COLOMBIA POTENCIA DE LA VIDA

ICANH

POLITICAS DEL GRUPO DE DIRECTORIO ACTIVO

INSTITUTO COLOMBIANO DE ANTROPOLOGÍA E HISTORIA

CONTENIDO

DEFINICIÓN DEL SERVIDOR DE DOMINIO 3

DEFINICIÓN DE LOS GRUPOS USUARIOS EN EL SERVIDOR DE DOMINIO 3

DEFINICIÓN DE USUARIOS VPN 4

POLÍTICAS DE CONTROLES DE SERVIDOR 5

Política del Servidor de dominio: 5

Miembro del Servidor de Dominio 5

Servidor de Red de Microsoft 5

Alcance de la Política 5

POLÍTICAS DE SEGURIDAD GENERAL 6

Políticas de cuenta/Política de contraseña 6

Políticas de cuenta/Política de bloqueo de contraseña 6

Políticas de cuenta/Política Kerberos 6

Políticas locales/Opciones de seguridad 7

Acceso de Red Seguridad en la Red 7

Políticas de clave pública/Sistema de cifrado de archivos 7

Alcance de la Política 7

POLÍTICA PERMISOS DE ADICIÓN AL DOMINIO 7

Alcance de la Política 8

POLÍTICA PERMISOS DE INSTALACIÓN 8

Componentes de instalación de windows. 9

Alcance de la Política 9

POLÍTICA PANEL DE CONTROL 9

Control Panel 10

Control panel de impresoras 10

Menú de inicio y barra de tareas 10

Alcance de la Política 10

POLÍTICA DE INACTIVIDAD POR TIEMPO 10

Política para equipos locales 10

Alcance de la Política 11

POLÍTICA FONDOS DE ESCRITORIO 11

Alcance de la Política 12

Alcance de la Política 12

POLÍTICA DE DESABILITACIÓN DEL PROXY DE LOS USUARIOS 13

Alcance de la Política 13

POLÍTICA DE PLUG AND PLAY. 14

Alcance de la Política 14

POLÍTICA DE ANTIVIRUS 15

Alcance de la Política 15

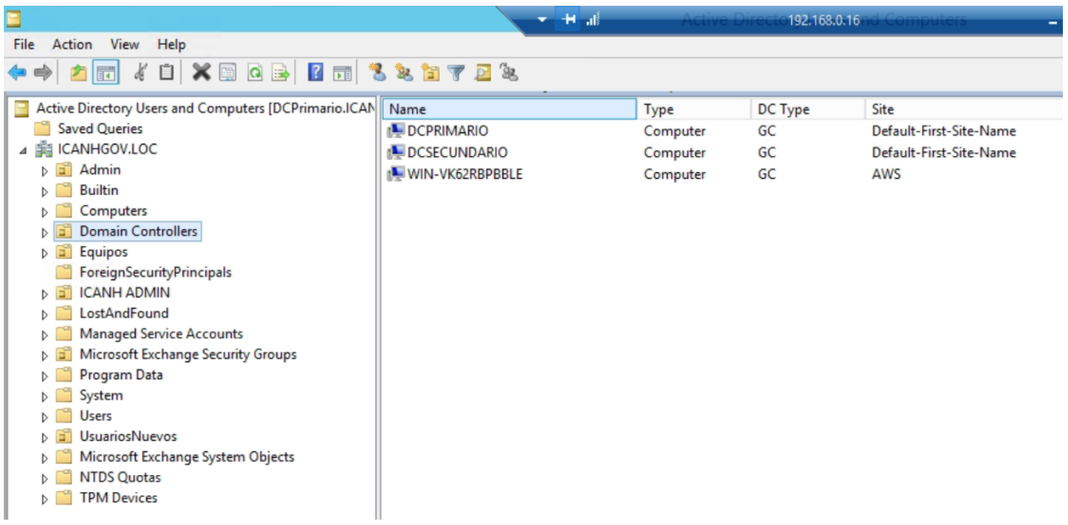
INSTALACIÓN DEL CERTIFICADO DE SOPHOS 15

Alcance de la Política 16

POLÍTICA DE ACCESO Y CONTROL DE USUARIOS 16

BIBLIOGRAFÍA 18

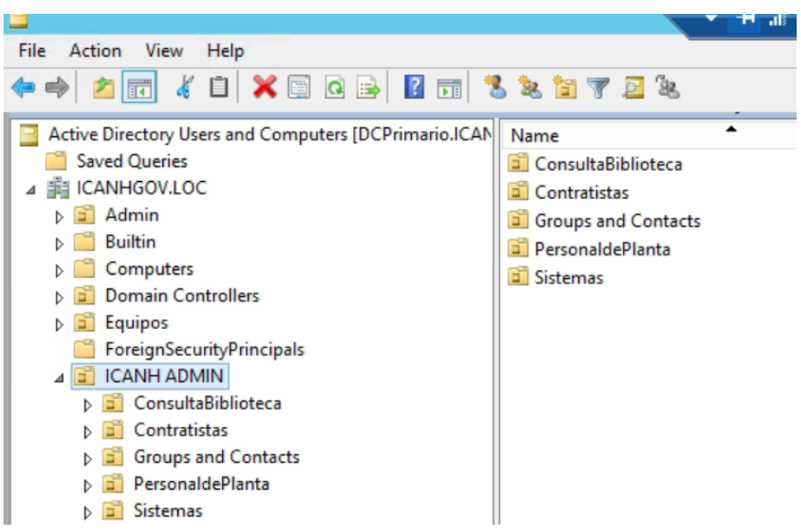
1. DEFINICIÓN DEL SERVIDOR DE DOMINIO



Domain Controllers:

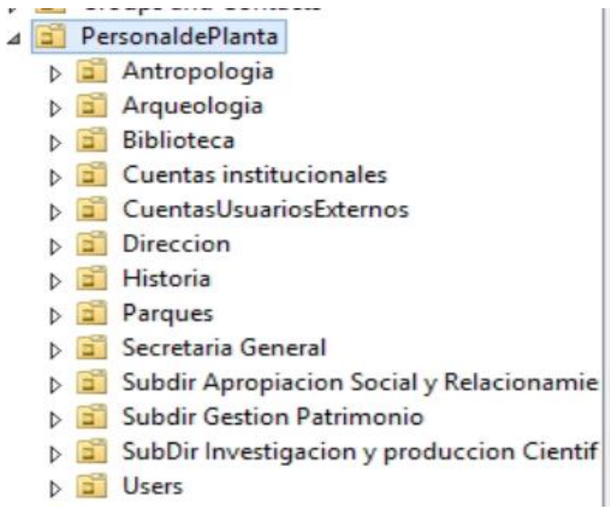
- Se definen dos servidores
  - DCPRIMARIO: Es el servidor principal que permite que los usuarios se conecten a la red del ICANH, puedan acceder a Internet y tener acceso a sus archivos en las unidades de drive o en las unidades compartidas
  - Dirección IP: 192.168.0.16
  - DCSECUNDARIO: Es un servidor secundario, permitiendo la redundancia dentro del sistema de red del ICANH, siempre está actualizado, en caso de una falla del servidor Principal el asume todas las responsabilidades en el manejo de la red y de los usuarios
  - Dirección IP: 192.168.0.17

2. DEFINICIÓN DE LOS GRUPOS USUARIOS EN EL SERVIDOR DE DOMINIO

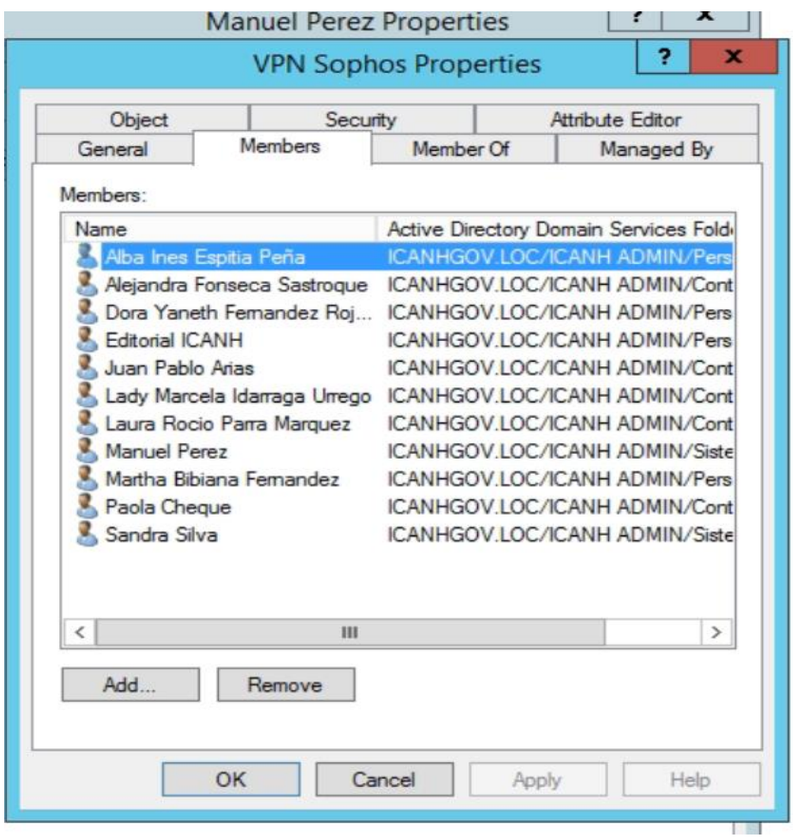


Existen varios grupos:

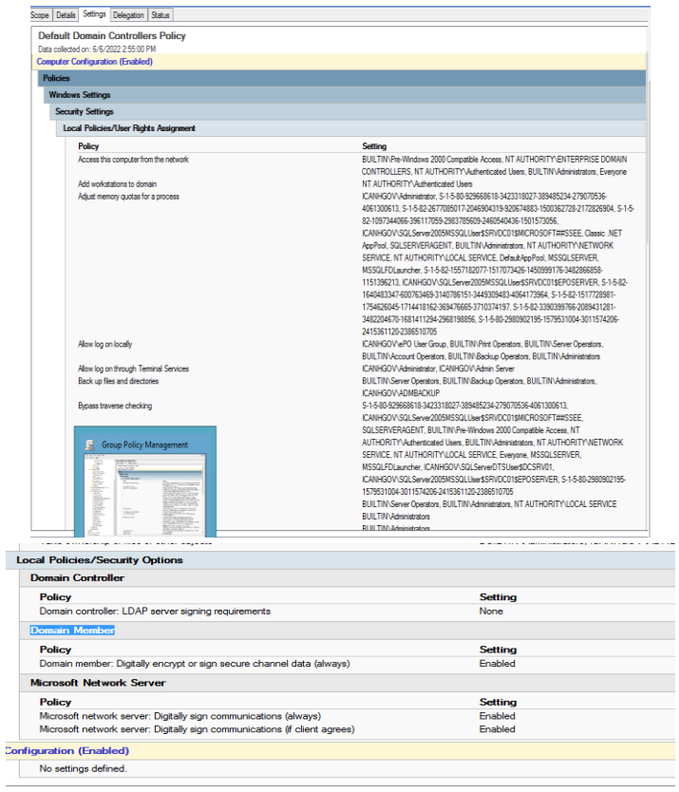
- Consulta Biblioteca: El usuario creado dentro de este grupo solo puede consultar la biblioteca, no navega en internet.
- Contratistas: se definen todos los contratistas del ICANH, sin tener en cuenta a qué área pertenecen
- Groups Contacts: Son todos los grupos y/o áreas al interior del ICANH
- Personal de Planta: Se encuentra todos los funcionarios del ICANH, clasificados en sus áreas.



3. DEFINICIÓN DE USUARIOS VPN



4. POLÍTICAS DE CONTROLES DE SERVIDOR



Configuración del Servidor habilitada

Política del Servidor de dominio:

- Domain controller: el servidor de dominio requiere LDAP (Permite identificar a los usuarios en el Directorio Activo, utilizando para ello el protocolo de encriptación Kerberos, con conexión SSL/TLS cifrada)

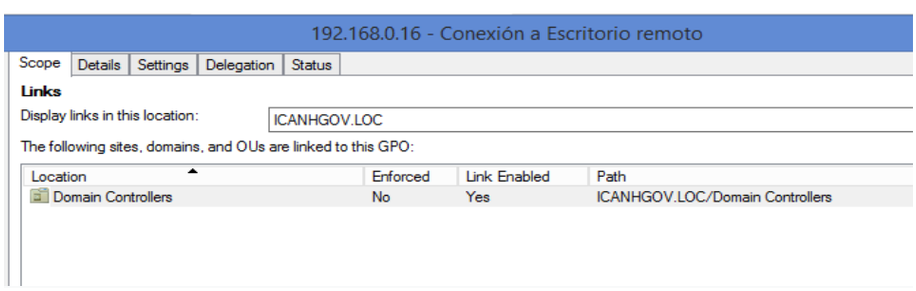
Miembro del Servidor de Dominio

- El canal de comunicaciones se encuentra encriptado

Servidor de Red de Microsoft

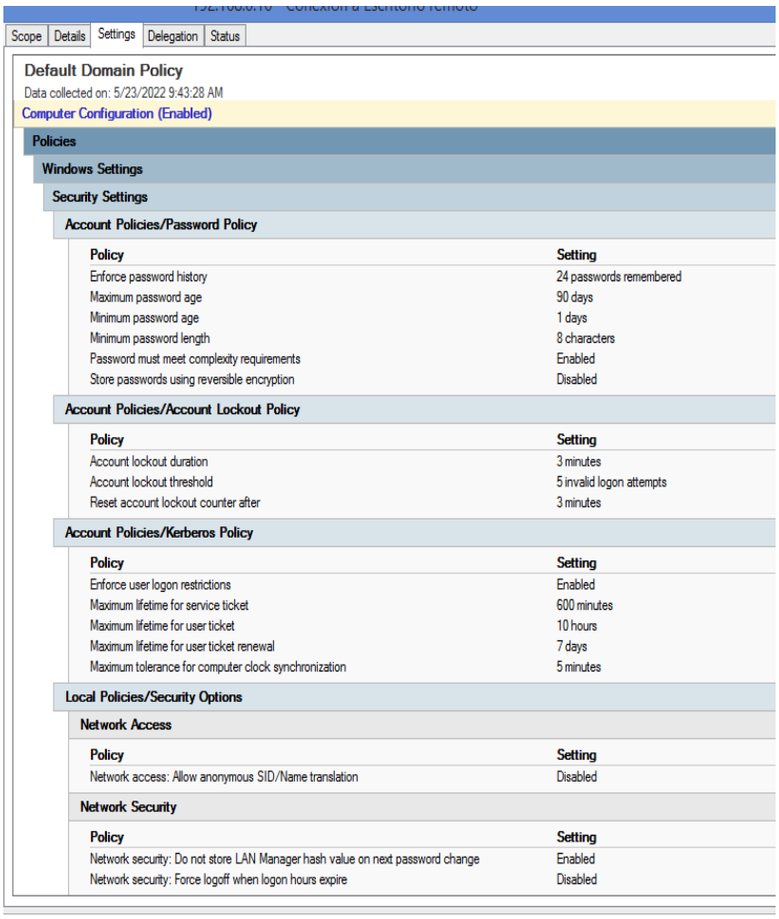
- Todas las comunicaciones se deben autenticar

Alcance de la Política



Se aplicará al controlador de dominio

5. POLÍTICAS DE SEGURIDAD GENERAL



Scope | Details | Settings | Delegation | Status

Default Domain Policy

Data collected on: 5/23/2022 9:43:28 AM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	3 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	3 minutes

Account Policies/Kerberos Policy

Policy	Setting
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

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

Políticas de cuenta/Política de contraseña

- Historial de contraseñas: el servidor recuerda 24 contraseñas
- Cada 90 días pide cambio de contraseña
- La duración mínima de la contraseña es de un día
- Longitud mínima de la contraseña es de 8 caracteres, utilizando caracteres especiales como $#%&*.
- La contraseña debe cumplir los requisitos de complejidad.
- El almacenado de la contraseña se guarda con cifrado no reversible

Políticas de cuenta/Política de bloqueo de contraseña

- El usuario se bloquea después de 5 intentos de inicio
- La duración del bloqueo es de 3 minutos.
- El contador de bloqueo se restablece después de 3 minutos

Políticas de cuenta/Política Kerberos

- Cuando el usuario inicia sesión se aplicarán todas las políticas
- Máximo tiempo de utilización de un servicio dentro del dominio es de 600 minutos

- El máximo tiempo de utilización que puedan acceder a los recursos de la red fuera de su horario de inicio de sesión es de 10 horas.
- Máximo tiempo que los usuarios puedan trabajar con una sesión y utilizar los recursos de red es de siete días
- La sincronización del reloj no puede exceder a más de 5 minutos de lo contrario no podrá acceder a los servicios de red

Políticas locales/Opciones de seguridad

- Se encuentra deshabilitado porque el usuario no puede registrarse con el número de identificación de otro usuario

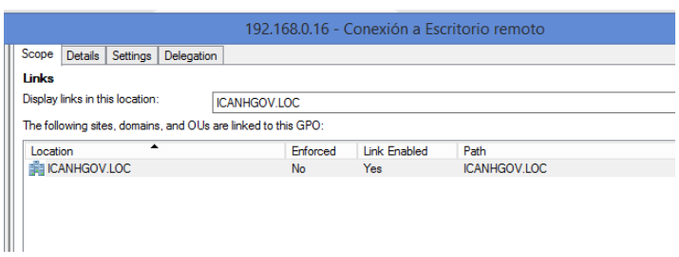
Acceso de Red Seguridad en la Red

- Está habilitada la generación del hash LM y el hash de Windows NT de la contraseña y se almacena en la base de datos SAM o directorio activo, pero no debe almacenar la contraseña antigua del administrador cuando se produce un cambio de contraseña.
- Se encuentra deshabilitado el forzar el cierre de sesión de los usuarios porque el horario de sesión no se ha definido para cada uno de los usuarios

Políticas de clave pública/Sistema de cifrado de archivos

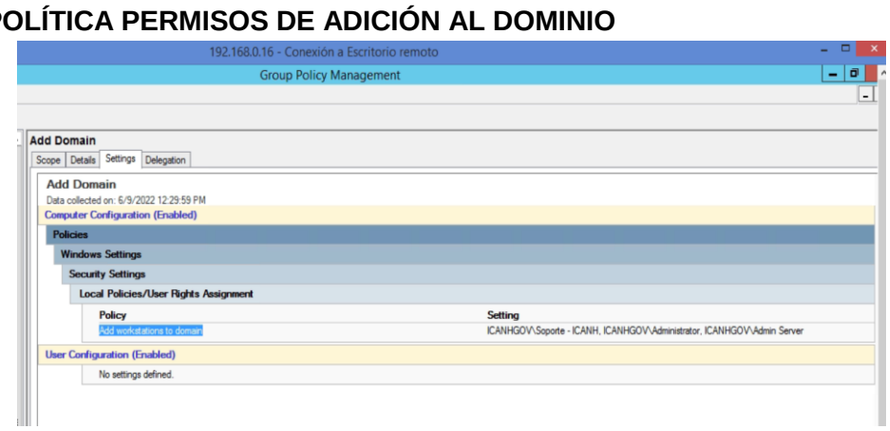
- Solo el administrador puede acceder a los certificados de los servidores y generar sistemas de encriptación

Alcance de la Política



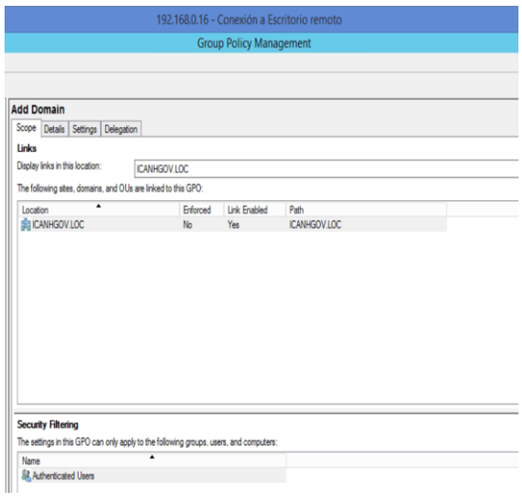
La política se aplicará a todo el dominio del ICANH

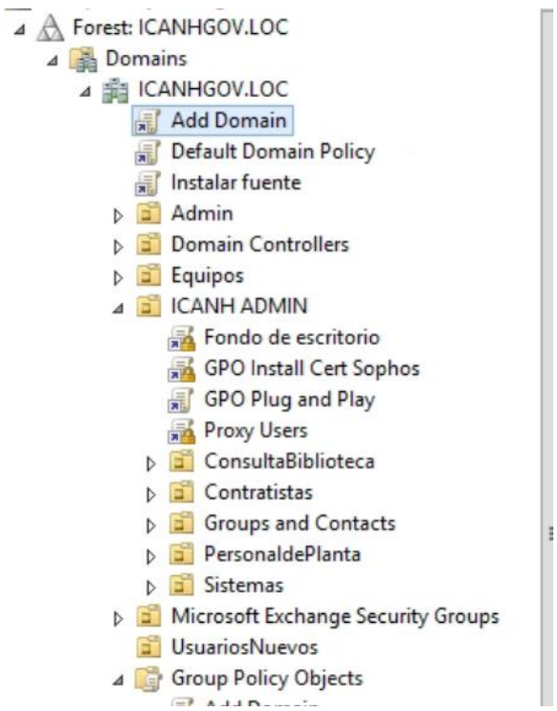
6. POLÍTICA PERMISOS DE ADICIÓN AL DOMINIO



- Define la adición de las diferentes PC's al dominio
- Solo lo puede hacer el usuario administrador, el admin server y el soporte

Alcance de la Política





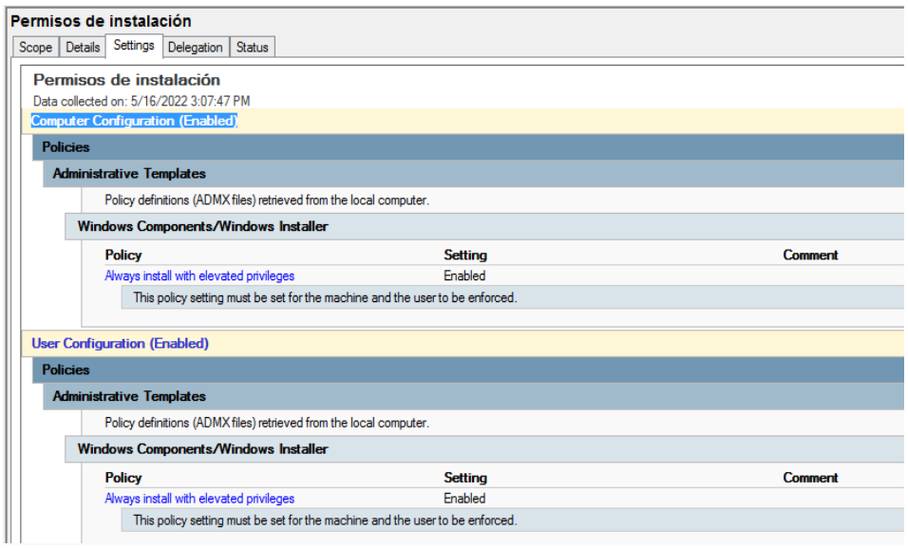
El alcance está definido a todo el dominio ICANHGOV.LOC

Como vemos el dominio está compuesto por

- Equipos
- Contratistas
- funcionarios
- Políticas de seguridad creadas
- Grupos

7. POLÍTICA PERMISOS DE INSTALACIÓN

Configuración de los computadores (habilitado)

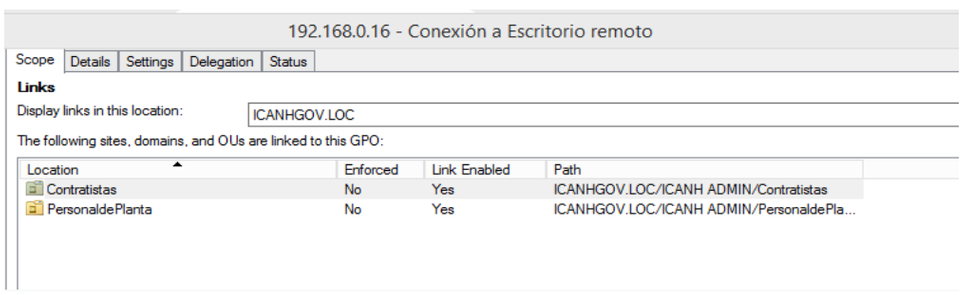


Componentes de instalación de Windows.

Definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

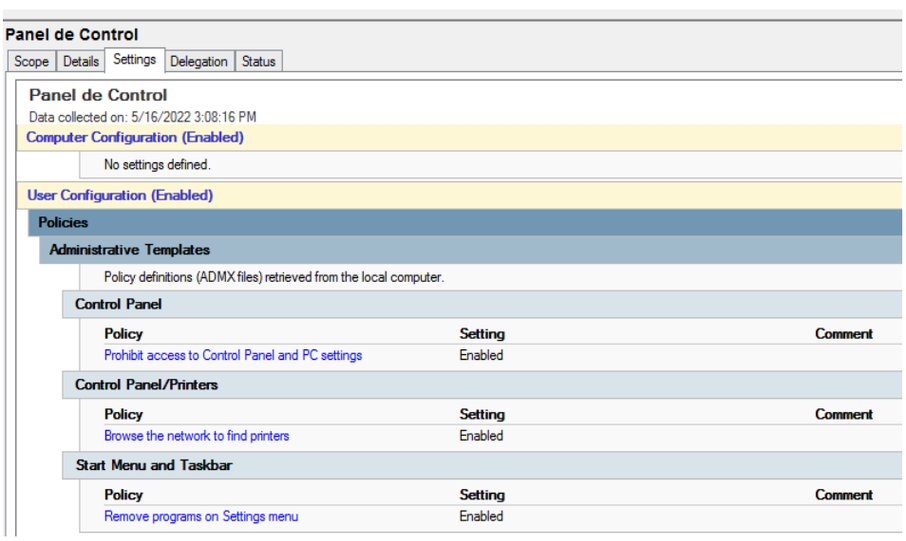
- Solo puede instalar aplicativos un usuario administrador
- La configuración se aplicará a los usuarios como a los computadores

Alcance de la Política



Se aplicará a todos los usuarios tanto contratistas como funcionarios de planta

8. POLÍTICA PANEL DE CONTROL



Las definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

Control Panel

- Se aplicará en la configuración de los computadores
- Se prohíbe el acceso al Panel de control y la configuración de los computadores

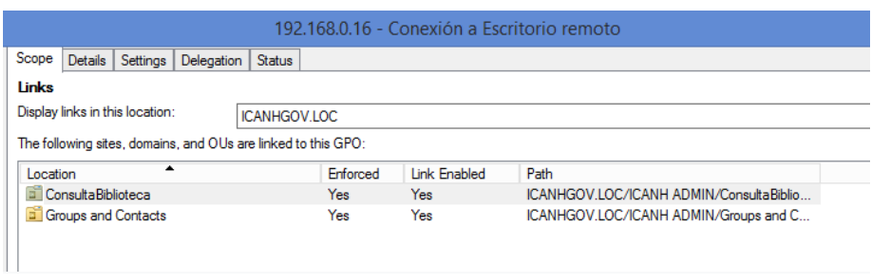
Control panel de impresoras

- Se puede explorar la red para encontrar impresoras

Menú de inicio y barra de tareas

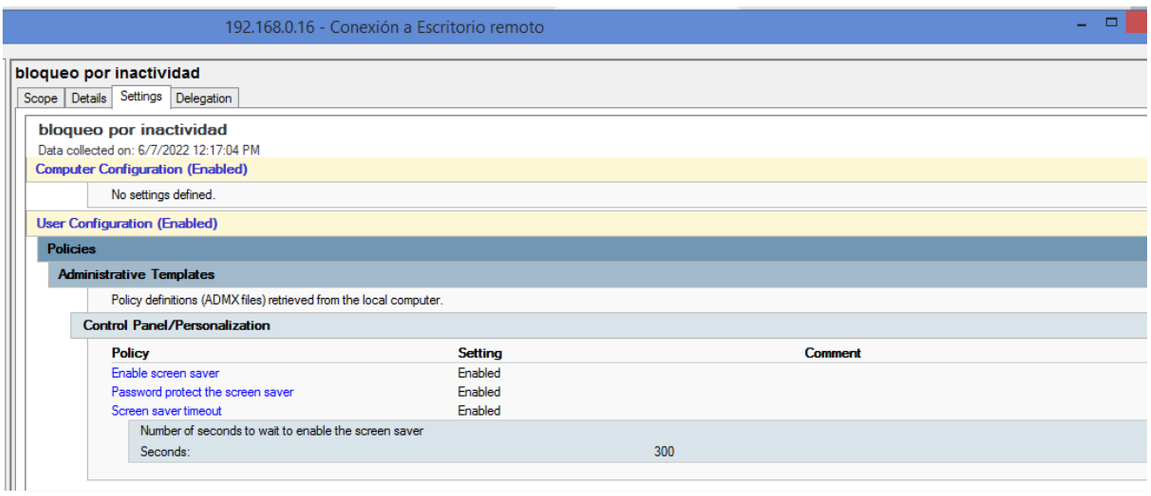
- Se elimina el acceso a las carpetas Panel de control, Instalación de Impresoras y del menú de inicio.

Alcance de la Política



- Se aplicará a usuario de consulta de biblioteca y a todos los usuarios pertenecientes a los diferentes grupos de ICANH y contacto

9. POLÍTICA DE INACTIVIDAD POR TIEMPO

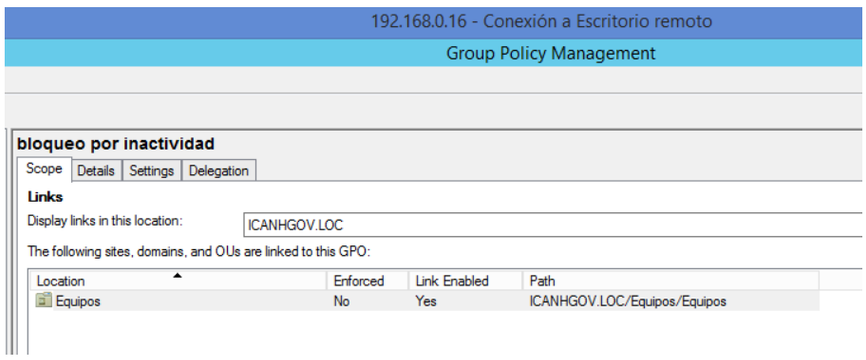


Las definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

Política para equipos locales

- Está activado el protector de pantalla
- Requiere de contraseña para desactivarlo
- Se activará el protector de pantalla después de inactividad de 300 segundos o 5 minutos

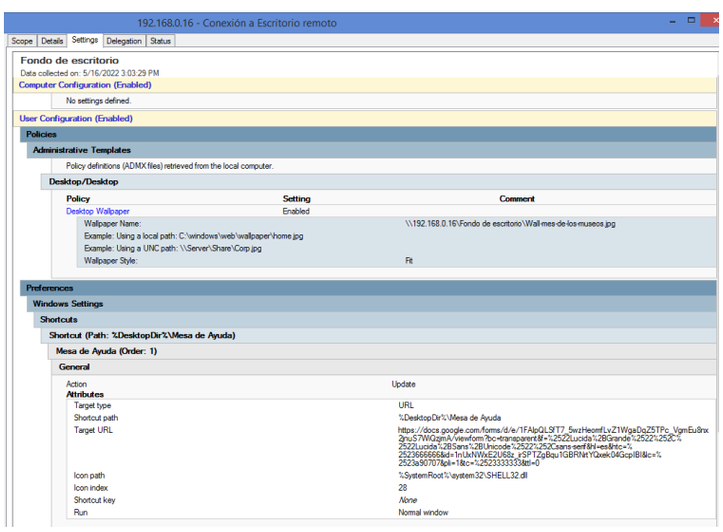
Alcance de la Política

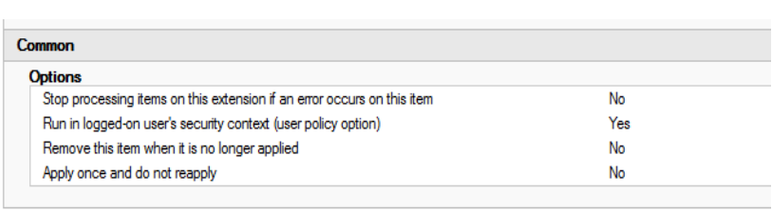


Se aplica a todos los equipos del ICANH

10. POLÍTICA FONDOS DE ESCRITORIO

(creados y enviados desde el servidor de dominio y son los fondos de escritorio en cada equipo, cuando se loguea)

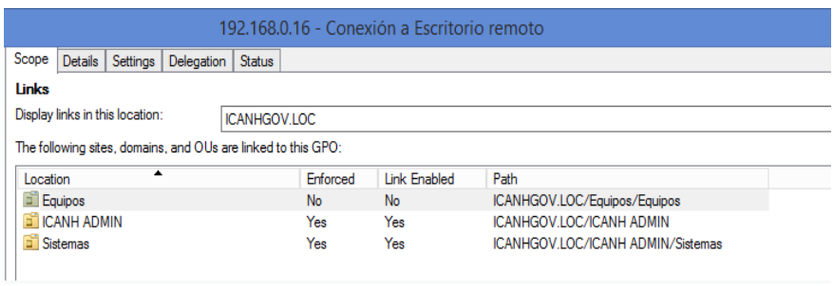




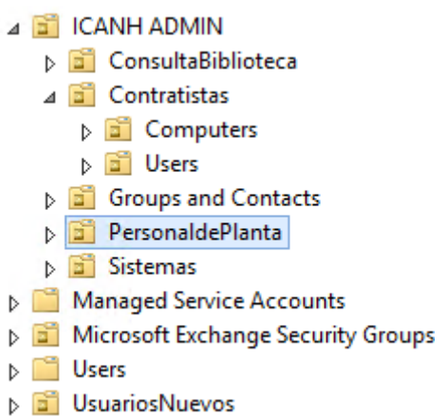
Definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

- El procesamiento del fondo de escritorio no se detiene si se produce un error en el intento de aplicarlo
- Ejecutar cuando el usuario haya iniciado sesión.
- No se puede remover el fondo de escritorio cuando se haya aplicado
- Se aplicará siempre.
- Crea en cada equipo un icono de la mesa de ayuda y lo vincula con un link a un documento de google

Alcance de la Política

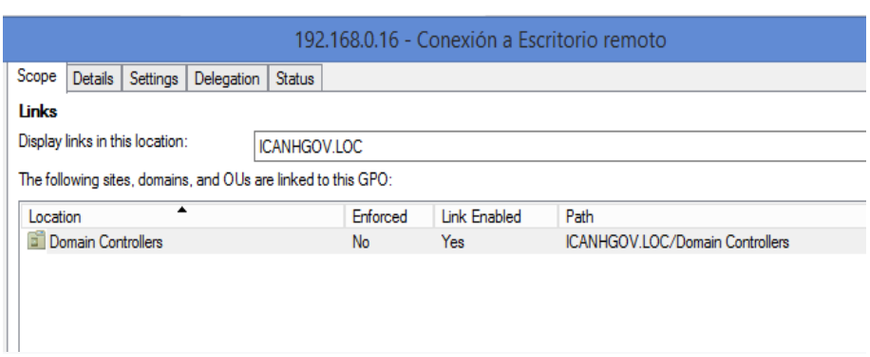


Se aplicará a todos los equipos del ICANH, a los que estén en el grupo ICANH ADMIN



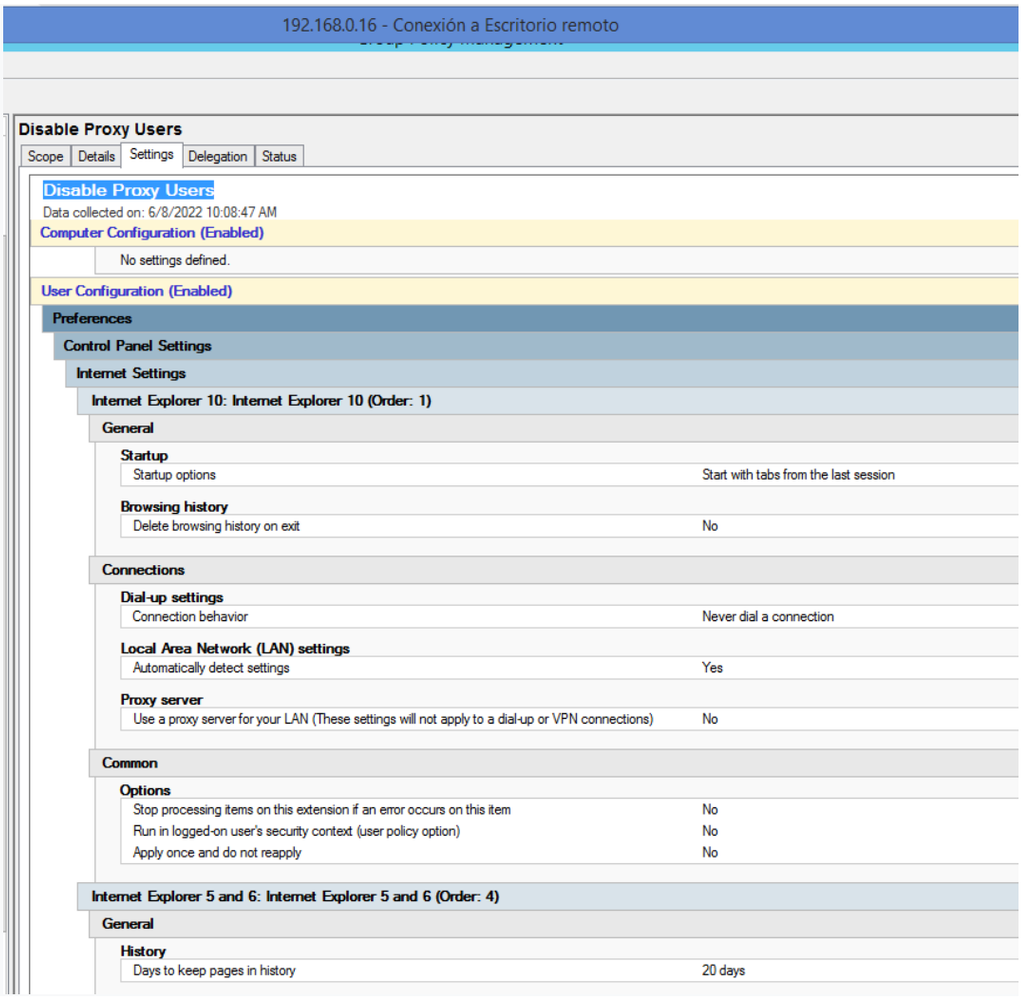
Es decir, se aplicará a todos los funcionarios, contratistas, a los grupos de contacto y a los computadores.

Alcance de la Política



Se aplicará al controlador de dominio

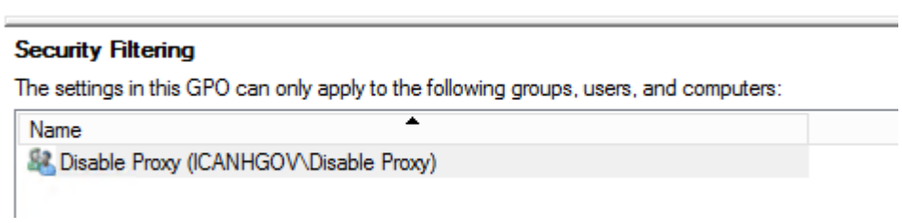
11. POLÍTICA DE DESABILITACIÓN DEL PROXY DE LOS USUARIOS



Esta política es la que permite la salida de los PC´s a internet y su configuración.

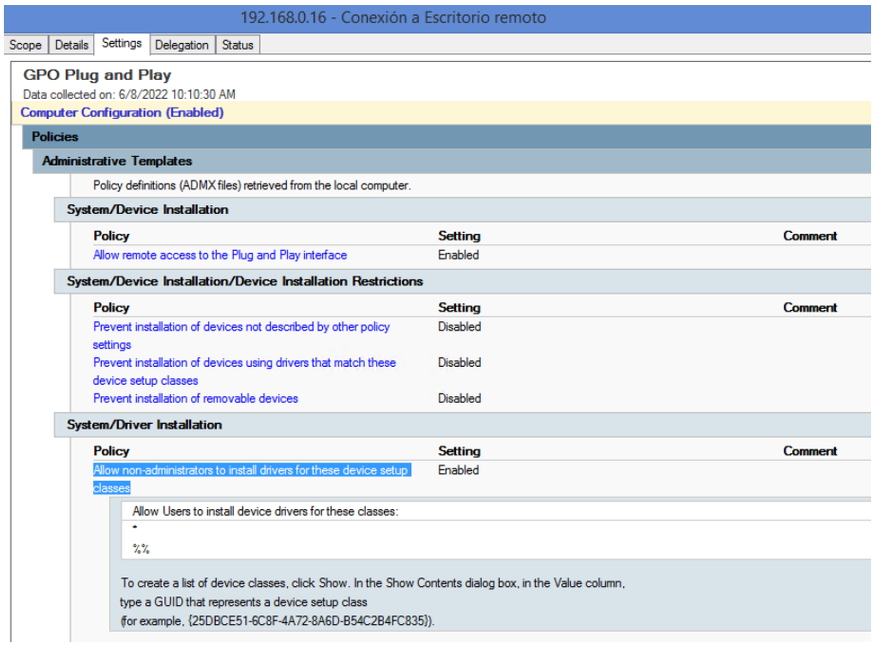
- La política se ejecuta al iniciar la sesión el usuario
- Detecta automáticamente la configuración
- No se puede Borrar el historial del proxy
- Para evitar que el usuario cambie la configuración del proxy, se deshabilita de la configuración del proxy en el equipo
- No se puede conectar a internet utilizando una VPN
- Guarda el historial de internet por 20 días

Alcance de la Política



Será aplicada a la configuración de todos los equipos y usuarios.

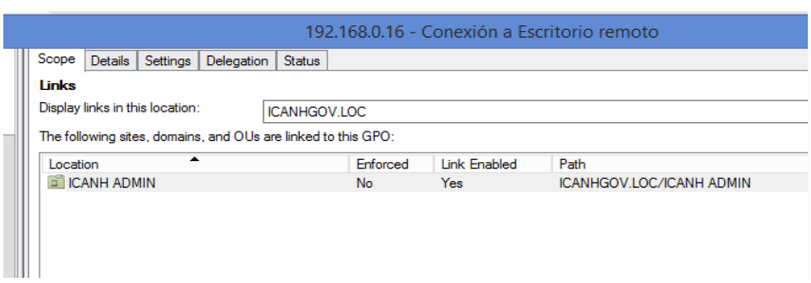
12. POLÍTICA DE PLUG AND PLAY.



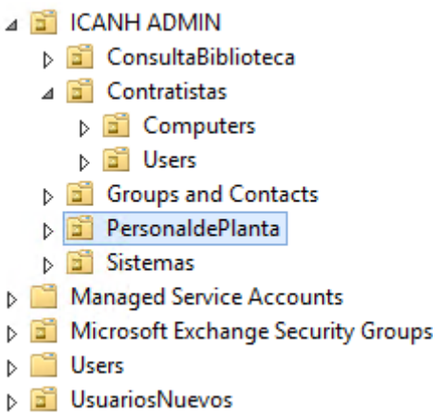
Las definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

- Permitir el acceso remoto a la interfaz de plug and play
- Impide la instalación de dispositivos en el equipo
- Prevenir la instalación de medios removibles
- Solo los administradores pueden instalar nuevos medios.

Alcance de la Política

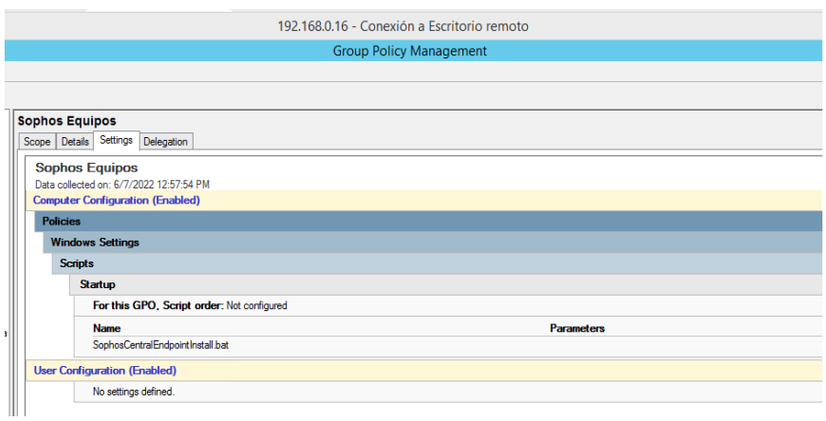


Se aplicará a todos los equipos del ICANH, a los que estén en el grupo ICANH ADMIN



Quiere decir que se aplicará a todos los funcionarios, contratistas, a los grupos de contacto y a los computadores.

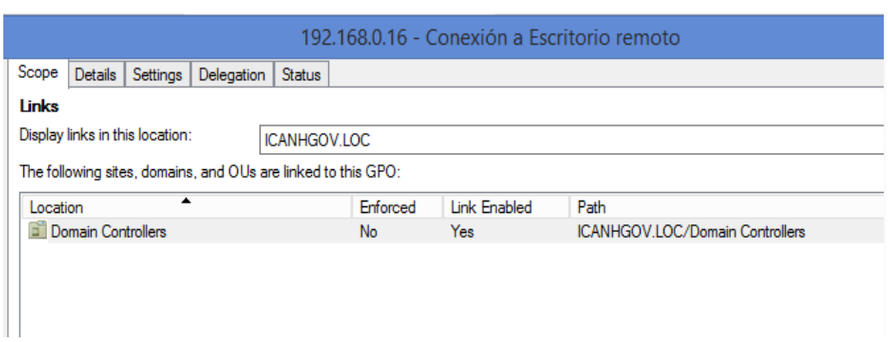
13. POLÍTICA DE ANTIVIRUS



Las definiciones de políticas (archivos ADMX) son almacenadas en el equipo local en el registro de Windows.

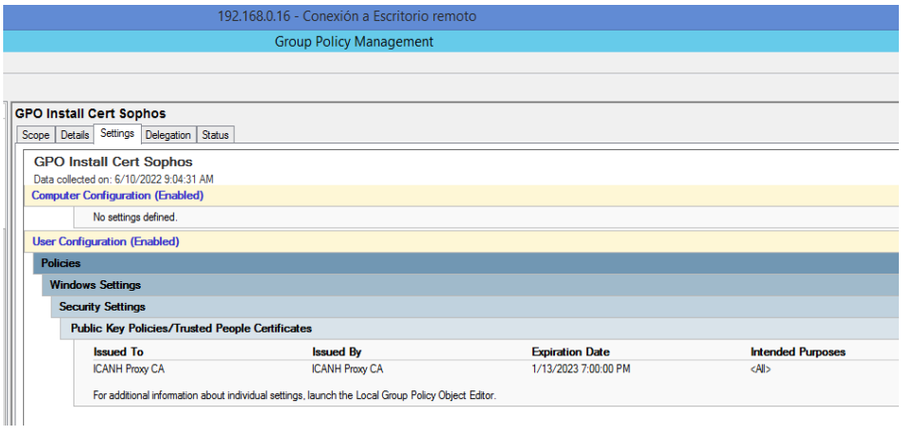
- Permite que la consola del antivirus pueda instalar el antivirus en cada equipo
- La política se aplicará utilizando un script, es una política de punto final y se ejecutará con un archivo llamado install.bat

Alcance de la Política

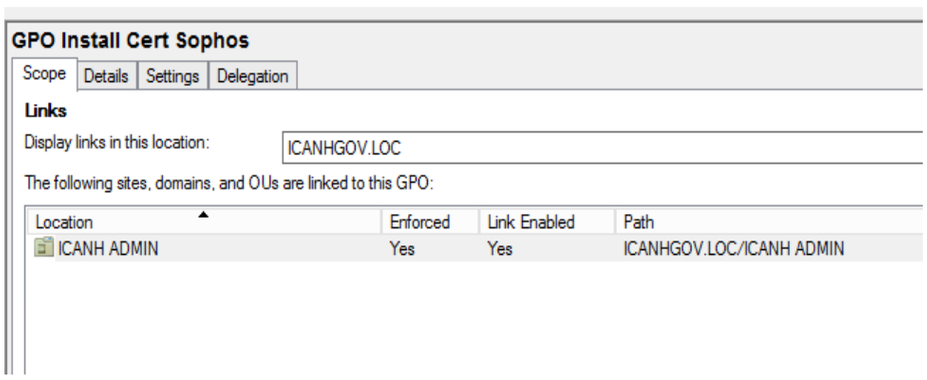


Se aplicará al controlador de dominio

14. INSTALACIÓN DEL CERTIFICADO DE SOPHOS



Alcance de la Política

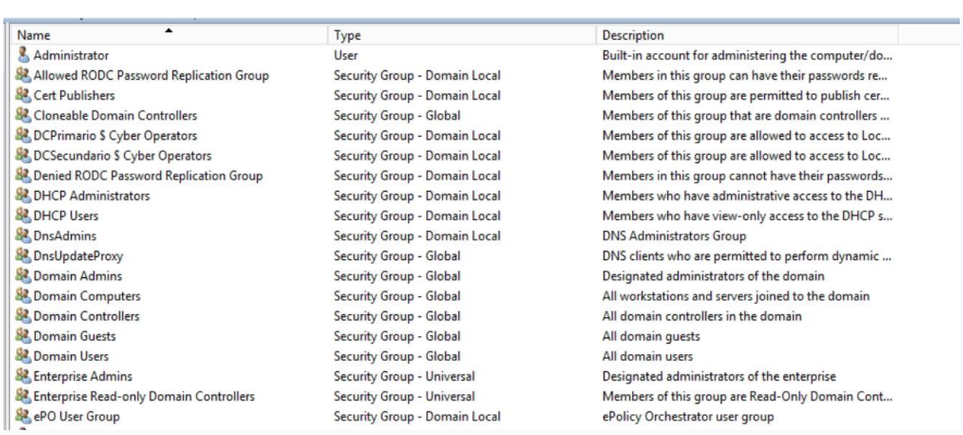


Se aplicará en todo el dominio

15. POLÍTICA DE ACCESO Y CONTROL DE USUARIOS

Cuando se define un nuevo usuario, se establece un vínculo entre el servidor de dominio utilizando para ello el Directorio Activo y un PC, al definir el usuario se establecen relaciones de confianza, las cuales se encuentran en diferentes grupos que trae por default el Windows Server como lo es el grupo de Distribución y el grupo de Seguridad.

Grupos definidos:



Name	Type	Description
Administrator	User	Built-in account for administering the computer/do...
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords re...
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish cer...
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers ...
DCPrimario $ Cyber Operators	Security Group - Domain Local	Members of this group are allowed to access to Loc...
DCSecundario $ Cyber Operators	Security Group - Domain Local	Members of this group are allowed to access to Loc...
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords...
DHCP Administrators	Security Group - Domain Local	Members who have administrative access to the DH...
DHCP Users	Security Group - Domain Local	Members who have view-only access to the DHCP s...
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic ...
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Cont...
ePO User Group	Security Group - Domain Local	ePolicy Orchestrator user group

En el domino ICANHGOV.LOC, solo se definió el grupo de seguridad, los cuales cuentan con un identificador de seguridad (SID). En consecuencia, pueden utilizarse en las ACL para controlar la seguridad de acceso a los recursos.

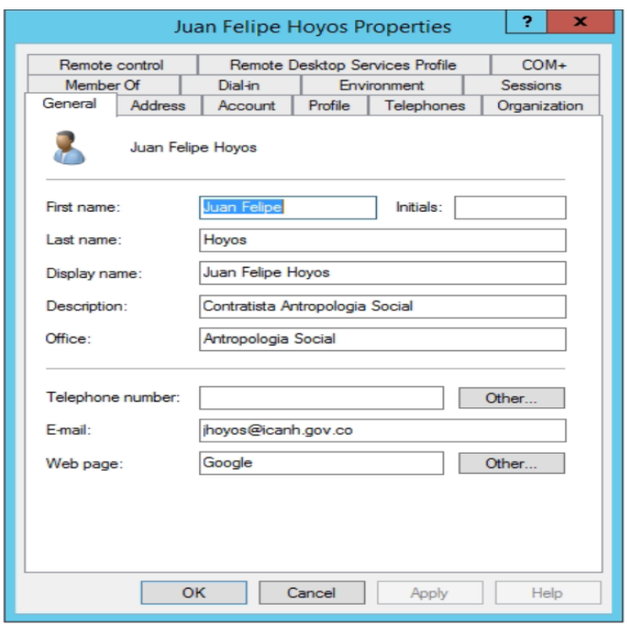
Existen tres tipos de usuario, en cada uno existen diferentes roles y esto determina el nivel de acceso al interior de un bosque de dominios o un solo dominio.

- **Grupo de seguridad local**, solamente puede otorgar derechos y permisos sobre los recursos que residen en el dominio, ejemplo para conceder a cinco usuarios acceso a una impresora determinada, ubicada dentro del dominio
- **Grupo de seguridad Global** es un grupo de seguridad o distribución que puede contener usuarios, equipo y grupos globales de su propio dominio, ejemplo, si tenemos un bosque de dominios y necesitamos que un usuario imprima en otro dominio el usuario debe pertenecer a este grupo.

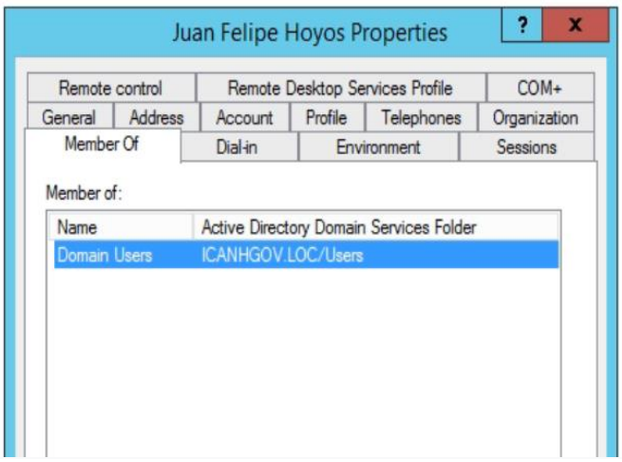
  De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque para que pueda utilizar cualquier recurso ubicado al interior del bosque.

- **Grupo Universal:** es un grupo de seguridad o distribución que puede contener usuarios, equipos, grupos universales y grupos globales de cualquier dominio del bosque

Cualquier cuenta de usuario que se cree en el dominio automáticamente se vuelve miembro de este grupo.



En la pantalla anterior vemos la definición de un usuario, en la pestaña Member of es donde se define a qué grupo pertenece



Solo pertenece al grupo de Domain User, que es a su vez miembro del Grupo global

Con la configuración de políticas de grupo creadas en el servidor y la clasificación de cada usuario se define la seguridad del entorno del ICANH.

16. BIBLIOGRAFÍA

Anexo B: cuentas con privilegios y grupos de Active Directory

Disponible en: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory

Grupos de seguridad de Active Directory

Disponible en: https://docs.microsoft.com/es-es/windows/security/identity-protection/access-control/active-directory-security-groups#bkmk-cloneabledomaincontrollers

Anexo I: Creación de cuentas de administración para cuentas protegidas y grupos en Active Directory

Disponible en: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/manage/component-updates/appendix-i--creating-management-accounts-for-protected-accounts-and-groups-in-active-directory

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción general del cambio**
01	2023-07-14	Se crea el documento con el fin de definir la del ICANH.

ELABORÓ:	REVISÓ:	APROBÓ:
Cargo: Profesional Área de Tecnologías y Sistemas de Información.	**Cargo:** Líder del Área de Tecnologías y Sistemas de Información. Profesional Secretaría General. Oficina Asesora de Planeación	**Cargo:** Secretaría General.
Fecha: 26/06/2023	**Fecha: 26/06/2023**	**Fecha: 14/07/2023**