

DISEÑO DE DIRECTORIO ACTIVO PARA LA SECRETARÍA DE SALUD
MUNICIPAL DE NEIVA

NESTOR IVAN CABRERA CARDOZO
CRISTIAN ANDRÉS PARRA CABRERA

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
NEIVA
2016

DISEÑO DE DIRECTORIO ACTIVO PARA LA SECRETARÍA DE SALUD
MUNICIPAL DE NEIVA



NESTOR IVAN CABRERA CARDOZO
CRISTIAN ANDRÉS PARRA CABRERA

Informe Final de Seminario Taller de Perfeccionamiento presentado como requisito
para optar el título de INGENIERO DE SISTEMAS

Asesor
PhD. MATEO LEZCANO

UNIVERSIDAD COOPERATIVA DE COLOMBIA
FACULTAD DE INGENIERÍAS
PROGRAMA DE INGENIERÍA DE SISTEMAS
NEIVA
2016

NOTAS DE ACEPTACIÓN

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Neiva, Enero de 2016

CONTENIDO

	Pág.
INTRODUCCION	11
1. PLANTEAMIENTO DEL PROBLEMA	14
1.1 DESCRIPCION DEL PROBLEMA	14
1.2 FORMULACION DEL PROBLEMA	14
2. JUSTIFICACION	15
3. OBJETIVOS	17
3.1 OBJETIVO GENERAL	17
3.2 OBJEIVOS ESPECIFICOS	17
4. MARCO REFERENCIAL	18
4.1 ESTADO DEL ARTE	18
4.2 MARCO TEORICO	24
4.2.1 Directorio	24
4.2.2 Directorio activo	25
4.2.3 Servicio de Directorio	26
4.2.4 Dominio	26
4.2.5 Objeto	27
4.2.6 Controlador de Dominio	28

4.2.7	Árboles	29
4.2.8	Bosque	29
4.2.9	Unidad Organizativa	30
4.2.10	Esquema	31
4.2.11	Sitio	31
4.2.12	Relaciones de Confianza	31
4.2.13	Control de acceso con Directorios	31
4.2.14	Seguridad	32
4.2.15	Control de Acceso	32
4.2.16	Políticas de Grupo (GPO)	33
5.	CRONOGRAMA DE ACTIVIDADES.	34
6.	RESULTADOS	35
6.1	FASE I – ENTENDIMIENTO DEL ENTORNO DE LA EMPRESA	35
6.1.1	Organigrama	35
6.1.2	Identificación de la estructura de la red	36
6.1.3	Objetos y recursos de la red	37
6.1.4	Identificación del software instalado	38
6.2	FASE II-DISEÑO DE DIRECTORIO ACTIVO	39
6.2.1	Estructura física	40
6.2.2	Estructura lógica	40
6.2.3	Carpetas y permisos	42
6.2.4	Políticas de grupo (GPO)	43

7. PRESUPUESTO	45
8. CONCLUSIONES	46
BIBLIOGRAFÍA	47

LISTA DE TABLAS

	Pág.
Tabla 1. Componentes	24
Tabla 2. Equipos de la red	37
Tabla 3. Impresoras de la red	37
Tabla 4. Recursos de la red	37
Tabla 5. Software instalado	38
Tabla 6. Presupuesto	45

LISTA DE FIGURAS

	Pág.
Figura 1. Dominio	26
Figura 2.Objeto	27
Figura 3. Controlador de dominio	28
Figura 4.Árbol	29
Figura 5.Bosque	30
Figura 6. Unidad Organizativa	30
Figura 7.Actividades	34
Figura 8.Organigrama de la Secretaria de Salud Municipal	35
Figura 9. Estructura de red	36
Figura 10.Diseño de directorio activo	39
Figura 11.Jerarquía de carpetas	42
Figura 12.Estructura Lógica con GPO Generales	44

PALABRAS CLAVES

IP, Servidor, Windows Server, Dominio, Controlador de dominio, Directorio Activo

RESUMEN

Para realizar el diseño del directorio activo de la Secretaria de Salud Municipal de Neiva, es importante definir un objetivo principal el establecimiento de normas y políticas que controlen el acceso y el uso de la información, para lo cual se debe contar con herramientas o servicios que ayuden en la administración del software y hardware que forma parte de cualquier red de computadoras corporativa.

La primera etapa del proyecto se destina a buscar los componentes principales para la implementación del servicio de directorio activo de la familia del sistema operativo Windows Server, tales como: Controladores del dominio, Sitios, Subredes, Dominio, Bosque, Arboles y Unidades organizativas. Después de haber especificado los puntos antepuestos, es significativo especificar que el objetivo principal de este proyecto es diseñar un directorio activo para la Secretaría de Salud del Municipio de Neiva que permita afrontar los problemas de seguridad corporativa.

En la etapa final, se efectúa el entendimiento del entorno de la empresa, donde se identificara la estructura de la red, recursos de la red, unidades organizativas y grupos. De la misma manera se presenta el diseño del directorio activo el cual modelara y se adaptará en una base de datos especializada que contendrá la información de las propiedades y ubicación de los diferentes tipos de recursos dentro de la red, lo cual permitirá una mejoría en la gestión de la seguridad de la empresa al asegurar la confidencialidad, integridad y disponibilidad de la información.

INTRODUCCION

Windows Server es la línea de productos para servidores, desarrollada por Microsoft Corporation, empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gates y Paul Allen que se dedica al sector del software y el hardware. La plataforma Windows Server es una poderosa herramienta que proporciona una infraestructura de aplicaciones para el trabajo en redes de computadoras.

Windows Server 2012 R2 es la última edición de la familia de sistemas operativos para servidores de la Microsoft y es el sucesor de Windows 2012 (ya se está trabajando en la nueva versión 2016).

La versión Server 2012 R2, combina la experiencia de Microsoft en la prestación de servicios en la nube a escala global en una infraestructura, junto con las nuevas características y mejoras en la virtualización, la administración, el almacenamiento, las redes, la infraestructura del escritorio virtual (VDI), la protección de la información y del acceso a la plataforma de aplicaciones y web.

Entre las características de este sistema operativo se destaca el Active Directory (Directorio Activo), que es una base de datos especializada o repositorio de datos en donde se almacenan datos claves del sistema operativo, como son la ubicación de los diferentes tipos de recursos dentro de la red.

El directorio activo se basa en un conjunto de protocolos y facilidades que permiten manejar apropiadamente la estructura de directorio de la red, entre las cuales se destacan las siguientes:

- El LDAP (protocolo ligero de acceso a directorios), es un protocolo estándar que permite la consulta de información contenida en directorios.
- ADSI (interfaces de servicio de active directorio) es un conjunto de herramientas de Microsoft, con interfaz orientada a objetos, que permite el acceso a las características de Active Directory Domain Services (servicio de dominio de directorio activo). ADSI maneja una estructura jerárquica que facilita el establecimiento de políticas a nivel empresarial, desplegar aplicaciones en varias terminales almacenando información en bases de datos centralizadas.
- DNS (Domain Name System), servicio de nombres de dominio que permite la administración de los computadores, constituyéndose en el servicio de asignación y resolución de nombres en internet.
- Kerberos, es un protocolo utilizado para la autenticación de los usuarios y maquinas.
- Certificados X.509, estándar que permite distribuir información a través de la red de forma segura.

La estructura del directorio activo posee dos componentes: físicos y lógicos, que se detallan a continuación.

Los componentes lógicos están constituidos por los elementos siguientes:

Dominio. Colección de objetos que forman un subconjunto administrativo.

Bosques. Es el mayor contenedor lógico dentro del directorio activo, abarca todos los dominios y los interconecta por relaciones de confianza, lo que permite a los dominios de un bosque confiar automáticamente en otros. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos identificados con sus colecciones de objetos y unidades organizativas.

Árboles. Colección de dominios que depende de una raíz común, se organizan en forma jerárquica.

Unidades organizativas. Contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio. Estableciendo una estructura lógica que representa de forma adecuada la organización y simplifica la administración.

En los componentes físicos se enmarcan los elementos siguientes:

Controladores del dominio. Contienen la base de datos de objetos del directorio para un determinado dominio, incluyendo la información relativa de seguridad siendo la responsable de la autenticación de objetos de su ámbito de control.

Sitios. Agrupación de computadoras ordenadas de formas lógicas y manipuladas por un controlador de dominio, puede estar en la misma zona.

Cuando se trata del acceso a la información existen dos puntos de vistas que pueden estar encontrados, por una parte están los empleados y socios de cualquier entidad que necesitan acceder desde sus dispositivos personales a los datos corporativos para poder realizar actividades remotas, tales como: comprobar el correo electrónico o utilizar aplicaciones empresariales avanzadas, entre otras; por otra parte los administradores de TI (tecnologías de información) de las organizaciones desean permitir ese nivel de acceso pero es necesario controlar los riesgos que conllevan las actividades de acceso de los primeros.

La información, en general, y el conocimiento en particular es el bien más importante de cualquier entidad, el presente trabajo tiene como objeto de estudio los servicios informáticos de la Secretaría de Salud Municipal de Neiva.

La mencionada institución garantiza los servicios informáticos con un conjunto de recursos, de hardware y software, entre los que cabe destacar un servidor HP ProLiant ML210e con sistema operativo Windows Server 2008 R2 instalado. Dicho servidor no usa las facilidades que proporciona el directorio activo, lo cual conspira contra el manejo adecuado de la información que se almacena en bases de datos

centralizadas y también dificulta la creación de políticas de seguridad a nivel empresarial.

Tomando en cuenta las inconsistencias enunciadas anteriormente, se diseñará un directorio activo que establecerá la comunicación entre los objetos de la red. El diseño permitirá la organización jerárquica de los directorios y contribuirá a mejorar las tareas de administración, a la vez que facilitará el acceso a la información. Todo lo cual incidirá positivamente en la seguridad corporativa, desde el punto de vista informático, de la Secretaría de Salud Municipal de Neiva.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCION DEL PROBLEMA

El estudio hecho al sistema informático de la Secretaría de Salud Municipal de Neiva, permitió detectar los problemas siguientes:

- Se desaprovecha la operatividad del Servidor HP ProLiant ML210e sobre el cual está instalado el sistema operativo Windows Server 2008 R2.
- No está establecido el directorio activo, sin el cual no existen objetos tales como: usuarios, equipos, grupos, que facilitarían los inicios de sesión de equipos conectados y la administración de políticas en toda la red.
- No existen estrategias de seguridad que ayuden a proteger los documentos.
- No están implementados servicios que simplifiquen el acceso a los sistemas y las aplicaciones, mediante mecanismos de autenticación y autorización de acceso.
- No existe una infraestructura escalable ni segura, lo que dificulta la administración de la información de los recursos de la red y de los datos.
- No existen Directivas de Grupo (GPO) que especifiquen las configuraciones de los usuarios y/o equipos.

1.2 FORMULACION DEL PROBLEMA

El presente trabajo se traza la meta de resolver las fallas detectadas y enunciadas anteriormente y para enfrentar el problema se hace la siguiente pregunta de investigación. ¿El diseño del directorio activo, protegerá la confiabilidad, integridad y disponibilidad de la información de la Secretaría de Salud del Municipio de Neiva?

2. JUSTIFICACION

El avance continuado que han tenido las tecnologías de la información y las comunicaciones y su uso masivo dentro de cualquier institución o empresa es una realidad del mundo empresarial del día de hoy. Ese avance ha traído, sin lugar a dudas grandes beneficios, pero debe tenerse sumo cuidado con el uso de los recursos porque las malas políticas pueden conducir a peligros diversos.

Es por eso que resulta muy importante el establecimiento de normas y políticas que controlen el acceso y el uso de la información, para lo cual se debe contar con herramientas o servicios que ayuden en la administración del software y hardware que forma parte de cualquier red de computadoras corporativa.

La Secretaría de Salud Municipal de Neiva realiza diversos procesos que están asociados al servicio que presta y muchos de ellos se hacen a través de su red de computadoras, en la cual no existe una estructuración adecuada que permita garantizar el acceso con seguridad a uno de sus bienes más preciado, la información.

Por los motivos apuntados anteriormente, el directorio activo, debe ser, y de seguro, será una herramienta útil para acceder y controlar el flujo informativo de la entidad, al establecer una base de datos distribuida que almacenará y organizará los elementos de red en una estructura de contención jerárquica que permitirá manejar y administrar adecuadamente el acceso a los diversos recursos compartidos, estableciendo los siguientes servicios:

- Intensificar la seguridad de la organización instaurando el servicio Active Directory Rights Management Services (AD RMS), que protegerá documentos mediante la implementación del servicio de manejo de derecho de la información (Information Rights Management -IRM) que controla los permisos de acceso a documentos, libros y presentaciones de forma que se impida, a personas no autorizadas, imprimir, reenviar o copiar la información confidencial.
- Simplificar el acceso a sistemas y aplicaciones mediante el mecanismo de autenticación y autorización de acceso basado en notificaciones, para mantener la seguridad de las aplicaciones implantando los servicios de federación de Active Directory (ADFS).
- Crear una infraestructura escalable, segura y administrable para los recursos de la red y los datos específicos de las aplicaciones habilitadas, constituyendo los servicios de dominio de Active Directory (AD DS).

- Implementar Directivas de Grupo (GPO) que especificarán las configuraciones de los usuarios y/o equipos, obteniendo el control de los equipos de la red, estableciendo configuraciones para los distintos componentes de sistema operativo.

La implementación del directorio activo permitirá una mejoría en la gestión de la seguridad de la empresa al asegurar la confidencialidad, integridad y disponibilidad de la información, todo lo cual impactará positivamente en la visión que tienen los usuarios de los servicios brindados por la entidad objeto de estudio.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un directorio activo para la Secretaría de Salud del Municipio de Neiva que permita afrontar los problemas de seguridad corporativa.

3.2 OBJETIVOS ESPECIFICOS

- Identificar los recursos, unidades funcionales y grupos de usuarios de la Secretaria Salud Municipal de Neiva.
- Identificar políticas de seguridad de la información que garanticen la finalidad de un SGSI (sistemas de gestión de seguridad de la información).
- Presentar el diseño del directorio activo.

4. MARCO REFERENCIAL

4.1 ESTADO DEL ARTE

Las versiones de Microsoft Exchange 4.0 hasta la 5.5 fueron las que dieron inicio al servicio de dominio de directorio activo que se basa en el estándar X.500 de servicios de directorio.

El estándar X.500 es un conjunto de recomendaciones para que los diseñadores de servicios de directorio puedan elaborar productos de forma conjunta. Está compuesto de los siguientes protocolos:

- Directory Access Protocol (DAP)
- Directory System Protocol (DSP)
- Directory Information Shadowing Protocol (DISP)
- Directory Operational Binding Management Protocol (DOP)

Para la familia de sistemas operativos Microsoft, el servicio de dominio de directorio activo se inició como una de sus características principales de Windows 2000 Server, Novell había desarrollado un producto similar en 1993 (siete años antes) y por eso Microsoft tuvo la ventaja de aprovechar los avances que habían alcanzados los servicios de directorio hasta ese momento.

Ya para el lanzamiento de Windows 2003 Server, el directorio activo contaba con varias mejoras como las que se describen a continuación:

- **Drag and Drop:** a diferencia de la versión en Windows 2000 Server, esta nueva versión permite arrastrar un objeto desde un contenedor hacia otro.
- **Nuevos comandos de línea:** Fueron incluidos varios comandos que se corren por consola, entre los que se pueden mencionar los siguientes:
 - Dsadd. Permite crear objetos a través de líneas de comandos.
 - Dsmove. Mueve objetos de un contenedor a otro.
 - Dsrm. Borra objetos del directorio activo.
 - Dsquery. Permite realizar una búsqueda de los objetos por medio de una pregunta.
 - Dsget. Permite ver los atributos de un objeto en particular del directorio activo.

Windows Server 2003 R2¹ es una actualización del sistema operativo Windows Server 2003, que facilita y hace más rentable la ampliación de la conectividad, el control a; identidades, ubicaciones, datos y aplicaciones, incluyendo los siguientes componentes al directorio activo:

¹ (Microsoft, 2005)

- Modo De Aplicación De Directorio Activo (ADAM - Active Directory Application Mode), funciona como un almacén de datos independientes. Su independencia hace posible el control local y la autonomía de servicios de directorios para aplicaciones específicas, proporcionando esquemas y contextos de nomenclatura flexible e independiente.
- Servicio de federación de directorio activo (ADFS - Servicios de Federación de Active Directory), presenta la funcionalidad de servirse del inicio de sesión de usuario único para autenticar al usuario en diversas aplicaciones web, lo que se logra mediante el uso compartido y seguro de identidades digitales.

Después de cinco años se presentó Windows Server 2008², con nuevas características y tecnologías que aumentaron la seguridad de los equipos y la productividad, a la vez que redujeron los gastos administrativos. En esta actualización del sistema operativo se destacan los cambios de roles y servicio del directorio activo detallados a continuación:

- Función de servicios de certificado de servidor de directorio activo (Certificate Server de Active Directory - AD CS), ofrece servicios personalizables para crear y administrar certificados de clave pública, lo que aumenta la seguridad al enlazar la identidad de una persona, un dispositivo o servicios con la clave privada correspondiente.
Adicionalmente se presentaron las siguientes actualizaciones:
 - Cifrado de nueva generación.
 - AD CS: compatibilidad con el Protocolo de estado de certificados en línea.
 - AD CS: Servicio de inscripción de dispositivos de red.
 - AD CS: Inscripción en web.
 - AD CS: configuración de directiva.
 - AD CS: agente de inscripción restringido.
 - AD CS: Enterprise PKI (PKIView).
- Función de servicios de dominio de directorio activo (AD DS), almacena información acerca de los usuarios, equipos y otros dispositivos de la red, lo que facilita administrar información con seguridad y simplifica el uso compartido de recursos y la colaboración entre los usuarios.
La versión introdujo los cambios siguientes:
 - AD DS: auditoria.
 - AD DS: directivas de contraseña muy específicas.
 - AD DS: controlador de dominio de solo lectura.
 - AD DS: servicios de dominio de directorio activo reiniciables.
 - AD DS: herramienta de montaje de base de datos.
 - AD DS: mejora de la interfaz de usuario.

(Microsoft, 2014)

- Función de servicios de federación de directorio activo (AD FS), función de servidor del sistema operativo empleada para crear una solución de acceso e identidad altamente extensible, escalable a internet y segura que puede funcionar en diversas plataformas. Incluye nuevas funcionalidades para facilitar la carga administrativa y mejora la exportación e importación de directivas ayudando a disminuir, al mínimo, los problemas de configuración.
- Función de servicios de directorio ligero de directorio activo (AD LDS), servicio de directorio del protocolo ligero de acceso a directorios (LDAP), que proporciona almacenamiento y recuperación de datos a aplicaciones habilitadas para el uso de directorios, sin las dependencias de los servicios de domino de directorio activo, siendo posible ejecutar varias instancias de AD LDS de forma simultánea en un único equipo.

AD LDS se distingue de AD DS principalmente en que no almacena entidad de seguridad de Windows. Mientras que AD LDS puede usar entidades de seguridad de Windows en las listas de control de acceso (ACL) que controlan el acceso a objetos de AD LDS. Además AD LDS no admite dominios ni bosques, directiva o catálogos globales.

- Función de servicios de administración de derechos de directorio activo (Active Directory Rights Management Services - AD RMS), incluye varias características nuevas, pensadas para aliviar la sobrecarga administrativa de AD RMS y aplicar su uso fuera de la organización, se destacan las siguientes mejoras: auto inscripción de clúster de AD RMS, integración con AD FS y nuevas funciones administrativas de AD RMS que posibilitan delegar tareas de AD RMS a diversos administradores.

El 4 de septiembre de 2012 nace Windows Server 2012³, que es la penúltima edición lanzada por Microsoft del sistema operativo Windows Server. La versión no tiene soporte para computadores con procesadores Intel Itanium y se venden cuatro ediciones Foundation, Essentials, Standard y Datacenter. El sistema presenta las siguientes novedades:

- Directorio activo, ha mejorado para permitir la administración de riesgos y facilita a sus usuarios el acceso desde una amplia gama de dispositivos en los cuales los administradores de TI (Tecnologías de Información) pueden asociar dispositivos con el directorio de la empresa con el fin de usar esa asociación como autenticación de segundo factor, desde cualquier ubicación con web Proxy de aplicaciones para administrar los riesgos con el control de acceso multifactor y la autenticación multifactor (MFA).
- Los Servicios de dominio de directorio activo (AD DS) implementan, de manera más rápida y sencilla, los controladores de dominio lo que aumenta la flexibilidad al permitir auditar y autorizar el acceso a archivos, así como la

³ (microsoft, 2015)

realización, de manera sencilla, de tareas administrativas de forma local o remota mediante interfaz gráfica y scripts. Se presentan las siguientes mejoras de servicio:

- Proporciona mayor compatibilidad con las funcionalidades de nubes públicas y privadas e implementación rápida de controladores de dominio mediante clonación.
 - Los procesos de actualización y preparación (dcpromo y adprep) se han reemplazados por un nuevo asistente para promoción de dominios optimizado, que se integra con el administrador del servidor y valida los requisitos previos, automatizando los bloques y dominios para lo que necesita únicamente de un conjunto de credenciales, consiguiendo instalar AD DS en un servidor de destino de forma remota.
 - Administración simplificada que incluye la funcionalidad clave de comportamientos encubiertos para regir los componentes sobre los que se construye el resto de servicio de directorio, la actualización AD DS incluye la asignación y escala mejoradas de RID (identificados relativos), la creación diferida de índices, varias mejoras de kerberos y compatibilidad con notificaciones.
- Novedades de servicios de administración de derechos de directorio activo (AD RMS), rol del servidor que proporciona herramientas de administración y desarrollo que funciona con tecnología de cifrado, certificados y autenticación, creando soluciones de protección confiables.
 - Las novedades que presenta AD RMS en Windows Server 2012, cambio en los requisitos de AD RMS y SQL server, permitiendo una mejor compatibilidad con la implementación remota obteniendo respuesta a los comentarios de los clientes que soliciten opciones de implementación más flexibles, igualmente cambios en la implementación de AD RMS para Server Manager y Windows PowerShell permitiendo mejorar la integración con el administrador del servidor.

Plataformas Similares

También existen varias distribuciones para quienes no deseen emplear el directorio activo de Windows Server. Alternativas tales como:

- **Samba**⁴ es un sistema de código libre basado en el protocolo CIFS (Common Interface File System), que permite a plataformas Unix poder actuar como servidores que interactúen con plataformas Windows.⁵

⁴ (Samba, 2015)

⁵ (E., 2015)

Samba provee servicios de:

- Manejo de archivos.
- Servidor de impresión.
- Autenticación de usuarios.
- Resolución de nombres.
- Búsqueda.

El 4 de marzo de 2015 fue lanzada la versión 4.2, presentando las novedades de:

- Compresión de ficheros transparentes en Btrfs, sistema de archivos que reemplaza a ext4, desarrollado por Oracle, con la participación de Red Hat, SUSE, Intel, entre otras buscando estabilidad.
- Añade módulo Snapper VFS.
- Mejoras en la seguridad y la usabilidad.
- Winbindd (mantenimiento del canal seguro de sesión) usa Samba AD DC por defecto.
- Novedades en el protocolo SMB2.
- Detección DCERPC para ataques “man in the middle”.
- Soporte para clustering.
- **OpenMandriva** es un software de código libre que posee las siguientes características:
 - Autenticación y manejo de usuarios, a través de LDAP.
 - Una interfaz WEB en PHP basada en AJAX llamada MMC (Mandriva Management Console), la cual consta de 6 módulos:
 - Manejo de usuarios y grupos.
 - Manejo de Cuentas Samba.
 - Manejo de impresión.
 - Manejo de envío de correo electrónico.
 - Integración con DNS y DHCP.
 - Un API de administración hecha en Python para LDAP, Samba y SQUID.
 - Manejo de lista negra de WEB proxy.
 - Un sistema de políticas que permite definir los permisos a los usuarios en los recursos de la red.

- **Novell eDirectory**

Mejor conocido como Novell Directory Service, es un servicio de directorio compatible con estándar X.500 lanzado por Novell en 1993, este permite manejar y acceder a los recursos de múltiples servidores y estaciones de trabajo en una red. Consiste en una base de datos jerárquica orientada a objetos, que puede representar la estructura de una empresa en un árbol lógico, incluyendo: unidades organizacionales, personas, posiciones, servidores, estaciones de trabajo, aplicaciones, impresoras, servicios y grupos, entre otros.

4.2 MARCO TEORICO

Directorio activo es una lista detallada de objetos, las cuales guardan información de cada elemento representado. Un directorio activo de dominio de servicios (AD DS), se basa en el concepto de dominio que introdujo Windows NT con el fin mejorar la administración, en la actualidad el objetivo es crear una estructura dinámica y fácilmente accesible, donde se pueda almacenar toda la información, sitios, ordenadores, usuarios, objetos compartidos y cualquier otro elemento que forme parte de la infraestructura de red de la organización accediendo de forma centralizada, igualmente los elemento almacenados pueden ser diferentes unos a los otros, usuarios, grupos, políticas de acceso y permisos entre otros.

La base de datos Microsoft Exchange Server reporta la información contenida a diferentes controladores de dominio a través de la red, de esta forma los usuarios creados en un determinado controlador de dominio podrán iniciar sesión en cualquier cliente unido a otro controlador de dominio diferente sin ninguna complicación.

Además la administración de las políticas será validada en toda la organización, permitiendo efectuar instalaciones de forma simultánea y centralizada en multitud de clientes o ejecutar actualizaciones críticas en toda la organización, igualmente establece políticas de grupo en diferentes niveles, un acceso sencillo al árbol de usuarios, computadores, impresoras y demás objetos.

En la estructura del servicio del directorio existen dos tipos de componentes como se evidencia en la tabla relacionada a continuación (Ruiz, 2013).

Tabla 1. Componentes

COMPONENTES FISICOS	COMPONENTES LOGICOS
Controladores del dominio	Dominio
Sitios	Bosque
Subredes	Arboles
	Unidades organizativas

4.2.1 Directorio

Reposito único para la información relativa de los usuarios y recursos de una organización (Ruiz P. , 2013).

Almacena información acerca de los atributos de los archivos o donde se encuentran físicamente en el dispositivo de almacenamiento.

4.2.2 Directorio activo

Base de datos especializada o repositorio de datos que almacena y contiene información de las propiedades y ubicación de los diferentes tipos de recursos dentro de la red, la principal ventaja es que puede utilizar LDAP (protocolo ligero de acceso a directorios), protocolo estándar que permite la consulta de información contenida en el directorio. También puede usar ADSI (Interfaces de servicio de active directorio) conjunto de herramientas de Microsoft, con interfaz orientada a objeto que permite el acceso a las características de directorio activo de servicios de dominio y establece políticas, a nivel empresarial, para: desplegar aplicaciones en varias terminales, almacenar informaciones en BD centralizadas, organizadas y accesibles. (Ruiz P. , 2013)

Según Gómez (Gomez Gomez, 2010), los estándares que facilitan la comunicación con otros servicios de directorio son:

- **LDAP** (Lightweighth Directory Access Protocol o Protocolo Ligero de Acceso a Directorio): Servicio que corre directamente sobre la pila de protocolos TCP/IP, define un método estándar para acceder y actualizar la información en un directorio; igualmente define el lenguaje usado por los programas del cliente para comunicarse con los servidores y también entre servidores, también define permisos, puestos por el administrador, para permitir a ciertos usuarios acceder a la base de datos y mantener datos privados.
- **DHCP** (Dynamic Host Configuration Protocol): Protocolo de configuración dinámica de ordenadores que permite administrar dinámicamente y de forma automatizada las direcciones de red.
- **DNS** (Domain Name System): Servicio de nombres de dominio que permite la administración de los computadores, constituyéndose en el servicio de asignación y resolución de nombres en internet, cumple tres funcionalidades principales:
 - Realiza la resolución de nombres al convertir los nombres de host a direcciones IP.
 - Utiliza las convenciones de nomenclatura para asignas el nombre a los dominios.
 - Almacena la información de los equipos para permitir atender inicios de sesión de red o consultas, adecuadamente, en Directorio Activo.
- **SNTP** (Simple Network Time Protocol): Protocolo simple de tiempo de red, el cual permite disponer un servicio de tiempo distribuido.
- **Kerberos**: Protocolo utilizado para la autenticación de los usuarios y maquinas.
- **Certificados X.509**: Estándar que permite distribuir información a través de la red de forma segura.

4.2.3 Servicio de Directorio

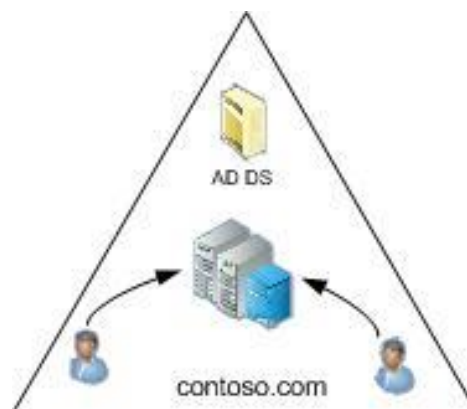
Es la colección de software, hardware, políticas y procedimientos administrativos que permite manejar la información en el directorio de manera que esté disponible para los usuarios, incluye los siguientes componentes (Santos, 2011):

- Información contenida en el directorio.
- Software asociado a los servicios que soportan la información.
- Software de los clientes.
- El hardware de los clientes y servidores.
- Software de soporte, tales como sistemas operativos y manipuladores de dispositivos.
- Estructura de la red.
- Las políticas y permisos.
- Software para mantener y monitorear el servicio de directorio.

4.2.4 Dominio

Colección de objetos, dentro del directorio, que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos identificados con sus colecciones de objetos y unidades organizativas. Se necesita el protocolo DNS para establecer el nombre del dominio. El Directorio Activo requiere por lo menos un servidor DNS. (Ruiz P. , 2013).

Figura 1. Domino⁶

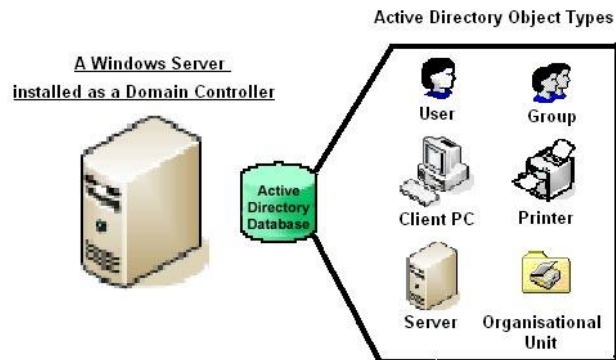


⁶ Tomado de: [https://technet.microsoft.com/es-es/library/gg398173\(v=ocs.15\).aspx](https://technet.microsoft.com/es-es/library/gg398173(v=ocs.15).aspx)

4.2.5 Objeto

Se utiliza como nombre genérico para referirse a cualquier componente que forme parte del directorio activo, dispone de una serie de características específicas, según la clase a la que pertenezca y un nombre que lo identifica de forma precisa.

Figura 2.Objeto⁷



Los objetos se organizan en tres categorías:

- **Usuarios:** Conjunto de permisos y de privilegios sobre determinados recursos organizados por grupos que simplifica la administración.
- **Recursos:** Son los diferentes elementos a los que se puede acceder (carpetas compartidas, impresoras, etc.).
- **Servicios:** Son las diferentes funciones a los que los usuarios pueden tener acceso.

Objetos que administra un dominio

- **Usuarios globales:** Son aquellos que son conocidos por todos los ordenadores del dominio, sus datos se almacenan en el directorio activo.
- **Usuarios locales:** Son aquellos cuyos datos se almacenan localmente y sus datos son visibles únicamente en esa computadora.
- **Grupos:** Visibles por todos los ordenadores del dominio. Existen dos tipos de grupos:
 - Grupos de distribución, utilizados para crear listas de distribución de correo electrónico.
 - Grupos de Seguridad, utilizados con fines de seguridad administrativa.

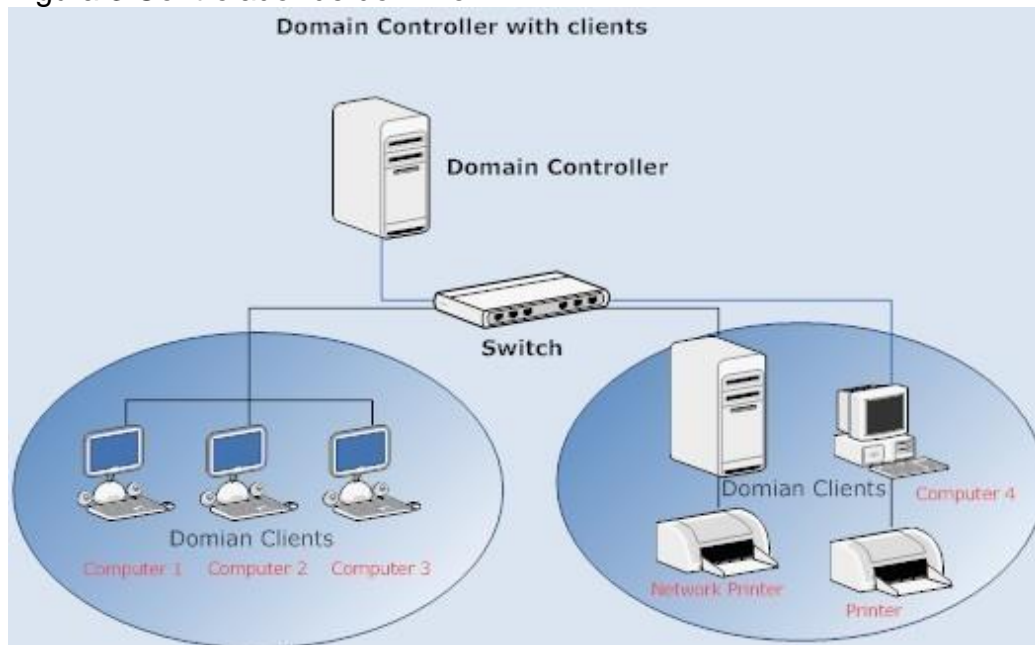
⁷ Tomado de: http://www.mcmcse.com/microsoft/guides/7010/introduction_to_active_directory.shtml

- **Equipos:** Se almacena una cuenta de equipo en el directorio activo por cada uno de los ordenadores miembros del dominio, identificándolos de manera única.
- **Unidades Organizativas:** Poseen la capacidad de contener otros objetos, se hace con el objetivo de delegar la administración de sus objetos a otros usuarios de distinto administrador de dominio.

4.2.6 Controlador de Dominio

Contiene la base de datos de objetos del directorio para un determinado dominio, incluyendo la información relativa de seguridad, es responsable de la autenticación de objetos de su ámbito de control.

Figura 3. Controlador de dominio⁸



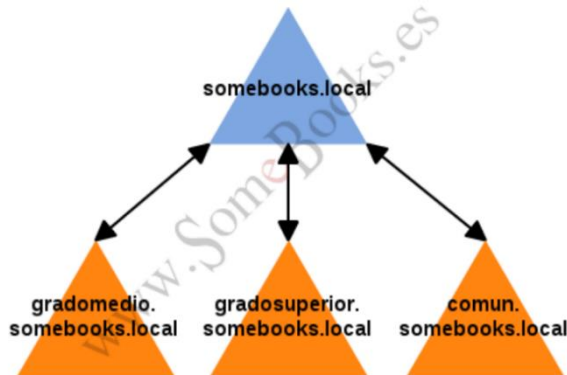
En un dominio pueden existir varios controladores de dominio, cada uno ellos desempeña un rol diferente dentro del directorio, teniendo la misma importancia bajo el mismo dominio.

^{8 8} Tomado de: <http://www.tech-faq.com/securing-domain-controllers.html>

4.2.7 Árboles

Es la colección de dominios que depende de una raíz común, se organizan de forma jerárquica y se representa por un espacio de nombres DNS común. El objetivo es fragmentar los datos del directorio activo, replicando solo las partes necesarias, lo que ahorra ancho de banda.

Figura 4.Árbol⁹



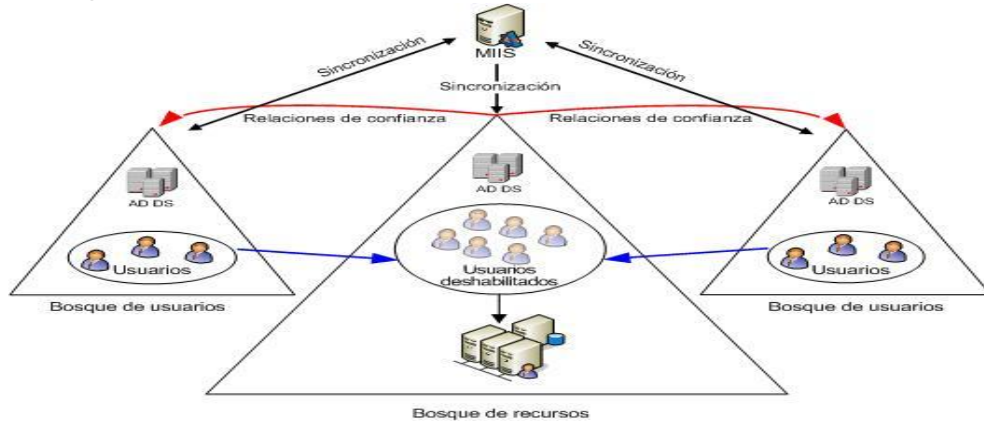
Es de notar que los usuarios que estén creados dentro de un dominio, este será reconocido automáticamente en todos los dominio que dependan jerárquicamente de él.

4.2.8 Bosque

Mayor contenedor lógico dentro del directorio activo, abarca a todos los dominios dentro de su ámbito y los interconecta por relaciones de confianza, lo que permite que los dominios de un bosque confíen automáticamente en otro y que los diferentes arboles puedan compartir recursos.

⁹ Tomado de: <http://somebooks.es/?p=3375>

Figura 5. Bosque¹⁰

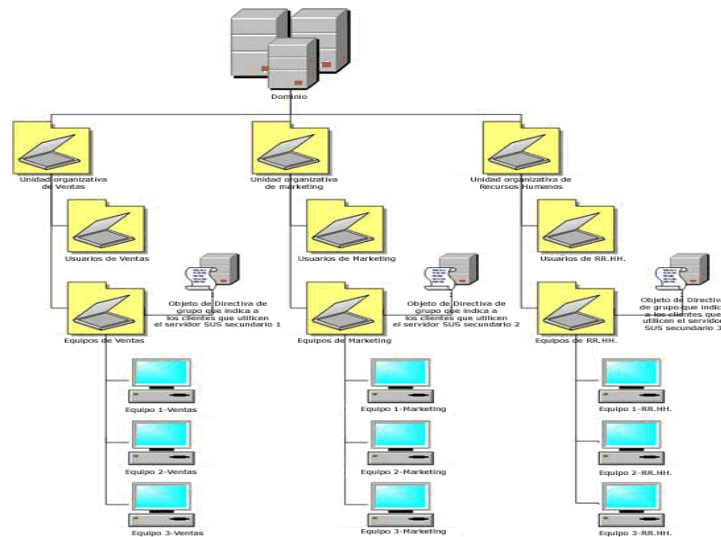


4.2.9 Unidad Organizativa

Contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio, siguiendo una jerarquía. Establece una estructura lógica que representa, de forma adecuada, la organización y simplifica la administración.

La unidad organizativa simplifica la delegación de autoridad sobre los objetos que contiene, a otros usuarios o grupos, lo cual es una forma de facilitar la administración en redes grandes dimensiones.

Figura 6. Unidad organizativa¹¹



¹⁰ Tomado de: [https://technet.microsoft.com/es-es/library/dd441359\(v=office.13\).aspx](https://technet.microsoft.com/es-es/library/dd441359(v=office.13).aspx)

¹¹ Tomado de: <https://sites.google.com/site/examengpo/home/unidad-organizativa>

4.2.10 Esquema

Estructura de la base de datos, se refiere a los atributos de cada tipo de información almacenada.

En ella se almacena y se manipulan los objetos dinámicamente como sea necesario. Basada en un comportamiento complejo la cual define qué tipo de objeto puede ser puesto en el directorio activo, cómo son definidos los objetos y cómo los objetos se integran con otros. Define la forma en que se almacenan los objetos en el directorio activo. Se compone de una lista de definiciones sobre objetos e incluso definiciones acerca de las definiciones de los objetos, estas definiciones se denominan metadatos o sea datos sobre datos, los cuales establecen los atributos o cualidades de los objetos.

4.2.11 Sitio

Agrupación de computadoras que se encuentran ordenados de forma lógica, se gerencia por un controlador de dominio que puede estar en la misma zona geográfica o localizarse en el otro extremo del planeta, siempre que estén unidos por conexiones adecuadas y en todo caso formando un mismo sitio.

4.2.12 Relaciones de Confianza

Método de comunicación seguro entre dominios, árboles y bosques, permite a los usuarios de un dominio de directorio activo autenticarse en otro dominio del directorio.

Existen dos tipos de relaciones de confianza: unidireccionales y bidireccionales, además las relaciones son transitivas, esto es: si A confía en B y B confía en C, entonces A confía en C.¹²

4.2.13 Control de acceso con Directorios

Precisa los elementos que compone un sistema básico de control de acceso, cuenta con la capacidad de validar a los usuarios con el propósito de conocer los permisos que se asignan.

¹² (Ruiz P. , 2013)

4.2.14 Seguridad

Es el proceso por el cual se protegen los recursos de información y se traza los objetivos siguientes:

- Proteger la confidencialidad, se refiere a la protección de los datos ante una revelación no autorizadas a terceras partes.
- Mantener la integridad, o sea tener la certeza de que los datos no son destruidos o alterados de forma no autorizada.
- Asegurar la disponibilidad, garantizar el funcionamiento continuo de los sistemas de cómputo.

4.2.15 Control de Acceso

Es la prevención del uso no autorizado de una fuente, refiriéndose al uso de archivos que contienen información vital para la organización, pero no debe interferir con la facilidad de uso.

Una vez que un usuario se autentica ante un sistema de control de acceso, si satisface las políticas del sitio, logrará convertirse en un usuario activo del sistema a través del inicio de sesión que crea el sistema operativo y desde ese momento todas sus acciones estarán ligadas a su identidad.

Protocolo AAA

Corresponde a un tipo de protocolo que realiza tres funciones: autenticación, autorización y contabilización.

Autenticación

Proceso utilizado con el objetivo de verificar la identidad de un usuario, mediante la comprobación de credenciales de acceso, ejecuta las operaciones siguientes:

- Reportar al servidor el nombre del usuario y la contraseña.
- El servidor recibe los datos y compara con su base de datos.
- Si la información es válida, permite el acceso al usuario.
- Si la información no coincide, se niega el acceso al usuario.

Igualmente, se refiere a la concesión de privilegios o restricciones específicas a una entidad o usuarios, basándose en su identidad autenticada. ¹³

¹³ (Santos, 2011)

4.2.16 Políticas de Grupo (GPO)

Las políticas o directivas de grupo (GPO) es un componente que posee la familia de sistemas operativos Windows, en el cual se definen las reglas o políticas que compondrá todo un ambiente de cuentas de usuario en un sistema informático; este tipo de reglas controlan el contenido al que los usuarios pueden acceder o no de acuerdo a la configuración aplicada mediante un sistema operativo Windows Server a cada usuario y/o equipo que se encuentre en un dominio, sitio o unidad organizativa. Generalmente la configuración de sistemas operativos y gestión de usuarios se lleva a cabo bajo un Directorio Activo. Las directivas de grupo locales (GPL) son directivas de grupo que sólo se aplican para un host local único. Fuente especificada no válida.

5. CRONOGRAMA DE ACTIVIDADES.

La figura 7 contiene el cronograma de trabajo para el desarrollo del proyecto, estableciendo las actividades a realizar y el tiempo que se dedica a la ejecución de cada una.

Figura 1. Actividades

Modo de	Nombre de tarea	Trabajo	Duraci	Comienzo	Fin
	▲ Proyecto Directorio Activo SSM de Neiva	0 horas	31 días	lun 05/10/15	lun 16/11/15
	Inicio	0 horas	0 días	lun 05/10/15	lun 05/10/15
	▲ Entendimiento del entorno de la empresa	0 horas	9 días	lun 05/10/15	jue 15/10/15
	Entrevista con el gerente	0 horas	1 día	lun 05/10/15	lun 05/10/15
	Identificación de la estructura de la red	0 horas	3 días	mar 06/10/15	jue 08/10/15
	Determinación de recursos de red, unidades organizativas y grupos de usuarios.	0 horas	4 días	vie 09/10/15	mié 14/10/15
	Informes de hallazgos	0 horas	1 día	jue 15/10/15	jue 15/10/15
	▲ Planeación Inicial	0 horas	16 días	vie 16/10/15	vie 06/11/15
	Definición del problema	0 horas	3 días	vie 16/10/15	mar 20/10/15
	Identificación de normatividad	0 horas	8 días	mié 21/10/15	vie 30/10/15
	Planeación de estructura de directorio activo	0 horas	3 días	lun 02/11/15	mié 04/11/15
	Definición de políticas de seguridad	0 horas	2 días	jue 05/11/15	vie 06/11/15
	▲ Diseño de directorio activo	0 horas	6 días	lun 09/11/15	lun 16/11/15
	Diseño de unidades organizativas	0 horas	2 días	lun 09/11/15	mar 10/11/15
	Diseño de sitios	0 horas	2 días	mié 11/11/15	jue 12/11/15
	Esquema de directorio activo	0 horas	2 días	vie 13/11/15	lun 16/11/15
	Final	0 horas	0 días	lun 16/11/15	lun 16/11/15

6. RESULTADOS

Para el óptimo desarrollo del proyecto se efectuara en dos fases, fase I entendimiento del entorno de la empresa, donde se identificara la estructura de la red, recursos de la red, unidades organizativas y grupos. En la fase II se presentara el diseño del directorio activo el cual modelara y se adaptará en una base de datos especializada que almacenara la información de las propiedades y ubicación de los diferentes tipos de recursos dentro de la red.

A continuación se documenta el desarrollo de casa una de las fases con su respectivo resultado.

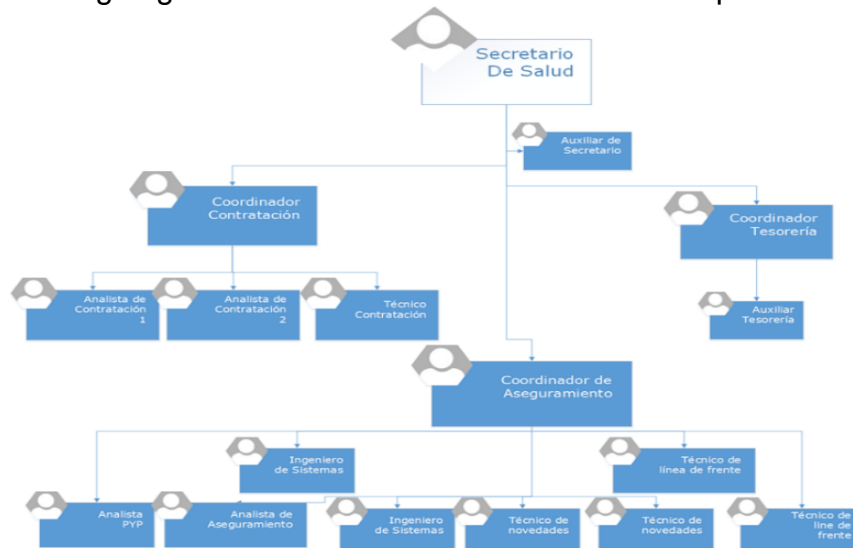
6.1 FASE I – ENTENDIMIENTO DEL ENTORNO DE LA EMPRESA

En esta fase del proyecto es necesario identificar la estructura de la red, los objetos y recursos que interactúan en la Secretaria de Salud Municipal de Neiva, estableciendo el diseño de directorio activo, el cual supla las necesidades de la compañía.

6.1.1 Organigrama

En la figura 8, se representa la estructura de la Secretaria de Salud y las personas que las dirigen e integran.

Figura 8. Organigrama de la Secretaria de Salud Municipal



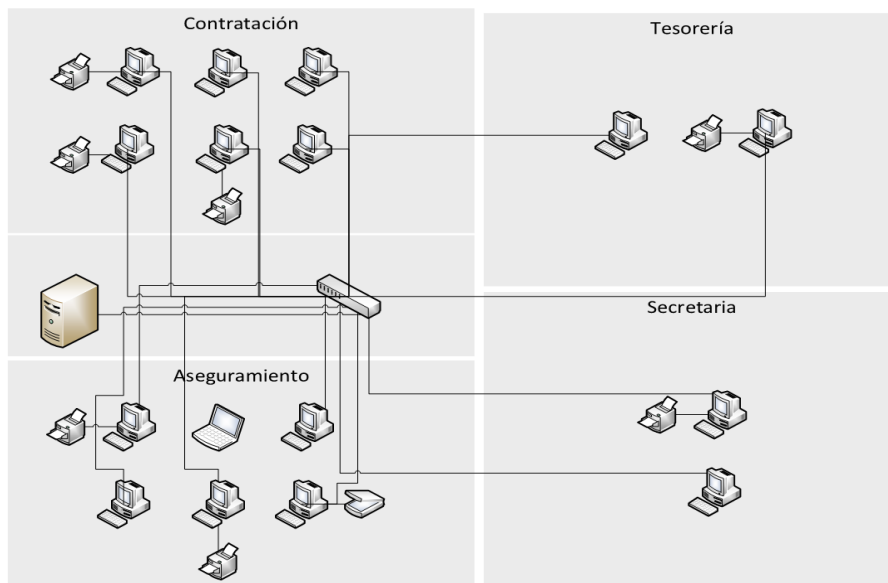
La entidad está compuesta por 17 empleados que trabajan en distintas áreas, Registrando 4 secciones en las que está dividida la entidad. En cada sección existe un director responsable y el grueso de la plantilla reside en los departamentos de área de aseguramiento. Las cuatro secciones son las siguientes:

- **Secretaría:** Garantiza el ejercicio efectivo del derecho a la salud de toda la población, a través de la implementación de un modelo de atención integral, equitativa, universal, participativa, centrada en el ser humano, la responsabilidad social y la sostenibilidad ambiental.
- **Tesorería:** lidera el proceso financiero del Municipio que incluye la consolidación, presentación ejecución y control presupuestal, la contabilización de todas las transacciones financieras, el control de los impuestos, la consecución y manejo de los recursos financieros.
- **Contratación:** Verifica y garantiza los procesos contractuales que se realicen en la secretaria se efectúen dentro de los parámetros legales internos y externos.
- **Aseguramiento:** Área que garantiza la continuidad del aseguramiento a los afiliados del régimen subsidiado en seguridad social en salud en el Municipio de Neiva.

6.1.2 Identificación de la estructura de la red

Se efectúa diagnóstico a la oficina de la Secretaria de Salud Municipal de Neiva como se indica en la figura 9, determinando estado actual recursos y componentes de la red:

Figura 9. Estructura de red



6.1.3 Objetos y recursos de la red

Tabla 2. Equipos de la red

ELEMENTOS DE LA RED	MARCA	MODELO	CANTIDAD	SISTEMA OPERATIVO	PROCESADOR	DISCO DURO	MEMORIA RAM
COMPUTADOR	HP COMPAQ	DX 2000 MT	6	Windows 7 Profesional	Intel Pentium 4 2.4 GHz	40 GB	512 MB DDR
	HP COMPAQ	DX 2000 MT	4	Windows XP	Intel Pentium 4 2.4 GHz	40 GB	512 MB DDR
	DELL	S20	5	Windows 8	Intel® Celeron® J1800 (1M Cache, 2.41 GHz)	500GB	4.0GB DDR3 1600 MHz
	HP COMPAQ	8200	3	Windows 7 Profesional	Intel Core i3-2100M	500 GB	4.0 GB
SERVIDOR	HP	Proliant ML370 G6	1	Windows Server 2008 R2	INTEL XEON E5649 (6 NÚCLEOS, 2.53 GHz)	24 TB	6 GB DDR3

Tabla 3. Impresoras de la red

ELEMENTOS DE LA RED	MARCA	MODELO	CANTIDAD	TECNOLOGIA DE IMPRESIÓN	VELOCIDAD DE COPIA	VELOCIDAD DE IMPRESIÓN	CICLO MENSUAL DEL SERVICIO
IMPRESORAS	HP	LaserJet M4345 MFP	1	Laser (Mono cromado)	43 ppm	43 ppm	200,000 impresiones
	HP	LaserJet P1102w	6	Láser	18 ppm	18 ppm	Hasta 5000 páginas
ESCANER	HP		1				

Tabla 4. Recursos de la red

ELEMENTO DE RED	MARCA	MODELO	CANTIDAD	PUERTOS	VELOCIDAD	CAPACIDAD DE ENCAMINAMIENTO
SWITCH	HP	1920	1	48	77.4 Mbps	104 ps

6.1.4 Identificación del software instalado

Tabla 5. Software instalado

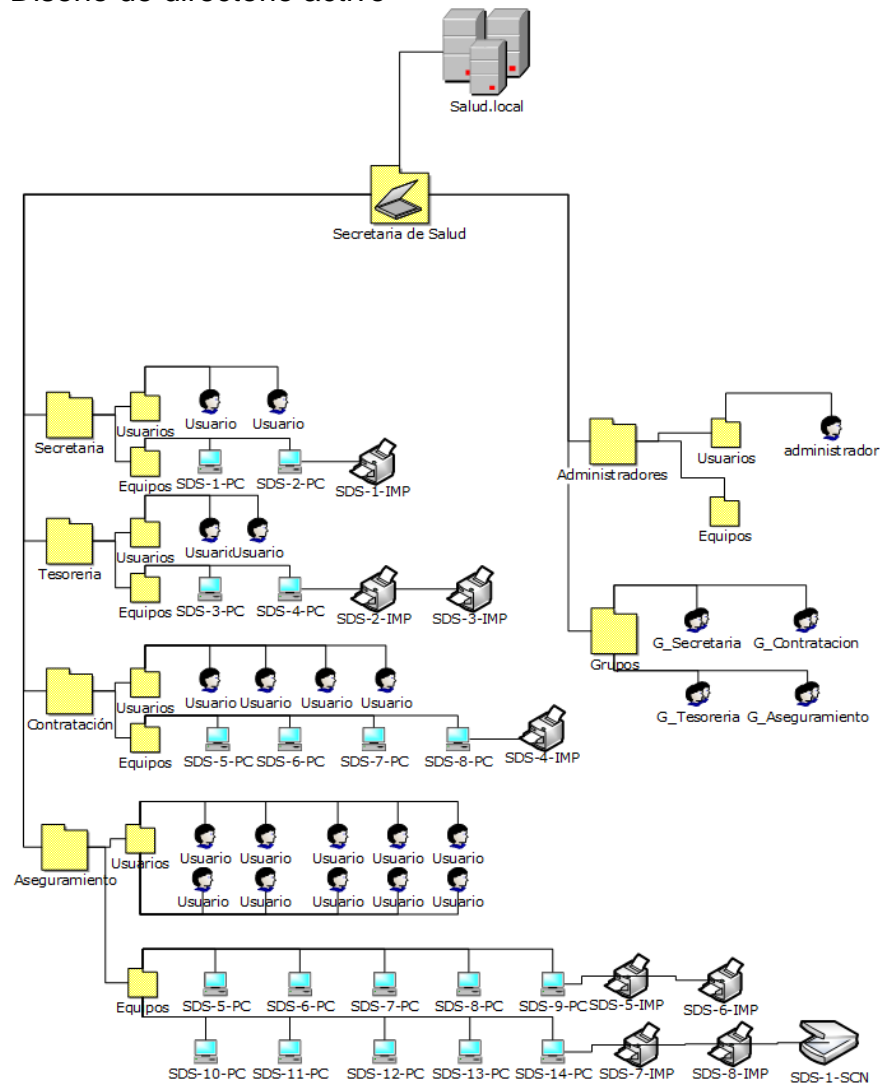
SOFTWARE	CANTIDAD	PROCENTAJE
Suite ofimática Microsoft Office Profesional plus 2007	9	50%
Suite ofimática Microsoft Office Profesional plus 2010	9	50%
Sistema Emasegura	1	6%
Skype 7.8	4	25%
CCleaner	6	38%
WinRAR 5.21	18	100%
Google Chrome	12	63%
Internet exporet	6	38%
Antivirus Kasperky 2015	18	100%
Sistema operativo Windows 8	5	25%
Sistema operativo Windows 7 Profesional	9	56%
Sistema operativo Windows XP	4	19%

Terminado el proceso de identificación, se determina que, no se encuentra estandarizado el sistema operativo, navegador web y suite de office en la entidad.

6.2 FASE II-DISEÑO DE DIRECTORIO ACTIVO

Antes de diseñar el directorio activo fue necesario conocer a fondo la estructura interna de la organización y de red, para asegurar el óptimo y confiable diseño del directorio activo separando la estructura lógica del dominio de la estructura física real, en la figura 10, se establece el diseño del directorio activo para la Secretaria de Salud Municipal de Neiva:

Figura 10. Diseño de directorio activo



De la misma manera, para efectuar el diseño del directorio activo es necesario tener en cuenta que para su correcto funcionamiento, en el servidor se deben implementar también los servidores DNS y DHCP.

El establecimiento del servidor DNS es necesario, ya que el directorio activo lo emplea para resolver nombres de host a direcciones IP, para asignar el nombre a los dominios por medio de la nomenclatura DNS y formalizar búsquedas de los objetos.

En cuanto al servidor DHCP, este es obligatorio para evitar direcciones IP duplicadas en la red que impidan su correcto funcionamiento.

6.2.1 Estructura física

Los controladores de dominio y los sitios son los dos componentes básicos que tienen que ver con la estructura física en la configuración de red de área local.

Como el diseño está basado solo en la sede principal de la secretaria de salud municipal de Neiva, definimos que solo habrá un sitio, por ende se establecerá un controlador de dominio que estará ubicado en la misma zona geográfica de los clientes a los que ofrece sus servicios y contendrá la base de datos de objetos del directorio para el dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control.

6.2.2 Estructura lógica

La estructura lógica de una red se compone de elementos intangibles como objetos, dominios, árboles y bosques.

El bloque de construcción básico del directorio activo es el objeto, un conjunto de atributos diferenciado y con nombre que representa un recurso de la red. Los atributos del objeto son características de objetos del directorio. Los objetos se pueden organizar en clases, que son agrupaciones lógicas de objetos. Los usuarios, grupos y equipos son ejemplos de clases de objeto diferentes.

En el nivel más bajo, algunos objetos representan entidades individuales de la red, como un usuario o equipo. Estos objetos se denominan hoja y no pueden contener otros objetos. Sin embargo, para facilitar la administración y simplificar la organización del directorio, puede colocar objetos hoja dentro de otros objetos denominados objetos contenedores. Los objetos contenedor también pueden contener otros contenedores de forma anidada, o jerárquica.

El tipo más común de objeto contenedor es una unidad organizativa (OU, Organizational Unit). Puede usar una unidad organizativa para organizar objetos de un dominio en algún tipo de agrupación lógica administrativa.

En la figura 10 se define un dominio para la secretaria de salud llamado “salud.local”, dado que al tener un único dominio acotará notablemente los costos tanto de hardware como de software, permitiendo centralizar fácilmente la administración. El nombre del dominio es pensado no sólo en base a la situación actual, se tiene en cuenta la evolución que se puede esperar de la empresa.

Para la secretaria de salud se estableció una unidad organizativa llamada “Secretaria de salud”, donde se encontrará de manera anidada los siguientes contenedores definidos de acuerdo a la estructura organizacional de dicho ente:

- Secretaria
 - Usuarios
 - Equipos
- Tesorería
 - Usuarios
 - Equipos
- Contratación
 - Usuarios
 - Equipos
- Aseguramiento
 - Usuarios
 - Equipos
- Administradores
 - Usuarios
 - Equipos
- Grupos

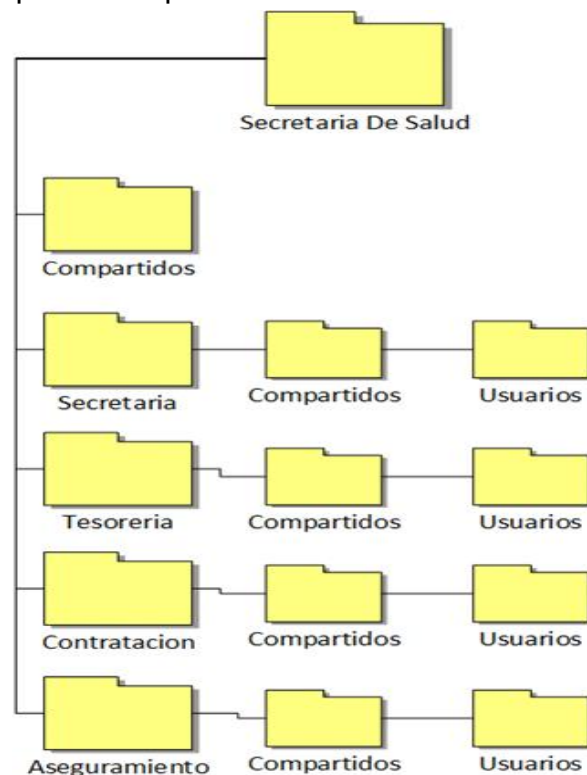
Todos los objetos de la red, ya sean hojas o contenedores, sólo pueden existir dentro de un dominio. Los dominios se usan para agrupar objetos relacionados con el fin de reflejar la red de una organización. Cada dominio que se crea almacena información acerca de los objetos que contiene, únicamente. Actualmente, el límite admitido para el número de objetos que puede mantener en un dominio es de un millón.

6.2.3 Carpetas y permisos

En el servidor existe una jerarquía de carpetas donde los empleados alojaran sus archivos, operando de la siguiente manera:

- Un carpeta llamada “Compartidos” donde todos los usuarios del directorio tendrán acceso, adicional tendrán permisos de lectura y escritura.
- Cada departamento cuenta con su propio directorio, solo los usuarios que pertenezcan al área asignada a la carpeta tendrán acceso a esta.
- Dentro de cada directorio, asignado a cada uno de los departamentos, se encuentra una carpeta denominada “Compartidos” donde solo los usuarios que hagan parte del departamento tendrán acceso y permisos de lectura y escritura.
- De igual manera, dentro de cada directorio, asignado a cada uno de los departamentos, se encuentra una carpeta con el nombre de cada uno de los empleados perteneciente al departamento, estas carpetas son de uso exclusivo de cada usuario y solo ellos cuentan con los permisos de acceso, lectura y escritura.

Figura 11. Jerarquía de carpetas



6.2.4 POLITICAS DE GRUPO (GPO)

Terminado el estudio de las necesidades de las políticas de grupo del directorio activo de las configuraciones de grupos de usuarios y equipos, que controlaran el acceso a los recursos de red. Creando un entorno de trabajo adaptable a las necesidades de cada usuario de la secretaria de salud, serán aplicadas las siguientes políticas:

- Plantillas administrativas / de escritorio
 - Los usuarios deben loguearse solamente de 7:00 am a 8:00 pm.
 - Debe usarse el papel tapiz de la empresa, no debe poder cambiarse.
 - Los usuarios deben cambiar su contraseña cada 30 días.
 - Definir que programas se deben ejecutar al inicio de la sesión del usuario.
 - La carpeta documentos de todos los usuarios apuntará a una carpeta independiente por usuario que esté dentro de la carpeta compartida \\controladordominio\publica.
 - Solo los administradores pueden apagar la máquina
 - Solo los administradores pueden cambiar la hora del sistema
 - Todas las máquinas tendrán permanente la unidad H: que apuntará a la ruta [\\controladordominio\compartida](#).

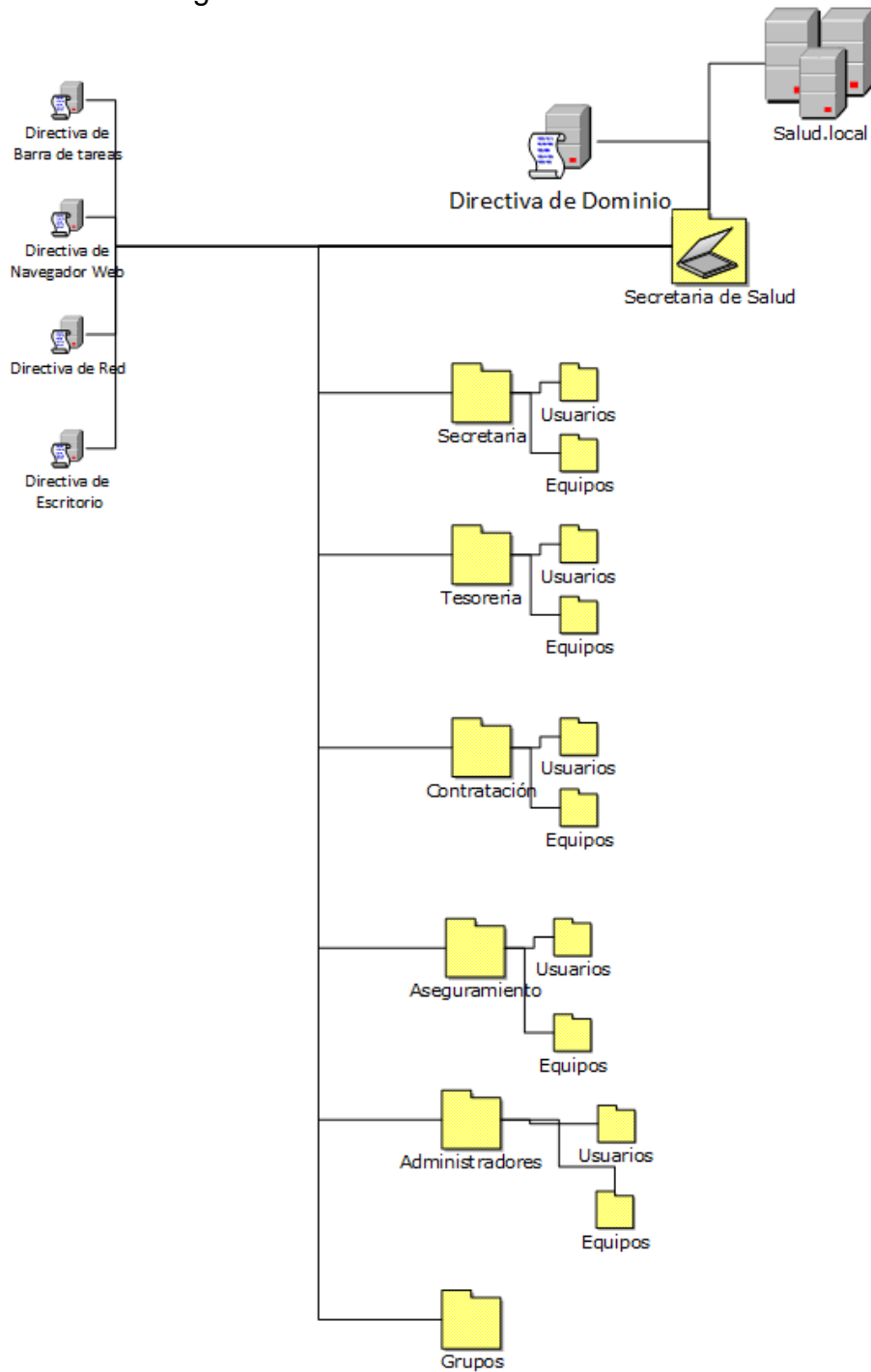
- Plantillas administrativas / Menú Panel de control / Inicio y barra de tareas.
 - Deshabilitar el menú Ejecutar del menú de inicio.
 - Desactivar el panel de control.
 - Desactivar Agregar / Quitar Programas.
 - Desactivar Pantalla en el Panel de Control.
 - Desactivar supresión de impresoras.

- Planillas administrativas navegador web.
 - Establecer página de inicio la dirección web de la compañía.
 - Deshabilitar el cambio de configuración del historial.
 - Deshabilitar cambiar la configuración de fuente.
 - Deshabilitar cambiar la configuración de idioma.
 - Deshabilitar el cambio de configuración de los archivos temporales de Internet.
 - Deshabilitar la personalización de la barra de herramientas del navegador botones.
 - Menú Herramientas: Opciones de Internet... Desactivar las opciones de menú.

- Plantillas administrativas / Red.
 - Prohibir la configuración avanzada de TCP / IP.

Es de anotar que al momento de la implementación se podrán añadir más directivas de según sea la necesidad.

Figura 12. Estructura Lógica con GPO Generales



7. PRESUPUESTO

Tabla 6. Presupuesto

PRESUPUESTO					
TIPO	DESCRIPCION	CANTIDAD		V.UNIT	V.TOTAL
TALENTO HUMANO	ENTENDIMIENTO DEL ENTORNO EMPRESARIAL	54	HORAS	\$ 20,000	\$ 1,080,000
	PLANEACION INICIAL	96	HORAS	\$ 20,000	\$ 1,920,000
	DISEÑO DE DIRECTORIO ACTIVO	36	HORAS	\$ 20,000	\$ 720,000
	ESTABLECIMIENTO POLITICAS GPO	20	HORAS	\$ 20,000	\$ 400,000
RECURSOS TECNICOS	COMPUTADOR HP Pavilion 13-s1511a (Procesador Intel Core i3-6100U con velocidad de 2,3GHz.Memoria RAM de 4GB. Disco duro de 500GB.)	2	UNIDAD	\$ 1,700,000	\$ 3,400,000
	IMPRESORA Multifuncional Hp 2645 Fax Escáner Copiadora	1	UNIDAD	\$ 140,000	\$ 140,000
	RESMA DE PAPEL	1	UNIDAD	\$ 20,000	\$ 20,000
TOTAL GASTOS					\$ 7,680,000

En la tabla número 2 se observa el cálculo del presupuesto de este proyecto, como talento humano se realiza el análisis de las horas durante las 5 semanas planteadas en el cronograma, se estima un costo promedio de 20.000 pesos colombianos por hora, teniendo un total de 206 horas, para un valor del desarrollo de 4'120.000 pesos colombianos. También se incluye en el presupuesto el valor de los recursos técnicos requeridos para el desarrollo del proyecto, como los computadores portátiles, la impresora multifuncional y resma de papel, con un valor de 3'560.000 pesos colombianos, siendo un valor total de 7'680.000 pesos colombianos en gastos.

8. CONCLUSIONES

La presente investigación se ha dedicado al estudio del directorio activo característica del sistema operativo Windows Server, durante el proceso se pudo evidenciar el conjunto de protocolos y facilidades que permiten manejar apropiadamente la estructura de directorio de la red que muchas organizaciones no le dan importancia suficiente al tema, desaprovechando el adecuado manejo de la información que se almacena en bases de datos centralizadas y dificultando la creación de políticas de seguridad a nivel empresarial. Incidiendo en La información el bien más importante de cualquier entidad, El propósito de este proyecto es concientizar al lector del valor que tiene, establecer el diseño del directorio activo en la entidad estableciendo una comunicación apropiada entre los objetos de la red, y la puesta en práctica de las políticas del grupo, en el directorio activo ayudando a los administradores a crear los ambientes de escritorio adaptados a la responsabilidad del trabajo de cada usuario de igual manera proporcionando el acceso a los recursos de una manera específica.

BIBLIOGRAFÍA

- Alegsa. (14 de 09 de 2015). Alegsa. Obtenido de Alegsa:
<http://www.alegsa.com.ar/Dic/directorio%20activo.php>
- Alvarez Londoño, A. V. (2013). Introducción. En A. V. Alvarez Londoño, GPL (directivas de grupo locales) en windows server 2008 R2 (pág. 3). MEDELLIN.
- E. I. P. (10 de 03 de 2015). Samba 4.2.0 disponible para su descarga. Obtenido de linuxadictos: <http://www.linuxadictos.com/samba-4-2-0-disponible-para-su-descarga.html>
- Francisco Durán Montoya, R. R. (28 de Julio de 2014). Proyecto de Consolidación del Centro de Datos. Obtenido de Proyecto de Consolidación del Centro de Datos: <http://200.0.207.69/handle/10786/782>
- Gomez Gomez, M. A. (2010). Definición LDAP. En M. A. Gomez Gomez, diseño e implementación del servicio de directorio activo (págs. 27-29). Pereira.
- Microsoft. (01 de 08 de 2005). Novedades en Windows Server 2003 R2. Obtenido de TechNet Microsoft: https://technet.microsoft.com/es-co/library/cc773240#BKMK_ADAM
- Microsoft. (12 de 01 de 2005). Protocolo de acceso al directorio. Obtenido de Microsoft: [http://technet.microsoft.com/es-es/library/cc737317\(Ws.10\).aspx](http://technet.microsoft.com/es-es/library/cc737317(Ws.10).aspx)
- Microsoft. (01 de 08 de 2005). technet microsoft. Obtenido de Novedades en Windows Server 2003 R2: <https://technet.microsoft.com/es-es/library/cc773240>
- Microsoft. (01 de 07 de 2014). Server 2008 y Windows Server 2008 R2. Obtenido de Tecnet Microsoft Windows: [https://technet.microsoft.com/es-es/library/dd349801\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/dd349801(v=ws.10).aspx)
- Microsoft, t. (20 de 10 de 2015). Windows Server 2012 R2 y Windows Server 2012. Obtenido de technet microsoft: <https://technet.microsoft.com/es-es/library/hh801901.aspx>
- Ruiz. (2013). Directorio Activo. Some & new books.es, 1.3 p.
----- Conceptos básicos en una estructura de directorio activo. some & news books.es, 1.7 p.

Samba. (29 de 10 de 2015). Historia de samba. Obtenido de Samba:
<https://www.samba.org/samba/history/>

Santos, A. A. (2011). Servicio de Directorio Activo. En A. A. Santos,
Implementación de un sistema de autenticación usando LDAP para control
de acceso a una red (págs. 28-29). Mexico.