

FIREWALL

(PROYECTO III)



Sayan Danery Aguirre Guzmán | 7690-17-7987
Jitzon Aldahir Mendez Gonzalez | 7690-17-8955
Nelson Steven Cifuentes Chilin | 7690-17-2711

SEGURIDAD Y AUDITORIA DE SISTEMAS | 05/11/2021
ING. MELVIN CALÍ

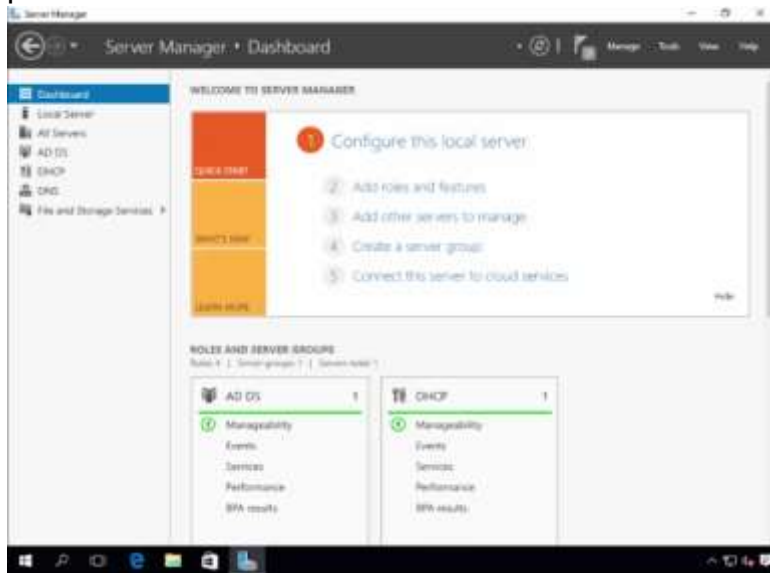
Documentación para Administración de usuarios y las políticas implementadas.

Preparando la estructura

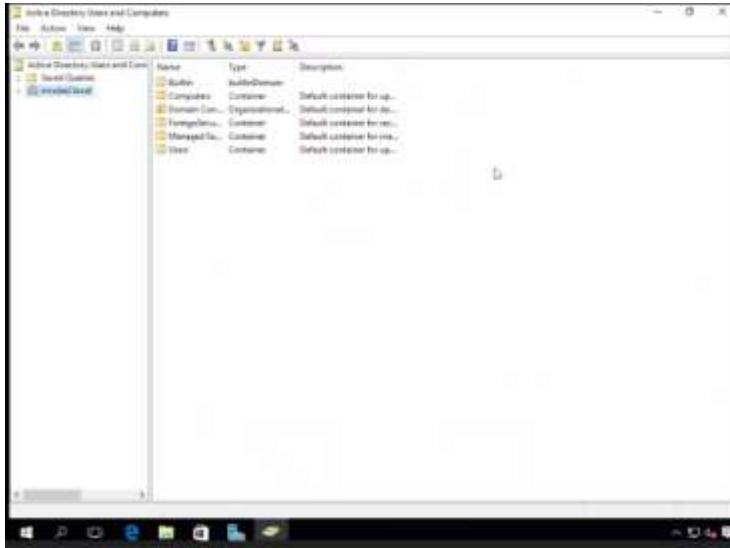
1. Como primer paso se procedió a crear el dominio, umg.local
2. Se creó el bosque.
3. Se crearon las estructuras organizativas.
4. Dentro de cada estructura se crean los usuarios.

Procedimiento para crear un usuario

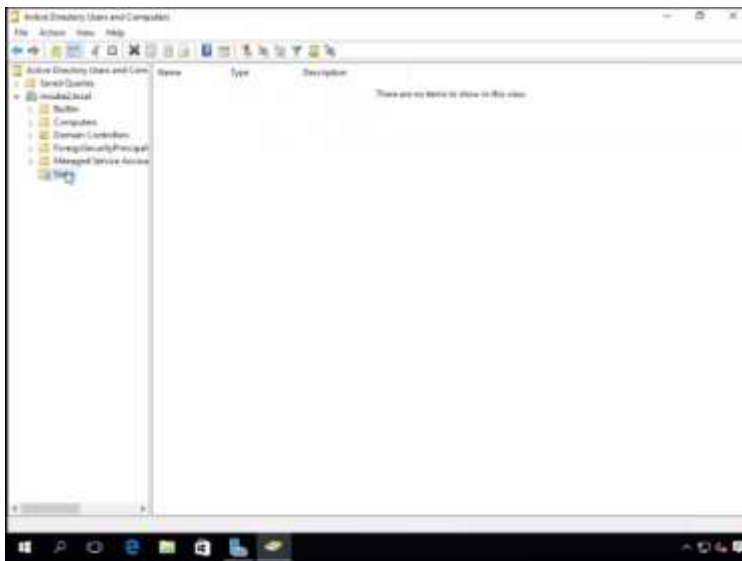
1. Desde la ventana de administrador de servidor podemos tener acceso desde la pestaña "TOOLS".



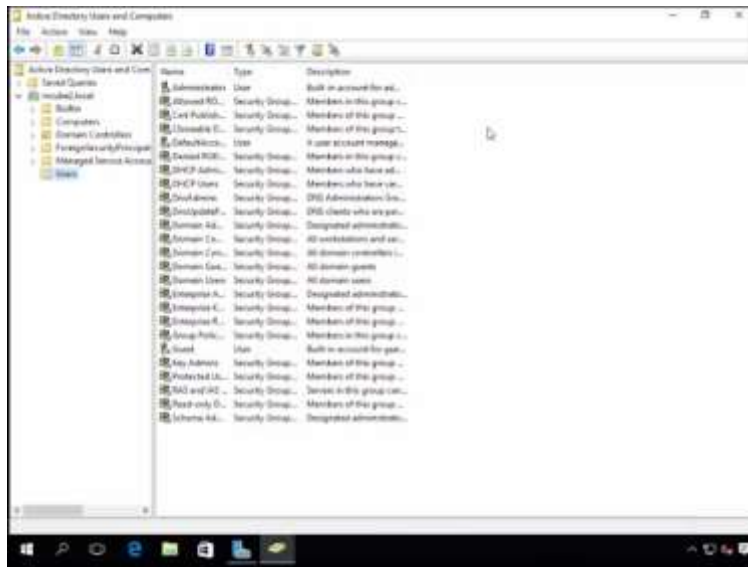
2. Entramos en la opción de “Active Directory Users and Computers”. En dicha ventana podemos crear usuarios y grupos.



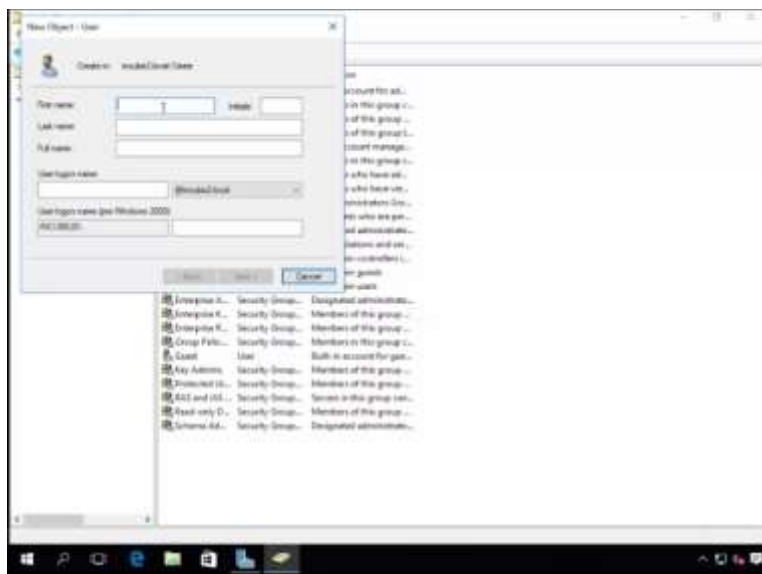
3. En las opciones del dominio nos dirigimos a la carpeta “Users”, ahí podremos ver los usuarios y grupos. Estos están representados por un icono de una sola persona y otro icono de varias personas, el icono de una sola persona significa “Usuario” y el de varias personas significa “Grupos”. Como se muestra en la imagen.



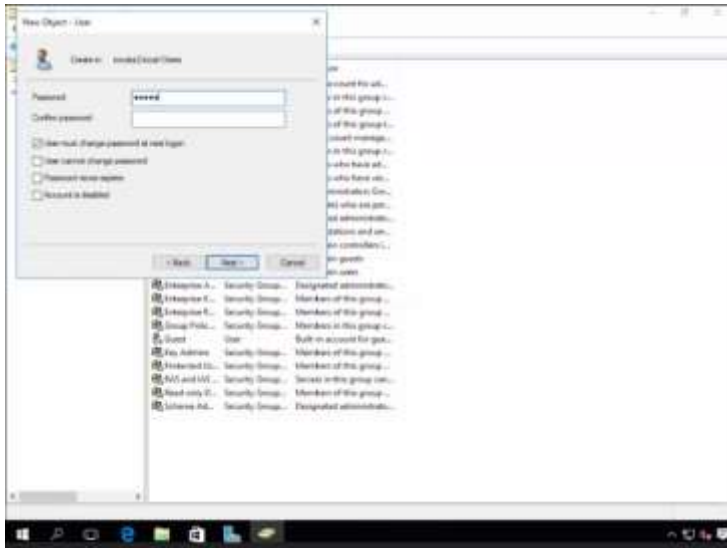
4. En esta misma sección, podemos agregar los usuarios o grupos, le damos “click” en las opciones que se nos ofrecen en la parte superior de la ventana.



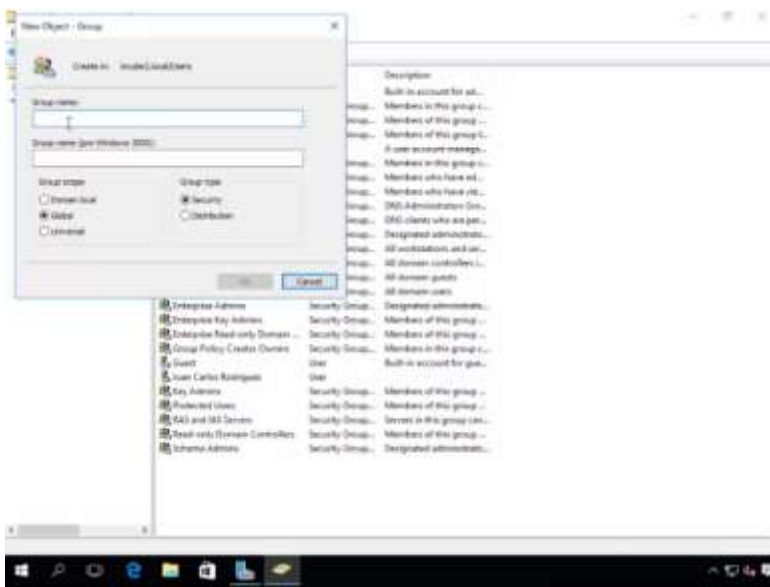
5. Al dar click en añadir un usuario se nos muestra una ventana en donde añadimos la información del usuario que deseamos agregar. Después de llenar los campos, elegimos “siguiente” y procedemos a crear la contraseña.



6. Esta contraseña puede ser creada para darle al usuario un primer ingreso luego podemos pedir que la contraseña sea re-establecida en el primer ingreso. Luego finalizamos dando click en “finalizar” y ya con esto hemos creado el usuario.

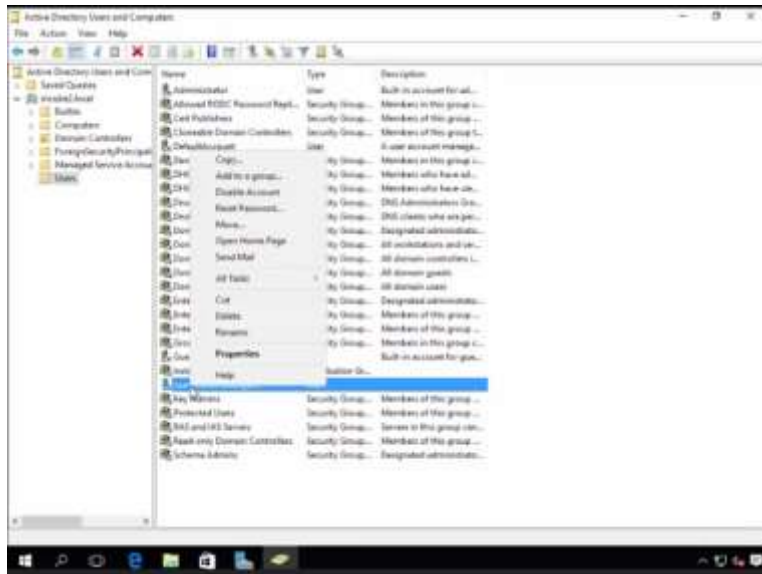


7. Luego introducimos la información del grupo “nombre” por ejemplo, también podemos elegir las configuraciones del grupo que estamos creando. Si deseamos añadir usuarios al grupo que creamos, damos “click derecho” sobre el usuario (en este caso el usuario que creamos anteriormente).

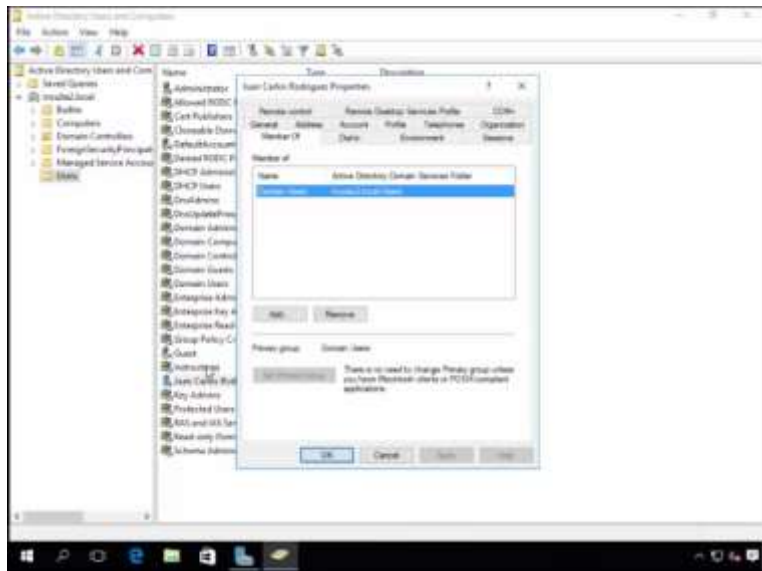


x

8. Buscamos la pestaña de propiedades, y accedemos, una vez dentro, buscamos la opción de “miembro de”.



9. Es aquí donde podemos añadir el usuario al grupo de creamos previamente. Damos clic en “añadir” y buscamos el grupo (también podemos escribir el nombre del grupo que creamos) y damos click en aceptar (para añadir el usuario al grupo). Ya el usuario pasa a ser miembro del grupo.

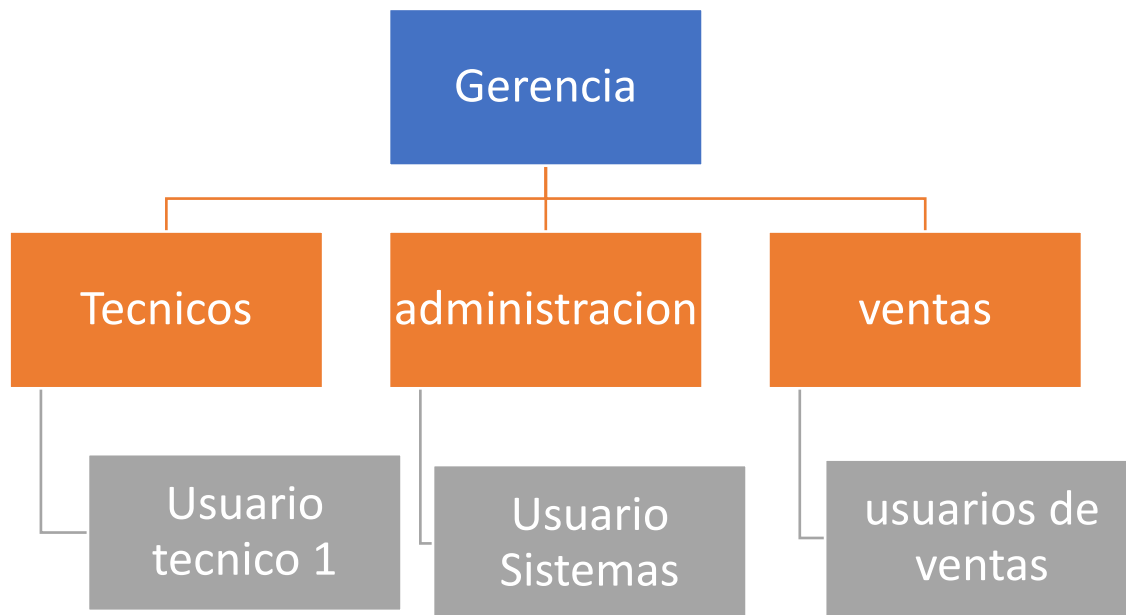


Lista de Roles

Se crearon unidades organizacionales, siendo las siguientes:

- Contabilidad
- Técnicos
- Administración

Diagrama del Negocio



Políticas de los Roles

Restricciones Estándar

General

Detalles

Dominio	umg.local
Propietario	UMG\Admin. del dominio
Estado de GPO	Habilitado

Esta lista solo incluye vínculos en el dominio del GPO.

Vínculos

Ubicación	Aplicado	Estado de vinculo	Ruta
TECNICOS	Si	Habilitado	umg.local/TECNICOS
ADMINISTRACION	Si	Habilitado	umg.local/ADMINISTRACION
VENTAS	Si	Habilitado	umg.local/VENTAS

Configuración del equipo

Directivas de cuenta / Directiva de Contraseñas

Directiva	Configuración
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 Caracteres
Vigencia máxima de la contraseña	45 días
Vigencia mínima de la contraseña	30 días

Configuración del usuario

Componentes de Windows / Internet Explorer

Directiva	Configuración
Impedir el cambio de configuración de proxy	Habilitado

Componentes de Windows/Windows Update

Directiva	Configuración
Quitar el acceso a todas las características de Windows Update	Habilitado

Menú Inicio y barra de tareas

Directiva	Configuración
Quitar vínculos y accesos a Windows Update	Habilitado

Panel de control/Agregar o quitar programas

Directiva	Configuración
Ocultar la opción "Agregar programas desde la red"	Habilitado
Ocultar la opción "Agregar programas desde Microsoft"	Habilitado
Ocultar la opción "Agregar un programa desde un CD-ROM o disquete"	Habilitado
Ocultar la página Agregar nuevos programas	Habilitado
Ocultar la página Agregar o quitar componentes de Windows	Habilitado
Ocultar la página Cambiar o quitar programas	Habilitado
Ocultar la página Configurar acceso y programas predeterminados	Habilitado
Quitar Agregar o quitar programas	Habilitado

Panel de control/Personalización

Directiva	Configuración
Habilitar protector de pantalla	Habilitado
Impedir cambiar el color y la apariencia	Habilitado
Impedir cambiar el fondo de pantalla	Habilitado
Impedir cambiar el protector de pantalla	Habilitado

Impedir cambiar iconos del escritorio	Habilitado
Impedir cambiar punteros del mouse	Habilitado
Impedir cambiar sonidos	Habilitado
Proteger el protector de pantalla mediante contraseña	Habilitado
Tiempo de espera del protector de pantalla	Habilitado

Red/Conexiones de red

Directiva	Configuración
Capacidad para habilitar o deshabilitar una conexión LAN	Deshabilitado
Prohibir el acceso a las propiedades de componentes de una conexión LAN	Habilitado
Prohibir el acceso a las propiedades de una conexión LAN	Habilitado
Prohibir la configuración TCP/IP avanzada	Habilitado

Sistema

Directiva	Configuración
Actualizaciones automáticas de Windows	Deshabilitado

Sistema/Acceso de almacenamiento extraíble

Directiva	Configuración
Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitado

Sistema/Administración de energía

Directiva	Configuración
Solicitar contraseña al reanudar tras hibernación o suspensión	Habilitado

Sistema/Directiva de grupo

Directiva	Configuración
Desactivar la actualización automática de los archivos ADM	Habilitado

Sistema/Servicios de configuración regional

Directiva	Configuración
Denegar el cambio de ubicación geográfica	Habilitado

Restricciones Gerencia

General

Detalles

Dominio	umg.local
Propietario	UMG\Admins. del domino
Estado de GPO	Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
GERENCIA	Si	Habilitado	umg.local/GERENCIA

Esta lista solo incluye vínculos en el dominio del GPO.

Configuración del equipo

Directivas de cuenta / Directiva de Contraseñas

Directiva	Configuración
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	45 días
Vigencia mínima de la contraseña	30 días

Componentes de Windows / Internet Explorer

Directiva	Configuración
Impedir el cambio de configuración de proxy	Habilitado

Restricciones Máximas

Visitas

Se creó el perfil de visitas el cual solo permitirá conectarse según los siguientes parámetros establecidos:

- Horario - Lunes a Sábado de 8:00 horas a 18:00 horas.
- No se permitirán conexiones remotas dentro de la red.
- El límite para sesiones inactivas será de 5 minutos.
- Para sesiones activas será de 1 hora.
- Para finalizar sesión desconectada será de 10 minutos.
- No tendrá acceso a dispositivos de almacenamiento.

General

Detalles

Dominio	umg.local
Propietario	UMG\Admins. del domino
Estado de GPO	Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
VISITAS	Si	Habilitado	umg.local/VISITAS

Esta lista solo incluye vínculos en el dominio del GPO.

Configuración del usuario

Active Desktop/Active Desktop

Directiva	Configuración
Deshabilitar todos los elementos	Habilitado

Carpetas Compartidas

Directiva	Configuración
Permitir publicación de carpetas compartidas	Deshabilitado

Componentes de Windows/Internet Explorer

Directiva	Configuración
Impedir el cambio de configuración de proxy	Habilitado

Componentes de Windows/Windows Update

Directiva	Configuración
Quitar el acceso a todas las características de Windows Update	Habilitado

Panel de Control

Directiva	Configuración
Ocultar los elementos especificados del Panel de control	Habilitado
Prohibir el acceso a Configuración de PC y a Panel de control	Habilitado

Panel de control/Personalización

Directiva	Configuración
Habilitar protector de pantalla	Habilitado
Impedir cambiar el color y la apariencia	Habilitado
Impedir cambiar el estilo visual de ventanas y botones	Habilitado
Impedir cambiar el fondo de pantalla	Habilitado
Impedir cambiar el protector de pantalla	Habilitado
Impedir cambiar el tema	Habilitado
Proteger el protector de pantalla mediante contraseña	Habilitado
Tiempo de espera del protector de pantalla	Habilitado

Red/Conexiones de red

Directiva	Configuración
Prohibir el acceso a las propiedades de componentes de una conexión LAN	Habilitado
Prohibir el acceso a las propiedades de una conexión LAN	Habilitado
Prohibir el acceso a propiedades de componentes de una conexión de acceso remoto	Habilitado

Prohibir el acceso al Asistente para nueva conexión	Habilitado
Prohibir el acceso al elemento Configuración avanzada en el menú Opciones avanzadas	Habilitado
Prohibir el acceso al elemento Preferencias de acceso remoto en el menú Opciones avanzadas	Habilitado
Prohibir el cambio de nombre de conexiones de acceso remoto privadas	Habilitado
Prohibir el cambio de propiedades de una conexión de acceso remoto privada	Habilitado
Prohibir la adición y eliminación de componentes de una LAN o una conexión de acceso remoto	Habilitado
Prohibir la conexión y desconexión de una conexión de acceso remoto	Habilitado
Prohibir la configuración TCP/IP avanzada	Habilitado

Sistema

Directiva	Configuración
Impedir el acceso a herramientas de edición del Registro	Habilitado
Impedir el acceso al símbolo del sistema	Habilitado

Sistema/Acceso de almacenamiento extraíble

Directiva	Configuración
CD y DVD: denegar acceso de escritura	Habilitado
CD y DVD: denegar acceso de lectura	Habilitado
Discos extraíbles: denegar acceso de escritura	Habilitado
Discos extraíbles: denegar acceso de lectura	Habilitado
Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitado
Unidades de disquete: denegar acceso de escritura	Habilitado
Unidades de disquete: denegar acceso de lectura	Habilitado

Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet

Directiva	Configuración
Desactivar el acceso a la Tienda	Habilitado
Desactivar el servicio de asociaciones de archivo de Internet	Habilitado
Desactivar Windows Online	Habilitado

Sistema/Instalación de controladores

Directiva	Configuración
-----------	---------------

Desactivar la intervención del usuario en búsquedas de controladores de dispositivo en Windows Update	Habilitado
---	------------

Sistema/Opciones de Ctrl+Alt+Supr

Directiva	Configuración
Quitar Administrador de tareas	Habilitado
Quitar Cerrar sesión	Habilitado
Quitar el bloqueo de equipos	Habilitado
Quitar la opción Cambiar contraseña	Habilitado

Sistema/Servicios de configuración regional

Directiva	Configuración
Denegar el cambio de ubicación geográfica	Habilitado
Denegar la invalidación de configuraciones regionales por parte del usuario	Habilitado
Limitar configuraciones regionales del usuario	Habilitado

Restricciones Sistemas

General

Detalles

Dominio	umg.local
Propietario	UMG\Admins. del domino
Estado de GPO	Habilitado

Vínculos

Ubicación	Aplicado	Estado de vínculo	Ruta
SISTEMAS	Si	Habilitado	umg.local/SISTEMAS

Esta lista solo incluye vínculos en el dominio del GPO.

Configuración del equipo

Directivas de cuenta / Directiva de Contraseñas

Directiva	Configuración
Las contraseñas deben cumplir los requisitos de complejidad	Habilitado
Longitud mínima de la contraseña	7 Caracteres
Vigencia máxima de la contraseña	45 días
Vigencia mínima de la contraseña	30 días

Configuración del usuario

Componentes de Windows/Internet Explorer

Directiva	Configuración
Impedir el cambio de configuración de proxy	Habilitado

Componentes de Windows/Windows Update

Directiva	Configuración
Quitar el acceso a todas las características de Windows Update	Habilitado

Panel de control/Personalización

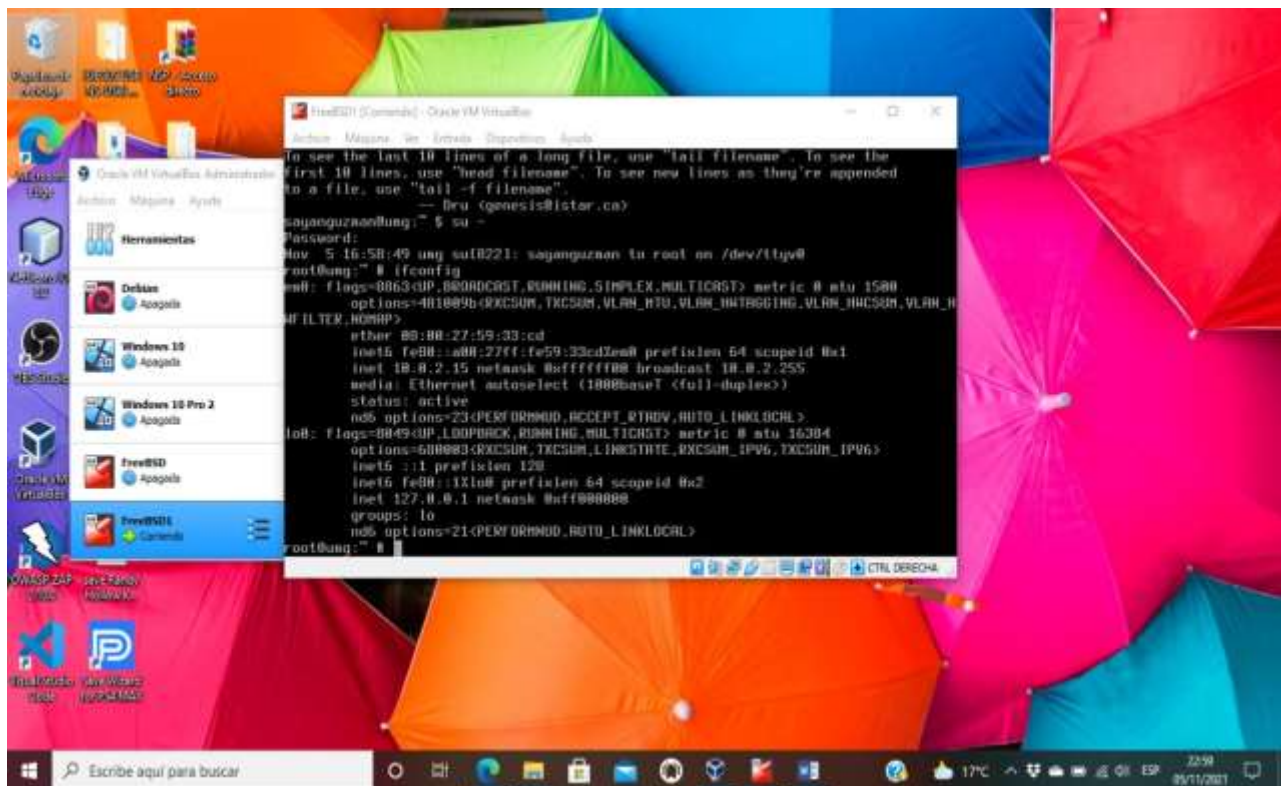
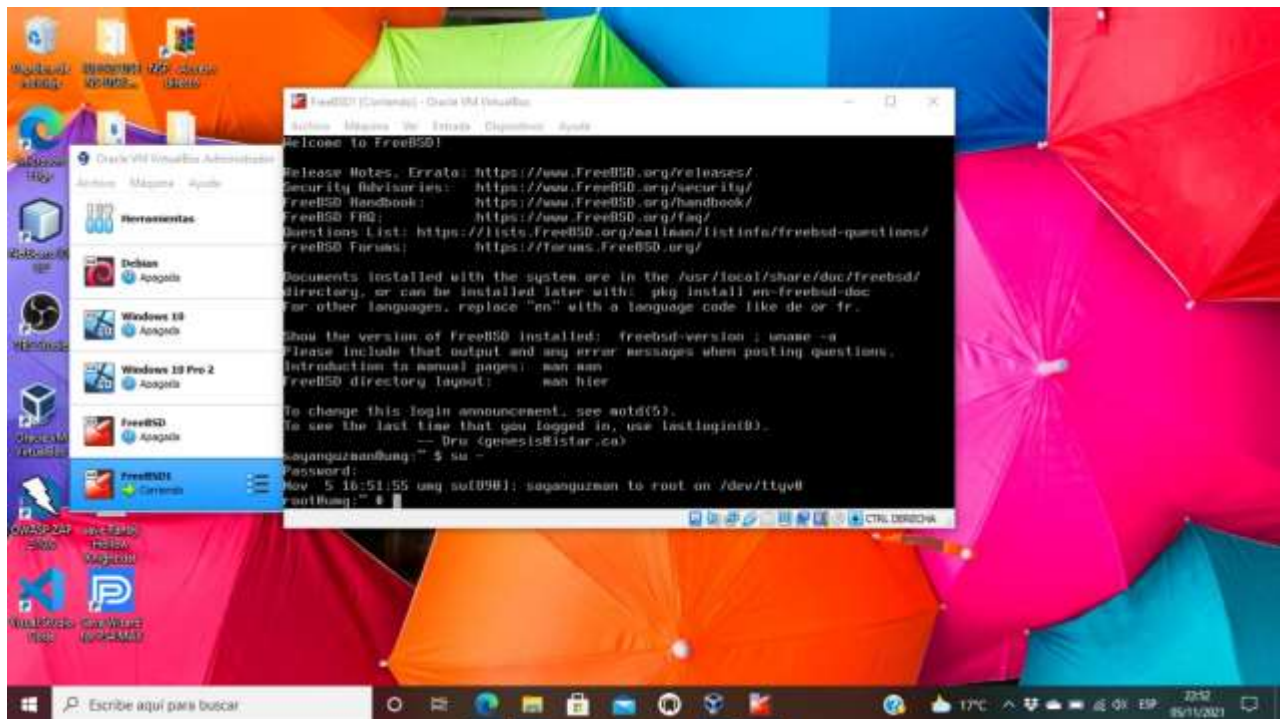
Directiva	Configuración
Habilitar protector de pantalla	Habilitado
Impedir cambiar el color y la apariencia	Habilitado
Impedir cambiar el estilo visual de ventanas y botones	Habilitado
Impedir cambiar el fondo de pantalla	Habilitado
Impedir cambiar el protector de pantalla	Habilitado
Impedir cambiar el tema	Habilitado
Impedir cambiar iconos del escritorio	Habilitado
Impedir cambiar la combinación de colores	Habilitado
Impedir cambiar punteros del mouse	Habilitado
Impedir cambiar sonidos	Habilitado
Prohibir seleccionar el tamaño de fuente del estilo visual	Habilitado
Proteger el protector de pantalla mediante contraseña	Habilitado
Tiempo de espera del protector de pantalla	Habilitado

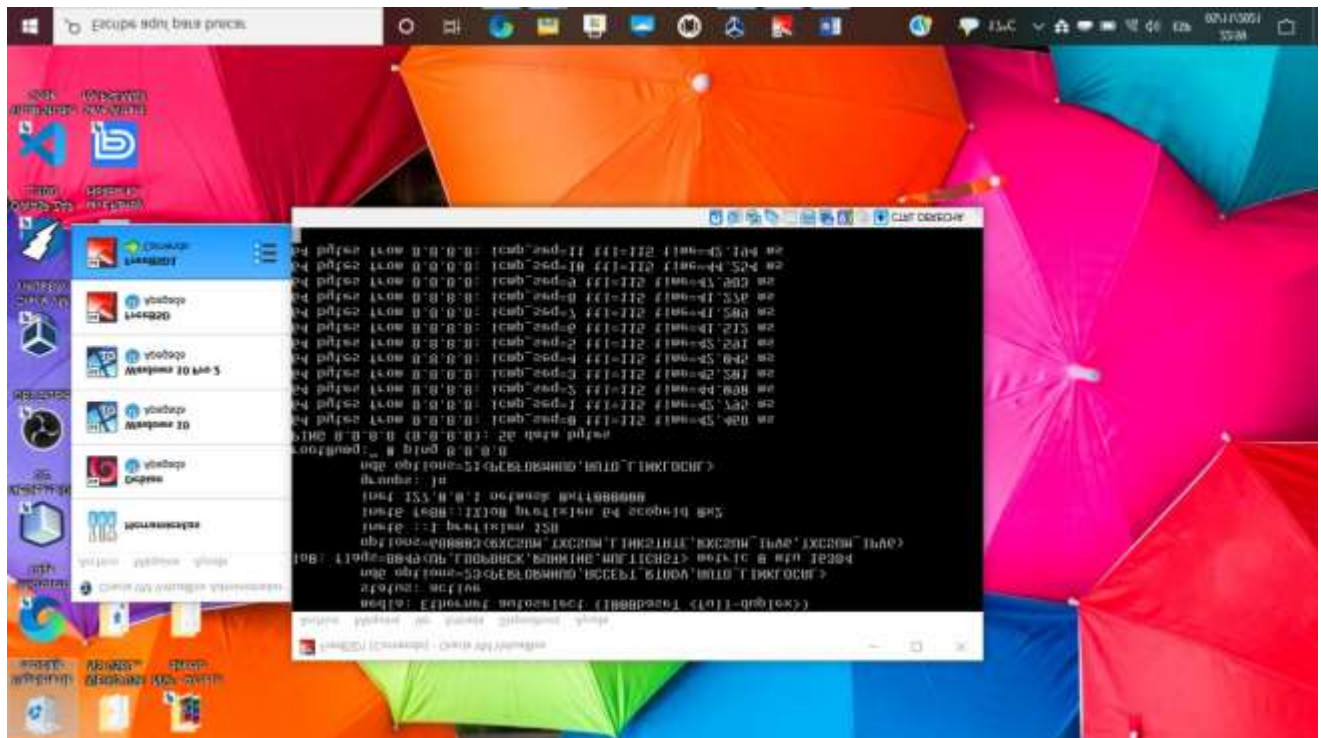
Número de segundos de espera hasta que se active el protector de pantalla – 300 Segundos.

Instalación de Unix:

Unix es un sistema operativo portable, multitarea y multiusuario; desarrollado en 1969 por un grupo de empleados de los laboratorios Bell de AT&T. El sistema, junto con todos los derechos fueron vendidos por AT&T a Novell, Inc.







Unix es un sistema operativo que nace a principios de los años 70, creado principalmente por Dennis Ritchie y Ken Thompson. Sus características técnicas principales son su portabilidad, su capacidad multiusuario y multitarea, su eficiencia, su alta seguridad y su buen desempeño en tareas de red. Pero Unix, más que una marca, también es una filosofía, que tiene por principios el minimalismo y el modularidad: hacer programas que hagan una sola cosa bien hecha, y que, al comunicarse entre sí, ejecuten tareas más complejas.

Un sistema Unix puede dividirse en tres áreas básicas: el núcleo del sistema operativo, el intérprete de comandos y algunos programas utilitarios. Lo demás que necesitamos, como las aplicaciones de usuario o la interfaz gráfica, son paquetes adicionales.

Por sus características técnicas y su filosofía abierta, existen diversos sistemas operativos que se conocen como derivados de Unix o sistemas de la familia Unix. Entre estos están FreeBSD y GNU/Linux; macOS también es un sistema Unix al igual que Android (derivado de Linux) e iOS (derivado de Mac OS X).