INSTALACIÓN DEL SYSTEM POLICIES EN LOS LABORATORIOS DE LA USI

1. INTRODUCCION

El system policies es una herramienta del Windows 95 que permite implementar una serie de restricciones en su entorno tal como permitir la ejecución de sólo un grupo de programas, desactivar el acceso al Panel de Control, desactivar el acceso al Entorno de Red, a unidades de disco, etc., todo ello con el objetivo de proteger al sistema de modificaciones y mantener un entorno estándar. Las restricciones se pueden definir para un usuario en particular o para un grupo de usuarios según convenga.

La instalación del system policies requiere que previamente se habilite el *inicio de sesión en el dominio de Windows NT* y los *perfiles de usuario personalizados*. Luego podemos proseguir con la instalación del system policies de dos maneras: ***manualmente,*** máquina por máquina, o en forma ***automática,*** en todas las PC's desde un servidor, cada una tiene sus ventajas y desventajas. Para el caso de las PC's del laboratorio se está usando una combinación de ambas tomando lo mejor de cada opción.

El system policies se instala en las computadoras de tal manera que se obliga al alumno a ingresar un usuario y una contraseña predeterminadas según el uso que el alumno

desee darle a la computadora. Por ejemplo, si el alumno desea usar los servicios internet en el laboratorio A debe ingresar el usuario INTA seguido de la contraseña USER. Luego el servidor valida al usuario y su contraseña en el dominio LABMICRO y empieza la carga del entorno predeterminado junto con las restricciones de seguridad. Con entorno nos referimos al *profile* o perfil del usuario, la serie de opciones y programas que aparecen a partir de que presionamos el botón INICIO, y a *restricciones* a las modificaciones que se hacen a los archivos *user.dat* y *system.dat*, es decir, los archivos que definen el *Registro*.

En el archivo USER.DAT se guarda información concerniente al usuario y en el archivo SYSTEM.DAT se almacena información con respecto al hardware del sistema.

El SYSTEM POLICIES actúa sobre el registro del sistema modificando los archivos USER.DAT y SYSTEM.DAT implementando las restricciones que el administrador crea conveniente.

Una computadora puede ser usada por distintos usuarios y el hardware sigue siendo el mismo. De la misma forma se puede habilitar un archivo USER.DAT para cada usuario con diferentes restricciones pero el SYSTEM.DAT es único en dicha computadora.

Debido a que se usará el System Policies con usuarios validados por el Servidor se puede usar todas las herramientas de Administración de usuarios de que dispone el servidor para imponer accesos permitidos, sólo en determinadas horas, a las computadoras de los laboratorios a determinados usuarios así como la implementación de Scripts para el mantenimiento de la PC.

Si se desea una revisión a profundidad de lo que puede hacer el System Policies se puede revisar el Resource Kit de Windows 95 en el Capítulo 15.

---

2. EL EDITOR DE POLITICAS (POLEDIT)

El programa POLEDIT.EXE es el editor de políticas del System Policies que nos permitirá crear archivos de extensión POL donde se definirán las rectricciones para un usuario en particular o para un grupo de usuarios definido en el dominio del Windows NT Server. También puede definirse restricciones para una máquina en particular más no para un grupo de ellas.

Al empezar a editar un nuevo archivo de políticas siempre aparecerán dos íconos: Default User y Default Computer. Aquellos usuarios que no estén definidos dentro del archivo de políticas cogerán las características del Default User, análogamente, aquellas computadoras que no estén definidas dentro del archivo de políticas cogerán las características del Default Computer.

El programa Poledit también nos permite modificar la configuración del registro de la computadora. Al abrir el registro encontraremos dos íconos: Local User y Local Computer. Local User es el usuario que obtenemos al oprimir Esc cuando se visualiza la ventana de inicio de sesión del Windows95. Análogamente con Local Computer.

El instalador del editor de políticas se encuentra en el CDROM instalador del Windows 95, directorio \ Admin\ Apptools\ Poledit. El tamaño de éste directorio es de 170Kb por lo que es más práctico tenerlo en un diskette para no depender de una lectora de CDROM.

Realmente no es necesario realizar el procedimiento de instalación ya que basta ejecutar el programa POLEDIT.EXE que viene en dicho directorio de instalación para ponerlo en marcha, lo cual es recomendable, pues la idea es que sólo los administradores tengan acceso a ésta poderosa herramienta. Instalándolo copiamos los ejecutables al disco duro y logramos que aparezca el ícono del Editor en Herramientas del Sistema del Menú Inicio con lo que otra persona no autorizada podría tener acceso al Editor.

Para instalarlo ir al *Panel de Control* y en *Agregar/Remover Programas* escoger la carpeta de *Instalación Windows*. Luego pulsar el botón *Utilizar disco...* e indicar la ruta al directorio de instalación del CDROM o diskette.

Finalmente dar *Aceptar* para culminar la instalación.

---

3. PROCEDIMIENTO PARA LA INSTALACIÓN DE POLITICAS DE SEGURIDAD EN LOS LABORATORIOS DE MICROCOMPUTACIÓN

El procedimiento consta de 5 etapas, la última es para efectos de desinstalación.

3.1. CREACION DE USUARIOS

3.2. DEFINICION DE LOS ENTORNOS

3.3. CREACION DE SCRIPTS DE USUARIO (LOGON SCRIPTS)

3.4. DEFINICION DE POLITICAS

3.5. INSTALACIÓN DEL SYSTEM POLICE EN UNA MÁQUINA

3.6. DESINSTALACIÓN DEL SYSTEM POLICE EN UNA MÁQUINA

3.1 CREACION DE USUARIOS

Lo que se desea lograr es que el estudiante no se distraiga con los servicios Internet durante las clases así como evitar la desconfiguración del sistema e instalación de programas extraños (variación del papel tapiz, resolución del monitor, multimedia, protocolos, protectores de pantallla, virus, juegos, otros programas, etc.).

Para cada laboratorio se han definido 5 usuarios autorizados usando el Administrador de Usuarios del Windows NT, por ejemplo, para el **laboratorio A** tenemos:

- INTA - Es el usuario que sólo usará los servicios de Internet. Contraseña USR.
- USERA - Usuario que sólo usará los programas instalados en la PC, menos los servicios Internet. Contraseña USR.
- MASTERA - Es el usuario que tiene acceso a todos los programas de la PC, incluído los servicios Internet. Éste usuario deberá ser solicitado con previa anticipación a la clase para proporcionar la contraseña correspondiente.
- CDUSER - Usuario para servicio de lectura de CDROM. Contraseña de conocimiento de los administradores y auxiliares de los laboratorios.
- AUXA - Es el usuario de mantenimiento. Tiene acceso al servidor de los laboratorios para instalación de programas así como a todos los programas instalados en la PC. Contraseña de conocimiento de los administradores y auxiliares de los laboratorios.

- INTA, USERA sólo tienen acceso a los programas que aparecen a través de los submenúes del botón Inicio.

- INTA, USERA, MASTERA, y CDUSER no tienen acceso a la red local del laboratorio y al Panel de Control

Para los demás laboratorios se definen los mismos usuarios cambiando la letra A por la correspondiente al laboratorio.

3.2 DEFINICION DE LOS ENTORNOS

Debemos crear el entorno de cada usuario o *profile*, es decir, los íconos, grupos de programas, y papel tapiz, que aparecerán al ingresar con un usuario determinado. El profile tiene la forma de un directorio con el nombre del usuario que a su vez tiene varios subdirectorios donde cada uno representa a un grupo de programas o documentos. El contenido final de cada subdirectorio son atajos o shortcuts a dichos programas o documentos. El profile define el perfil del usuario.

Los profiles serán descargados desde el directorio Entornos del servidor Andrómeda a las máquinas de los laboratorios. El directorio Entornos está compartido como Entornos$ para evitar su visualización.

Después de crear y compartir el directorio Entornos debemos seguir los siguientes pasos para la creación del profile de un usuario. Sea *nombus* el nombre del usuario que ha sido escogido, entonces:

En el servidor:

1. Compartir a Entornos para que el usuario *nombus* tenga acceso de lectura/escritura.

2. Ingresar al Administrador de Usuarios del Servidor.

3. Escoger el usuario *nombus* al que se le va a crear el entorno y oprimir el botón Profile.

4. En el espacio denominado Home Directory escoger Connect y escribir U: \\Andromeda\entornos$\nombus.

5. Finalmente dar OK dos veces para salir y guardar la configuración.

6. Si se desea configurar el Home Directory de más usuarios regresar al paso 2.

En la computadora del laboratorio:

1. En la PC modelo habilitar el inicio de sesión en el dominio de Windows NT (Panel de control-Ícono Red-Cliente para redes Microsoft-Propiedades) y los perfiles de usuario personalizados (Panel de control - Ícono contraseñas - Perfiles de usuario - Los usuarios pueden personalizar sus preferencias y configuración de escritorio). Reiniciar la PC.

2. Ingresar a la PC con el usuario *nombus* y configurar el escritorio, papel tapiz, programas del menú inicio según convenga. Por ejemplo, el usuario internet sólo necesita los programas para internet, adicionalmente el explorer y los accesorios de windows 95. Configurar cada programa según se requiera.

3. Salir de la sesión para ingresar con el nombre de otro usuario. Es en éste momento que se transfiere el entorno que ha diseñado para *nombus* hacia el directorio Entornos del servidor Andromeda.

4. Si se desea crear el entorno de otro usuario regresar al paso 8.

5. Una vez creados los entornos o perfiles compartir el directorio Entornos del servidor como Sólo lectura, de ésta manera mantendremos la configuración frente a variaciones en el perfil del usuario *nombus*.

3.3 CREACION DE SCRIPTS DE USUARIO (LOGON SCRIPTS)

Una vez creados los entornos o perfiles de cada usuario estos serán descargados en una máquina en la que se ha sido activado por primera vez el inicio de sesión en el dominio del Windows NT y el uso de perfiles de usuario personalizado. Si el usuario realiza modificaciones en el entorno éstas deberán ser grabadas en el servidor, sin embargo, al estar el directorio Entornos como sólo lectura el perfil se mantendrá invariante. Lamentablemente si el servidor encuentra un perfil en la máquina de fecha más reciente o distinto al que guarda no lo reemplazará. Es por ello que debemos ejecutar un Script de usuario que elimine el entorno o perfil almacenado en la PC, de esta manera el servidor, al no encontrar un perfi en la PC, descargará el perfil que hemos diseñado.

Para habilitar los Logon Scripts:

1. Ir al Administador de Usuarios del servidor, escoger, por ejemplo, el usuario USERA y presionar el botón Profile.

2. En el espacio llamado Logon Script Name escribir el nombre del archivo batch a ejecutar, en este caso USER.BAT. Presionar OK dos veces para salir.

3. Luego crear el bachero que ha de servir no sólo para USERA si para USERB, USERC, ... El bachero se almacena en el directorio POLITICAS compartido como NETLOGON. (Previamente se configura dicha ruta en : *Panel de Control - Server - Botón Replication - Logon Script Path=C:\Politicas*) con el nombre USER.BAT.

Análogamente se han creado los bacheros AUXI.BAT, MASTER.BAT, INTERNET.BAT y CDUSER.BAT.

3.4. DEFINICION DE POLITICAS

Siguiendo con el ejemplo del laboratorio A, definimos ahora las políticas de seguridad para cada usuario del laboratorio usando el Police Editor.

Para ello creamos un nuevo archivo de políticas con File-New File, aparecerán por defecto el usuario Default User y la computadora Default Computer. Definimos un nuevo usuario dentro del Police Editor con Edit-Add User y enseguida hacemos doble click sobre su ícono, aparecerán una serie de opciones, mostradas más adelante, que se activarán a criterio del administrador. Definidas las restricciones para cada usuario en el laboratorio A, para el usuario por defecto y para la computadora por defecto, guardamos el archivo como SAFEA.POL dentro del directorio compartido como NETLOGON del Windows NT controlador de dominio, que en éste caso es el servidor Andromeda.

Cuando se carge el System Policies, en una PC del laboratorio A, afectará a aquellos usuarios que estén definidos en el archivo Safea.pol y aquellos que no estén definidos (usuarios extraños) asumirán las restricciones del usuario por defecto (Default User). Todas las computadoras asumirán las rectricciones de Default Computer.

Análogamente tenemos SAFEB.POL para el laboratorio B, SAFEC.POL para el laboratorio C, ...

RESTRICCIONES APLICADAS A UNA COMPUTADORA

Las restricciones que se aplican a una computadora son las siguientes:

Network

Access Control

User-level Access Control

Authenticator Name:

Authenticator Type:

Logon

Logon Banner

Caption: Aviso de la Unidad de Servicios Informáticos

Text: Ha sido activado el sistema de politicas de seguridad. Sólo los usuarios INTX y USERX están autorizados a usar ésta máquina. En ambos casos usar la contraseña USR.

Require Validation by Network for Windows Access

Microsoft Client for NetWare Networks

Preferred server

Server name:

Support long file names

Support long file names on:

Search Mode

Search Mode:

Disable Automatic NetWare Login

Microsoft Client for Windows Networks

Log on to Windows NT

Domain name: LABMICRO

Display domain logon confirmation

Disable caching of domain password

Workgroup

Workgroup name:

Alternate Workgroup Workgroup name:

File and printer sharing for NetWare Networks

Disable SAP Advertising

Passwords

Hide share passwords with asterisks

Disable password caching

Require alphanumeric Windows password

Minimum Windows password length

Length:

Dial-Up Networking

Disable dial-in

Sharing

Disable file sharing

Disable print sharing

SNMP

Communities

Communities:

Permitted managers

Permitted managers:

Traps for 'Public' community

Trap configuration:

Internet MIB (RFC1156)

Contact Name:

Location:

Update

Remote Update

Update Mode:

Path for manual update:
\\Andromeda\netlogon\safex.pol

Display error messages

Load-balance

System

Enable User Profiles

Network path for Windows Setup

Path:\\Andromeda\disk\win95es

Network path for Windows Tour

Path:

Note: the path must end in TOUR.EXE

Run

Items to run at startup:vshwin32.exe

THD32.EXE

internat.exe

Run Once

Items to run once at startup:

Run Services

Services to run at startup:vshwin32.exe

RESTRICCIONES APLICADAS A UN USUARIO

Las restricciones que aplicamos a un usuario son las siguientes
(marcadas en azul las restricciones aplicadas al usuario USERX) :

Control Panel

Display

Restrict Display Control Panel

Disable Display Control Panel

Hide Background page

Hide Screen Saver page

Hide Appearance page

Hide Settings page

Network

Restrict Network Control Panel

Disable Network Control Panel

Hide Identification Page

Hide Access Control Page

Passwords

Restrict Passwords Control Panel

Disable Passwords Control Panel

Hide Change Passwords page

Hide Remote Administration page

Hide User Profiles page

Printers

Restrict Printer Settings

Hide General and Details pages

Disable Deletion of Printers

Disable Addition of Printers

System

Restrict System Control Panel

Hide Device Manager page

Hide Hardware Profiles Page

Hide File System button

Hide Virtual Memory button

Desktop

Wallpaper

Wallpaper name:

Tile wallpaper

Color scheme

Scheme name:

Network

Sharing

Disable file sharing controls

Disable print sharing controls

Shell

Custom Folders

Custom Programs Folder

Path to get Programs items from:

Custom Desktop Icons

Path to get Desktop icons from:

Hide Start Menu subfolders

Check this if you use a custom Programs Folder or custom Desktop icons.

Custom Startup Folder

Path to get Startup items from:

Custom Network Neighborhood

Path to get Network Neighborhood items from:

Custom Start Menu

Path to get Start Menu items from:

Restrictions

Remove 'Run' command

Remove folders from 'Settings' on Start Menu

Remove Taskbar from 'Settings' on Start Menu

Remove 'Find' command

Hide Drives in 'My Computer'

Hide Network Neighborhood

No 'Entire Network' in Network Neighborhood

No workgroup contents in Network Neighborhood

Hide all items on Desktop

Disable Shut Down command

Don't save settings at exit

System

Restrictions

Disable Registry editing tools

Only run allowed Windows applications

List of allowed applications:

Disable MS-DOS prompt

Disable single-mode MS-DOS applications

En *List of allowed applications:* ingresaremos el nombre de los archivos ejecutables correspondientes a los programas permitidos. Tener en cuenta que en programas para DOS no basta con registrar el nombre del archivo EXE o COM del ejecutable sino que además hay que registar al archivo PIF correspondiente.

A continuación se tiene un listado de los archivos ejecutables agrupados por aplicación:

DOS

1. command.com
2. ms-dos.pif

COMUNES

1. explorer.exe
2. scandskw.exe
3. defrag.exe
4. notepad.exe
5. calc.exe
6. mspaint.exe
7. wordpad.exe
8. winhelp.exe
9. mplayer.exe
10. cdplayer.exe

11. sndrec32.exe
12. sndvol32.exe

MICROSOFT OFFICE 95

1. winword.exe
2. powerpnt.exe
3. excel.exe
4. msaccess.exe
5. findfast.exe
6. fastboot.exe

INTERNET

1. finger.exe
2. hgopher.exe
3. lview1b.exe
4. netscape.exe
5. telnet.exe
6. winwhois.exe
7. ws_ftp32.exe
8. iexplore.exe

MCAFEE SCAN ANTIVIRUS

1. vshcfg32.exe
2. scan32.exe
3. edisk32.exe

TSP

1. tsp.exe
2. tsp.pif

RATS

1. rats386.exe
2. rats386.pif

EPI

1. epi.exe
2. epi.pif

SPSS

1. spsstran.exe
2. spsswin.exe
3. tbook.exe
4. spsstsni.exe

MS PROJECT

1. winproj.exe

MATHEMATHICA

1. math.exe

SQL GUPTA (SOLO)

1. qckfinal.exe
2. sqlwin50.exe
3. dbwservr.exe

FOXPRO

1. foxprow.exe

PASCAL

1. bp.exe
2. Borland Pascal.pif
3. tdx.exe
4. tdx.pif
5. turbo.exe
6. Turbo Pascal.pif
7. bpw.exe
8. tdw.exe
9. tprofw.exe
10. shed.exe
11. winsight.exe
12. winspctr.exe
13. workshop.exe

ECONOMETRIC VIEW

1. eviews.exe

AUTOCAD R13

1. tbook.exe
2. acad.exe
3. dtextrw.exe (solo para la version en CD)

MICROSTATION (PARA WINDOWS 95 Y NT)

1. ustation.exe

WINZIP

1. winzip32.exe

FRONTPAGE

1. tcptest.exe
2. fpexplor.exe
3. fpeditor.exe

PAGEMAKER 6.0

1. ppd.exe
2. register.exe
3. pm6.exe
4. deapp.exe
5. table25.exe

UTILIDADES SOUND BLASTER

1. ctwave32.exe
2. tareader.exe
3. textole.exe
4. tacontrl.exe
5. sndole32.exe
6. tadict.exe
7. remote32.exe
8. ctmix32.exe
9. ctmidi32.exe
10. ctcd32.exe
11. awecp32.exe

CYBER SITTER

1. internat.exe
2. initsys.exe

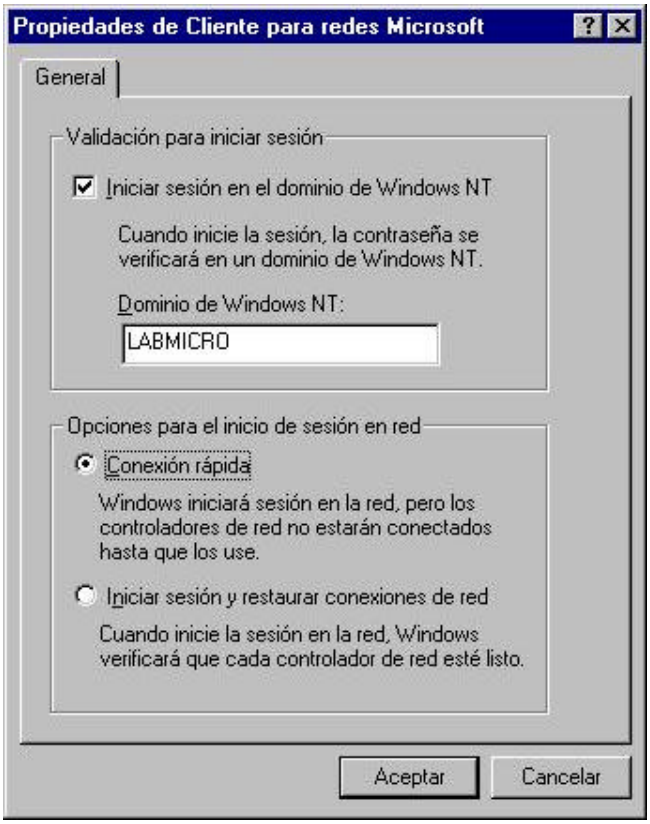
3.5. INSTALACIÓN DEL SYSTEM POLICE EN UNA MÁQUINA

Luego de activar el habilitar el inicio de sesión en el dominio de Windows NT (Panel de control-Ícono Red-Cliente para redes Microsoft-Propiedades) y los perfiles de usuario personalizados (Panel de control - Ícono contraseñas - Perfiles de usuario - Los usuarios pueden personalizar sus preferencias y configuración de escritorio), debemos configurar la máquina para que descarge la política diseñada para el salón donde se encuentra. Para ello debemos ejecutar el Editor de Políticas sin necesidad de instalarlo en el disco duro de la PC de tal manera que el usuario no tenga acceso a esta herramienta posteriormente. Sólo debemos copiar los archivos del directorio \Admin\Apptools\Poledit del CDROM instalador del Windows95 en un diskette para poder ejecutar el Editor de Políticas (Poledit.exe) desde las disketteras de las computadoras.

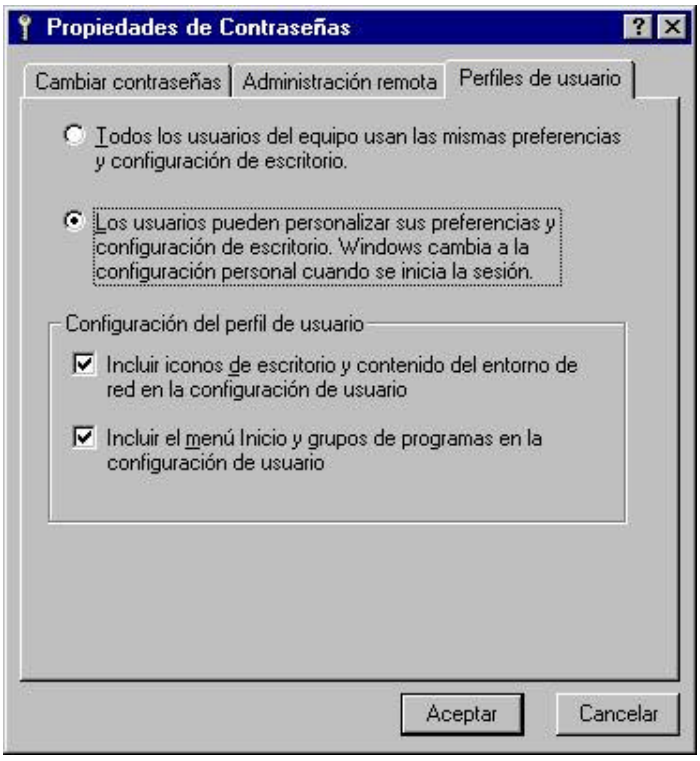
Debemos seguir entonces los siguientes pasos:

1. Preparar la máquina con una configuración estándar, es decir, con el software correspondiente al salón, sin papel tapiz, resolución 800*600, color 16 bits, apariencia estándar de windows 95, sin salvador de pantalla, conexión a la red del laboratorio y a internet, impresora Laser Jet 4P, configuración regional Español-Perú, teclado Español(México) -Latinoamericano. El último punto es muy importante pues los perfiles de usuario han sido diseñados usando éste tipo de teclado. Un teclado distinto ocasionará que, la segunda vez que ingresemos al recuadro de logon, el teclado quede inhabilitado pues surge un conflicto entre el teclado definido localmente en la computadora con el teclado personalizado del usuario. Ésta es una falla o bug del Windows 95 que debemos tener en cuenta.

2.Habilitar el inicio de sesión en el dominio de Windows NT (Panel de control-Ícono Red-Cliente para redes Microsoft-Propiedades)

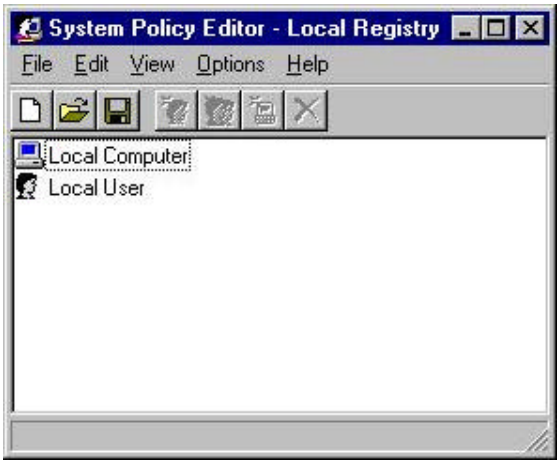


y los perfiles de usuario personalizados (Panel de control - Ícono contraseñas - Perfiles de usuario - Los usuarios pueden personalizar sus preferencias y configuración de escritorio).

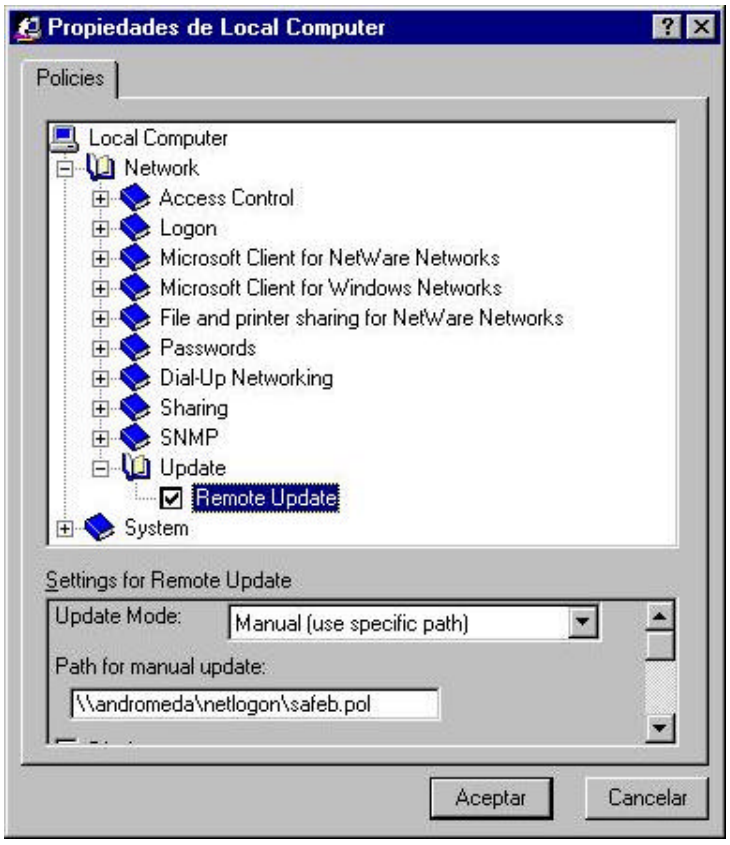


3. Ejecutamos el programa Poledit desde un diskette. Si nos pide una plantilla escogemos ADMIN.ADM .

4. Ir al menú, escoger File y luego Open Registry.

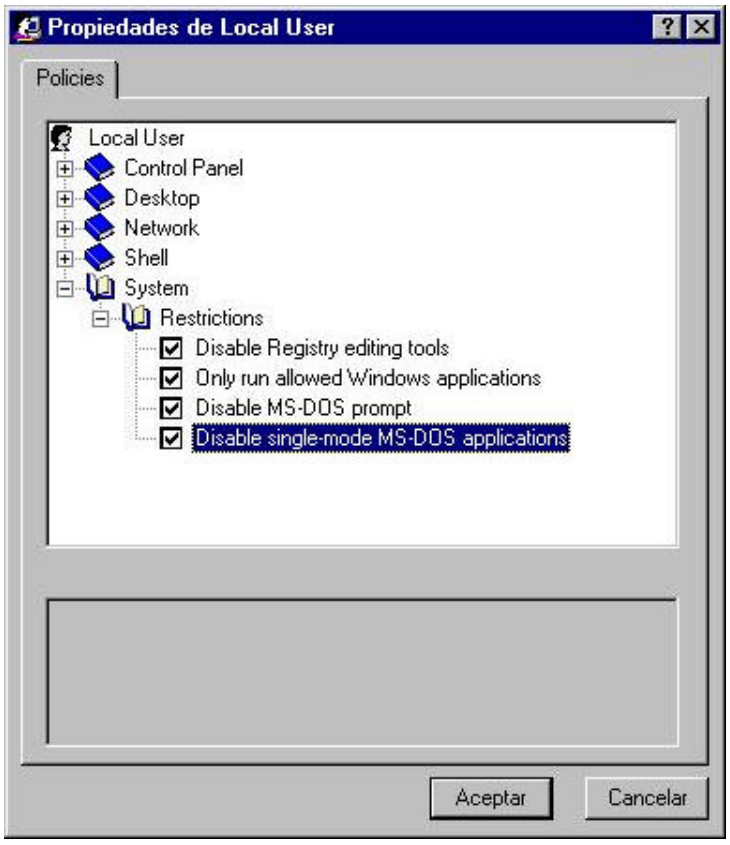


5. Hacer doble click en *Local Computer*, seguir la ruta *Network-Update-Remote Update*. Escoger *Update Mode Manual* y en *Path for manual update* escribir la ruta de red hacia el archivo se seguridad (archivo de extensión POL). Por ejemplo, para el caso del laboratorio B tendríamos: \\andromeda\netlogon\safeb.pol

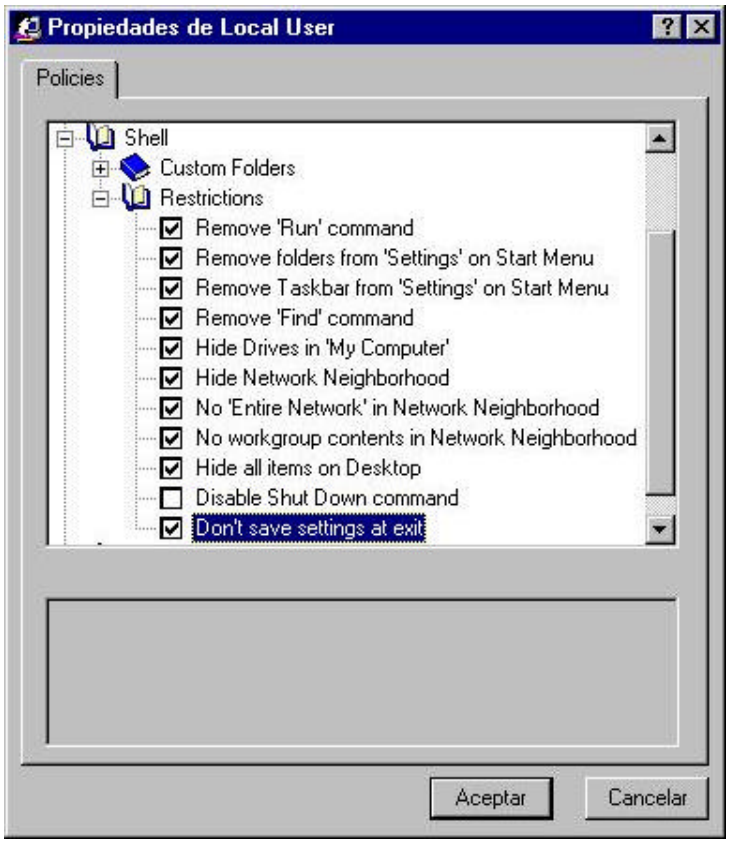


Adicionalmente podemos activar el *Load-balance* para lograr un balance de carga en el servidor cuando reciba muchas solicitudes de carga de perfiles y políticas. Finalmente dar Aceptar.

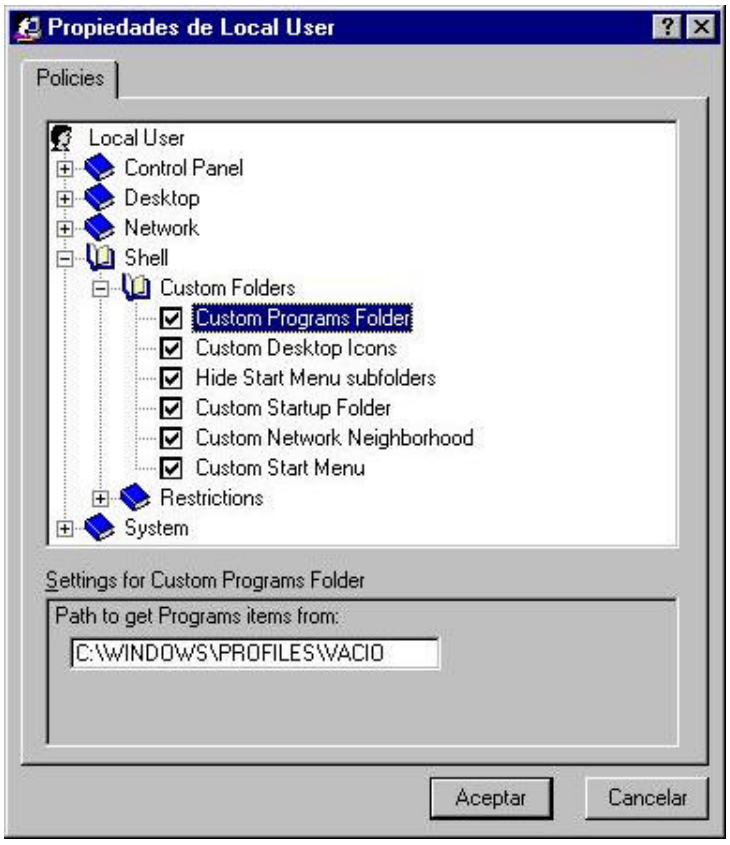
6. Hacer doble click en *Local User*. Marcar todas las opciones que aparecen en la ruta *System-Restrictions.*



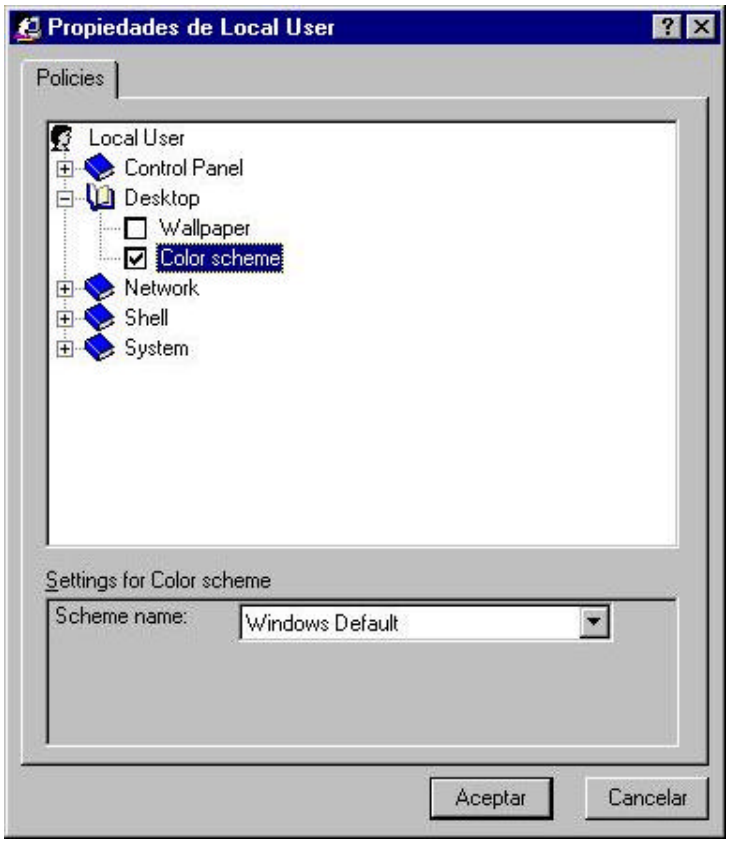
Igualmente en *Shell-Restrictions* menos en la opción *Disable Shut Down command*.



En *Shell-Custom Folders* marcar cada opción e ir escribiendo a la vez en *Path to get Programs items from:* la ruta C:\WINDOWS\PROFILES\VACIO.
Finalmente dar Aceptar.

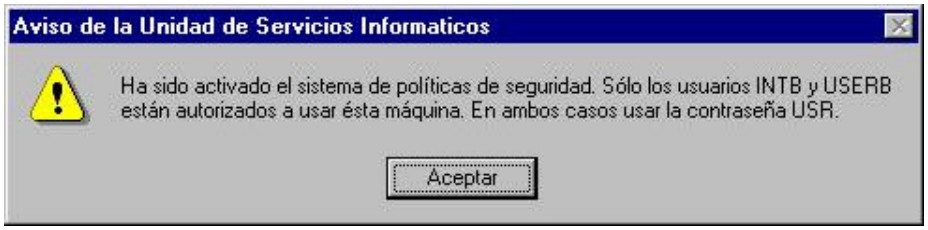


En la sección *Desktop* dejar en blanco la casilla de *Wallpaper*, marcar *Color scheme* y escoger *Windows Default* en el recuadro *Scheme name:*



6. Guardar la configuración con File-Save y reiniciar la computadora para un usuario distinto.

7. Comprobamos el funcionamiento del Police. Haciendo ESC debemos obtener una pantalla sólo en verde y una barra de tareas sin programas para ejecutar. Reiniciamos la máquina para un usuario definido en el laboratorio. Ingresamos con INTX, donde X es la letra de un laboratorio, y la contraseña USR. Debemos obtener un entorno con los programas de internet donde no puede ejecutarse otro programa que los visualizados en la barra de tareas y en el escritorio. Reiniciamos la máquina para ingresar con otro usuario. Debe observarse la presentación de un pantalla donde indique que sólo los usuarios INTX y USERX pueden ingresar al sistema . Por ejemplo, para el laboratorio B observaremos la siguiente ventana:



Ingresando con USERX debemos obtener sólo acceso a programas de clases, no existe acceso a internet. Se puede probar también con los demás usuarios. Finalmente si ingresamos con un usuario que no está definido en el salón sólo

obtendremos un entorno vacío, sin papel tapiz y una barra de tareas sin programas para ejecutar.

3.6. DESINSTALACIÓN DEL SYSTEM POLICE EN UNA MÁQUINA

Para una máquina que ha sido configurada con el System Policies observar que es diferente abrir el registro de la computadora durante la sesió n de un usuario que abrir el registro después de hacer Esc a la ventana de inicio de sesión. Si abrimos el registro durante la sesión de un usuario, al que se le han aplicado las políticas de seguridad, observaremos un Local User y un Local Computer afecta dos por el System Police y correspondientes al del usuario con el que se ha ingresado. Modificaciones hechas en el Local User y/o en Local Computer durante una sesión de usuario tendrán efecto sólo hasta que terminemos la sesión pues una vez reiniciada seguiremos con la configuración inicial debido a que las configuraciones del System Police tienen prioridad y han sido ***aplicadas a la máquina, no a un usuario***.

El entorno que obtenemos al hacer Esc a la ventana de inicio de sesión es el que nos permitirá hacer modificaciones en el Registro del sistema para poder desinstalar el System Police, sin embargo, en la sección anterior la máquina se configuró para que al hacer Esc no se obtuviera ningún tipo de acceso a la máquina. Tenemos entonces que ingresar al Modo Seguro del Windows 95 y desde aquí desactivar el System Police.

Debemos seguir los siguientes pasos:

1. Ingresar al *Modo Seguro a Prueba de Fallas* del Windows95, para ello reiniciar la PC y enseguida presionar F8.

2. Ejecutar el Poledit y desmarcar todas las opciones indicadas en los pasos 5 y 6 de la sección anterior. Guardar.

3. Adicionalmente también desactivar las opciones indicadas en el paso 1, sección anterior, correspondiente al inicio de sesión en el dominio del Windows NT y la activación de perfiles personalizados.

Ésta página ha sido elaborada por Genghis Ríos Kruger usando el editor Html del Netscape Gold 3.01.

Cualquier consulta, sugerencia o comentario será bien recibida escribiendo al e-mail: **grios@pucp.edu.pe**
