disable offline page hit logging	Enabled
Disable all scheduled offline pages	Enabled
Disable channel user interface completely	Enabled
Disable downloading of site subscription content	Enabled
Disable editing and creating of schedule groups	Enabled
Subscription Limits	Enabled

Administrative Templates/Windows Components/Internet Explorer/Browser Menus

Policy	Setting
--------	---------

**PAG. 8**

Tools menu: Disable Internet Options... menu option	Enabled
Help menu: Remove 'Tip of the Day' menu option	Enabled
Help menu: Remove 'For Netscape Users' menu option	Enabled
Help menu: Remove 'Send Feedback' menu option	Enabled

Administrative Templates/Windows Components/Internet Explorer /Toolbars

Policy	Setting
Disable customizing browser toolbar buttons	Enabled
Disable customizing browser toolbars	Enabled
Configure Toolbar Buttons	Enabled

Administrative Templates/Windows Components/Windows Explorer

Policy	Setting
Remove the Folder Options menu item from the Tools menu	Enabled
Disable Windows Explorer's default context menu	Enabled
Hides the Manage item on the Windows Explorer context menu	Enabled
Only allow approved Shell extensions	Enabled
Hide Hardware tab	Enabled
Disable UI to change menu animation setting	Enabled
Disable UI to change keyboard navigation indicator setting	Enabled
Disable DFS Tab	Enabled
Request credentials for network installations	Enabled

Administrative Templates/Windows Components/Windows Explorer/Common Open File Dialog

Policy	Setting
Hide list of recently used files	Enabled

Administrative Templates/Windows Components/Task Scheduler

Policy	Setting
Hide Property Pages	Enabled
Prevent Task Run or End	Enabled
Disable Drag-and-Drop	Enabled
Disable New Task Creation	Enabled
Disable Task Deletion	Enabled
Disable Advanced Menu	Enabled
Prohibit Browse	Enabled

Administrative Templates/Start Menu & Taskbar

Policy	Setting
--------	---------

Disable and remove links to Windows Update	Enabled
Add Logoff to the Start Menu	Enabled
Disable drag-and-drop context menus on the Start Menu	Enabled
Disable changes to Taskbar and Start Menu Settings	Enabled
Disable context menu for taskbar	Enabled
Clear history of recently opened documents on exit	Enabled
Disable personalized menus	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled

Administrative Templates/Desktop

Policy	Setting
Do not add shares from recently opened documents to the My Network Places folder	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Disable adjusting desktop toolbars	Enabled
Don't save settings at exit	Enabled

Administrative Templates/Desktop/Active Desktop

Policy	Setting
Enable Active Desktop	Enabled
Disable all items	Enabled
Prohibit adding items	Enabled
Prohibit editing items	Enabled
Prohibit deleting items	Enabled
Prohibit closing items	Enabled
Add/Delete items	Enabled
Active Desktop Wallpaper	Enabled
Allow only bitmapped wallpaper	Soap Bubbles.bmp

Administrative Templates/Control Panel/Display

Policy	Setting
Disable Display in Control Panel	Enabled

Administrative Templates/Network/Offline Files

Policy	Setting
Disable user configuration of Offline Files	Enabled
Synchronize all offline files before logging off	Enabled
Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled

Administrative Templates/System

Policy	Setting
Don't Display welcome screen at logon	Enabled
Disable Autoplay	Enabled

Administrative Templates/System/Logon/Logoff

Policy	Setting
Disable change password	Enabled
Run Logon scripts synchronously	Enabled
Limit profile size	Enabled 30000 kb
Run these programs at user logon	Enabled Iexplore.exe

**Políticas de Grupo en OU CCDUsers**

En la OU CCDUsers se creó la política de grupo "CCD Users GPO". Esta política está definida, para que el usuario solo pueda hacer uso de las aplicaciones permitidas, no pueda acceder a la configuración de la máquina, y tener una cuota de espacio en disco preestablecida.

A continuación se muestran los valores configurados:

**Sección User Configuration**

Windows Settings/Internet Explorer Maintenance

Policy	Setting
Security	Security Zones and Content Rating: Language: Moderate Expletives Nudity: Revealing Attire Sex: Passionate Kissing Violence: Fighting

Administrative Templates/Windows Components/Internet Explorer

Policy	Setting
Search: Disable Search Customization	Enabled
Disable external branding of Internet Explorer	Enabled
Disable importing and exporting of favorites	Enabled
Disable changing Advanced page settings	Enabled
Disable changing home page settings	Enabled

Use Automatic Detection for dial-up connections	Enabled
Disable caching of Auto-Proxy scripts	Enabled
Display error message on proxy script download failure	Enabled
Disable changing Temporary Internet files settings	Enabled
Disable changing history settings	Enabled
Disable changing color settings	Enabled
Disable changing link color settings	Enabled
Disable changing font settings	Enabled
Disable changing language settings	Enabled
Disable changing accessibility settings	Enabled
Disable Internet Connection wizard	Enabled
Disable changing connection settings	Enabled
Disable changing proxy settings	Enabled
Disable changing Automatic Configuration settings	Enabled
Disable changing ratings settings	Enabled
Disable changing certificate settings	Enabled
Disable changing Profile Assistant settings	Enabled
Disable AutoComplete for forms	Enabled
Do not allow AutoComplete to save passwords	Enabled
Disable changing Messaging settings	Enabled
Disable changing calendar and contact settings	Enabled
Disable the Reset Web Settings feature	Enabled
Disable changing default browser check	Enabled
Identity Manager: Prevent users from using Identities	Enabled

Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel

Policy	Setting
Disable the General page	Enabled
Disable the Security page	Enabled
Disable the Content page	Enabled
Disable the Connections page	Enabled
Disable the Programs page	Enabled
Disable the Advanced page	Enabled

Administrative Templates/Windows Components/Internet Explorer/Offline Pages

Policy	Setting
Disable adding channels	Enabled
Disable removing channels	Enabled
Disable adding schedules for offline pages	Enabled
Disable editing schedules for offline pages	Enabled
Disable removing schedules for offline pages	Enabled
Disable offline page hit logging	Enabled
Disable all scheduled offline pages	Enabled
Disable channel user interface completely	Enabled
Disable downloading of site subscription content	Enabled
Disable editing and creating of schedule groups	Enabled
Subscription Limits	Enabled

Administrative Templates/Windows Components/Internet Explorer/Browser Menus

Policy	Setting
Tools menu: Disable Internet Options... menu option	Enabled
Help menu: Remove 'Tip of the Day' menu option	Enabled
Help menu: Remove 'For Netscape Users' menu option	Enabled
Help menu: Remove 'Send Feedback' menu option	Enabled

Administrative Templates/Windows Components/Internet Explorer /Toolbars

Policy	Setting
Disable customizing browser toolbar buttons	Enabled
Disable customizing browser toolbars	Enabled
Configure Toolbar Buttons	Enabled

Administrative Templates/Windows Components/Windows Explorer

Policy	Setting
Remove the Folder Options menu item from the Tools menu	Enabled
Remove "Map Network Drive" and "Disconnect Network Drive"	Enabled
Disable Windows Explorer's default context menu	Enabled
Hides the Manage item on the Windows Explorer context menu	Enabled
Only allow approved Shell extensions	Enabled
Hide these specified drives in My Computer	Enabled All Drives
Hide Hardware tab	Enabled
Disable UI to change menu animation setting	Enabled
Disable UI to change keyboard navigation indicator setting	Enabled
Disable DFS Tab	Enabled
No "Computers Near Me" in My Network Places	Enabled
No "Entire Network" in My Network Places	Enabled
Request credentials for network installations	Enabled

Administrative Templates/Windows Components/Windows Explorer/Common Open File Dialog

Policy	Setting
Hide list of recently used files	Enabled

Administrative Templates/Windows Components/Microsoft Management Console

Policy	Setting
Restrict the user from entering author mode	Enabled
Restrict users to the explicitly permitted list of snap-ins	Enabled

Administrative Templates/Windows Components/Task Scheduler

Policy	Setting
Hide Property Pages	Enabled
Prevent Task Run or End	Enabled
Disable Drag-and-Drop	Enabled
Disable New Task Creation	Enabled
Disable Task Deletion	Enabled
Disable Advanced Menu	Enabled
Prohibit Browse	Enabled

Administrative Templates/Windows Components/Windows Installer

Policy	Setting
Disable media source for any install	Enabled

Administrative Templates/Start Menu & Taskbar

Policy	Setting
Disable and remove links to Windows Update	Enabled
Remove Network and Dial-up Connections from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Add Logoff to the Start Menu	Enabled
Disable and remove the Shut Down command	Enabled
Disable drag-and-drop context menus on the Start Menu	Enabled
Disable changes to Taskbar and Start Menu Settings	Enabled
Disable context menu for taskbar	Enabled
Clear history of recently opened documents on exit	Enabled
Disable personalized menus	Enabled
Gray unavailable Windows Installer programs Start Menu shortcuts	Enabled

Administrative Templates/Desktop

Policy	Setting
Do not add shares from recently opened documents to the My Network Places folder	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's toolbars	Enabled
Disable adjusting desktop toolbars	Enabled
Don't save settings at exit	Enabled

Administrative Templates/Desktop/Active Desktop

Policy	Setting
Enable Active Desktop	Enabled
Prohibit changes	Enabled
Disable all items	Enabled
Prohibit adding items	Enabled
Prohibit editing items	Enabled
Prohibit deleting items	Enabled
Prohibit closing items	Enabled
Add/Delete items	Enabled
Active Desktop Wallpaper	Enabled
Allow only bitmapped wallpaper	Rhododendron.bmp

Administrative Templates/Control Panel

Policy	Setting
Disable control panel	Enabled

Administrative Templates/Control Panel/Add/Remove Programs

Policy	Setting
Disable Add/Remove Programs	Enabled

Administrative Templates/Control Panel/Display

Policy	Setting
Disable Display in Control Panel	Enabled

Administrative Templates/Control Panel/Printers

Policy	Setting
Disable deletion of printers	Enabled

Administrative Templates/Network/Offline Files

Policy	Setting
Disable user configuration of Offline Files	Enabled
Synchronize all offline files before logging off	Enabled
Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled

Administrative Templates/Network/ Network and Dial-up Connections

Policy	Setting
Prohibit deletion of RAS connections	Enabled
Prohibit deletion of RAS connections available to all users	Enabled

**PAG. 15**

Prohibit connecting and disconnecting a RAS connection	Enabled
Prohibit enabling/disabling a LAN connection	Enabled
Prohibit access to properties of a LAN connection	Enabled
Prohibit access to current user's RAS connection properties	Enabled
Prohibit access to properties of RAS connections available to all users	Enabled
Prohibit renaming LAN connections or RAS connections available to all users	Enabled
Prohibit renaming of RAS connections belonging to the current user	Enabled
Prohibit adding and removing components for a LAN or RAS connection	Enabled
Prohibit enabling/disabling components of a LAN connection	Enabled
Prohibit access to properties of components of a LAN connection	Enabled
Prohibit access to properties of components of a RAS connection	Enabled
Prohibit access to the Network Connection wizard	Enabled
Prohibit viewing of status statistics for an active connection	Enabled
Prohibit access to the Dial-up Preferences item on the Advanced menu	Enabled
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled
Prohibit configuration of connection sharing	Enabled
Prohibit TCP/IP advanced configuration	Enabled

## Administrative Templates/System

Policy	Setting
Don't Display welcome screen at logon	Enabled
Disable the command prompt	Enabled
Disable registry editing tools	Enabled
Disable Autoplay	Enabled

## Administrative Templates/System/Logon/Logoff

Policy	Setting
Disable Task Manager	Enabled
Disable Lock Computer	Enabled
Disable change password	Enabled
Disable Logoff	Enabled
Run Logon scripts synchronously	Enabled
Limit profile size	Enabled 30000 kb
Run these programs at user logon	Enabled lexplore.exe

### Políticas de Grupo en OU CCDComputers

Para esta OU se restringieron las carpetas a las que pueden acceder un usuario, aplicándose este GPO a nivel computadora ("CCD Computers GPO"). Y restringiéndose el acceso de acuerdo al tipo de usuario, limitando a los usuarios de la OU CCDUsers a la carpeta de "Mis documentos".

A continuación se muestra la configuración definida:

### Sección Computer Configuration

Windows Settings/Security Settings/File System

File	Permissions
%SystemDrive% (Replace Permissions)	Domain Administrators Full Control ccdadministrator Full Control
%SystemDrive%\Documents Settings\%username%\Mis Documentos (Replace Permissions)	and ccdusers Full Control

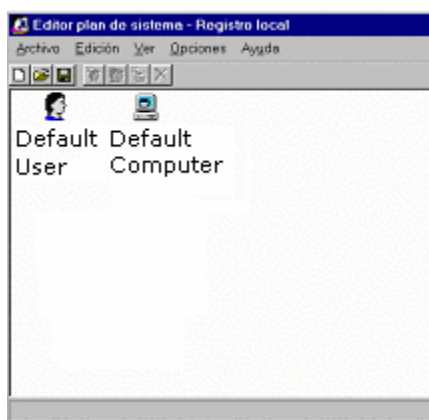
## Políticas Aplicadas a clientes Windows 95/98

La forma en como se definen las políticas para estos clientes, es a través del uso de la herramienta Poedit (parte del sistema operativo). No existe un control tan amplio como lo sería a través del Directorio Activo en un dominio 2000, pero ofrece un control aceptable.

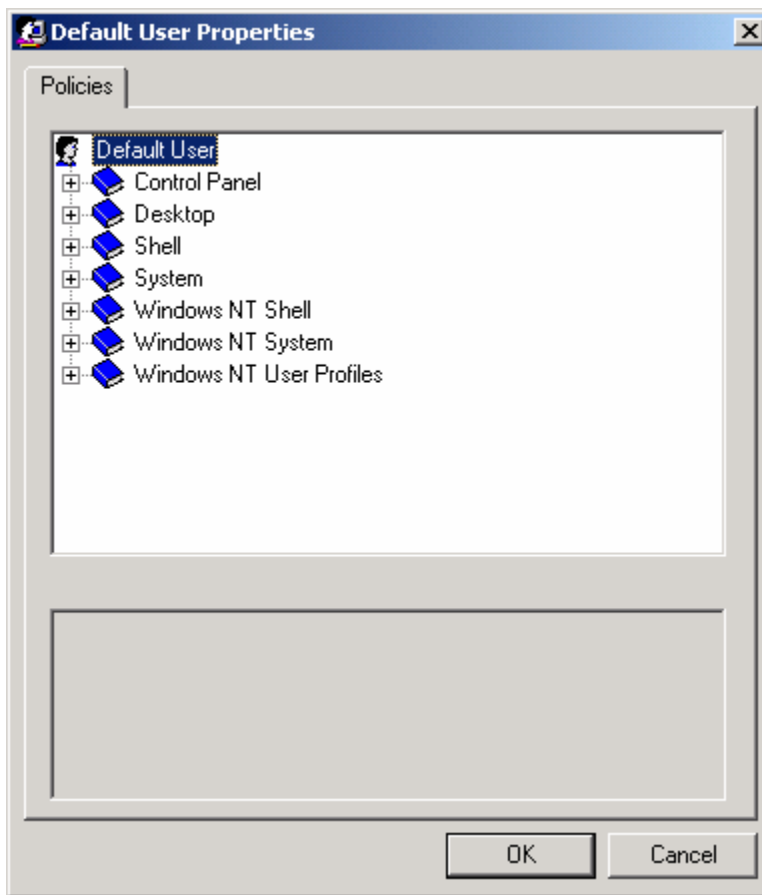
Con el uso de Poedit en el cliente 98 se generó un archivo .pol que se colocó en el share de Netlogon del Domain Controller. Este archivo contiene las restricciones que se aplicarán a los usuarios que se autentifiquen en clientes 95/98 que formen parte del dominio (para este caso "pruebas").

### Definición de Políticas en Poedit

Para activar el programa y definir las restricciones es necesario "Ejecutar -> Poedit". Pulsando en el menú "Archivo -> Archivo Nuevo" se muestran dos iconos en la ventana del programa: "Default User" y "Default Computer".



Pulsando sobre "Default User" se abrirán las opciones de configuración de Windows para ese usuario.



A través de esta pantalla accedemos a las opciones para restringir a nuestros usuarios. Para ello debemos de crear un "grupo de usuarios" que se debe de mapear con un grupo de seguridad definido en el Directorio Activo, al cual se le aplicarán las restricciones que nosotros definamos en esta área.

Las opciones que se configuraron para "ccdusers" (grupo de usuarios) en el ambiente de pruebas fueron:

Control Panel/Display

Policy	Setting
Restrict Display	Enabled Todas las opciones

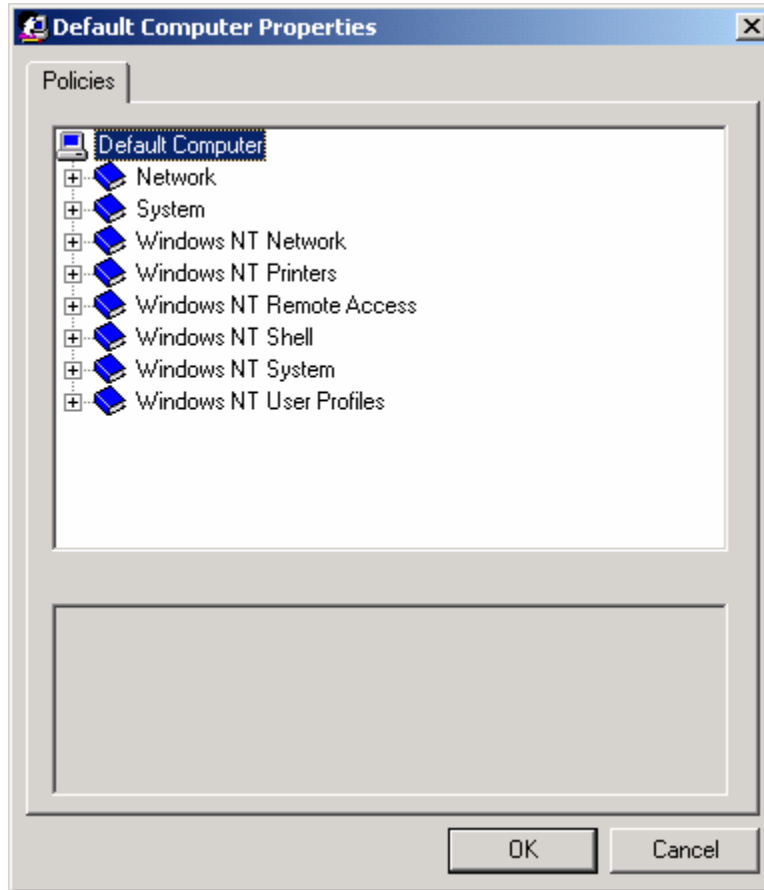
Shell/Restrictions

Policy	Setting
Remove Run command from Start Menu	Enabled
Hide Drives in My Computer	Enabled
Hide Network Neighborhood	Enabled
Hide all items on desktop	Enabled
Remove Shut Down command from Start Menu	Enabled

System/Restrictions

Policy	Setting
Disable Registry editing tools	Enabled

En lo que respecta a "Default Computer" las opciones son las siguientes:



Y la configuración que se definió es la siguiente:

Network/System Policies Update

Policy	Setting
Remote Update	Enable Mode: Manual Path: <a href="#">\\contel\netlogon\config.pol</a> Error Messaging: Enabled

System

Policy	Setting
Run	Enabled explore.exe

Esta configuración la salvamos como config.pol y movemos el archivo al recurso compartido "Netlogon" en el Domain Controller .

Cuando los clientes con Windows 95/98 se agreguen al dominio, y se intente acceder a la máquina con un usuario registrado, se aplicarán las restricciones definidas en el archivo config.pol.

Se pueden definir más restricciones, pero no todas a través de Poedit, sino creando un .reg (archivo para configurar el registry) que se aplique directamente en los clientes; o configurando manualmente algunas opciones de nuestro equipo, como en el siguiente ejemplo:

*Explorador de Windows apuntando a un directorio fijo sin posibilidad de ir a otro.*

Es posible hacer que el explorador de Windows quede apuntando a un determinado directorio o unidad sin posibilidad de desplazarnos a través de los demás directorios o unidades, lo que puede permitirnos bloquear el acceso a determinadas partes del equipo a cualquier usuario, evitando que estos borren o pongan programas y archivos en directorios que no deseamos.

Para ello ir a Inicio -> Programas -> Explorador de Windows y pulsando con el botón derecho del ratón abrir sus propiedades. En el cuadro de diálogo que aparece escribir en el campo destino: c:\windows\explorer.exe /e, /root, c:\mis documentos.

Con esto hacemos que la ventana del explorador sólo apunte al directorio mis documentos sin posibilidad de desplazarnos por los demás.

También podemos hacer que apunte a una determinada unidad, por ejemplo A: sin posibilidad de acceder al disco duro, escribiendo lo siguiente: c:\windows\explorer.exe /e, /root, A:\

