1. OBJETIVO

Atender requerimientos relacionados con la implementación y funcionamiento del servicio de directorio activo, permitiendo el acceso e interconexión a los diferentes elementos que componen la red de la UAE DIAN.

2. DOCUMENTOS RELACIONADOS

Tipo de documento	Código	Titulo	Modo de uso	Clasificación documento
Procedimiento	PR-IIT-0460	Gestión de requerimientos	Digital	Interno

3. DEFINICIONES Y SIGLAS

- **Acceso privilegiado**. Acceso a un sistema de información con privilegios superiores a los otorgados a los usuarios normales del sistema, son los accesos que tiene, por ejemplo, los administradores del sistema.

  Fuente. UAE DIAN - Dirección de Gestión de Innovación y Tecnología.

- **Directorio Activo (DA) o (AD por sus siglas en ingles)**. Active Directory almacena información acerca de los objetos de una red y facilita su búsqueda y uso por parte de los usuarios y administradores. Active Directory usa un almacén de datos estructurado como base para una organización jerárquica lógica de la información del directorio.

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/ad-ds-getting-started

- **Bosque**. Un bosque es una colección de uno o varios dominios Active Directory que comparten una estructura lógica común, un esquema de directorio (definiciones de clase y atributo), una configuración de directorio (información de replicación y sitio) y un catálogo global (funcionalidades de búsqueda en todo el bosque). Los dominios del mismo bosque se vinculan automáticamente con relaciones de confianza transitivas y de dos vías.

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

- **Dominio**. Un dominio es una partición en un Active Directory de datos. La creación de particiones de datos permite a las organizaciones replicar datos solo en el lugar donde se necesitan. De esta manera, el directorio se puede escalar globalmente a través de una red que tenga un ancho de banda disponible limitado. Además, el dominio admite varias otras funciones principales relacionadas con la administración, entre las que se incluyen: Identidad de usuario en toda la red, Autenticación, Replicación.

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

- **Controlador principal de dominio (PDC)** - Para evitar que en Windows se produzcan actualizaciones conflictivas, Active Directory realiza las actualizaciones de ciertos objetos en un

modo de maestro único. En el modelo de maestro único, solo uno de los DC del directorio tiene permiso para procesar las actualizaciones. Es similar al rol dado de controlador de dominio principal (PDC) en versiones anteriores de Windows, como Microsoft Windows NT 3.51 y 4.0. En versiones anteriores de Windows, el PDC es responsable de procesar todas las actualizaciones de un dominio determinado.

Fuente: Consultado en https://learn.microsoft.com/es-mx/troubleshoot/windows-server/identity/fsmo-roles

- **Controlador de dominio (RODC)**. el controlador de dominio de solo lectura (RODC). Esto proporciona un controlador de dominio para su uso en sucursales donde no se puede colocar un controlador de dominio completo. La intención es permitir que los usuarios de las sucursales inicien sesión y realicen tareas como el uso compartido de archivos o impresoras incluso cuando no haya conectividad de red con sitios concentradores.

  Fuente: Consultado en https://learn.microsoft.com/es-mx/windows/win32/ad/rodc-and-active-directory-schema

- **Cuenta de usuario**. Una cuenta de usuario identifica de forma única a una persona que usa un sistema informático. La cuenta indica al sistema que aplique la autorización adecuada para permitir o denegar el acceso de ese usuario a los recursos. Las cuentas de usuario se pueden crear en Active Directory y en equipos locales, y los administradores los usan para: Represente, identifique y autentique la identidad de un usuario; Autorizar (conceder o denegar) el acceso a los recursos; Audite las acciones que se llevan a cabo en una cuenta de usuario.

  Fuente: Consultado en https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/understand-security-principals

- **Cuenta de equipo**. Por defecto, un equipo pertenece a un grupo de trabajo. Para poder iniciar una sesión en el dominio, el equipo debe pertenecer al dominio. Como con la cuenta de usuario, el equipo posee un nombre de inicio de sesión (atributo sAMAccountName), una contraseña y un SID. Esta información de identificación permite autenticar sobre el dominio a la cuenta de equipo. Si la autenticación se produce con éxito, se establece una relación de seguridad entre el controlador de dominio y el puesto

  Fuente: Consultado en https://www.ediciones-eni.com/open/mediabook.aspx?idR=a7ac08a5305b8c0948d416ef6d84bf5d.

- **POLFA**. Policía Fiscal y Aduanera.

- **Servidor de archivos**. Permite almacenar y compartir la información no estructurada (archivos de Word, Excel, PDF, imágenes, Visio, archivos de texto, etc…) en una ubicación del sistema informático.

  Fuente: Consultado en https://www.jmsolanes.net/es/servidor-de-archivos

- **Unidad Organizacional (UO)**. Las unidades organizacionales (UO) se pueden usar para formar una jerarquía de contenedores dentro de un dominio. Las unidades organizacionales se utilizan para agrupar objetos con fines administrativos, como la aplicación de la directiva de grupo o la delegación

de autoridad. Una OU es la unidad más pequeña dentro de un Dominio en la que le podemos asignar configuraciones de las directivas de grupo, adicionalmente permiten agrupar lógicamente objetos como cuentas de usuario, cuentas de servicio o cuentas de equipos.

Fuente: Understanding the Active Directory Logical Model. Consultado en https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

- **Usuarios**. Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

  Fuente: Consultado en https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

4. DESARROLLO DEL TEMA

1.1 Generalidades para atender solicitudes relacionadas con el directorio en la red

- La oficina de Seguridad de la información – OSI o quien haga sus veces, establece políticas en materia de seguridad, y con base en ellas los administradores implementan dichas políticas a través de las herramientas que contempla el directorio activo.

- Los controladores de dominio principal, secundario y los servidores requeridos para la prestación del servicio de directorio activo deben estar instalados y configurados previamente.

- El directorio activo se basa en una estructura jerárquica de objetos. Los objetos se enmarcan en tres grandes categorías: Recursos (p.ej. impresoras), Servicios (p.ej. recursos de archivos) y Usuarios (usuarios y grupos).

- Cada objeto del directorio activo representa una entidad individual, ya sea un usuario, un equipo, una fuente compartida de datos y sus atributos. Los objetos pueden contener otros objetos como las unidades organizacionales, en donde se ubican los usuarios en el directorio activo.

- El directorio activo permite que los usuarios tengan un único inicio de sesión independientemente del equipo que usen. A partir del ingreso del usuario y contraseña al Domino, cada usuario podrá acceder a los recursos de red a los que esté autorizado. Hay que tener en cuenta que los recursos de red pueden ser carpetas, archivos, equipos, servicios del directorio, etc. De igual manera, el servicio de terceros (aplicaciones desarrolladas por externo o contratistas) puede apoyarse en el directorio para su funcionamiento.

- En el directorio activo de la UAE DIAN, se tiene un bosque en el cual está un único dominio: DIAN.LOC, compuesto por servidores Controladores de Dominio – PDC y DC en el Nivel Central y Controladores de Dominio de solo lectura (RODC) en las Direcciones Seccionales más grandes del país. Estos, tienen como finalidad aumentar la seguridad y permitir un mejor servicio de autenticación en la red (logeo) por distribución geográfica. Los usuarios del directorio activo de la UAE DIAN corresponden a los usuarios internos y externos definidos en el presente documento.

- La distribución de las unidades organizacionales de usuarios y computadores en el directorio activo de la UAE DIAN está dada por las Direcciones Seccionales; en estas unidades organizacionales puede haber otras subunidades organizacionales para agrupar objetos con características comunes.

- Para obtener permisos de escritura en la carpeta pública, los Directores de Gestión, Subdirectores, o Jefes de Coordinación, según sea el caso, deberán realizar la solicitud a través de la herramienta de gestión de la mesa de servicio, indicando el nombre del usuario responsable de disponer información en la carpeta pública, como también el nivel de permisos (leer, escritura, modificación, etc). La información que puede ser almacenada en las carpetas públicas, será exclusivamente la relacionada con la gestión directa del área.

- Las solicitudes relacionadas con el directorio activo son recibidas a través de la herramienta de gestión de la mesa de servicio.

- Las solicitudes de creación de cuentas de usuario interno deben ser solicitadas por el jefe inmediato del usuario que requiere la cuenta.

- Las solicitudes de restablecimiento de contraseñas pueden ser realizadas directamente por el colaborador responsable de su cuenta de usuario.

- Previo a la asignación de los accesos privilegiados se deberá contar con la plena identificación del funcionario o usuario para corroborar la idoneidad del ejercicio de las funciones a su cargo, las necesidades del acceso con relación a las actividades fijadas, su ubicación y demás funciones asignadas. Los accesos privilegiados deben revisarse mensualmente por parte del Subdirector de Infraestructura Tecnológica y de Operaciones, para identificar cambios y privilegios no autorizados de acuerdo con las competencias del cargo.

1.2 Descripción de actividades para atender solicitudes relacionadas con el directorio en la red

- Recibir los requerimientos relacionados con el directorio en la red y llevar a cabo su clasificación.

  - ✓ Creación, actualización o eliminación de cuentas de usuarios.
  - ✓ Creación, actualización y/o modificación de los grupos de usuarios contenidos en la unidad organizacional usuarios en todas las seccionales.
  - ✓ Restablecimiento de contraseñas
  - ✓ Creación o eliminación de equipos de la unidad organizacional
  - ✓ Crear, modificar, eliminar colas de impresión.
  - ✓ Solicitar la creación de carpetas en la ruta denominada dian.loc\publiconc.

Para inactivación de usuario de red, el requerimiento se recibe a través de la herramienta de gestión de la mesa de servicio, por parte de la Subdirección de Gestión del Empleo Público o quien haga sus veces, donde se indican las personas que han sido retirados de la entidad.

- Gestionar la creación, actualización o eliminación de cuentas de usuarios acuerdo con el numeral 4.3 y 4.4. Si el requerimiento está relacionado con un usuario interno deberá ser ejecutado por la Coordinación de Soporte Técnico al Usuario o quien haga sus veces; si el requerimiento está relacionado con un usuario externo, refiriéndose a proveedores, pasantes, CGR, etc.) deberá ser

ejecutado por la Subdirección de Infraestructura Tecnológica y de Operaciones o quien haga sus veces.

- Cerrar el caso en la herramienta de gestión de la mesa de servicio.
- Mantener actualizada la base de conocimiento y la información de salud de la Plataforma.
- Elaborar informes de ajustes y novedades presentadas en el servicio de Directorio Activo. En este informe se consignan las configuraciones realizadas, los incidentes presentados en el servicio y la gestión realizada para su solución.

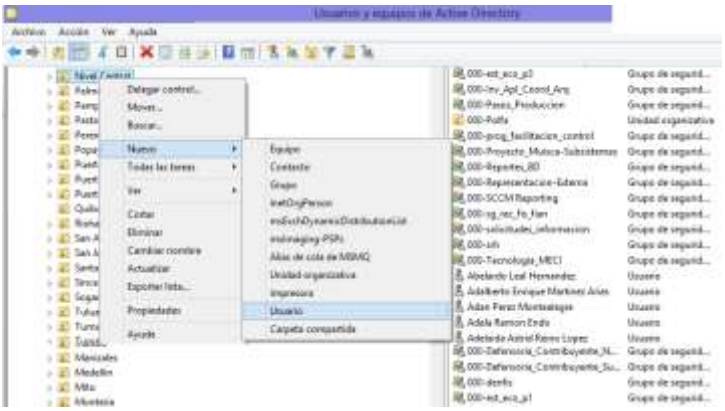
1.3 Generalidades para la creación de cuentas de usuario

- Los nuevos usuarios internos en la UAE DIAN, deben ser creados previa verificación de la creación de usuario en la planta de personal.
- Si los usuarios son externos, la creación se hará por el(os) responsable(s) de administrar el Directorio Activo. La razón es que ninguno de estos funcionarios trabaja funcionalmente en cada seccional y por ello no se ubican en la Unidad de Organización (UO) de usuarios.
- Si los usuarios son internos, la creación la realizará la Coordinación de Soporte Técnico al Usuario o quien haga sus veces, adscrita a la Subdirección de Soluciones y Desarrollo o quien haga sus veces.
- Las cuentas de usuario en el dominio Dian.loc se denominan de la siguiente forma: La inicial del primer nombre seguido del primer apellido e inicial del segundo apellido (si tiene).
- Para crear una cuenta de usuario se debe revisar en el Directorio Activo que su nombre de inicio de sesión o cuenta no tenga homónimos, esto puede hacerse mediante una búsqueda en la consola de administración del Directorio Activo o en el correo electrónico.
- Si tiene homónimos, debe incluirse un número consecutivo al final del nombre. Si existe una cuenta homónima, la nueva cuenta a crear deberá terminar en un número empezando con uno (1) y así sucesivamente.
- Los usuarios POLFA, se deben crear dentro de una sub-unidad organizacional la cual debe ser creada con el siguiente estándar: 0xx-polfa donde 0xx es el código de la seccional.
- Si se requiere un traslado de usuario, debe realizarse la solicitud para hacer el respectivo cambio de Unidad Organizacional y continuar con la actualización del perfil.
- La eliminación de usuarios no existe, se debe informar a los colaboradores responsables de administrar el Directorio Activo para realizar la inactivación de la cuenta.
- Las cuentas de usuario, así como las contraseñas son personales e intransferibles, estas contraseñas son la garantía de seguridad que tienen el Usuario y la entidad, de la información que ingresa, se consulta, se modifica y/o se elimina de las bases de datos; así mismo, debe tenerse en cuenta, que toda investigación que se lleve a cabo por el uso de las soluciones tecnológicas, recaerá

sobre el Usuario propietario de la cuenta de usuario con el cual se hayan realizado acciones sobre el sistema y que se encuentre identificado dentro del mismo.

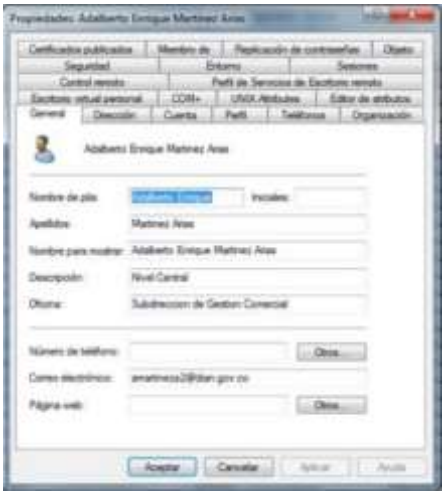
1.4 Pasos para crear una cuenta de usuario

- Para crear un usuario se debe usar la herramienta Centro de Administración de Directorio Activo. Debe ubicarse en la Unidad Organizativa Usuarios e ir a la UO de la seccional correspondiente. Clic Derecho -> Nuevo -> Usuario



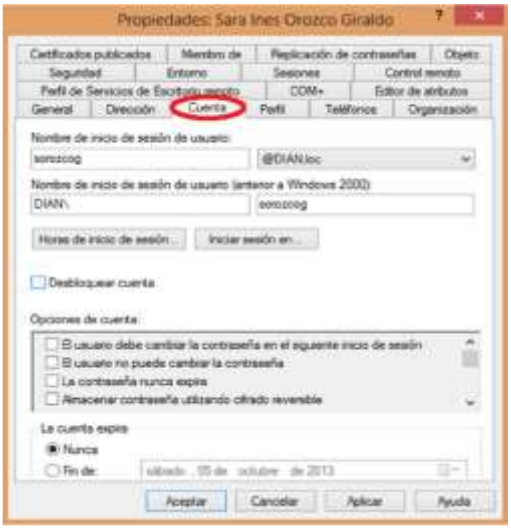
- En la pestaña General deben diligenciar toda la información que se observa en la siguiente imagen.

Descripción: Es la unidad organizacional a la que pertenece; debe ir la primera letra en mayúscula y el resto en minúscula y el correo electrónico.

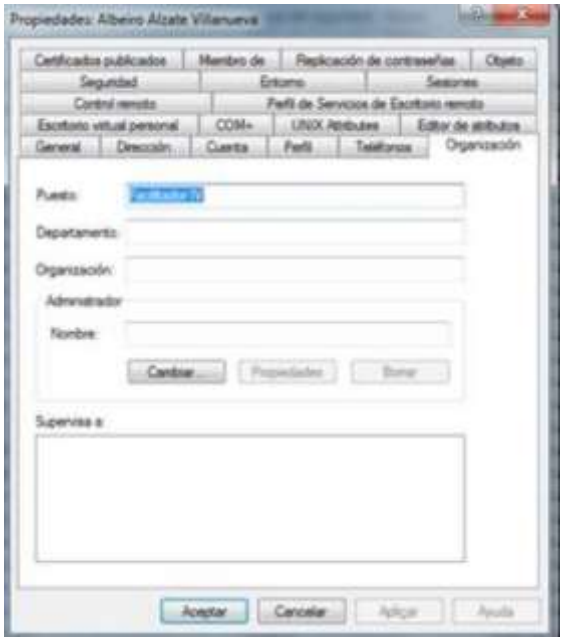


- En la pestaña Dirección se debe colocar el número de cédula en el espacio de apartado postal y en ciudad el nombre de la ciudad.

- La pestaña Cuenta debe aparecer de la siguiente manera.



- En la pestaña Organización en la casilla Puesto se coloca el empleo del colaborador a quien se le creará la cuenta, de acuerdo con el rol del empleo asociado publicado en la Diannet.



1.5 Pasos para crear una Impresora

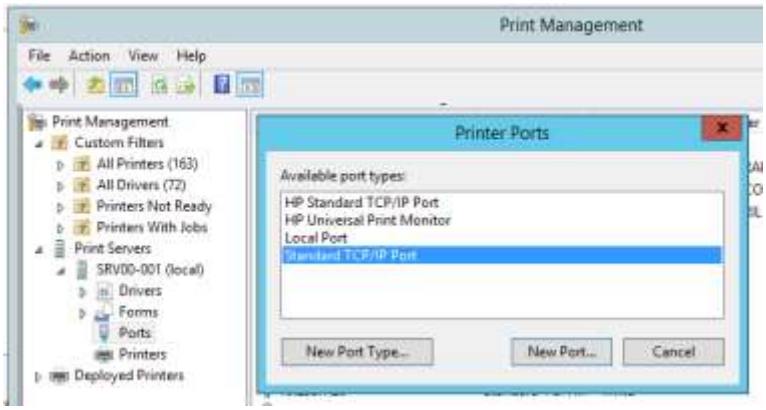
La creación de Impresoras en Red se realiza en el servidor de Impresión que para el caso de nivel central es el SRV00-001; para las diferentes seccionales el servidor es el identificado como SRVXX-002, donde XX es el Código de la Seccional. Para crear la impresora de red se requiere:
Nombre: Con el siguiente estándar IXXXAAAA-00C, donde XXX es el código de la seccional, AAAA es la identificación de la dependencia donde se instalará, y C es el consecutivo

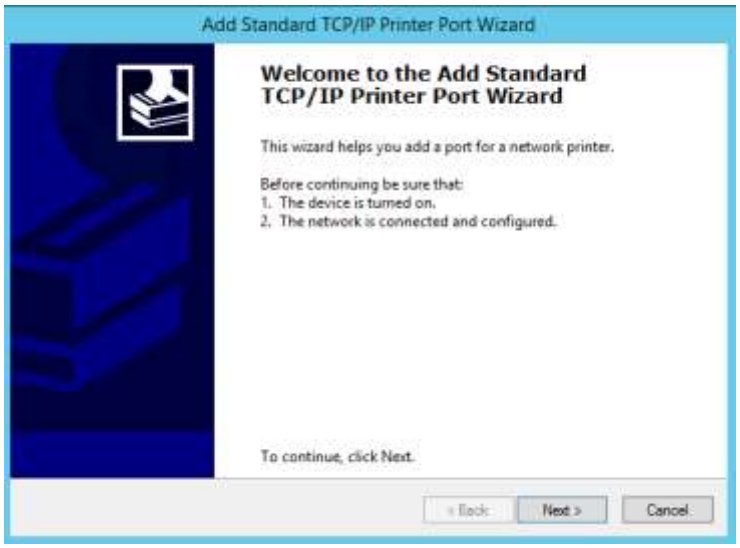
Dirección IP: Depende de la red o subred donde se conecte físicamente la impresora.

Se crea de la siguiente manera, haciendo uso de la herramienta Print Manager:

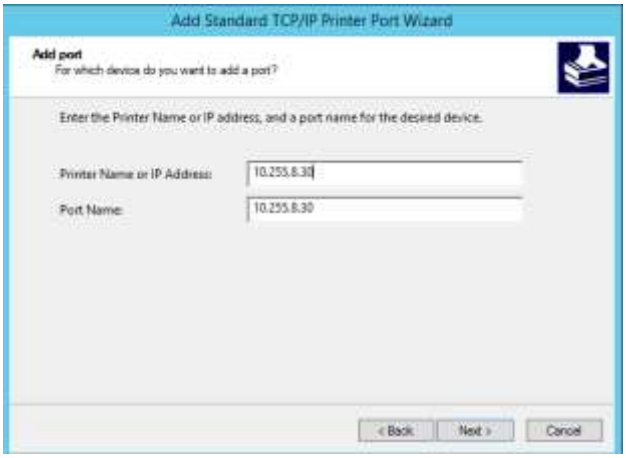
- Debemos asegurar que el puerto identificado con la IP que se le va a asignar esté creado en el servidor. Si no está, el puerto se crea así:

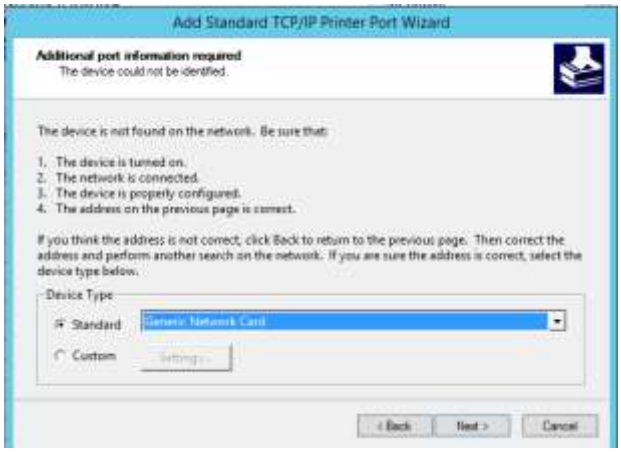
Por la opción Ports / click derecho Add Port… / Seleccionar Standard TCP/IP Port / New Port.. / Next



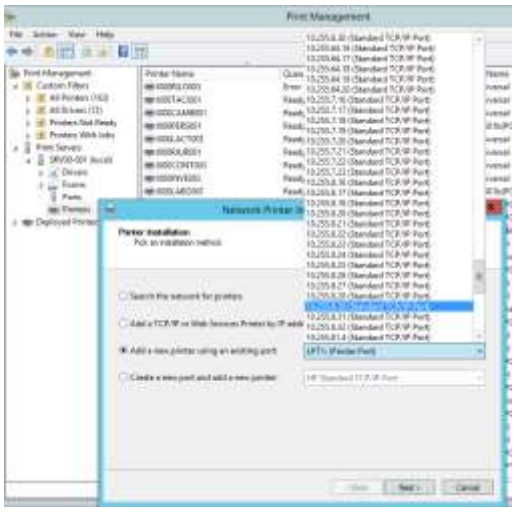


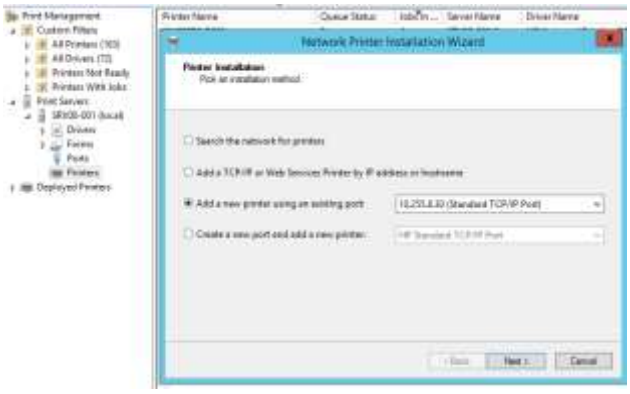
- Digitamos la IP que se va a asignar / Next / Generic Network Card / Finish



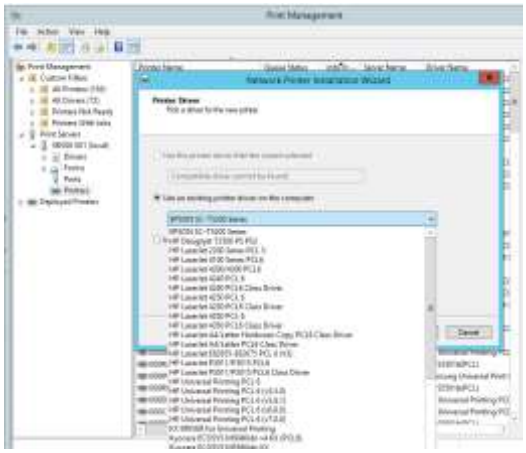


- Ahora creamos la Impresora así: **Printers** / Clic derecho **Add Printer**… / Add a new printer using an existing port / seleccionamos el puerto que vamos a asignar

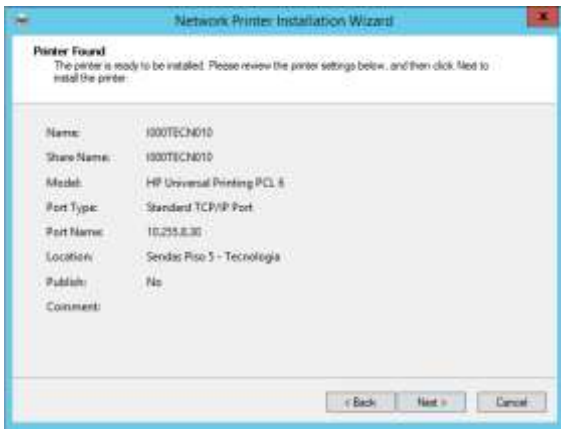




- Luego seleccionamos el **driver** que vamos a configurar; esto dependen de la marca y modelo de la impresora física.

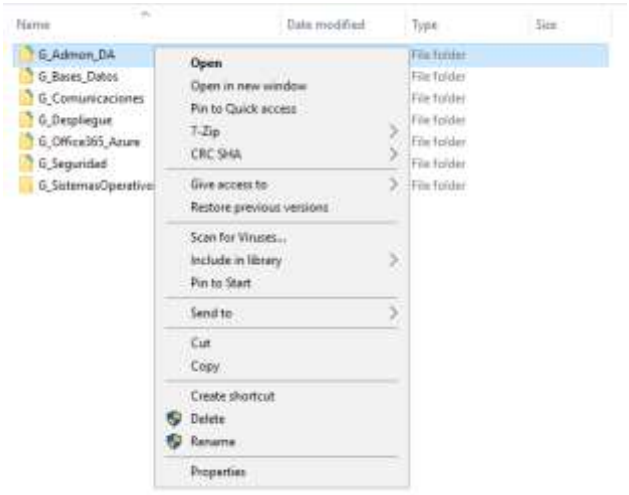


- Especificamos el nombre que se le va a asignar y se marca la opción de compartir; se comparte con el mismo nombre. En el campo **Location** se identifica el Edificio, piso y dependencia. Next / Next

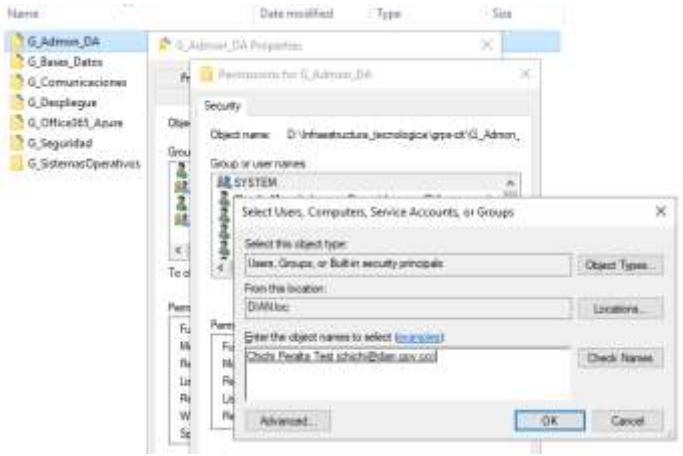


1.6 Pasos para asignar permisos sobre carpeta publica

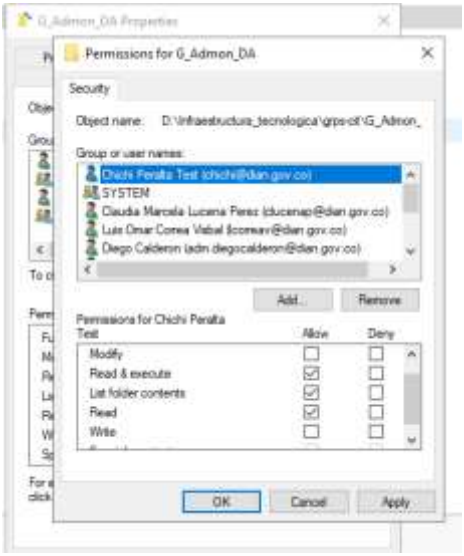
- Una vez se recibe la solicitud, se ingresa al servidor donde se encuentra la carpeta que especifican, dar clic derecho / **Properties**



- Seleccionar la pestaña **Security** / **Edit** / **Add /** se escribe el **nombre del funcionario** o cuenta de red / **OK**



- Por último, se selecciona el tipo de permiso que se va a dar (lectura y ejecución / escritura / modificación) y OK



5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de Cambios	Tipo de información
	Desde	Hasta		
1	10/09/2021	14/11/2022	Versión inicial, Se deroga el procedimiento PR-SI-0139 Administración del directorio en la red. Se deroga el instructivo IN-SI-0011 Creación de cuentas de usuario.	No aplica
2	15/11/2022		Versión 2 que reemplaza lo establecido en la versión 1. Se cambió el nombre del documento, se actualizaron las definiciones y el desarrollo del tema. Se actualiza la plantilla del presente documento, de acuerdo con la versión 5 del procedimiento "*PR-PEC-0001 Documentación del sistema de gestión*".	Esta versión corresponde a información pública

Elaboró:	Diego Mauricio Calderón Pérez **Elaboración técnica**	Inspector I	Subdirección de Infraestructura Tecnológica y de Operaciones

	Juan Pablo Serna Botero **Elaboración técnica**	Gestor IV	Coordinación Centro de Gestión de Proyectos de Innovación y Tecnología CENIT
	Tito Alejandro Menjura **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
	Alfredo A. Ahumada A. **Elaboración Metodológica**	Gestor II	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Olga Lucía Hurtando Hurtado	Inspector III	Subdirección de Infraestructura Tecnológica y de Operaciones
Aprobó:	Héctor Leonel Mesa Lara	Subdirector	Subdirección de Infraestructura Tecnológica y de Operaciones