



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

**Implementación de un Dominio con Windows Server
2019 en una Dependencia Universitaria**

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

P R E S E N T A

MIGUEL ANGEL CAMBRAY RAMÍREZ

ASESORA DE INFORME

M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS



Ciudad Universitaria, Cd. Mx., 2024

Tabla de contenido

Índice de figuras	6
Índice de tablas	9
Introducción	10
Capítulo 1	11
Presentación de la empresa e ingreso al campo laboral	11
1.1 Ingreso al campo laboral	11
Capítulo 2	13
Proyectos en los que he participado	13
2.1 Dirección General del Colegio de Bachilleres	13
2.1.1 Misión	13
2.1.2 Objetivo.....	13
2.2 Sistema de Inscripciones en los 20 planteles del Colegio de Bachilleres	14
2.2.1 Problemática.....	14
2.2.2 Objetivo.....	15
2.2.3 Desarrollo e implementación.....	16
2.2.4 Resultados	19
2.3 Proyecto 1era. Edición del registro de aspirantes al examen COMIPEMS (Comisión Metropolitana de Instituciones Públicas de Educación Media Superior)	19
2.3.1 Problemática.....	20
2.3.2 Objetivo.....	20
2.3.3 Actividades realizadas para llevar a cabo la implementación	21
2.3.4 Resultados	22
Capítulo 3	24
Antecedentes y teoría de redes como base del proyecto	24
Introducción	24
3.1 Dirección General de presupuesto (DGPO), Dirección de Informática, Coordinación de Soporte Técnico	25
3.1.1 Misión	25
3.1.2 Objetivo.....	25
3.2 Problemática	25
3.3 Justificación del proyecto	27
3.4 Objetivos	28
3.5 Marco teórico: Concepto de redes informáticas y/o de computadoras	29

3.6 Características de una red informática y sus componentes.....	29
3.7 Topologías de red	32
3.8 Criterios de red.....	34
3.9 Tipos de redes informáticas	36
3.9.2 Redes de área metropolitana (MAN – Metropolitan Area Network).....	36
3.9.3 Redes de área amplia (WAN – Wide Area Network).....	37
3.10 Elementos activos y pasivos de una red informática	37
3.11 Elementos pasivos de la red.....	39
3.11.1 Cable de red. Cable CAT5e vs cable CAT6a	39
3.11.1.1 Ancho de banda de CAT5e vs CAT6a.....	40
3.11.1.2 Longitud máxima de cable CAT5e vs CAT6a.....	41
3.11.2 Rack de comunicaciones.....	42
3.11.3 Site o sala de comunicaciones.....	44
3.12 Elementos activos de la red.....	45
3.12.1 Access point.....	46
3.12.2 Servidores.....	47
3.12.3 HUB´s o concentradores y Switches o conmutadores.....	48
3.13 Seguridad física y lógica de la red.....	50
3.14 Medidas para asegurar la red	52
3.15 Intranet	53
3.16 Diferencia entre intranet y red LAN	53
3.17 Diferencia entre intranet e internet	53
Capítulo 4	55
Proyecto: Implementación de un Dominio con Windows Server para sustituir una red con Grupos de trabajo en Servidores independientes	55
4.1 Grupo de trabajo	55
4.1.1 Características de un grupo de trabajo	56
4.1.2 Ventajas del grupo de trabajo	57
4.1.3 Desventajas del grupo de trabajo.....	57
4.2 Definición de dominio.....	58
4.2.1 Ventajas de un dominio.....	59
4.2.2 Desventajas de un dominio.....	59
Capítulo 5	61
Diseño ingenieril	61
5.1 Análisis del proyecto	61

5.2 Diagnóstico	62
5.3 Descripción de la propuesta	63
5.4 Estudio técnico	64
5.5 Estructura temática	64
5.6 Tipo de investigación	65
5.7 Técnica de recolección de información	66
5.8 Diseño	66
5.9 Implementación	67
Capítulo 6	68
Instalación y configuración de Windows Server 2019	68
6.1 Windows Server 2019, ventajas y desventajas	68
6.1.1 Ventajas	68
6.1.2 Desventajas	69
6.2 Requisitos mínimos	69
6.3 Versiones de Windows Server	71
6.4 Instalación de Windows Server 2019	73
6.4.1 Proceso de instalación de Windows Server 2019.....	74
6.4.2 Primeros pasos con Windows Server 2019.....	77
6.4.3 Configuración de las funciones de red de Windows Server 2019	78
6.5 Instalación del dominio	84
6.5.1 Procedimiento para convertir un servidor Windows Server 2019 en Controlador de Dominio (DC)	85
6.5.2 Instalación del rol Servicios de Dominio de Active Directory	85
6.5.3 Añadiendo un segundo controlador de dominio para el dominio existente.....	106
6.5.4 Configurar el servidor DNS del controlador de dominio principal	107
6.5.5 Configuración de reenviadores	114
6.5.6 Configurar las características de red del nuevo servidor	118
6.5.7 Unir el nuevo servidor como cliente del dominio	119
6.5.8 Añadir el rol Servicios de dominio de Active Directory al nuevo servidor	121
6.5.9 Promocionar el nuevo servidor como controlador de dominio secundario	126
6.5.10 Ajustando la configuración de red del nuevo controlador de dominio secundario	130
6.5.11 Comprobar los servidores DNS.....	131
6.5.12 Replicar los controladores de dominio.....	132

6.5.13 Comprobando la replicación.....	135
6.6 Unir un cliente Windows 10 al dominio.....	136
6.6.1 Configurando la red del equipo cliente.....	137
6.6.2 Comprobación de que la configuración de red es correcta.....	137
6.6.3 Cambiar el nombre del equipo y unirlo al dominio.....	138
6.7 Creando Unidades Organizativas y asignarles contenido	141
6.7.1 Crear una nueva unidad organizativa.....	141
6.8 Crear cuentas de usuario en el dominio	143
6.8.1 Operaciones frecuentes sobre cuentas de usuario de un dominio Windows Server 2019.....	146
6.9 Directivas de grupo (GPO).....	147
6.9.1 Definiendo Directiva de grupo o GPO.....	147
6.9.2 Instalar la Consola de Administración de Directivas de Grupo.....	149
6.9.3 Ejemplo de implementación de una GPO.....	150
Capítulo 7	157
Conclusiones.....	157
Recomendaciones.....	159
Definiciones	160
Referencias.....	166

Índice de figuras

Figura 2.2.3.1	Programa típico en el editor de Turbo Pascal versión 7.....	16
Figura 2.3.3.1	El programa dBase III Plus creado por Ashton-Tate en 1979	21
Figura 2.3.3.2	Utilería de Clipper para el manejo de datos.	22
Figura 3.2.1	Red informática con topología en estrella.	26
Figura 3.7.1	Representaciones gráficas de algunas topologías de red.	33
Figura 3.11.1.2	Cable CAT5e y cable CAT6a.	42
Figura 3.11.2.1	Rack de la DGPO.....	43
Figura 3.11.2.2	Distribución de un rack de 2 metros.	44
Figura 3.11.3.1	Site de la DGPO.	45
Figura 3.12.1.1	Access Point de la serie 550 de HPE Aruba instalados en la DGPO.....	46
Figura 3.12.2.1	Servidor PowerEdge T630, y PowerEdge T130, controlador de dominio principal y secundario.....	48
Figura 3.12.3.1	Switch Aruba HPE 2930f instalados en el rack de la DGPO.....	50
Figura 6.4.1.1	Instalación de Windows Server 2019, configuración de idioma.....	75
Figura 6.4.1.2	Instalación de Windows Server 2019, selección del sistema operativo a instalar.	75
Figura 6.4.1.3	Instalación de Windows Server 2019, tipo de instalación.	76
Figura 6.4.1.4	Instalación de Windows Server 2019, gestión de discos del equipo.	76
Figura 6.4.2.1	Administrador del Servidor después de instalar Windows Server 2019.....	77
Figura 6.4.2.2	Opciones de actualización.....	78
Figura 6.4.3.1	Configuración de red.....	79
Figura 6.4.3.2	Estado de la red.....	79
Figura 6.4.3.3	Cambiar opciones del adaptador.	80
Figura 6.4.3.4	Icono de la tarjeta de red del servidor.	80
Figura 6.4.3.5	Información de la conexión ethernet.....	81
Figura 6.4.3.6	Propiedades de la conexión ethernet del servidor.	82
Figura 6.4.3.7	Propiedades del protocolo de Internet versión 4 TCP/IPv4.	82
Figura 6.4.3.8	Configuración por servidor antes de la implantación del dominio.....	83
Figura 6.4.3.9	Configuración básica de un firewall con DMZ.....	84
Figura 6.5.2.1	Localizando la herramienta Administrador del Servidor.....	86
Figura 6.5.2.2	Agregar roles y características.....	86
Figura 6.5.2.3	Asistente para Agregar roles y características.....	87
Figura 6.5.2.4	Seleccionar tipo de instalación.	88
Figura 6.5.2.5	Seleccionar servidor de destino.....	89
Figura 6.5.2.6	Seleccionar roles del servidor.....	90
Figura 6.5.2.7	Confirmando el agregar las características elegidas.	90
Figura 6.5.2.8	Lista de roles seleccionados para instalar.	91
Figura 6.5.2.9	Selección de características a instalar.	92
Figura 6.5.2.10	Servicio de Active Directory y recomendaciones de la instalación de otras características.....	93
Figura 6.5.2.11	Confirmar selecciones de instalación.....	94
Figura 6.5.2.12	Advertencia de reinicios sin notificaciones previas.	94

Figura 6.5.2.13	Confirmar y aceptar el reinicio automático de la instalación.	95
Figura 6.5.2.14	Progreso de la instalación.	95
Figura 6.5.2.15	Opción de promover este servidor a controlador de dominio.	96
Figura 6.5.2.16	Especificando el nuevo dominio.	97
Figura 6.5.2.17	Seleccionar nivel de funcionalidad del nuevo bosque y dominio.	98
Figura 6.5.2.18	Contraseña de modo de restauración de servicios de directorio (DSRM).	99
Figura 6.5.2.19	Especificar opciones de delegación DNS.	100
Figura 6.5.2.20	Nombre de dominio NetBIOS.	100
Figura 6.5.2.21	Rutas de acceso de las bases de datos y archivos de registro.	101
Figura 6.5.2.22	Resumen de opciones de instalación.	102
Figura 6.5.2.23	Script de Windows Power Shell de la instalación.	102
Figura 6.5.2.24	Comprobación de requisitos previos.	103
Figura 6.5.2.25	Reinicio por instalación de Servicios de Active Directory.	103
Figura 6.5.2.26	Primer inicio de sesión.	104
Figura 6.5.2.27	Propiedades del equipo.	105
Figura 6.5.2.28	Propiedades del servidor. Nombre completo del equipo y dominio.	106
Figura 6.5.4.1	Accediendo al Servidor DNS del controlador de dominio principal.	108
Figura 6.5.4.2	Administrador DNS para crear una Nueva zona inversa.	109
Figura 6.5.4.3	Asistente para nueva zona inversa.	109
Figura 6.5.4.4	Elegir tipo de zona para la nueva zona inversa.	110
Figura 6.5.4.5	Ámbito de replicación de zona de Active Directory.	110
Figura 6.5.4.6	Elegir crear búsqueda inversa para IPv4 o IPv6.	111
Figura 6.5.4.7	Establecer el rango de red que será atendido por el servidor DNS.	112
Figura 6.5.4.8	Elegir tipo de actualización dinámica.	112
Figura 6.5.4.9	Finalización del asistente para nueva zona.	113
Figura 6.5.4.10	Zona de búsqueda inversa creada.	114
Figura 6.5.5.1	Propiedades del dominio en el servidor DNS.	114
Figura 6.5.5.2	Reenviadores en el servidor.	115
Figura 6.5.5.3	Editar reenviadores.	116
Figura 6.5.5.4	Direcciones IP de los servidores DNS de reenvío.	117
Figura 6.5.7.1	Unión del nuevo servidor al dominio.	120
Figura 6.5.7.2	Computadoras y DC unidos al dominio.	121
Figura 6.5.8.1	Autenticación al dominio del DC secundario.	122
Figura 6.5.8.2	Agregar roles y características del DC secundario.	123
Figura 6.5.8.3	Rol de Servicios de dominio de Active Directory a instalar.	124
Figura 6.5.8.4	Confirmar selecciones de instalación.	125
Figura 6.5.9.1	Uniendo el nuevo DC a un dominio existente.	127
Figura 6.5.9.2	Opciones del controlador de dominio secundario.	128
Figura 6.5.10.1	Ajuste de la configuración del protocolo TCP/IPv4 del nuevo DC secundario.	130
Figura 6.5.11.1	Configuración del Servidor DNS del DC principal.	132
Figura 6.5.12.1	Comprobando la existencia de los dos controladores de dominio.	133
Figura 6.5.12.2	Comprobando la replicación entre los dos DC.	134
Figura 6.5.12.3	Actualizar sitios y Servicios de Active Directory.	134
Figura 6.5.12.4	Generando la replicación entre los DC.	135

Figura 6.5.13.1 Comprobando la replicación entre los dos DC.....	136
Figura 6.5.14.2.1 Comprobación de la correcta configuración de red del cliente.....	138
Figura 6.5.14.3.1 Cambiar nombre al equipo cliente.....	139
Figura 6.5.14.3.2 Cambio de pertenencia de grupo de trabajo a dominio del nuevo equipo cliente.	140
Figura 6.5.16.1 Crear una Unidad Organizativa.	142
Figura 6.5.16.2 Asignándole nombre a la nueva Unidad Organizativa.	142
Figura 6.5.17.1 Unidades Organizativas del dominio sobre las cuales se pueden crear usuarios..	143
Figura 6.5.17.2 Creando un nuevo usuario en una UO.....	144
Figura 6.5.19.2.1 Instalando la característica Administración de directivas de grupo.	149
Figura 6.5.19.2.2 Abrir consola de Administración de Directivas de Grupo desde la ventana Ejecutar.....	150
Figura 6.5.19.3.1 Representación del orden de procesamiento de las GPO.	152
Figura 6.5.19.3.2 Consola Administración de Directivas de Grupo.....	153
Figura 6.5.19.3.3 Crear una GPO y vincularla.	153
Figura 6.5.19.3.4 Asignándole un nombre a la nueva GPO.	154
Figura 6.5.19.3.5 Configurando las acciones de la política de grupo.....	154
Figura 6.5.19.3.6 Habilitando la Política elegida para que tenga efecto sobre la UO deseada.	155
Figura 6.5.19.3.7 Mensaje indicando que no es posible la acción solicitada debido a la aplicación de una política.....	155

Índice de tablas

Tabla 2.2.3.1 Los 20 planteles del Colegio de Bachilleres.....	18
Tabla 3.7.1 Topologías de red y su descripción.....	33
Tabla 3.10.1 Ejemplos de elementos activos y pasivos en una red informática	38
Tabla 3.11.1.1 Calibres de cable de red y sus respectivas velocidades y frecuencias.....	41
Tabla 3.14.1 Protocolos de seguridad física y lógica en una red.....	52
Tabla 5.2.1 Segmentos de red para cada área de la DGPO.....	62
Tabla 5.4.1 Características del controlador de dominio principal.....	64
Tabla 5.4.2 Características del controlador de dominio secundario.....	64
Tabla 6.2.1 Características del Controlador de dominio principal	71
Tabla 6.2.2 Características del Controlador de dominio secundario.	71
Tabla 6.4.1 Bloqueos y límites de las versiones Standard y DataCenter de Windows Server 2019.	74
Tabla 6.5.5.1 Servidores DNS públicos y gratuitos.....	118

Introducción

El presente trabajo escrito pretende dejar de manifiesto y exponer, la puesta en práctica de los conocimientos adquiridos durante la carrera de Ingeniería en Computación. Aunque un estudiante o egresado de Ingeniería en Computación puede desempeñar actividades del ámbito laboral y profesional, desde analista programador, ingeniero de soporte, comercializador de sistemas de cómputo, entre otros, y una vez adquirida la experiencia suficiente, hasta cargos de dirección, director de centros de cómputo, puestos gerenciales según el ramo, administrador de desarrollo de software, instructor o investigador.

En este trabajo, se exponen algunos proyectos en los cuales he participado en distintas entidades universitarias a las cuales me incorporé, en el ámbito laboral, incluso a la par de mis estudios de licenciatura. Entidades en las que, además de aprender y adquirir experiencia, me permitieron poner en práctica mis conocimientos alcanzados durante la carrera.

Se exponen las experiencias y participaciones en proyectos en mi estancia en la Dirección General del Colegio de Bachilleres y en la Dirección General de Presupuesto (DGPO), instituciones públicas de educación media superior y superior, respectivamente.

Capítulo 1

Presentación de la empresa e ingreso al campo laboral

1.1 Ingreso al campo laboral

Fue en la Dirección General del Colegio de Bachilleres donde incursioné por primera vez al campo laboral, en el año 1992. Poniendo en práctica mis primeros conocimientos básicos en programación que, al ser estudiante, en la Facultad de Ingeniería, en ese entonces, adquirí conocimientos de programación con Turbo Pascal, C y Basic. Así que, al tener esa oportunidad laboral, para mí fue perfecto ya que contaba con los conocimientos básicos en la programación de los lenguajes antes mencionados y que se aplicaban en esta institución. Y con el paso del tiempo, fortalecí en gran medida mis habilidades con estas herramientas de desarrollo, además de aprender otras como dBase 3 Plus y Clipper, de mucho uso por aquellos años. Así como también, adquirir habilidades y experiencia en trabajar con grupos de personas afines y trato con usuarios finales.

Del año 1998 a la fecha, he tenido la fortuna de laborar en la Dirección General de Presupuesto (DGPO) de la Universidad Nacional Autónoma de México (UNAM). Persiguiendo la idea de crecer personalmente, como en experiencia laboral, y en conocimientos relacionados a mi carrera, se dio la oportunidad de incorporarme a esta dependencia universitaria dentro del campus de la misma universidad. Lo que me vino perfecto, dado que continuaba con mis estudios en la Facultad de Ingeniería y estar cerca tanto del lugar de trabajo como de mi lugar de estudios, vino a facilitarme mucho la vida.

En esta dependencia crecí mucho en conocimientos y experiencia ya que aquí, el abanico de oportunidades de aprendizaje fue muy amplio. Pude realizar actividades que van desde redes, soporte técnico, apoyo a usuarios, compras de equipos de

cómputo, desarrollo, bases de datos, administración de servidores Windows, entre otras actividades. Y de este periodo de tiempo y lugar de trabajo, es de donde nace el proyecto motivo del presente trabajo de titulación.

Capítulo 2

Proyectos en los que he participado

2.1 Dirección General del Colegio de Bachilleres

El Colegio de Bachilleres es una institución educativa, creada por decreto presidencial en 1973, que ofrece estudios de nivel medio superior en 20 planteles ubicados en la Zona Metropolitana de la Ciudad de México.

2.1.1 Misión

Formar ciudadanos competentes para realizar actividades propias de su condición científica y momento tecnológico, histórico, social, económico, político, y filosófico, con un nivel de dominio que les permita movilizar y utilizar, de manera integral y satisfactoriamente, conocimientos, habilidades, destrezas y actitudes pertenecientes a las ciencias naturales, las ciencias sociales y las humanidades.

2.1.2 Objetivo

Su objetivo es que los estudiantes egresen con una formación académica integral, de calidad, con motivación e interés por aprender, con adopción de los valores universales que les permitan una adecuada inserción en la sociedad y un buen desempeño en sus actividades académicas o laborales.

2.2 Sistema de Inscripciones en los 20 planteles del Colegio de Bachilleres

Me incorporé laboralmente al Centro de Análisis y Desarrollo de Sistemas (CADS), en mayo de 1992, donde di mis primeros pasos desarrollando pequeñas aplicaciones en Turbo Pascal con el compilador desarrollado por Borlan, dado que ya tenía un poco de experiencia adquirida en la Facultad.

2.2.1 Problemática

Por aquellos años, muchas empresas, dependencias o instituciones, tanto públicas como privadas, en cierto momento, se tenían que enfrentar al hecho de que cuando se trataba de registrar gran cantidad de personas, el proceso se convertía en algo tedioso y engorroso, muchas veces, en pérdida de información de las mismas personas por el hecho de que al no existir los sistemas informáticos para tal efecto, regularmente se les entregaba formatos o plantillas en papel, en los cuales las personas llenaban con la información o datos solicitados y muchas veces, las formas en papel se extraviaban o perdían o traspapelaban de tal manera que su registro no existía o estaba erróneo por no entender lo que se había plasmado en dichos formatos.

Esto también sucedía con el proceso de las distintas inscripciones en los planteles del Colegio. Además de invertir mucho tiempo y mucho personal en tales procesos, se enfrentaban a los problemas descritos en el párrafo anterior.

2.2.2 Objetivo

Ya con algún tiempo en la institución, además de poner en práctica mis conocimientos básicos en el lenguaje de programación Pascal, y a su vez, fortalecerlos; ya que era con lo que aprendí a programar en la Facultad de Ingeniería, formé parte importante del grupo de trabajo encargado de desarrollar las aplicaciones de las distintas inscripciones que el Colegio realiza a lo largo de cada semestre escolar en cada uno de los 20 planteles distribuidos en la Ciudad de México y área metropolitana.

Dicho grupo de trabajo tuvo como objetivo, implementar un sistema de registro de estudiantes para los procesos de inscripciones que cada semestre se realiza en todos los planteles del Colegio. Dicho sistema tendría que ser capaz de hacer más efectivos y eficientes los procesos de registro de inscripciones de los estudiantes de esta casa de estudios. Como metodología de desarrollo se seleccionó el lenguaje de programación Turbo Pascal de Borland que era el lenguaje que la institución utilizaba y que aprendí en la Facultad y que su uso estaba en boga en esos años. Además, de que su utilización obligaba al desarrollo de programas bien escritos, escritos con claridad y relativamente libre de errores. Además de que era un lenguaje orientado para poder ser utilizado en cualquier tipo de computadora. Debido a la facilidad de su implementación, y al volumen de documentos que iba manejar el proyecto, así como un diseño flexible de las interfaces de la aplicación del sistema de registro de inscripciones que se planteaba implementar.

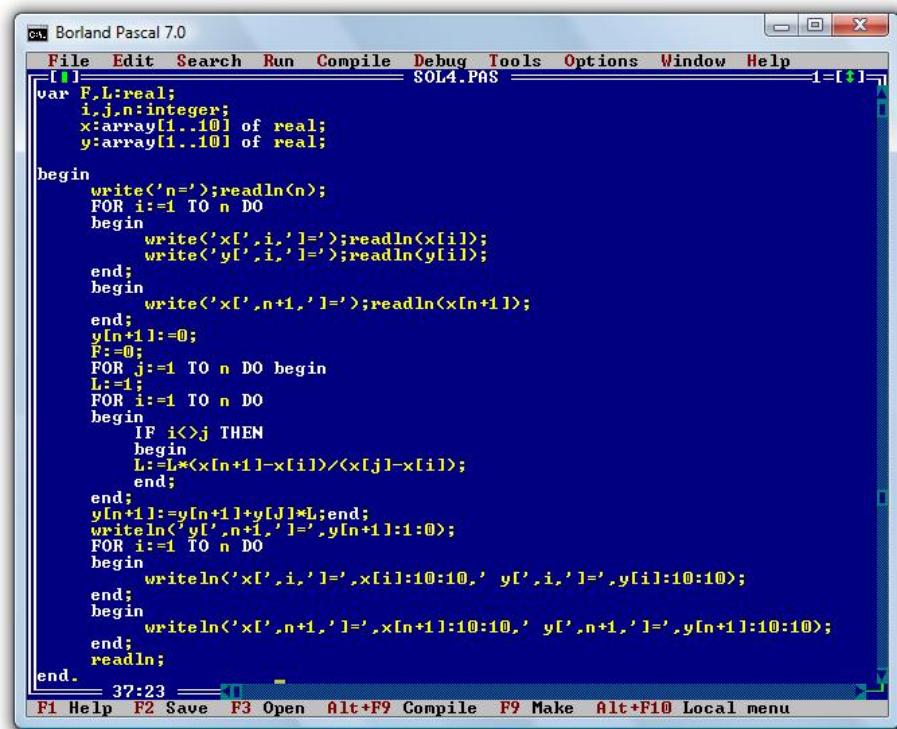
Se desarrollarían 3 aplicaciones con ligeras diferencias entre sí. Estas aplicaciones eran: Inscripción Normal, Inscripción a Examen de recuperación e Inscripción a Exámenes Extraordinarios.

2.2.3 Desarrollo e implementación

La programación que Turbo Pascal nos brinda, que es estructurada, pero se realizaba localmente al equipo, es decir, los ejecutables se podían ejecutar en los distintos equipos destinados para cada proceso de inscripción en cada plantel. No se contaba con una estructura de cliente servidor para los desarrollos que se hacían.

A la par, se desarrollaron también, utilerías de apoyo para llevar a cabo cada una de las inscripciones de la mejor manera.

En la figura 2.2.3.1, se puede apreciar el código escrito en un típico programa en Turbo Pascal.



```
var F,L:real;
    i,j,n:integer;
    x:array[1..10] of real;
    y:array[1..10] of real;

begin
  write('n=');readln(n);
  FOR i:=1 TO n DO
  begin
    write('x[' ,i, ' ]=');readln(x[i]);
    write('y[' ,i, ' ]=');readln(y[i]);
  end;
  begin
    write('x[' ,n+1, ' ]=');readln(x[n+1]);
  end;
  y[n+1]:=0;
  F:=0;
  FOR j:=1 TO n DO begin
    L:=1;
    FOR i:=1 TO n DO
    begin
      IF i<>j THEN
      begin
        L:=L*(x[n+1]-x[i])/<x[j]-x[i]>;
      end;
    end;
    y[n+1]:=y[n+1]+y[j]*L;end;
    writeln('y[' ,n+1, ' ]=',y[n+1]:1:0);
    FOR i:=1 TO n DO
    begin
      writeln('x[' ,i, ' ]=',x[i]:10:10, ' y[' ,i, ' ]=',y[i]:10:10);
    end;
    begin
      writeln('x[' ,n+1, ' ]=',x[n+1]:10:10, ' y[' ,n+1, ' ]=',y[n+1]:10:10);
    end;
  end;
  readln;
end.
```

Figura 2.2.3.1 Programa típico en el editor de Turbo Pascal versión 7.

La información se guardaba en archivos de texto planos, con la información sensible codificada. Debido al volumen de datos, se tuvieron que implementar algoritmos de

búsqueda rápidos. Se entregaba al alumno, su comprobante de inscripción que también la aplicación lo generaba. Para tal efecto, y dado que los planteles tenían los mismos modelos de impresoras, la programación de impresión para comprobantes de inscripción, reportes, se hacía con los códigos proporcionados por los manuales técnicos de las mismas impresoras, que, en esos años, se incluían en papel.

Terminadas las aplicaciones, se destinó un periodo de tiempo para hacer el recorrido por la Ciudad de México y área metropolitana, visitando cada uno de los 20 planteles para realizar la instalación de la aplicación y una capacitación al personal de Asuntos Escolares en la instalación, el uso y manejo del programa y la información obtenida. Se les dejaba el disco con la aplicación, la instalación y utilerías para el cierre de la captura y copia de los archivos de la inscripción de cada equipo utilizado, a discos flexibles, los cuales serían enviados al Centro de Análisis y Desarrollo de Sistemas, CADS, para el manejo de la información de cada plantel.

Se puede decir, que las aplicaciones eran prácticamente las mismas para las distintas inscripciones llevadas a cabo a lo largo de cada semestre. Solo se diferenciaba en los nombres de cada inscripción, fechas, manera de tratar y utilizar la información. Dichas aplicaciones tenían por objetivo, capturar los datos del alumno, como nombre, semestre, matrícula, plantel, y materias solicitadas.

La tabla 2.2.3.1, muestra la relación de los 20 planteles del Colegio de Bachilleres distribuidos por zonas en la Ciudad de México y su área metropolitana.

Tabla 2.2.3.1 Los 20 planteles del Colegio de Bachilleres.

Zona Norte	Zona Centro	Zona Sur
 Plantel 1 El Rosario	 Plantel 3 Iztacalco	 Plantel 4 Culhuacán <small>"Lázaro Cárdenas"</small>
 Plantel 2 Cien Metros <small>"Elsa Acuña Rosetti"</small>	 Plantel 6 Vicente Guerrero	 Plantel 13 Xochimilco- Tepepan <small>"Quino Méndez y Cardín"</small>
 Plantel 5 Satélite	 Plantel 7 Iztapalapa	 Plantel 14 Milpa Alta <small>"Telón Villanova Rojas"</small>
 Plantel 8 Cuajimalpa	 Plantel 9 Aragón	 Plantel 15 Contreras
 Plantel 11 Nueva Atzacolco	 Plantel 10 Aeropuerto	 Plantel 16 Tiáhuac <small>"Manuel Chavarría Chavarría"</small>
 Plantel 18 Tlilhuaca- Azcapotzalco	 Plantel 12 Nezahualcóyotl	 Plantel 17 Huayamilpas- Pedregal
 Plantel 19 Ecatepec		 Plantel 20 Del Valle <small>"Marta Romero"</small>

Debido a que las aplicaciones se ejecutaban en distintos equipos independientes, obviamente, había duplicidad debido a que un alumno, pudo haberle faltado una materia y volvía a formarse en otra fila y realizar otra inscripción, ya sea de la materia faltante o bien realizar otra inscripción completa.

Terminado cada periodo de inscripción, cada plantel enviaba su conjunto de discos flexibles conteniendo los archivos de la captura. El CADS se encargaba de concentrarlos y haciendo uso de las utilerías de apoyo, unía los distintos archivos de la captura en uno sólo por cada plantel. Este archivo a su vez, se sometía a un proceso de depurado para evitar las duplicidades, dejando sólo un registro por alumno con las materias solicitadas.

Terminada la depuración y tratamiento de la información de cada uno de los planteles, y con el visto bueno de las autoridades correspondientes, se realizaba la impresión de toda la captura de la inscripción por plantel. Para la impresión se utilizaban impresoras de impacto y papel stock.

Por último, se regresaba a los planteles, un disco con solo un archivo de la inscripción y la impresión correspondiente para el uso que al plantel le conviniera.

2.2.4 Resultados

Como resultado, se obtiene la agilización del proceso de registro a las distintas inscripciones, y, por lo tanto, se asegura mayor número de estudiantes registrados. Se concluyó, que era indispensable seguir empleando estos recursos devenidos de las tecnologías y hechos a la medida para cumplir con los objetivos relacionados con la optimización de los sistemas de registro de los estudiantes para el proceso de inscripciones en los planteles del Colegio de Bachilleres, pues reducía en gran medida el tiempo de duración de dichos procesos de registro.

2.3 Proyecto 1era. Edición del registro de aspirantes al examen COMIPEMS (Comisión Metropolitana de Instituciones Públicas de Educación Media Superior)

En 1995, las instituciones de educación media superior en México acordaron un proceso para que los jóvenes egresados de las secundarias obtuvieran un lugar a través de una dinámica transparente y equitativa.

Fue así que nació el examen de la COMIPEMS, que tenía y tiene el objetivo de evaluar los conocimientos obtenidos por las y los jóvenes en la educación básica. Los estudiantes son seleccionados para obtener un lugar en una institución de educación media superior. Por ejemplo, alguna preparatoria o CCH de la Universidad Nacional Autónoma de México (UNAM), una vocacional del Instituto Politécnico Nacional (IPN), Conalep o Colegio de Bachilleres.

En 1996, se realizó por primera vez el examen. Las instituciones involucradas eran: el Colegio de Bachilleres, el Colegio Nacional de Educación Profesional Técnica (CONALEP), la Dirección General de Educación Tecnológica Agropecuaria (DGETA), la Dirección General de Educación Tecnológica Industrial (DGETI), la Dirección General de Bachillerato (DGB), el IPN, la Secretaría de Educación del Gobierno del Estado de México, la Universidad Autónoma del Estado de México (UAEMex) y la UNAM.

2.3.1 Problemática

Antes de la creación de la COMIPEMS, las nueve instituciones públicas que la integran llevaban a cabo sus respectivos concursos de ingreso de manera independiente. Esta situación promovía un desacoplamiento entre la oferta disponible y la demanda, así como pago de varias cuotas de examen, fechas de exámenes que se empalmaban, asignación de varios lugares a un mismo aspirante, y saturación de ciertos planteles mientras que otros permanecían con espacios disponibles.

2.3.2 Objetivo

Se pretendía ordenar en un solo concurso el ingreso de los estudiantes en las instituciones que componen la Comisión Metropolitana de Instituciones Públicas de Educación Media Superior (COMIPEMS), garantizando que cada aspirante obtenga un lugar en los miles de aulas diseminadas en el valle de México. Sustituyendo con ello, la antigua práctica en la que cada estudiante tomaba parte de forma independiente en los mecanismos y tiempos de selección de cada organismo educativo. Naturalmente, la peregrinación que hacían los padres de familia para matricular a sus hijos generaba mayor costo y trámites, con el consecuente

sometimiento de los jóvenes a varios exámenes, tal como todavía ocurre en numerosas ciudades del país.

2.3.3 Actividades realizadas para llevar a cabo la implementación

A mediados del mes de marzo de 1996 se forma un grupo de trabajo para comenzar con el desarrollo de la aplicación que se encargaría del registro de los datos personales de los aspirantes, así como de sus opciones de instituciones de educación media superior a ingresar y, muy importante, su domicilio; ya que, con base en este último dato, se haría la asignación de la sede a la cual el aspirante acudiría a realizar el examen.

Se llevó a cabo y se trató de seguir de la manera más apegada, un calendario de actividades y de avances. La programación se realizó con Clipper, y dBase y algunas utilerías para el manejo de los archivos de datos. Debido a que al Colegio sólo se le asignó la parte de captura de datos de aspirantes, el personal que participó era solo del Colegio.

En las figuras 2.3.3.1 y 2.3.3.2, se muestran pantallas de algunas de las herramientas utilizadas para llevar a cabo esta tarea.



Figura 2.3.3.1 El programa dBase III Plus creado por Ashton-Tate en 1979



Figura 2.3.3.2 Utilería de Clipper para el manejo de datos.

La COMIPEMS proporcionó los distintos catálogos como son Planteles tanto de secundarias, como de instituciones de Educación Media Superior, códigos postales, colonias, calles, que fueron utilizados en el proceso de desarrollo de la aplicación y obviamente, en el proceso de registro.

Se asignaron al Colegio de Bachilleres varias sedes como responsable del registro de aspirantes, distribuidas en el área metropolitana. En las cuales, el Colegio dispuso de personal propio, con la previa capacitación para tal evento.

Terminado el proceso de registro de los aspirantes a nivel medio superior, las bases de datos se entregaron a la COMIPEMS para manipular y tratar la información recolectada para organizar el universo de aspirantes en las sedes donde realizaría el examen el 23 de junio de 1996 de acuerdo a la distancia más cercana a sus domicilios.

2.3.4 Resultados

Terminado el proceso, se puede decir, que la COMIPEMS había alcanzado su propósito y objetivo principal de orientar y apoyar a los estudiantes de secundaria y

a quienes han terminado este nivel educativo para la continuación de sus estudios. Asignando de acuerdo a las preferencias de los mismos aspirantes y de acuerdo a su domicilio y promedio de salida de la secundaria, el plantel educativo medio superior que más cerca quedara a su domicilio. Esto se logró y se ha logrado principalmente poniendo a su disposición de manera clara y completa toda la información relativa a las opciones ofrecidas en el nivel en el total de planteles de las nueve instituciones que integran la COMIPEMS.

Capítulo 3

Antecedentes y teoría de redes como base del proyecto

Introducción

Las redes informáticas cumplen una función muy importante en cualquier compañía o empresa. A través de ellas, se espera mejorar la operación dentro de la misma y son fundamentales para resultados óptimos.

Es por esto que toda empresa, sin importar su tamaño, debiera contar con una red informática de cualquier topología dependiendo de la infraestructura con la que se cuente o la que se desee implementar.

Una red informática nos ofrece muchas funcionalidades, desde compartir archivos, recursos, acceder a bases de datos, tener comunicación con otras redes y usuarios dentro y fuera de la empresa, envío de mensajes, carga y descarga de información, las cuales se pueden ver afectadas si no se implementa una red informática adecuada.

Teniendo esto claro, en el año 2022 surge la necesidad de cambiar el esquema actual de la red informática de la DGPO, que consiste de varios servidores independientes con grupos de trabajo con el sistema Operativo Windows Server 2019 a un esquema de red informática con un Dominio con el mismo Sistema Operativo dado que se cuenta con las licencias del mismo. Es decir, lo que se busca lograr, es optimizar de la mejor manera posible, el funcionamiento de la red, así como el tener mucho más control de los recursos e infraestructura, información y control de acceso de los usuarios a los distintos recursos de la red.

3.1 Dirección General de presupuesto (DGPO), Dirección de Informática, Coordinación de Soporte Técnico

Área perteneciente a la Dirección de Informática de la Dirección General de Presupuesto, responsable de brindar asistencia y solución de problemas relacionados con Tecnologías de la Información, así como con el Hardware y Software de un equipo de cómputo, o algún otro dispositivo electrónico o mecánico utilizado por los usuarios de la dependencia, a fin de que les permita realizar su trabajo de la manera más eficiente, práctica y rápida posible.

3.1.1 Misión

Brindar apoyo al usuario interno para el normal desarrollo de tareas diarias y resolver problemas y/o averías relacionadas a la utilización de software y de hardware.

3.1.2 Objetivo

Brindar el apoyo al área administrativa para resolver dudas o problemas que se presenten en la ejecución de software o en el funcionamiento de hardware y proveer una solución integral frente a las dificultades que se presenten.

3.2 Problemática

La DGPO contaba con una red informática de tipo o topología de estrella, en la cual se tenían conectados los distintos servidores con sus distintos propósitos, así como usuarios, impresoras, concentradores, entre otros. La funcionalidad era relativamente eficiente porque con sus pros y sus contras, se tenía el control de los

usuarios y de la información, así como de los dispositivos de uso común y servicios de internet y correo electrónico.

La figura 3.2.1 muestra como estaba estructurada la red de la dependencia con cada uno de los servidores con los que se contaba.

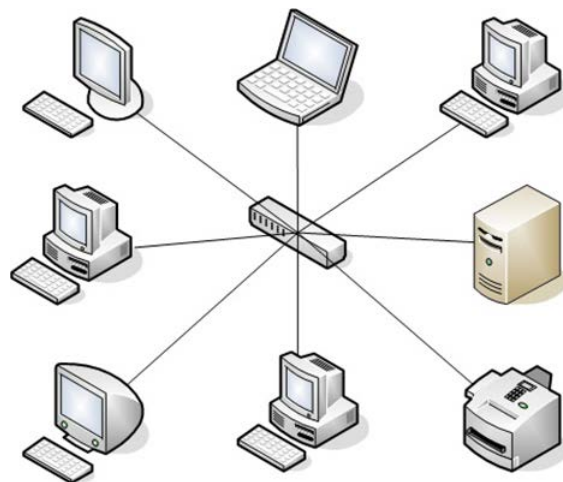


Figura 3.2.1 Red informática con topología en estrella.

Se dificultaba llevar a cabo la correcta gestión de recursos porque en la mayoría de las veces, los usuarios se repetían en los distintos servidores, había que tener muy presente dar de alta los usuarios en los distintos servidores de la misma manera en cómo estaban dados de alta en los otros, así como asignar los mismos permisos y dar accesos a los distintos recursos a los que tenía permitido el acceso. De no ser así, el acceso a recursos o información no era del todo posible.

Los equipos de los usuarios se preparaban con las características según el área a la que el usuario perteneciera, es decir, no todas las aplicaciones, sistemas, y recursos compartidos eran los mismos para todos. Y no se aplicaba ninguna restricción a los mismos, motivo por el cual, cada usuario era libre de poner el fondo de pantalla que quisiera, si le ponía o no protector de pantalla, podía navegar en internet por donde él o ella quisiera, así que podíamos encontrarnos con que cualquier empleado podía

estar viendo y escuchando videos, su novela, película o serie favorita, chateando, y los más arriesgados, hasta viendo páginas para adultos.

Por todas estas y más situaciones, nos encontrábamos con que los equipos se alentaban, ya sea porque tenían algún virus, malware, spyware o cualquier bicho informático (bugs) que afectaba el rendimiento de los equipos, y que cuando se les preguntaba qué habían hecho, ellos no sabían nada o no habían hecho nada extraño o fuera de lo normal.

Por esto, y otra serie de situaciones, el área Soporte Técnico de donde yo formo parte, nos enfrentábamos a estar tratando de solucionar esos problemas provocados por todas esas series de circunstancias no controladas.

3.3 Justificación del proyecto

Los dominios constan de uno o más servidores llamados Controladores de Dominio (DC), y se encargan de la gestión de la seguridad, permisos de usuarios y equipos a través de GPO's (Directivas de Grupo). Un dominio de Windows es una red creada de computadoras donde todos esos equipos, cuentas de usuarios, impresoras, permisos de seguridad, se encuentran dentro de una base de datos, lo que viene siendo el Directorio Activo (Active Directory). Lo forman uno o más servidores que funcionan entre ellos como central donde gestionan la autenticación de todos los usuarios, cuando se inicia sesión los datos se verifican en los servidores centrales.

Las cuentas de dominio necesitan de cuentas de tipo Active Directory; así, podrán iniciar sesión en los ordenadores que forman parte del dominio. Los Controladores de Dominio gestionan las computadoras que forman parte del dominio en cuestión, incluso, miles de computadoras pueden formar parte de un solo dominio. Diferentes redes locales pueden albergar a computadoras que se encuentran bajo un mismo dominio.

Cualquier cuenta de dominio puede iniciar sesión en una computadora bajo el mismo dominio, simplemente utilizando sus credenciales de acceso.

Con base en estas ventajas y a la problemática descrita en la sección 3.2, se expone ante el director de informática el proyecto de migrar la red actual a una red con un dominio basado en Windows Server. Se utilizará el mismo Windows Server instalado en la red actual con servidores independientes y con grupos de trabajo. Esto para aprovechar que se tienen las licencias del sistema operativo y sólo se va hacer uso de las características que vienen incluidas con el mismo Windows Server que no se están explotando y que brindarán una estructura de red mucho más controlada y robusta.

3.4 Objetivos

Objetivo general: Se pretende convertir la red informática actual, basada en servidores independientes y con grupos de trabajo a una red en la cual, sea más eficiente y rápido administrar cambios en la arquitectura de usuarios y permisos. Que sea de manera centralizada y se apliquen a todos los equipos de los usuarios de manera general y no yendo a cada equipo a hacerlo.

Objetivos específicos:

- Analizar el estado actual de la red para determinar los cambios necesarios y llevar a cabo el objetivo general.
- Determinar la mejor solución en operatividad y administración de la red para implementar el dominio a implantarse.
- Establecer hardware y software necesarios.
- Realización de pruebas para verificar la efectividad.

3.5 Marco teórico: Concepto de redes informáticas y/o de computadoras

Teniendo en cuenta que todo este trabajo se basa en una red informática, infraestructura de la misma, es necesario entonces dejar claro qué es una red informática o red de computadoras.

La sociedad actual demanda que intercambiemos información de muy distintos y diversos tipos, ya sea con nuestras familias, amigos, o compañeros de trabajo, formando de este modo, una gran red de contactos. De manera análoga, esto no es diferente en el universo informático, y cuando existe una conexión entre distintos dispositivos, hablamos de una red informática.

3.6 Características de una red informática y sus componentes

Una red informática puede definirse como un conjunto de dispositivos electrónicos interconectados entre sí por un medio -físico o inalámbrico- cuya finalidad es compartir los mismos recursos de la red, como una conexión a Internet e intercambiar información.

Compuesta por dispositivos que actúan alternadamente como emisor o receptor a lo largo del flujo informativo, la red consiste en un poderoso sistema de comunicación en el que intervienen los siguientes elementos:

Servidor

Máquina que ejecuta el sistema (Sistema Operativo) de red usado por las otras estaciones de trabajo, regula y/o controla el tráfico de los archivos entre los diferentes dispositivos funcionando de este modo como centro de control responsable de procesar la información que fluye por una red.

Dispositivos -Hardware-

Los equipos que integran una red informática se dividen en 2 grupos:

Dispositivos de red

Son los elementos que permiten acceder a la información y comunicarse. Este es el caso de los siguientes componentes:

- **Módem:** convierte la señal analógica en digital y viceversa. Es un dispositivo que conecta tu red doméstica con tu proveedor de servicios de Internet, o ISP (Internet Service Provider).
- **Tarjeta de interfaz de red:** Responsable de tomar la información de un dispositivo y enviarla por el medio de conexión.
- **Punto de acceso:** Dispositivo que crea una red inalámbrica WLAN (Wireless Local Area Network) y proyecta la señal Wi-Fi en una determinada región.
- **Bridges:** Habilitan la conexión de varias redes LAN (Local Area Network).
- **Routers:** Elementos cuya función radica en distribuir la señal.
- **Switches:** La función básica es la de unir o conectar dispositivos en red.

Dispositivos de usuario final

Son equipos que se conectan a la red con la finalidad de acceder a los recursos o a la información como pueden ser una *tablet*, una computadora, una *smart TV* y/o una *notebook*.

Medios de conexión

Los medios permiten la interconexión entre los diferentes dispositivos de una red, ya sea de forma física o inalámbrica.

Sistema de cableado o guiado

Integrado por cables, establece los enlaces entre los diferentes dispositivos de la red como la fibra óptica, el cable coaxial o par trenzado –**UTP/STP**.

Sistema inalámbrico o no guiado

Este tipo de medio no utiliza conductores físicos por lo que transportan las señales por medio de radiofrecuencia, ondas infrarrojas o frecuencias de microondas. Como es una vía más sensible, puede sufrir interferencias y distorsiones a raíz de la actividad de otras comunicaciones inalámbricas.

Software

Son los programas necesarios para gestionar el sistema operativo comprendiendo de esta manera, las instrucciones lógicas y los protocolos que guían el funcionamiento de los diferentes dispositivos.

En resumen, podemos concluir que el concepto de red informática es la unión entre dos o más computadoras con el objetivo de compartir información o distintos tipos de recursos a los usuarios de los diferentes puntos de acceso.

3.7 Topologías de red

La topología de red es un concepto que hace referencia a la forma en la que está dispuesta una red, incluyendo sus nodos –puntos de intersección, conexión o enlace de varios elementos– y las líneas utilizadas para asegurar la transmisión y recepción de datos de manera correcta y segura. Dependiendo de este arreglo, se pueden evitar cortes innecesarios o incrementar el flujo de la información transmitida.

Topología es un término utilizado para definir la manera cómo se estructura una red informática considerando la disposición de las máquinas, los *hubs* y los *switches*, es decir, la dinámica de conexión entre todos los elementos de la red.

En esencia, la forma cómo se organizan las máquinas en una red interfiere no solo en la calidad de la conexión, sino también en su estabilidad.

La figura 3.7.1 y la tabla 3.7.1 siguientes, presentan las distintas topologías de red y sus definiciones, así como las representaciones gráficas de algunas de las topologías más comunes.

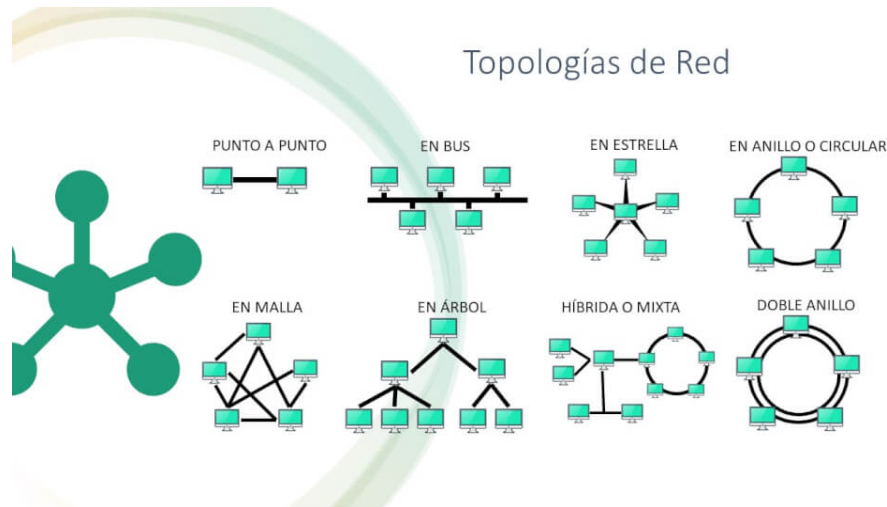


Figura 3.7.1 Representaciones gráficas de algunas topologías de red.

Tabla 3.7.1 Topologías de red y su descripción.

Topología	Descripción
Topología de Bus	También se le conoce como topología de red troncal, bus o línea. En esta red todos los dispositivos se conectan directamente a un canal y no existe otro vínculo entre nodos. Los datos fluyen a lo largo del cable a medida que viaja a su destino. Se instala fácilmente, tiene poco cableado y es fácil aumentar o disminuir el número de aparatos que se adjuntan a la red. Algunos inconvenientes son problemas de congestión, colisión y bloqueo. Además, si existe un problema en el canal, todos los dispositivos quedarán desconectados.
Topología de Anillo	En esta red cerrada, los nodos se configuran en un patrón circular con estructura de anillo. Cada nodo se vincula con los dos contiguos. Al llegar un mensaje a un dispositivo, este comprueba los datos de envío y si no es el receptor, lo pasa al siguiente, y así sucesivamente hasta que lo recibe el destinatario. Ofrece mejor rendimiento que la de bus, es fácil de instalar, pero los nodos no pueden enviar mensajes al mismo tiempo. Es decir que no puede desconectarse ningún dispositivo o se perderá la conexión entre todos.
Topología de Estrella	Es el tipo de topología más común. En ella los dispositivos se conectan a un punto central (hub) que actúa a modo de servidor. Este hub gestiona la transmisión de datos a través de la red. Permite que todas las estaciones se comuniquen entre sí. Sin embargo, si el nodo central tiene algún error, toda la red queda expuesta y puede provocarse una desconexión. Existe también la topología de estrella extendida también conocida como jerárquica o de árbol que funciona igual pero cada elemento que se conecta al nodo central se convierte en el centro de otra estrella.
Topología de Árbol	Esta red tiene un punto de enlace troncal y a partir de este se ramifican los demás nodos. El eje central es como el tronco del árbol. Las ramas se conectan con los concentradores secundarios o los nodos de control y los dispositivos conectados se conectan a los branches. Puede ser de árbol binario en el que cada nodo se fragmenta en dos enlaces o árbol backbone, un tronco con un cable principal que lleva información al resto de nodos ramificados. Entre las ventajas de esta topología está que no se presentan problemas entre los subsiguientes dispositivos si falla uno, reduce el tráfico de red y es compatible con muchos proveedores de hardware y de software. Es aconsejable para redes de gran tamaño.
Topología de Malla	En esta clase de red informática todos los componentes o nodos están interconectados y enlazados directamente mediante vías separadas. La ventaja es que si una conexión falla, existen caminos alternativos para que la información fluya por varias rutas alternativas. Para ello debe haber una limitada cantidad de dispositivos que unir.
Topología híbrida o mixta	Esa topología mezcla dos o más topologías de red diferentes. Adaptar su estructura a las necesidades físicas del lugar en el que se realiza la instalación, así como a los requerimientos de seguridad, velocidad e interconexión. Es fiable porque permite detectar errores y resolver problemas de forma sencilla, es eficaz, escalable y flexible. Sin embargo, es difícil detectar fallas, tiene diseño complejo y difícil y el mantenimiento es caro.
Topología totalmente conexas	En este caso existe un enlace directo entre todos los pares de sus nodos. Se trata de redes caras de configurar, pero siempre con un alto grado de confiabilidad. Existen muchas rutas para los datos que ofrecen la gran cantidad de enlaces redundantes entre nodos. Esta topología se usa sobre todo en aplicaciones militares.

Aunque actualmente la topología de red más utilizada en la actualidad es la de estrella gracias a las ventajas que presenta como son; la alta escalabilidad (permite agregar nuevos nodos de forma sencilla) y la rapidez y facilidad que ofrece para detectar fallas y solucionarlas, se podría indicar que no existe una topología que destaque por encima de las demás como "la mejor". "La mejor" topología será siempre la que se adapte y consiga que sea más eficiente la red de la organización para la que está diseñada. Y en este caso, es la que se utiliza dadas las ventajas mencionadas y a que así se implementó desde que fue concebida en la dependencia. Por lo anterior, si se está pensando en implementar una red informática, la topología en estrella es la que recomendaría en base a mi experiencia con ella, y las ventajas que ofrece.

3.8 Criterios de red

Aunque no seamos conscientes de ello, todos utilizamos redes informáticas en casa o en el trabajo ya que estas interconectan celulares, computadoras entre otros dispositivos. Para que todos estos dispositivos funcionen de la manera más eficiente es necesario planificar la topología de red.

Esencialmente, una topología de red se divide en dos niveles:

- **Físico.** Identifica cómo se conectan los terminales y dispositivos de forma física, utilizando cables y antenas.
- **Lógico.** Considera la manera en la que una red transfiere tramas de un nodo al siguiente. También toma en cuenta las subredes que existen y cómo estas se interconectan.

Contar con una red informática bien estructurada –física y lógicamente– es esencial para asegurar el buen funcionamiento de todos los componentes vinculados. No

importa si son computadoras de escritorio o portátiles, impresoras, servidores, televisiones, proyectores, *hubs* (concentradores), *switches*, enrutadores, cámaras de seguridad o cualquier otro dispositivo que deba acoplarse; la red debe tener la capacidad para crecer y adaptarse a los nuevos requerimientos sin provocar cortes.

Para que una red sea considerada eficiente y efectiva esta debe satisfacer cierto número de criterios entre los más importantes se encuentran el rendimiento, la fiabilidad y la seguridad.

Rendimiento

Se puede medir de muchas formas incluyendo tiempo de tránsito y respuesta. Determina la cantidad de usuarios que pueden acceder a la red al mismo tiempo. Una red con bajo rendimiento y alta latencia tiene dificultades para enviar y procesar grandes volúmenes de datos, lo que provoca congestión y un rendimiento deficiente de las aplicaciones. Se mide en bits por segundo (bps), megabits por segundo (Mbps), o gigabits por segundo (Gbps).

Fiabilidad

Además de la exactitud en la entrega de los datos, que se refiere a los registros sin errores que pueden utilizarse como fuente de información fiable. La fiabilidad se mide por la frecuencia de fallo de la misma, el tiempo de recuperación de un enlace frente a un fallo y la robustez de la red ante una catástrofe. La robustez de la red es una característica crucial para garantizar su supervivencia y funcionalidad continua ante fallas aleatorias y condiciones adversas. Imaginémonos un router que se avería en su servicio de internet o un fallo en el suministro eléctrico. Obviamente, estas fallas afectarían a la red en su conjunto y el impacto en sus componentes y su capacidad para llevar a cabo sus funciones esenciales y básicas se verían seriamente

afectadas. Estos aspectos se tienen que considerar de manera primordial para el diseño de una red informática para que sea resistente a este tipo de fallas.

Seguridad

Los aspectos de la red incluyen protección de datos frente a accesos no autorizados, protección de datos frente a fallos y modificaciones e implementaciones de políticas y procedimientos para recuperarse de interrupciones y pérdidas de datos.

En este sentido, se puede hablar de seguridad física y seguridad lógica. La diferencia es que la seguridad física protege el sitio o site, y todo lo que se encuentre dentro de él, mientras que la seguridad lógica, protege el acceso a los sistemas informáticos.

3.9 Tipos de redes informáticas

3.9.1 Redes de área local (LAN - Local Area Networks)

Son redes telemáticas formadas por un conjunto de dispositivos (generalmente computadoras) interconectados entre sí en un área de extensión limitada. Esta área puede abarcar desde una sala de unas decenas de metros cuadrados, hasta la extensión ocupada por varios edificios próximos entre sí.

3.9.2 Redes de área metropolitana (MAN – Metropolitan Area Network)

Como su nombre lo indica, son redes destinadas a dar servicio a un núcleo metropolitano concreto, extendiéndose a distancias de entre 10 y 100 km. Normalmente, son redes desplegadas por compañías de telecomunicaciones para ofrecer en todos los hogares de una ciudad servicios de conexión a Internet,

televisión por cable, telefonía, entre otros servicios. Proporcionan sus servicios con conexiones de alta velocidad que varían desde varias decenas de Mbps hasta varios cientos de Mbps. El medio de transmisión mayoritariamente usado es la fibra óptica.

3.9.3 Redes de área amplia (WAN – Wide Area Network)

Redes de área mundial a nivel país o continental. Una red WAN es una red de comunicaciones que permite la comunicación de dispositivos sin límite de distancia. Para ello, generalmente se hace uso de los servicios e infraestructuras de comunicaciones proporcionados por los operadores de telecomunicación.

La red instalada en la DGPO, es una red con topología estrella implementada así, desde su origen. Recientemente, se decidió contratar una empresa que se encargara de sustituir el cableado de red de categoría 5E (CAT5e) a categoría 6A (CAT6a). Dicha empresa, además de llevar a cabo todo el cableado, también implementó un rack de comunicaciones con la finalidad de que éste, aloje los equipos y sistemas de comunicaciones, como servidores, switches, telefonía, junto con todo el cableado necesario para el correcto funcionamiento de la red. Ya que es un elemento fundamental en todo sistema de comunicaciones y que alberga equipos de alto valor, como lo son los distintos servidores, que a su vez resguardan información muy valiosa y delicada para la DGPO. Además, muy importante para que las actividades y servicios que presta la dependencia se mantengan disponibles las 24 horas del día, los 365 días del año.

3.10 Elementos activos y pasivos de una red informática

Como ya se mencionó anteriormente, se reestructuró la red completa de la DGPO por parte de una empresa. Esto implicó cambiar totalmente el cableado de red, e

implementar y conformar una sala de comunicaciones o site donde se alojaría la infraestructura de red nueva. Al estructurar dicha red, se emplearon diferentes componentes que permiten que la información se transmita de un sistema a otro, ya que, como cualquier forma de comunicación, requiere de un emisor, un canal, un mensaje y un receptor. Específicamente, hablamos de los dispositivos de red. Y hablando de dispositivos de red tenemos que hablar de **dispositivos activos** y **dispositivos pasivos**, los cuales se involucraron en la mencionada reestructuración de red. La diferencia que existe entre un dispositivo activo y uno pasivo es que los dispositivos pasivos, se utilizan para interconectar los enlaces de la misma red de datos, mientras que los dispositivos activos se encargan de distribuir en forma lógica y activa la información a través de la red.

Como dispositivos activos se puede mencionar los hub o concentradores, enrutador o router, switches, modem. Y como dispositivos pasivos jacks o conectores, cableado, fibra óptica, patch panel, canaletas. La tabla 3.10.1 presenta algunos ejemplos más de dispositivos activos y pasivos.

Tabla 3.10.1 Ejemplos de elementos activos y pasivos en una red informática

Elementos activos y pasivos de una red informática	
Activos	Pasivos
Switches	SITE o Closet principal
Routers	IDF o closet secundario
Servidores	Cables de fibra óptica
Antenas	Patch panel
Tarjetas de red	Cableado
PC´s	Racks
Concentradores	Patch cords
HUB´s	Sistemas de canalización

Parte fundamental en la ya mencionada reestructuración de la red de la DGPO, fue el cambio total del cableado de red, la implementación de un rack de comunicaciones, así como de una sala de comunicaciones o site. Por lo mismo,

vamos a profundizar más en estos elementos o dispositivos de una red informática para entender también el porqué de los cambios e implementaciones en los mismos.

3.11 Elementos pasivos de la red

3.11.1 Cable de red. Cable CAT5e vs cable CAT6a

Se sustituyó el cableado categoría 5e que se tenía originalmente a uno de categoría 6a que es mucho mejor y más actualizado. Actualmente, la tecnología en cables Ethernet son actualizados de manera continua para aumentar las velocidades del ancho de banda y reducir el ruido, por lo que seleccionar uno que brindara las mejores características y desempeño, y hacer una inversión fuerte en infraestructura de red, garantiza dejarla preparada para un futuro a mediano y largo plazo sin problemas serios de obsolescencia.

Categoría 5e: Esta es una versión mejorada de Cat5 y es compatible con las mismas especificaciones. En cambio, Cat5e es capaz de soportar velocidades de transmisión de hasta 1 Gbps y una distancia máxima de 100 metros. En este caso es adecuado para redes domésticas y pequeñas empresas con un tráfico de red moderado, pero se estaría un tanto limitados además de que actualmente ya no es una categoría recomendada por el estándar.

Categoría 6a: Se trata de una versión mejorada de Cat6 y es capaz de soportar velocidades de transmisión de hasta 10 Gbps y una distancia máxima de 100 metros. Cat6a es el más adecuado para redes empresariales con un tráfico de red alto y una gran cantidad de dispositivos conectados. También es compatible con tecnologías de red de 40 Gbps y 100 Gbps. Es la mejor opción calidad-precio para aquellos que quieran montar una red informática con excelentes prestaciones y velocidades en

desempeño con muy buen margen de tiempo para pensar en cambiarse nuevamente.

Como puede observarse, hay diferentes tipos de cables de red, y cada uno tiene sus propios usos y beneficios en función de la velocidad de transmisión y la distancia máxima que pueden soportar. El cableado de red es uno de esos componentes que son vitales para las infraestructuras de hoy en día. Estos permiten la comunicación entre los dispositivos, para lo cual cada vez es más demandada la velocidad de transferencia y capacidades en general. En estos últimos años, es clara una evolución en este tipo de cableado de forma constante, en parte gracias a las nuevas tecnologías o mejoras en las velocidades y latencias de las transmisiones. Es por esto que la evolución no cesa, ya que siempre se tendrá alguna tecnología que mejore a la anterior. Por eso es bueno planear y planificar una infraestructura que nos permita permanecer vigentes durante un periodo de tiempo largo hasta que las tecnologías nos alcancen y los estándares indiquen que es necesario volver a actualizar la infraestructura de red.

En conclusión, los próximos estándares de red apuntan a un aumento lógico en las capacidades. Así como en la simplificación de las infraestructuras. Todo esto es algo que aumenta su demanda de forma considerable, por lo cual es importante estar preparados. Especialmente cuando sabemos que es necesario para mantener las infraestructuras con un funcionamiento óptimo.

3.11.1.1 Ancho de banda de CAT5e vs CAT6a

CAT5e llega al tope a velocidades de 1 Gbps con un ancho de banda de hasta 100 MHz. Y el CAT6a a 10 Gbps con hasta 250 MHz de ancho de banda.

Como se puede ver, la principal diferencia entre los cables CAT5e y CAT6a reside en el ancho de banda que puede admitir el cable para las transferencias de datos. Los cables CAT6a han sido diseñados para trabajar con frecuencias de hasta 250 MHz, en comparación con los 100 MHz de los cables CAT5e. Esto significa que un cable CAT6 puede procesar más datos al mismo tiempo. Es similar a la diferencia entre una autopista de 2 y otra de 4 carriles. En ambas se podrá circular a la misma velocidad, pero una autopista de 4 carriles soporta mayor tráfico al mismo tiempo.

La tabla 3.11.1.1 presenta las relaciones de los distintos calibres de cables de red con sus correspondientes velocidades y frecuencias.

Tabla 3.11.1.1 Calibres de cable de red y sus respectivas velocidades y frecuencias.

CATEGORÍA	VELOCIDAD	FRECUENCIA
CAT 5	100 Mbit/s	100 MHz
CAT 5E	1000 Mbit/s	100 MHz
CAT 6	1000 Mbit/s	250 MHz
CAT 6A	10000 Mbit/s	500 MHz
CAT 7	10000 Mbit/s	600 MHz

3.11.1.2 Longitud máxima de cable CAT5e vs CAT6a

Tanto CAT5e como CAT6a ofrecen longitudes de hasta 100 m por segmento de red. Las velocidades máximas alcanzables nunca se lograrán más allá de esta longitud. Esto puede dar como resultado una conexión lenta o con fallos, o incluso una

desconexión. Si hay que cubrir distancias mayores a los 100m, se puede amplificar la señal mediante repetidores o conmutadores.

CAT5e y CAT6a son cables de pares trenzados. Ambos utilizan cables de cobre, con 4 pares trenzados (8 hilos) por cable (Figura 3.11.1.2).

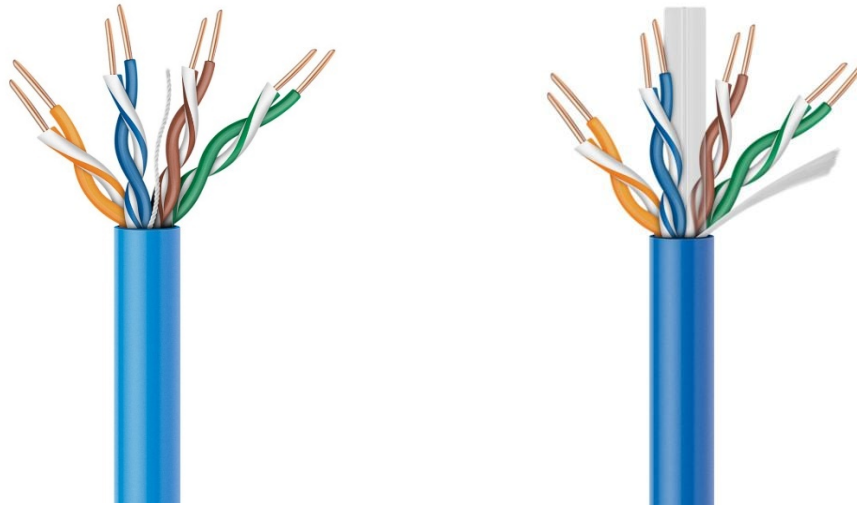


Figura 3.11.1.2 Cable CAT5e y cable CAT6a.

3.11.2 Rack de comunicaciones

Es una estructura metálica de diseño sencillo. Tiene como principal finalidad alojar aquellos equipos, redes y sistemas de telecomunicaciones, como servidores, switches, computadoras, sistemas de redes y telefonía, junto con todo el cableado necesario para su correcto funcionamiento.

Si bien hay en el mercado diferentes modelos, todos los racks de comunicaciones deben cumplir con ciertos estándares o características en común para ofrecer la funcionalidad necesaria. Esto se debe a la importancia que tienen dentro de una instalación de esta naturaleza.

Por ejemplo, las medidas estándar que debe ofrecer un rack son de 19 pulgadas de ancho y 42U de altura. En cuanto a la profundidad, es más común que haya variaciones, pero debe ser lo suficientemente espaciosa para que cualquier *hardware* quepa fácilmente. Además, será hasta el fondo del rack donde se ubiquen los cables, con los cuales se debe tener especial cuidado.

La altura interior de los racks se mide en unidades de altura conocidas como unidades U. Una unidad de altura U equivale a 50 milímetros de longitud.

Otro aspecto a tener en cuenta es la temperatura. No hay que perder de vista que los equipos que se resguardan dentro del rack, se alimentan de energía eléctrica y, por ende, expulsan calor. Si estos equipos llegan a sobrecalentarse, su funcionamiento puede verse afectado, e incluso puede presentarse riesgo de incendio. La figura 3.11.2.1 es del rack que se implementó en la DGPO después de terminada la reestructuración completa de la red.



Figura 3.11.2.1 Rack de la DGPO.

En el gráfico de la figura siguiente, figura 3.11.2.2, se muestra una disposición habitual de un armario de comunicaciones o **rack**. Es de 42 U de altura (más de 2 metros como muestra la escala a la izquierda) De arriba a abajo tiene un SAI (Sistema de Alimentación Ininterrumpida), un router, el panel de conexiones RJ45, un monitor y teclado (poco frecuente), una unidad de backup en cinta, la CPU servidor, una matriz de discos NAS y una regleta de enchufes.

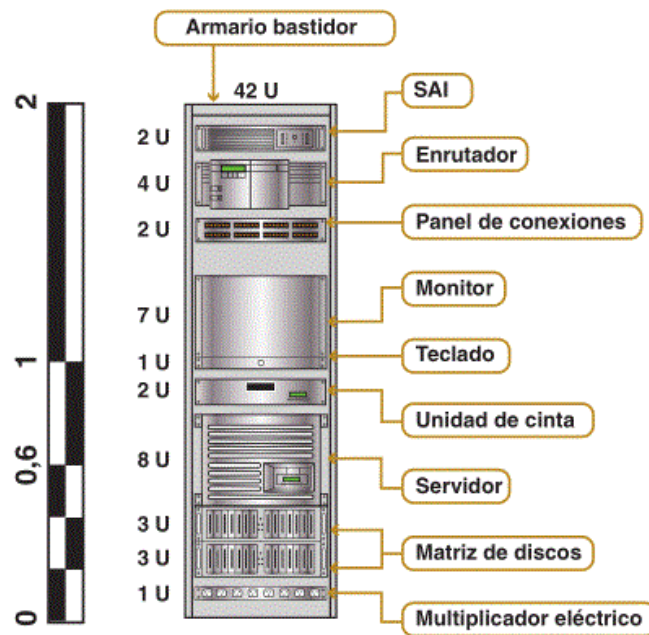


Figura 3.11.2.2 Distribución de un rack de 2 metros.

3.11.3 Site o sala de comunicaciones

Tanto el rack de comunicaciones, como los distintos servidores de bases de datos, de archivos, se encuentran alojados dentro del site de comunicaciones de la dependencia, figura 3.11.3.1. De vital importancia para el correcto funcionamiento de toda la infraestructura de red y comunicaciones de la dependencia. Es un área pequeña de aproximadamente 16 metros cuadrados de superficie. Obedeciendo a la mayoría de usos y normas que rigen a los sites de comunicaciones.

Cuenta con seguridad, climatizado y con acceso controlado con huella digital solo para personal autorizado, tomas de energía eléctrica reguladas con un sistema de energía eléctrica que respalda a los equipos de cómputo del edificio, además de No-break dedicados que respaldan a cada equipo o dispositivo dentro del site, que garantiza que los equipos críticos puedan seguir funcionando por un rango de tiempo en caso de un corte de energía eléctrica.



Figura 3.11.3.1 Site de la DGPO.

3.12 Elementos activos de la red

Son aquellos dispositivos o equipos que se encargan de distribuir en forma activa la información a través de la red, como concentradores, access point, switches, router, entre otros. Además, se encargan de distribuir banda ancha a determinada cantidad de equipos en una red.

3.12.1 Access point

También conocidos como WAP (Wireless Access Point) son dispositivos de red que interconectan equipos inalámbricos, creando una red de área local inalámbrica, interconectando tarjetas de red, celulares o varios equipos. Al mismo tiempo sirve para interconectarse con otra red externa.

También se pueden conectar a una red cableada, donde puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Estos puntos de acceso se conectan a un *router*, *switch*, o *hub* por un cable Ethernet; y proyecta una señal Wi-Fi en ciertas áreas designadas. Incluso tienen asignadas direcciones IP, para que puedan ser configurados.

En pocas palabras, la función principal de los Access Point es permitir la conectividad con la red, haciendo a un lado la tarea de direccionamiento de servidores, enrutadores y switches.

En la DGPO se instalaron Access Point para interiores de la serie 550 de HPE Aruba Networking. La siguiente figura presenta el modelo instalado.



Figura 3.12.1.1 Access Point de la serie 550 de HPE Aruba instalados en la DGPO.

3.12.2 Servidores

Son dispositivos de cómputo que almacenan, distribuyen y suministran información. Los servidores funcionan basándose en el modelo "cliente-servidor". El cliente puede ser tanto una computadora como una aplicación que requiere información del servidor para funcionar. Por tanto, un servidor ofrecerá la información demandada por el cliente siempre y cuando el cliente esté autorizado. Los servidores pueden ser físicos o virtuales.

En el caso de ser físico, se trata de un hardware, también conocido como *host* (anfitrión), es un equipo de cómputo integrado a una red de nodos basados en software, figura 3.12.2.1. Por otra parte, los servidores virtuales (VPS, *Virtual Private Server*) son softwares que proporcionan servicios a otros programas (clientes).

Los servicios que prestan los servidores son requeridos continuamente y, por tanto, la mayoría de los servidores nunca se apagan. Si un servidor dejara de funcionar, eso puede causar muchos problemas a los usuarios. Por tanto, los servidores suelen estar programados para ser tolerantes a fallos.

Dentro del mundo de los servidores hay una gran variedad. Los más usados y/o conocidos son los siguientes:

- Servidor web
- Servidor DNS
- Servidor Proxy
- Servidor de correo electrónico
- Servidor FTP



Figura 3.12.2.1 Servidor PowerEdge T630, y PowerEdge T130, controlador de dominio principal y secundario.

3.12.3 HUB´s o concentradores y Switches o conmutadores

Un HUB, o más conocido en español como *concentrador*, es un dispositivo mediante el cual se pueden conectar varios dispositivos entre sí, para que puedan comunicarse. Es capaz de crear una red de computadoras conectadas entre sí y además con posibilidad de ampliarse mediante otros dispositivos similares.

Recordando qué es el modelo OSI y en qué consiste, el HUB Ethernet trabaja en la capa física de este modelo, o en la capa de acceso al medio si hablamos del modelo TCP/IP. Es decir, un Concentrador se encarga de recibir una señal de datos y repetirla para enviarla por sus diferentes puertos. Entonces, básicamente estamos hablando de un repetidor.

El HUB funciona como un punto central de conexión y repite la señal que recibe a tantos puertos como equipos haya conectados en ellos. Luego cada equipo se encargará de identificar si la información que recibe es útil y le pertenece, o va destinada a otro.

En la actualidad, no se recomienda el uso del HUB y definitivamente sí el uso del Switch. Ambos dispositivos son capaces de “repetir” la señal de datos de una fuente hacia los equipos que están conectados a él, pero hay una diferencia importante. Un HUB no es capaz de distinguir si la información que pasa por él va dirigida a un ordenador u otro. Este dispositivo se limita a recibir la información y repetirla para todos sus puertos, independientemente de lo que haya conectado en ellos. A esto se le llama broadcast, recibir una y enviar a todos. Un problema que tienen los HUB es la rápida saturación del ancho de banda, debido a la repetición masiva de los datos.

Por su parte, un Switch o Conmutador es la versión inteligente de un HUB, en este caso es un dispositivo que trabaja en la capa de enlace de datos del modelo OSI y es por esto que son los más utilizados en redes actualmente. Físicamente es similar a un HUB, pero en su interior existe un programa informático o firmware que es capaz de entender la información que por él viaja y enviarla solamente al nodo que la necesita. Entonces la ventaja es obvia, el ancho de banda estará mucho más optimizado y seremos capaces de comunicar ordenadores entre sí de forma independiente y sin necesidad de enviar toda la información a todos los puertos.

Por supuesto, un HUB no se puede gestionar, ya que no tiene ningún tipo de software accesible, mientras que un Switch sí que tiene esta posibilidad (no todos), estos dispositivos incorporan cortafuegos, por ejemplo. Es por esto que son los dispositivos más utilizados al día de hoy para crear redes internas cableadas de alta velocidad y eficiencia.

En el proyecto de reestructuración llevado a cabo en la DGPO, además de cambiar todo el cableado de red, también se colocaron switches en el rack que se dejó instalado del tipo de la figura 3.12.3.1, como varios patch panel ethernet Cat6a para mantener organizado el site o sala de comunicaciones, así como para facilitar el traslado, adición o cambio de la infraestructura de cableado en el futuro.



Figura 3.12.3.1 Switch Aruba HPE 2930f instalados en el rack de la DGPO.

3.13 Seguridad física y lógica de la red

Una red LAN permite que todos los dispositivos dentro de una empresa, estén interconectados. Es un tipo de red muy útil para transferir datos y archivos entre usuarios. Al contar con conexión a Internet se pueden realizar muchas tareas, aunque también estamos expuestos a otros peligros.

Con la expansión de Internet y sus múltiples funciones, los ataques que se pueden recibir diariamente se multiplican y es necesario contar con los mejores servicios de ciberseguridad. Algunos de los más famosos, como un ataque de malware, pueden hacer que perdamos todos los datos e información delicada, mientras que otros comprometen la seguridad, como los escuchas. Aunque no es de vida o muerte, sí es importante que se conozca y se tenga en cuenta, sobre todo para saber cómo poder evitarlos o, en caso contrario, cómo poder combatirlos.

La seguridad física y la seguridad lógica son dos aspectos de un plan de seguridad de la información y son necesarios para implementar la seguridad en las empresas.

La seguridad lógica se refiere a los controles específicos establecidos para administrar el acceso a los sistemas informáticos y los espacios físicos dentro del site o sala de comunicaciones. Usar una puerta cerrada para salvaguardar la entrada de la sala de servidores del site puede ser una mejor práctica de seguridad física, pero tener que participar en factores para abrir la puerta es una forma de seguridad lógica.

La seguridad lógica ayuda a proteger contra amenazas conocidas como ataques cibernéticos, pero también protege a los centros de datos de sí mismos. El error humano es una de las causas más frecuentes de tiempo de inactividad y otras desgracias de TI, ya sea por negligencia o intención maliciosa.

Si bien las amenazas físicas pueden incluir robo, vandalismo con daño físico, las amenazas lógicas son aquellas que pueden dañar los sistemas de software, datos o red sin dañar realmente el hardware.

La seguridad lógica protege el software informático al desalentar el acceso de usuarios mediante la implementación de identificaciones de usuario, contraseñas, autenticación, y tarjetas inteligentes.

La seguridad física evita y desalienta a los atacantes a ingresar a un edificio instalando cercas, alarmas, cámaras, y en casos mucho más rígidos, guardias de seguridad y perros, control de acceso electrónico, detección de intrusos y controles de acceso de administración.

La diferencia entre la seguridad lógica y la seguridad física es que la seguridad lógica protege el acceso a los sistemas informáticos y la seguridad física protege el site y todo lo que se encuentra dentro del mismo.

El término Seguridad lógica se utiliza coloquialmente para referirse a medidas electrónicas como los permisos dentro del sistema operativo o las reglas de acceso en las capas de la red, como el firewall, enrutadores y conmutadores. La seguridad física se usa tradicionalmente para describir puertas de entrada controladas, videovigilancia y otras medidas físicas.

3.14 Medidas para asegurar la red

Teniendo presente las posibilidades de riesgo antes mencionadas, es importante preguntarse de qué manera se puede proteger la red. Regularmente, este proceso comienza desde la misma implementación y puesta en marcha de la misma, cuando se realiza un proceso minucioso para desarrollar la seguridad, siguiendo los protocolos recomendados para los dos tipos de seguridad. Algunos protocolos tanto de seguridad física como de seguridad lógica, se presentan en la tabla 3.14.1.

Tabla 3.14.1 Protocolos de seguridad física y lógica en una red

Protocolos de seguridad física	
Seguridad de red física	Tareas como mantener actualizado el hardware, software, servidores y enrutadores, activar los parches de seguridad y realizar un respaldo periódico de datos e información es una base fundamental que debe realizarse para asegurar el buen funcionamiento de la red LAN.
Uso de contraseñas	Estas son fundamentales para asegurarnos de que tan solo aquellas personas que de verdad lo necesitan tienen acceso al sistema, a la nube o al almacenamiento privado. Es imprescindible el uso de contraseñas seguras, con un mínimo de 8 caracteres, con letras mayúsculas y minúsculas, así como símbolos y signos de puntuación, y que esta cambie periódicamente. Cabe destacar que el uso de nombres, acrónimos, fechas o datos conocidos o accesibles no son recomendados para su uso como contraseñas.
Verificación de identidad	Con el fin de confirmar que quienes acceden al sistema son quienes dicen ser, se deben establecer datos de autenticación. Además del usuario y la contraseña, que pueden ser robados en algún momento, otros sistemas como la huella digital o el lector de retina pueden complicar el acceso a la red LAN de intrusos.
Protocolos de seguridad lógica	
Soluciones de software y hardware	Además de las medidas anteriores, en la seguridad de una red LAN pueden emplearse software y hardware para mitigar ataques, por ejemplo: programas de cifrado y protección de datos o hardware que permitan el reconocimiento de usuarios para impedir intrusiones.
Implementación de antivirus, firewall, y demás.	Los virus, el phishing y los troyanos son ejemplos de amenazas lógicas que se pueden descargar o propagar inadvertidamente mediante el uso de unidades flash. En el peor de los casos, un ataque no solo afecta a un solo dispositivo, sino que se propaga a través de una red, robando datos confidenciales o apagando los sistemas operativos.
Control de acceso seguro	Controlar de forma remota qué dispositivos tienen acceso a la red LAN, pudiendo confirmar o denegar el uso de esta, puede ayudarnos a mantener a raya a los hackers.

3.15 Intranet

Una intranet es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como internet, por lo que solo los miembros de esa organización tienen acceso a ella.

3.16 Diferencia entre intranet y red LAN

Ambos conceptos hacen referencia a una "red interna" la diferencia es el contexto en el que se utilizan.

LAN se refiere a la infraestructura, y diseño de una red, donde se incluye el cableado, los puntos de acceso, equipos de comunicación como routers, switches.

Por otro lado, intranet, se utiliza para referirse más bien a los servicios que esta red presta a los usuarios, como acceso a bases de datos, sitios web internos.

3.17 Diferencia entre intranet e internet

Si bien ambos términos comparten varias características similares, suelen generar confusión y, en algunos casos, hasta se piensa que son exactamente lo mismo.

Partimos de la premisa que en ambos entornos se comparte información. Para el caso particular de internet, la información es de carácter público. Es decir, cualquier persona con una conexión a internet puede acceder a ella. Se compone de todas aquellas computadoras que estén conectadas a la red informática global (World Wide

Web). En términos de infraestructura, sería difícil de materializarlo ya que crece exponencialmente y es a nivel global.

Por otro lado, está la intranet, que también es un entorno para compartir información, sólo que esta se encuentra localizada en una red específica, y sólo pueden acceder a ella los usuarios que sean 'admitidos' en ella. De manera que se trata de una red privada. Un claro ejemplo es la red de una empresa específica, en donde se comparte información confidencial y que concierne a la misma. En estos casos la cantidad de computadoras/usuarios es tangible y generalmente limitada, y la accesibilidad está dada por un método de ingreso encriptado (clásico caso de usuario y contraseña).

Cabe aclarar que ambos entornos pueden coexistir. De hecho, la intranet generalmente depende de internet, más aún en redes que no están conectadas físicamente.

Capítulo 4

Proyecto: Implementación de un Dominio con Windows Server para sustituir una red con Grupos de trabajo en Servidores independientes

Primero voy a explicar en qué consiste un grupo de trabajo y dominio y las ventajas e inconvenientes para cada uno. Así será mucho más fácil entender, conocer y tener más claro por qué la decisión de implementar un dominio en este caso, ya que depende de varias variables.

Los dominios y grupos de trabajo son las maneras de organizar computadoras en las redes informáticas, ya sea oficina o empresa. Son muchas las diferencias, pero las más importantes están enfocadas en la organización, administración, seguridad y jerarquía de los equipos que lo conforman, y de manera centralizada, siendo éstas, las principales diferencias entre los dos esquemas. Los equipos que tienen de sistema operativo Windows en una red se encuentran dentro de un grupo de trabajo o de un dominio. Lo usual es tener en las redes domésticas un grupo de trabajo (Workgroup) y las empresariales que se encuentran en oficina o empresa, son organizados por un Dominio (Domain).

4.1 Grupo de trabajo

En los grupos de trabajo, cada equipo se usa de forma totalmente individual, desde gestión, configuraciones y seguridad que tenga implementada. Cada equipo de cómputo es independiente de los demás en los usuarios que tiene creados, y su gestión de autenticación se realiza en cada equipo de forma independiente. No es como un dominio, donde se gestiona en otros equipos (Servidores) de forma general a todos los equipos.

Como son independientes, a la hora de conectarse a otros equipos (a carpetas compartidas) se deberá proporcionar usuario y contraseña (si no se ha definido de forma general a todos sin contraseña). Estando en un dominio se puede gestionar las unidades desde el servidor y a los usuarios, por lo que esta gestión es más cómoda.

4.1.1 Características de un grupo de trabajo

Los puntos importantes de los que consta un grupo de trabajo son:

- Todos los equipos son jerárquicamente iguales, es decir, que ninguno manda sobre otros, cada uno es individual y realiza su jerarquía individual, ni manda sobre otros.
- Al ser individuales, cada uno de los equipos en un grupo de trabajo tiene sus cuentas de usuario. Al no haber una gestión general, sólo es posible entrar en cualquier equipo (iniciar sesión) si se conoce su usuario y contraseña. No hay passwords de administradores generales.
- No tiene protección de contraseña, por lo que, al ser independientes, es más fácil recibir un ataque. Al no ser las contraseñas y usuarios centralizados no es posible resetear desde el servidor central ningún usuario o contraseña.
- El tope que suele haber dentro de un grupo de trabajo no suele ser más de 20 computadoras.
- Aquí a nivel de redes deben estar en la misma subred.

4.1.2 Ventajas del grupo de trabajo

Para analizar la conveniencia de implementar un grupo de trabajo, es importante considerar las ventajas e inconvenientes que se tendrían implementando un grupo de trabajo.

- Es más económico que comprar un servidor, no sólo por la computadora sino por la licencia de Windows Server que se va a tener que comprar. Y también la licencia de las computadoras cliente, ya que no todas las versiones son compatibles con Dominio (son algo más caras).
- Tiene menos gasto de energía eléctrica e infraestructura al no tener un equipo o más como servidores y permanecer siempre encendidos para que puedan funcionar todos los usuarios, además de climatización.
- Existe un ahorro al no tener que pagar soporte para la gestión y mantenimiento de una infraestructura más grande como es una de Dominio.
- Es mucho más fácil y rápido configurar los equipos en un grupo de trabajo.

4.1.3 Desventajas del grupo de trabajo

- Es más incómodo a la hora de gestionar los usuarios y cambios que se deseen realizar en todos los equipos ya que se tendrá que hacer en cada uno de ellos, no hay gestión centralizada.
- Cuando crezca la empresa y sean más de 20 usuarios, se tendrá que cambiar el esquema de servidores independientes a un dominio y la migración será más costosa y complicada al tener que migrar toda la información a cuentas de dominio en lugar de cuentas locales. Y todo esto en cada uno de ellos.

- La seguridad no es controlada ni centralizada por lo que, si se pretende realizar jerarquías, auditorías, chequeos generales, es necesario estar en un Dominio.
- En un grupo de trabajo las contraseñas (autenticación) se gestionan localmente en cada equipo. En un dominio se gestionan las contraseñas desde el controlador de dominio (Servidor) de forma centralizada.

4.2 Definición de dominio

Los dominios constan de uno o más servidores que son los "Controladores de Dominio" (DC = Domain Controller) y son los encargados de gestionar muchos aspectos como son la seguridad, permisos de usuarios y equipos a través de GPO's (Directivas de Grupo). Un dominio de Windows es una red creada de computadoras donde todos esos equipos, cuentas de usuario, impresoras, permisos con su gestión de seguridad y demás, se encuentran dentro de una base de datos central, lo que viene siendo el Directorio Activo (Active Directory = AD).

Lo componen uno o más servidores que funcionan entre ellos como central donde gestionan la autenticación (login) de todos los usuarios, ya que cuando se realiza un inicio de sesión los datos no se verifican en las computadoras locales, sino en los servidores centrales. Ahora bien, es importante identificar si interesa implementar un Dominio para una oficina, en este y en la mayoría de los casos sí, pero no en todos. Lo mejor es que se analicen las ventajas y desventajas de montar un dominio Windows Server en una oficina.

4.2.1 Ventajas de un dominio

- Es más eficiente y rápido a la hora de realizar y gestionar cambios en la arquitectura de usuarios, permisos, credenciales, ya que se gestionan de manera central y se pueden aplicar directamente en todas las computadoras de la empresa de forma automática, sin ir a cada una de ellas.
- Se pueden tener miles de equipos en un dominio, no como el límite de 20 que se tiene en un grupo de trabajo.
- Multitud de opciones interesantes como creación de perfiles móviles, esto es para que el servidor albergue los perfiles de los usuarios y eso da la libertad de que al iniciar sesión en cualquier equipo de la oficina aparecerán sus datos y configuraciones. Lo que viene siendo movimiento libre.
- Mucho más seguro, tanto la posibilidad de gestión interna (limitando accesos, perfiles, reseteo de cuentas, cambios automáticos de plantillas de seguridad) todo esto centralizado.
- Los equipos pueden encontrarse en diferentes redes locales.

4.2.2 Desventajas de un dominio

- Tiene más gasto de energía eléctrica e infraestructura ya que es necesario poner individualmente y protegidos de acceso físico a los servidores controladores del dominio (puede ser 1 o más).
- Requiere tener bien configurados y gestionados los servidores de dominio y su mantenimiento, ya que deberá contar con personal calificado que lleve un soporte correcto.

- La inversión es más elevada debido al costo por las licencias tanto de los servidores (con Windows Server) y de los equipos cliente (computadoras de los usuarios) ya que deben tener versiones que acepten integrarlos en un dominio.

Capítulo 5

Diseño ingenieril

5.1 Análisis del proyecto

La infraestructura de red de la DGPO era de varios servidores Windows Server 2019 de manera independiente. La cual, de una u otra manera, cubría las necesidades de red de la dependencia. Resguardando la información de usuarios, recursos compartidos, seguridad, bases de datos de Microsoft SQL Server, impresoras.

Dicha infraestructura presentaba varios fallos debido a la independencia de los servidores ya que los usuarios tenían que ser registrados en todos y cada uno de ellos, y muchas veces, no se reproducían todos sus permisos y privilegios presentado problemas para accesos a información o servicios y recursos compartidos.

Los usuarios, sobre todo los que tienen cierta experiencia, se tomaban la libertad de poder modificar las características de red y en repetidas ocasiones, perdían la conexión a sus recursos compartidos e información, ponían los tapices que querían, escuchaban música, veían videos, películas, telenovelas, que se reflejaba en el consumo del ancho de banda y muchas veces afectando en los procesos importantes de manejo de información que lleva a cabo la Dirección de Informática. Debido a todo eso y más, se provocaban fallos en los servicios por la ralentización en la red teniendo que paralizar actividades y obviamente, ocasionando retrasos y molestias. Por estos y otros motivos, se hace necesario la implementación de alguna tecnología que reduzca todos estos problemas o bien, que los evite. Surge entonces el proyecto de implementar un dominio con Windows Server 2019 el cual, por sus características, permita solventar y evitar toda esta problemática.

5.2 Diagnóstico

Actualizar infraestructura de red: Esto era necesario y se solventó con la actualización de la infraestructura completa de la red. Esta la llevó a cabo una empresa externa y se habló ampliamente de ello en capítulos anteriores.

Organización de segmentos de la red: Ejecutar un plan de organización de segmentación de la red de la DGPO. Esto también lo llevó a cabo la empresa encargada de actualizar la infraestructura de red asignando segmentos de red distintos para cada área de la DGPO. Como se puede observar en la tabla 5.2.1.

Tabla 5.2.1 Segmentos de red para cada área de la DGPO.

Área	Segmento de red
Dirección general	10.10.1.X
Dirección de análisis, registro y control	10.10.5.X
Dirección de Programación Presupuestal Institucional	10.10.3.X
Dirección de Integración Presupuestal	10.10.4.X
Dirección de Estudios Administrativos	192.168.142.X
Dirección de Informática	10.10.6.X
Unidad Administrativa	10.10.2.X

Mejoramiento de la plataforma WiFi: Puntos de acceso inalámbricos de Aruba, instalados e implementados por la misma empresa que actualizó la infraestructura de red.

Seguridad: Se tiene implementado el firewall PFSense. Con esta herramienta se gestiona y analizan logs, se genera de manera automatizada informes, análisis de vulnerabilidades, escaneo de red, correlación de eventos. Con el objetivo de

mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información de la dependencia.

Servidores: Disponer de dos servidores para controladores de dominio, principal y secundario, con discos duros con espacio más que suficiente, así como memoria RAM, con el objetivo de ampliar capacidad, almacenamiento y rendimiento.

5.3 Descripción de la propuesta

La propuesta de dos servidores controladores de dominio, consiste en brindar una solución efectiva en caso de que uno de los dos servidores falle, el otro tomaría el control y administración de los recursos mientras se prepara un servidor más para suplir el que presentó la falla.

En caso de que el controlador de dominio principal fuera el que fallara, el controlador de dominio secundario se promovería a controlador principal y tomaría el control dado que tiene las mismas funciones y contiene toda la información y prácticamente ningún usuario notaría el fallo ya que el servidor que queda en funcionamiento, seguiría dando los servicios dado que en la instalación de dichos servidores se implementó también la replicación entre ellos.

La principal funcionalidad será la de proteger la información y mejorar las cargas de trabajo en cada servidor ya que los dos estarán accesibles y sincronizados garantizando que, en caso de algún fallo en alguno de los dos, el que queda disponible, sigue dando servicio a los usuarios.

5.4 Estudio técnico

Para llevar a cabo la replicación y sincronización entre los dos controladores de dominio, y garantizar así el servicio óptimo a los usuarios evitando fallas y retrasos en la gestión de la red minimizando el tiempo de inactividad por fallas, se cuenta con dos servidores, tablas 5.4.1 y 5.4.2, de los cuales ya se habló de sus características en capítulos anteriores pero que se repiten para dejar claros y cubiertos los requisitos de hardware.

Tabla 5.4.1 Características del controlador de dominio principal.

Modelo	PowerEdge T630
Fabricante	DELL Inc.
BIOS	2.15.0
Procesador	Intel® Xeon® CPU E5 2620 v3 @ 2.40 GHz (12 CPU´s)
Memoria RAM	8192 MB
Versión DirectX	DirectX 12
Adaptadores de RED	BroadCom NetXtreme Gigabit Ethernet

Tabla 5.4.2 Características del controlador de dominio secundario.

Modelo	PowerEdge T130
Fabricante	DELL Inc.
BIOS	0.06
Procesador	Intel® Xeon® CPU E3 1220 v6 @ 3.00 GHz (4 CPU´s)
Memoria RAM	16384 MB
Versión DirectX	DirectX 12
Adaptadores de RED	BroadCom NetXtreme Gigabit Ethernet

5.5 Estructura temática

La metodología utilizada para la realización del proyecto, consistió en dividirlo en dos fases. La primera fase o inicial, fue la de levantamiento de información y objetivos a alcanzar. Continuando con la segunda fase, la del diseño lógico y diseño físico.

En la primera fase, también conocida como fase de análisis. Se definió la metodología de trabajo, en donde se estableció el ámbito y parámetros a seguir para el análisis de todos los procesos actuales.

Se realizó el levantamiento de información, realizando el análisis general de cómo venía funcionando la DGPO. Cuáles eran los fallos o problemática detectando la falta de un esquema tecnológico necesarios que ayudaran a realizar las actividades propias de la DGPO en su total cabalidad. De igual manera, se fijaron las necesidades y objetivos que la dependencia buscaba con la implementación del nuevo esquema de red.

5.6 Tipo de investigación

Se realizó una investigación aplicada, es decir, se llevó a la práctica los conocimientos personales. Puesto que se proponía diseñar e implementar un esquema de red para la gestión de usuarios y recursos compartidos de la dependencia, ésta tuvo una participación muy activa en el desarrollo del proyecto.

Se aprovechó también, la experiencia adquirida durante los años de 2000 a 2003 en los cuales tuve la oportunidad de trabajar con la versión de Windows Server 2000 también en una dependencia universitaria. En ese primer acercamiento con Windows Server, llevé a cabo la implementación de un dominio mucho más pequeño ya que sólo era para una subdirección y sólo se implementó un controlador de dominio. En realidad, se trataba del todavía Windows NT pero que había adoptado el nombre de Windows 2000 Server por estar a inicios de la década de los años 2000. Estaba pensado para usuarios avanzados, negocios y empresas, servidores de red, archivos y carpetas.

Dentro de las tareas que se podían realizar se incluían: crear cuentas de usuarios, asignar recursos y privilegios, actuar como servidor web, FTP, servidor de impresión, DNS o resolución de nombres de dominio, servidor DHCP, entre otros servicios básicos. Dicho sistema operativo era muy eficiente comparado con su antecesor y su principal punto fuerte era el Active Directory, herramienta desde la cual se podía administrar toda la infraestructura de red de una organización.

Me di a la tarea de investigar para la versión 2019 que era la que se iba a implementar en el presente proyecto, además de que se implementaría un esquema de dos controladores de dominio en lugares geográficos y subredes distintas. Por lo que era necesario ponerse al día respecto a la nueva versión 2019 que se pensaba implementar.

5.7 Técnica de recolección de información

La recolección de la información se realizó mediante entrevistas con la Dirección de Informática en las cuales se exponían las ideas y propuestas y se retroalimentaban con sugerencias y nuevas ideas de tal manera que se robusteció la idea original del proyecto.

5.8 Diseño

En esta parte, entra la instalación y configuración de Windows Server 2019 en los dos servidores disponibles como partes fundamentales del proyecto. Todo este proceso se explica detalladamente en el capítulo 6 hasta dejarlos a punto para tomar la administración completa de usuarios y recursos y que es así como quedaría funcionando la red.

5.9 Implementación

La redundancia es uno de los pasos para lograr una alta disponibilidad en los servicios y tiene que ver directamente con mantener siempre la información disponible en más de un sitio o repositorio primario, para que, en caso, de un error humano, de software, o cualquier otro tipo de problema, se tenga la facilidad de responder a cualquier solicitud de la información. Eliminando si no al 100%, si en un muy alto porcentaje, los posibles fallos por cuestiones de mal uso de los recursos de la red por parte de los usuarios o por fallas propias en la infraestructura.

La implementación de un dominio con Windows Server 2019 es la propuesta llevada a cabo para evitar en lo posible, los malos hábitos de uso de la red de la DGPO, así como para tener una mejor administración de los recursos de red y de los usuarios en el uso de estos recursos, manteniendo la integridad de la información, así como su disponibilidad.

Todo este proceso de implementación se detalla en el capítulo 6. Al cual se puede recurrir como una guía para implementar desde la instalación y configuración de Windows Server 2019, hasta la implementación de un dominio bajo este sistema operativo.

Capítulo 6

Instalación y configuración de Windows Server 2019

6.1 Windows Server 2019, ventajas y desventajas

Es una distribución de Microsoft para el uso en servidores. Es lo que se llama un sistema multiproceso y multiusuario.

Windows Server está desarrollado en C++ y ensamblador. Una de sus características más destacadas para equipos de trabajo, es que es un sistema multiusuario. Por lo tanto, es un sistema que pueden utilizar todos los empleados de una determinada empresa, centralizando así la gestión y administración de archivos.

Las ventajas que ofrece Windows Server como Sistema Operativo son relevantes para favorecer el trabajo de los programadores y desarrolladores y, por tanto, mejorar los resultados corporativos. Tiene una administración muy sencilla, de modo que el sistema se puede manejar de forma rápida y eficiente. Además, destaca por ser muy flexible.

La primera versión del sistema fue Windows 2000 Server, lanzada a principios del nuevo milenio. Fue concebida para ser el servidor de archivos, impresión y web de PYMEs. Una solución extraordinaria para cuando no era necesario contar con un servidor dedicado a cada tarea, pudiendo así tener todo centralizado en un único servidor. Era capaz de soportar hasta cuatro procesadores.

6.1.1 Ventajas

La curva de aprendizaje en Windows Server es mucho menor que en otros sistemas, en parte porque es bastante similar a las versiones de escritorio que se conocen desde hace décadas que si bien en la versión para servidores incorpora herramientas

y servicios diferentes lo hace de la misma forma haciendo que el sistema se sienta familiar.

- Es fácil de administrar.
- Hay mucha documentación oficial que facilita su uso.
- Menor tiempo de desarrollo.
- Aprendizaje sencillo.

6.1.2 Desventajas

No es un sistema que se caracterice por ser seguro, no tanto porque sea malo en ese sentido sino porque al estar directamente relacionado con los Windows de escritorio es de la familia de sistemas operativos más usado y por lo tanto es un blanco favorito de criminales y malware.

- Hay que pagar por la licencia para utilizarlo.
- Windows es uno de los sistemas operativos con más fallos de seguridad.
- Hacen falta conocimientos de administrador avanzado para la instalación y configuración de alto nivel.
- Consume más cantidad de recursos en comparación con otros sistemas operativos para servidores.
- Hay que reiniciar después de una actualización.

6.2 Requisitos mínimos

Para el caso que se trata en este informe y como ya se mencionó en un principio, se utiliza Windows Server 2019 debido a que ya se contaba con el software y sus licencias. Se tenía instalado en varios servidores, pero no con todas sus características, por lo tanto, los servidores eran independientes. Los requisitos para utilizar Windows Server 2019 son relativamente estrictos.

Procesador: El rendimiento del procesador depende tanto de la frecuencia de reloj como del número de núcleos y tamaño de la caché. El procesador debe tener como mínimo 64 bits a 1,4 GHz. Además, tiene que ser compatible con el conjunto de instrucciones.

RAM: La memoria RAM debe ser como mínimo de 512 MB. En caso de querer instalar Servidor con Experiencia de Escritorio, la capacidad tiene que ser de al menos 2 GB.

ROM: Cualquier equipo que ejecute Windows Server 2019 tiene que incluir un adaptador de almacenamiento compatible con las características de la arquitectura PCI Express. La memoria ROM mínima exigida es de 32 GB.

Adaptador de red: En cuanto a los adaptadores de red, deben tener una capacidad de rendimiento mínima de 1 GB y ser compatibles con la especificación de arquitectura PCI Express.

Otros: Además, Microsoft establece otros requisitos: unidad de DVD, módulo de plataforma segura, monitor que admita resolución Super VGA, acceso a Internet y sistema basado en UEFI 2.3.1c.

Para el proyecto, se nos proporcionaron dos equipos de cómputo, un servidor DELL, destinado a ser el controlador de dominio principal, y además de otro servidor DELL de características menores destinado a ser el controlador de dominio secundario. Cada uno con las siguientes características mostradas en las tablas 6.2.1 y 6.2.2:

Tabla 6.2.1 Características del Controlador de dominio principal

Modelo	PowerEdge T630
Fabricante	DELL Inc.
BIOS	2.15.0
Procesador	Intel® Xeon® CPU E5 2620 v3 @ 2.40 GHz (12 CPU´s)
Memoria RAM	8192 MB
Versión DirectX	DirectX 12
Adaptadores de RED	BroadCom NetXtreme Gigabit Ethernet

Tabla 6.2.2 Características del Controlador de dominio secundario.

Modelo	PowerEdge T130
Fabricante	DELL Inc.
BIOS	0.06
Procesador	Intel® Xeon® CPU E3 1220 v6 @ 3.00 GHz (4 CPU´s)
Memoria RAM	16384 MB
Versión DirectX	DirectX 12
Adaptadores de RED	BroadCom NetXtreme Gigabit Ethernet

6.3 Versiones de Windows Server

A lo largo de la historia han existido numerosas versiones de Windows Server.

- **Windows 2000 Server**

La primera versión de la distribución fue lanzado a principios del año 2000. Por aquel entonces se trataba como un software para la implementación en servidores de servicios web.

- **Windows Server 2003**

Solo tres años después nació la segunda versión, con mejoras considerables en el ámbito de la seguridad.
- **Windows Server 2008**

En 2008 nació la tercera versión de Windows Server, que guardaba grandes similitudes con Windows Vista. La razón es que ambos sistemas compartían determinadas áreas del código.
- **Windows Server 2008 R2**

Es una versión mejorada de Windows Server 2008. Fue una gran revolución en el sector informático ya que fue el primer Sistema Operativo de 64 bits lanzado por Microsoft.
- **Windows Server 2012**

El principal objetivo de esta versión no era otro que captar suscriptores.
- **Windows Small Business Server**

Tal y como su propio nombre indica, este Sistema Operativo está especialmente desarrollado para pequeñas empresas.
- **Windows Essential Business Server**

Muy similar a la anterior, pero esta versión está pensada para empresas de tamaño medio.
- **Windows Home Server**

Microsoft lanzó esta versión para hogares. Así, las personas que vivían en una misma vivienda podían compartir documentos y copias de seguridad, entre otros archivos, de forma segura.
- **Windows Server 2016**

La penúltima versión del SO lanzada por la empresa norteamericana. También recibe el nombre de Windows Server vNext.

- **Windows Server 2019**

El sistema está construido sobre la base de Windows Server 2016. Ya en plena era digital, apuesta por la virtualización y la nube, ofreciendo a las empresas un entorno híbrido en el que pueden aprovechar las ventajas de entornos locales y nubes públicas.

- **Windows Server 2022**

Actualmente, la opción más segura y estable de Windows Server. La seguridad es una de los puntos fuertes de esta versión, además de su compatibilidad total con Azure, el servicio en la nube de Microsoft.

6.4 Instalación de Windows Server 2019

Se describe el proceso de instalación de Microsoft Windows Server 2019 de manera simplificada señalando las partes consideradas importantes o relevantes del proceso y detallando la importancia de las mismas con algunas imágenes.

Este proceso, se puede considerar una guía rápida para instalar y configurar un servidor completo de Windows Server que dé soporte a los equipos de una red con el mismo sistema operativo. Se señala el punto en donde el servidor es sólo un servidor independiente y se continúa el proceso de instalación y configuración del mismo instalando roles, funciones y Active Directory, donde éste último es la piedra angular de Windows Server para un dominio.

Como la mayoría de los clientes en la DGPO son Windows 10 y algunos Windows 11, el tipo de servidor que se ha seleccionado es Windows Server 2019 Standard.

Microsoft proporciona su sistema en versiones Essentials, Standard y Datacenter. Se selecciona Standard porque es la más versátil y equilibrada para una pequeña y mediana empresa, sin gran limitación de procesadores, RAM ni conexiones a carpetas compartidas. La tabla 6.4.1 presenta algunas de las características

comparativas entre las versiones 2019 Standard y Datacenter de Windows Server 2019.

Tabla 6.4.1 Bloqueos y límites de las versiones Standard y DataCenter de Windows Server 2019.

Bloqueos y límites	Windows Server 2019 Standard	Windows Server 2019 Datacenter
Número máximo de usuarios:	Según licencias CAL	Según licencias CAL
Número máximo de conexiones SMB	16,777,216	16,777,216
Número máximo de conexiones RRAS	Sin límite	Sin límite
Número máximo de conexiones IAS	2,147,483,647	2,147,483,647
Número máximo de conexiones RDS	65 535	65 535
Número máximo de sockets de 64 bits	64	64
Número máximo de núcleos	Sin límite	Sin límite
RAM máxima	24 TB	24 TB
Puede usarse como invitado de virtualización	Sí; 2 máquinas virtuales, más un host de Hyper-V por licencia	Sí; máquinas virtuales ilimitadas , más un host de Hyper-V por licencia
El servidor puede unirse a un dominio	sí	Sí
Protección de red y firewall de Edge	no	No
DirectAccess	sí	Sí
Códecs de DLNA y streaming de archivos multimedia web	Sí, si se instala como servidor con Experiencia de escritorio	Sí, si se instala como servidor con Experiencia de escritorio

6.4.1 Proceso de instalación de Windows Server 2019

Se arranca el servidor con el medio de instalación con Windows Server 2019 introducido. Primeramente, se debe elegir el idioma que se va a instalar, figura 6.4.1.1, formato de hora y moneda y teclado o método de entrada. *Siguiente.*

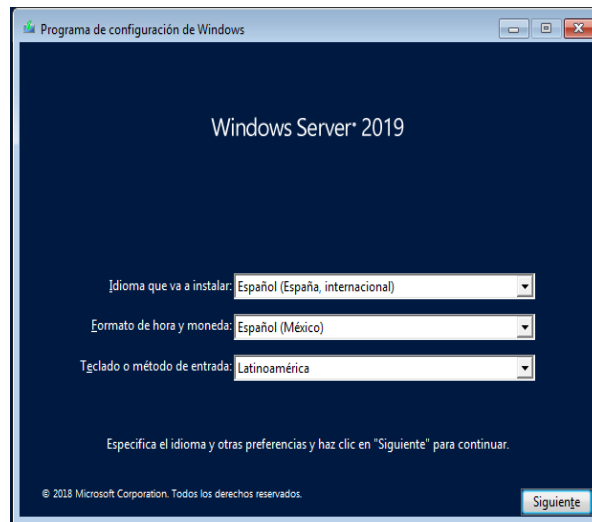


Figura 6.4.1.1 Instalación de Windows Server 2019, configuración de idioma.

En la siguiente pantalla que se presenta, elegir *Instalar ahora*. La instalación se iniciará.

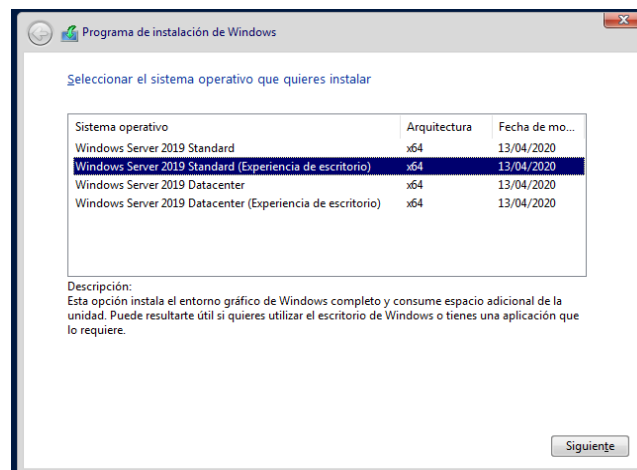


Figura 6.4.1.2 Instalación de Windows Server 2019, selección del sistema operativo a instalar.

Seleccionar *Windows Server 2019 Standard (con experiencia de escritorio)*, figura 6.4.1.2. Permite usar el sistema con entorno gráfico, además de disponer del esquema completo de roles y características.

Aceptar los *Términos de licencia y avisos aplicables*. Elegir o definir el tipo de tarea a realizar, que puede ser:

Actualización, si se cuenta con un sistema ya preinstalado, o *Personalizada*, con la cual será posible seleccionar el disco donde se instalará el sistema operativo o bien particionar el mismo según sea necesario. Figura 6.4.1.3.

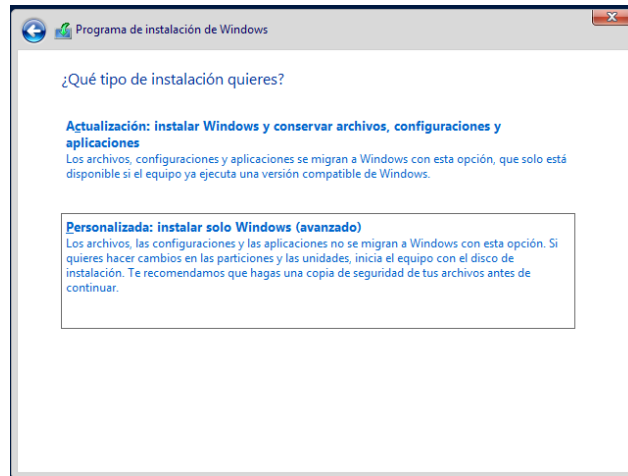


Figura 6.4.1.3 Instalación de Windows Server 2019, tipo de instalación.

Se continúa con la gestión de los discos, figura 6.4.1.4, en este caso, se selecciona el único disco de forma completa. Previamente, se realizó una gestión del RAID con la utilidad de la que dispone el servidor. Pulsar *Siguiente* para iniciar con la instalación.

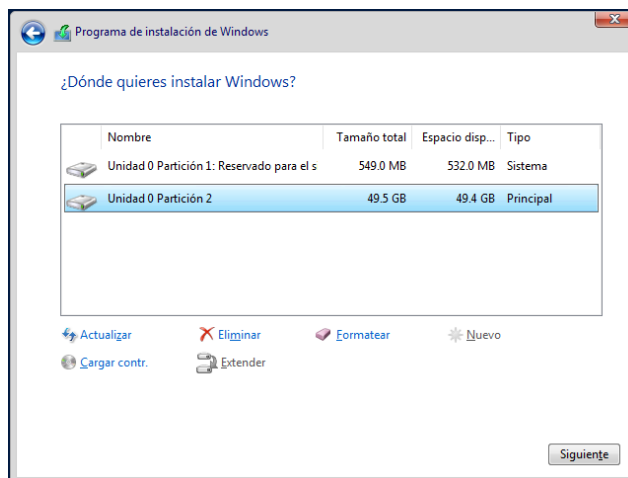


Figura 6.4.1.4 Instalación de Windows Server 2019, gestión de discos del equipo.

Comienza la copia y preparación de los archivos de instalación, y se instalan características y actualizaciones. Al finalizar, el equipo se reinicia. Al reiniciar, se solicita definir la contraseña de la cuenta de administrador del equipo y/o servidor; que debe de cumplir con una serie de condiciones de complejidad.

6.4.2 Primeros pasos con Windows Server 2019

Se inicia el sistema por primera vez con las credenciales antes mencionadas. Y primeramente se presenta la pantalla del Administrador del Servidor como se ve en la figura 6.4.2.1. Es muy recomendable instalar todas las actualizaciones disponibles, antes de seguir con cualquier tipo de acción. Es una práctica muy recomendada, activar las actualizaciones para otros productos de Microsoft, como para productos de terceros para un mejor desempeño y funcionamiento del software instalado, figura 6.4.2.2. Actualizar es una práctica imprescindible en todos los sistemas operativos.

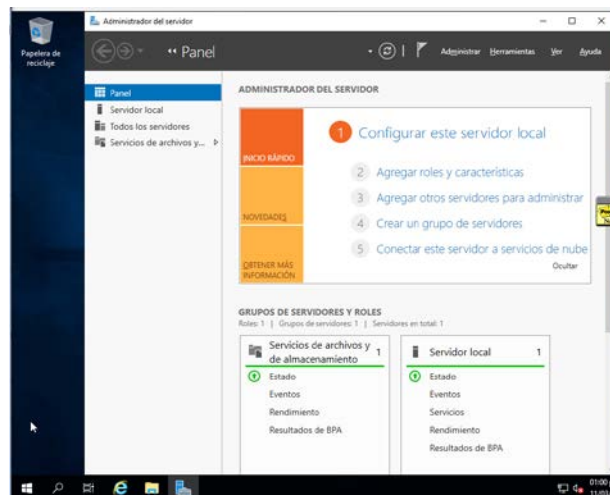


Figura 6.4.2.1 Administrador del Servidor después de instalar Windows Server 2019.

De igual manera, es muy recomendable revisar el *Administrador de dispositivos*, para comprobar si están todos instalados o se necesita instalar algún driver que no haya

encontrado *Windows Update*. Se debe obtener la versión más reciente en la web del fabricante.

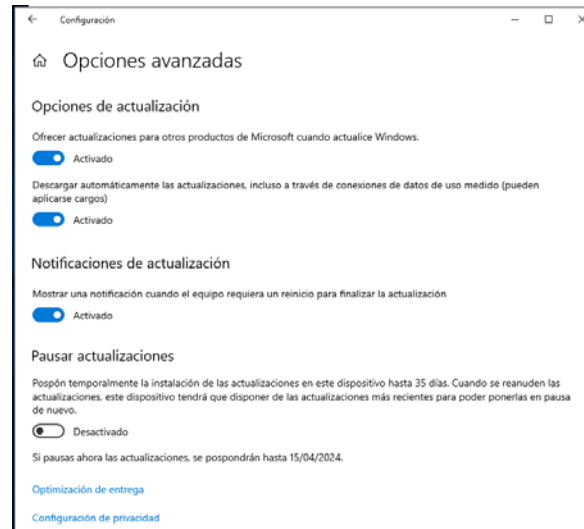


Figura 6.4.2.2 Opciones de actualización.

Como se trata de un servidor PowerEdge de DELL, se instalan los programas de gestión y los drivers mediante el último *Service Pack for PowerEdge* de DELL.

Se cambia el nombre generado automáticamente durante la instalación por el nombre del servidor que se haya definido.

6.4.3 Configuración de las funciones de red de Windows Server 2019

Un aspecto importante en la instalación e implementación de servidores Windows Server, es la obtención de una *dirección IP* para el equipo. Lo típico es que los servidores tengan valores fijos, que no cambien con cada arranque, para facilitar su localización en la red. Esta acción es la que a continuación se describe, y no sólo se establece un valor fijo para la *dirección IP*, también para la máscara de subred, la puerta de enlace e incluso el *servidor DNS* para el servidor.

La forma más sencilla de conseguirlo consiste en hacer clic con el botón derecho del ratón sobre el icono que representa la conexión de red en la Barra de tareas. Como se muestra en la figura 6.4.3.1.

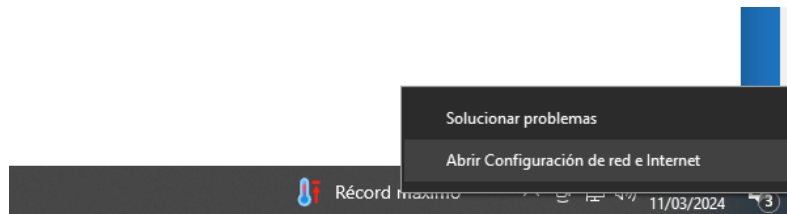


Figura 6.4.3.1 Configuración de red.

En el menú de contexto que aparece, elegir *Abrir el Centro de redes y recursos compartidos*. Al hacerlo, se abre la herramienta de configuración, con la categoría *Red e Internet* seleccionada.

De forma predeterminada, aparecerá activa la opción Estado. Sin embargo, la que nos interesa es Ethernet, figura 6.4.3.2. Click sobre la opción Ethernet.

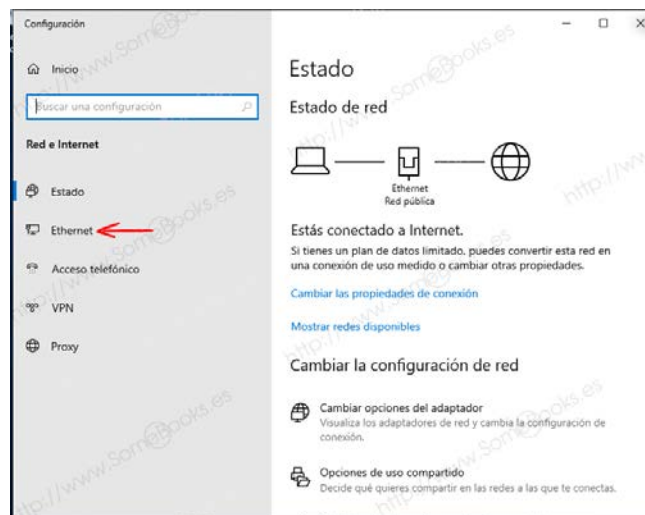


Figura 6.4.3.2 Estado de la red.

Al hacerlo, la parte derecha de la ventana cambia y muestra las opciones relacionadas con la configuración *ethernet*, figura 6.4.3.3.

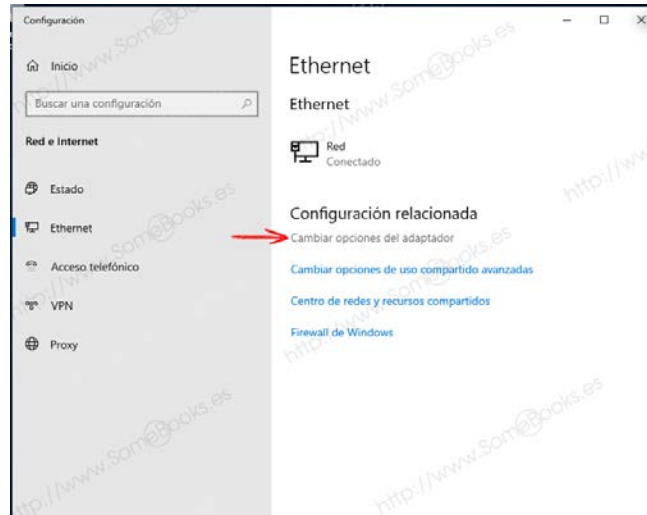


Figura 6.4.3.3 Cambiar opciones del adaptador.

De este modo, se llega a la ventana *Conexiones de red*, que contiene un elemento por cada conexión disponible. En este caso, sólo una. Figura 6.4.3.4.

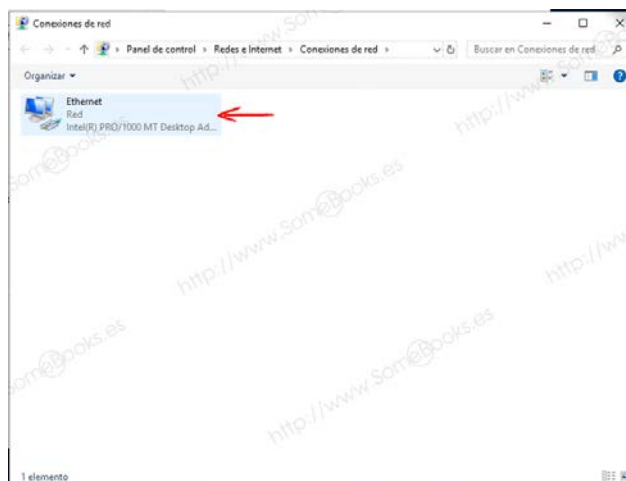


Figura 6.4.3.4 Icono de la tarjeta de red del servidor.

Así, se consigue que aparezca la ventana *Estado de Ethernet* con toda la información sobre la conexión, como lo muestra la figura 6.4.3.5. Observar que la entrada *Conectividad IPv6* indica que no tiene acceso a la red. El motivo es que la red local en la que se está trabajando no dispone de conectividad para el protocolo *TCP/IPv6*.

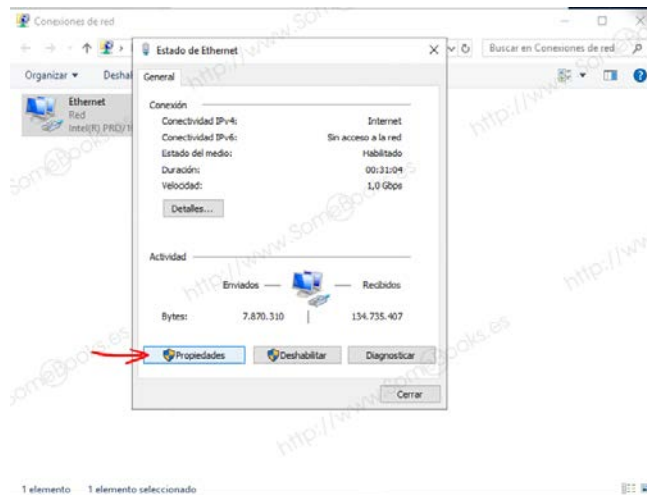


Figura 6.4.3.5 Información de la conexión ethernet.

Se puede ver el tiempo que lleva habilitada la conexión, que en este caso coincide con el tiempo desde que se inició el sistema, su velocidad y la cantidad de información transmitida.

De esta forma, se consigue que se muestre la ventana *Propiedades de Ethernet*, en la cual se puede encontrar, y también configurar, el tipo de tarjeta de red que se está utilizando y todos los elementos disponibles para esta conexión. Figura 6.4.3.6.

Como se dijo anteriormente, no se dispone de conectividad IPv6, así que se puede hacer click sobre la casilla de verificación que hay junto a la entrada Protocolo de Internet versión 6 (TCP/IPv6) para deshabilitarla. De esta forma, se evita consumir recursos del sistema de forma innecesaria.

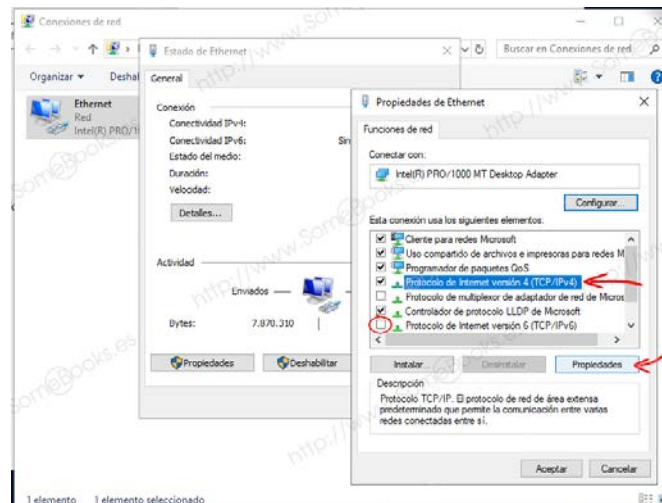


Figura 6.4.3.6 Propiedades de la conexión ethernet del servidor.

En la ventana de *Propiedades: Protocolo de Internet versión 4 (TCP/IPv4)* fijar los valores adecuados para la red local como se muestra en la figura 6.4.3.7.

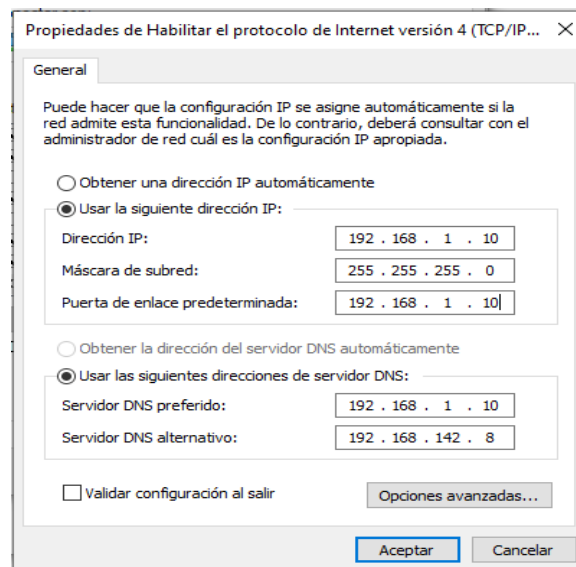


Figura 6.4.3.7 Propiedades del protocolo de Internet versión 4 TCP/IPv4.

Hasta este punto, se tiene un servidor independiente con Windows Server 2019 funcional para una pequeña red local. Servidores de este tipo y con estas características, son los que se tenían antes de comenzar con el presente proyecto.

Se contaba con servidor de archivos, servidor de impresión, servidor de bases de datos en SQL Server, servidor de correo institucional, entre otros, y en cada uno se reproducían casi la totalidad de los usuarios. Con esta configuración, también se tenía toda la problemática descrita anteriormente. Se tenía salida a internet con la protección de un firewall *PFSense*, que es una distribución personalizada de FreeBSD adaptado para su uso como Firewall y Enrutador. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de computadoras, y además cuenta con una interfaz web sencilla para su configuración. La siguiente figura 6.4.3.8 representa como estaba la configuración para cada servidor independiente con los usuarios.

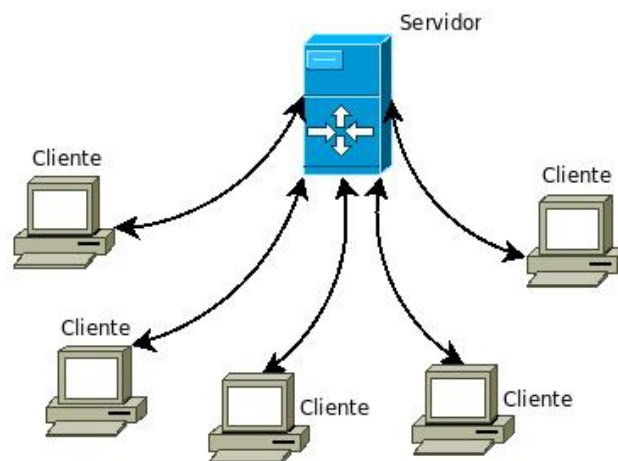


Figura 6.4.3.8 Configuración por servidor antes de la implantación del dominio.

Y la figura 6.4.3.9 representa la red después de instalado el dominio y el firewall *PFSense* protegiendo el nuevo esquema de red.

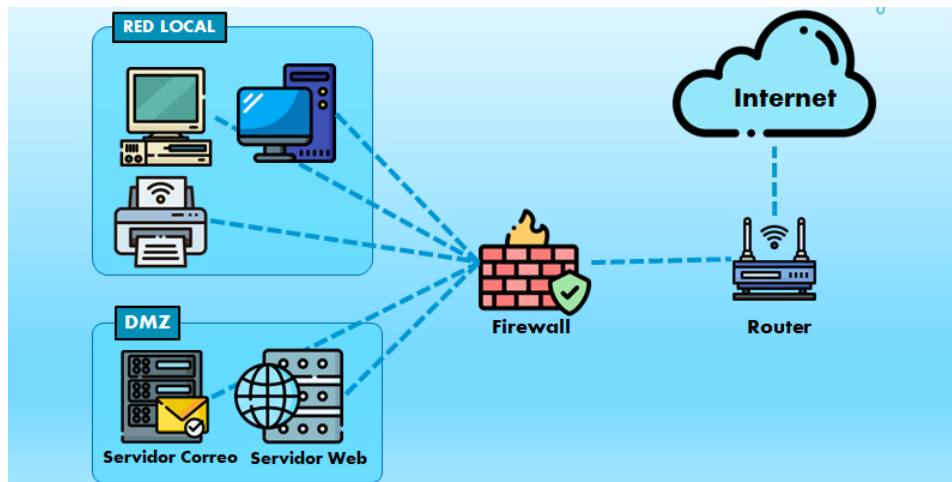


Figura 6.4.3.9 Configuración básica de un firewall con DMZ.

6.5 Instalación del dominio

Recapitulando, un dominio de *Active Directory Domain Services (AD DS)* permite almacenar, y administrar, toda la información relativa a una organización. Esto incluirá sitios, computadoras, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red.

Además, permitirá establecer políticas, sobre los diferentes objetos, que serán válidas en toda la organización. Incluso se podrán realizar operaciones, como la instalación de programas, o la aplicación de actualizaciones críticas, de forma simultánea y centralizada, en muchos de los equipos cliente.

6.5.1 Procedimiento para convertir un servidor Windows Server 2019 en Controlador de Dominio (DC)

En lo relativo a la instalación del dominio, Windows Server 2019 se sigue la misma estructura que las versiones anteriores:

- Primero, se instala el rol *Servicios de dominio de Active Directory*.
- A continuación, convertir (promocionar) el servidor en un controlador de dominio.

Esto debido a que son muchos los roles que puede desempeñar un servidor Windows Server 2019 en una red, y no tendría sentido que todos ellos estuviesen instalados de forma predeterminada. Así que es cuestión del administrador del sistema quien decide la función que deba realizar el servidor. Y el primer paso siempre será instalarla.

Por otro lado, la tarea de convertir un equipo con *Windows Server 2019*, en un controlador de dominio de *Active Directory*, aunque no es complicada, sí es un poco larga. Por ese motivo, primeramente, se recomienda la instalación del rol *Servicios de dominio de Active Directory*. Y más adelante se mostrará cómo realizar la tarea de promoción del servidor.

6.5.2 Instalación del rol Servicios de Dominio de Active Directory

La instalación de roles y características de *Windows Server 2019*, se realiza desde la herramienta *Administrador del servidor*. Lo usual es que se abra automáticamente al iniciar sesión con la cuenta de *Administrador*, pero si se ha cerrado por algún motivo, se puede encontrar fácilmente, haciendo clic sobre el botón *Inicio*.

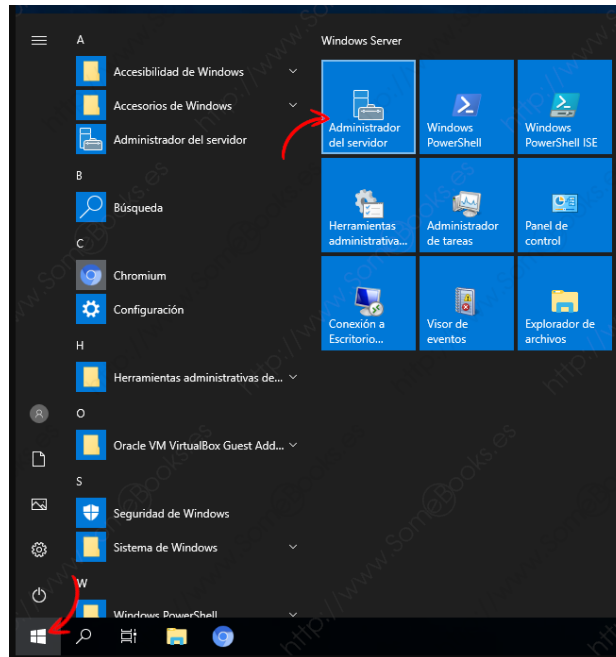


Figura 6.5.2.1 Localizando la herramienta Administrador del Servidor.

Después, sólo hacer click sobre el icono que representa la herramienta. Como lo muestra la figura 6.5.2.1. Una vez abierta la ventana del *Administrador del servidor*, comenzar haciendo click sobre el enlace *Agregar roles y características* de la página principal de la ventana. Figura 6.5.2.2.

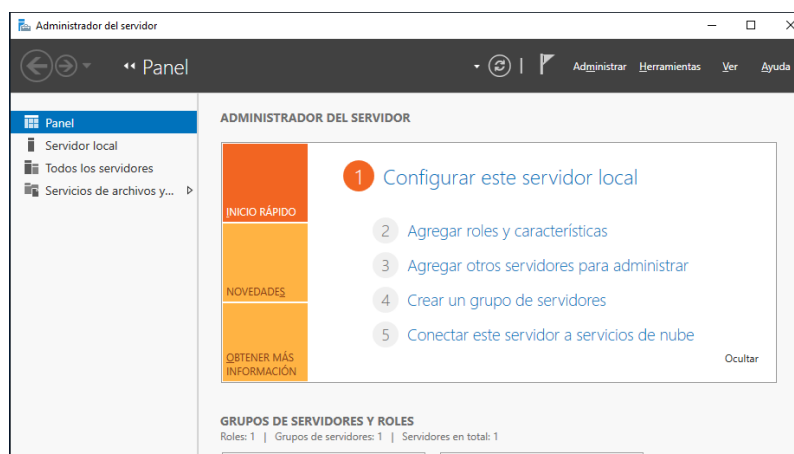


Figura 6.5.2.2 Agregar roles y características.

Si no se está en la página principal, se puede recurrir al menú *Administrar* en la esquina superior derecha, que contiene una opción con el mismo título.

Al hacerlo, se iniciará el *Asistente para agregar roles y características*. Este asistente no es específico de *Active Directory*, pero puede guiar a través de la instalación de otras funciones tan diversas como *DNS*, *Internet Information Server (IIS)*, *fax*. Ver figura 6.5.2.3.

Es importante seguir las recomendaciones del propio asistente en cuanto a asegurarse de que la contraseña de la cuenta de *Administrador* es segura, que la configuración de red es correcta, que se dispone de direcciones IP estáticas y que se han instalado las últimas actualizaciones de seguridad en el sistema operativo.

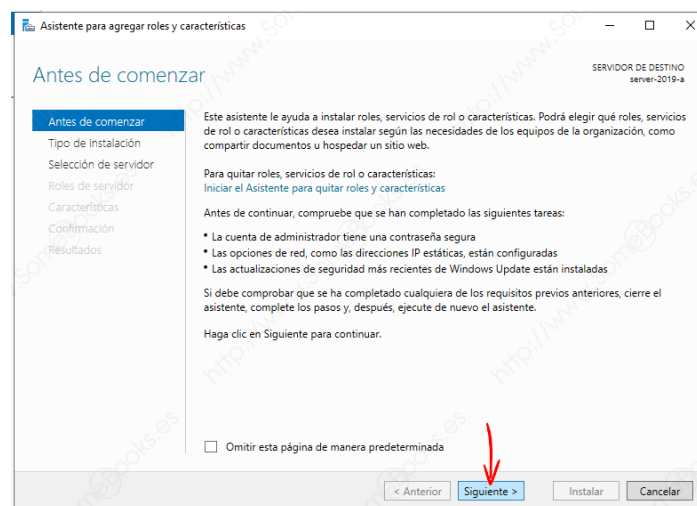


Figura 6.5.2.3 Asistente para Agregar roles y características.

Se tiene la posibilidad de instalar los servicios de escritorio remoto de forma independiente. Sin embargo, de momento sólo se llevará a cabo la instalación de roles y características. Figura 6.5.2.4.

Elegir *Instalación basada en características o en roles* y dar click sobre el botón *Siguiente*.

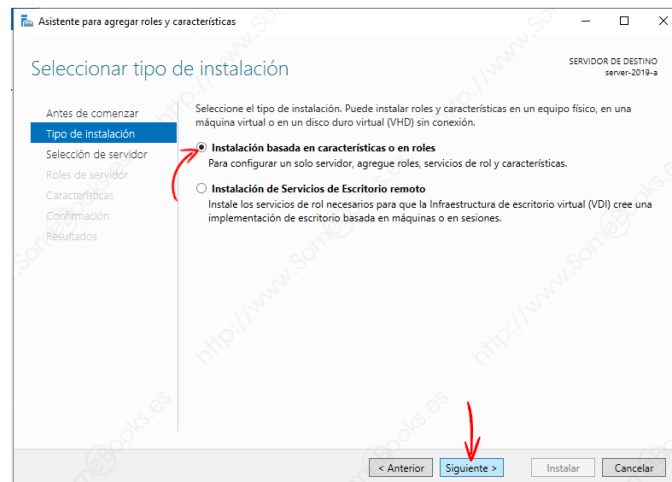


Figura 6.5.2.4 Seleccionar tipo de instalación.

Una característica muy interesante que se tiene a disposición desde el *Administrador del Servidor* de *Windows Server*, es la posibilidad de usar el *Asistente para Agregar roles y características* para instalarlas en el disco duro virtual (*VHD*) sin que éste tenga que estar unido a una máquina virtual (o que lo esté, pero que la máquina virtual esté apagada). Esto facilita los cambios en una instalación virtual a la vez que reduce el esfuerzo administrativo.

Si se necesitara cubrir esta tarea, en el siguiente paso elegir la opción *Seleccionar un disco duro virtual*. Esto se muestra en la figura 6.5.2.5.

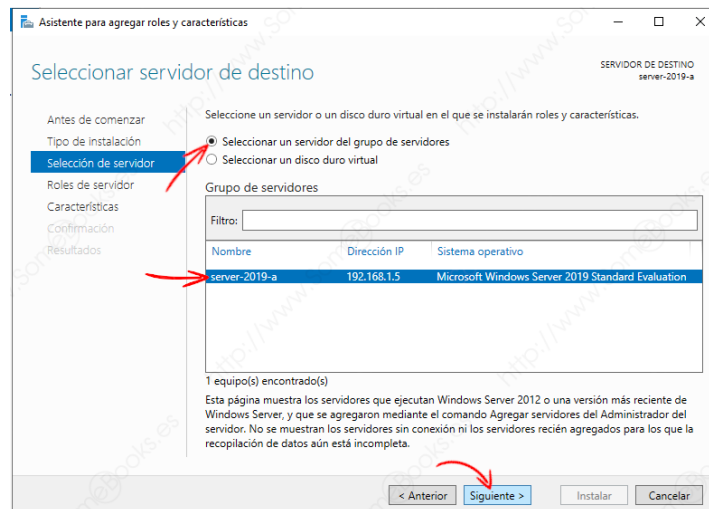


Figura 6.5.2.5 Selección de servidor de destino.

Sin embargo, en este caso, se necesita instalar el rol del *Directorio Activo* en el sistema con el que se está trabajando, por lo que la opción elegida será *Seleccionar un servidor del grupo de servidores*. De esta forma, se obtendrá una lista con los servidores en la red local que ejecutan *Windows Server 2019*. Lógicamente, sólo se muestran los servidores que estén funcionando y se haya completado su recopilación de datos. En este caso, sólo aparece el servidor en el que se está trabajando.

Dar click sobre el servidor y, a continuación, sobre el botón *Siguiete*. Como se muestra en la figura 6.5.2.5.

En la siguiente etapa, se tiene que elegir el servicio o servicios que se desea instalar. Tener en cuenta que, para que *Active Directory* funcione correctamente, es preciso tener instalado un *Servidor DNS*. Sin embargo, aquí se deja sin seleccionar para comprobar que, más adelante, el asistente lo habrá seleccionado de forma predeterminada. Esto se muestra en la figura 6.5.2.6.

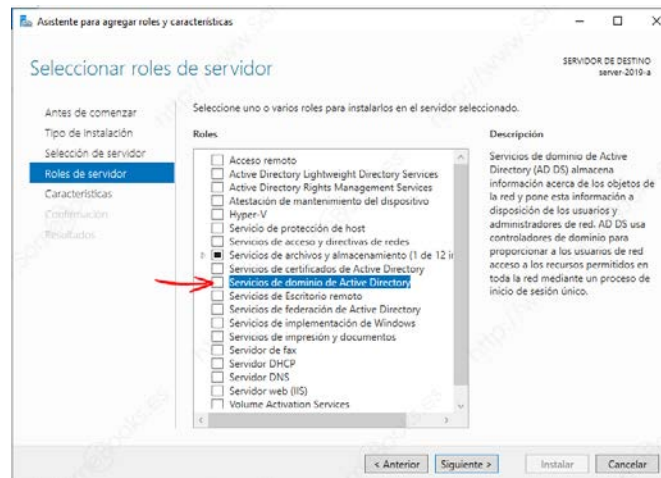


Figura 6.5.2.6 Selección de roles del servidor.

Activar la entrada *Servicios de dominio de Active Directory*. Observar que, a la derecha de la lista, en el cuadro *Descripción*, aparece una breve explicación del rol sobre el que se esté en ese momento.

Al hacerlo, el asistente muestra un aviso indicando que los servicios elegidos dependen de otros roles y características que se necesitan instalar también de forma complementaria.

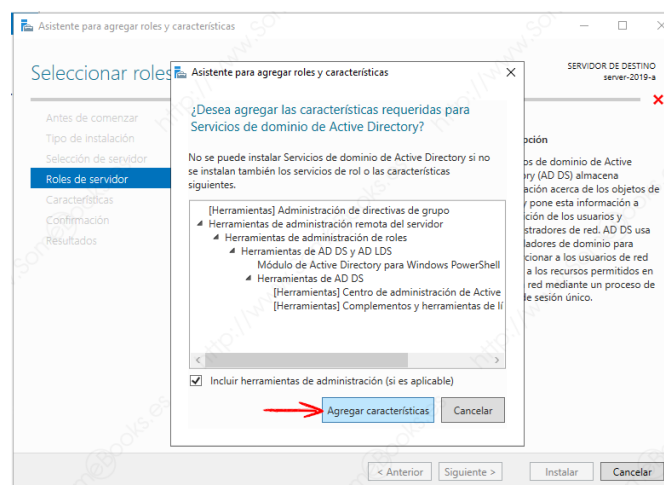


Figura 6.5.2.7 Confirmando el agregar las características elegidas.

Limitarse a dar click sobre el botón *Agregar características*, como se muestra en la figura 6.5.2.7. Al volver a la ventana del asistente, se comprueba que la línea *Servicios de dominio de Active Directory* ya aparece seleccionada. Figura 6.5.2.8.

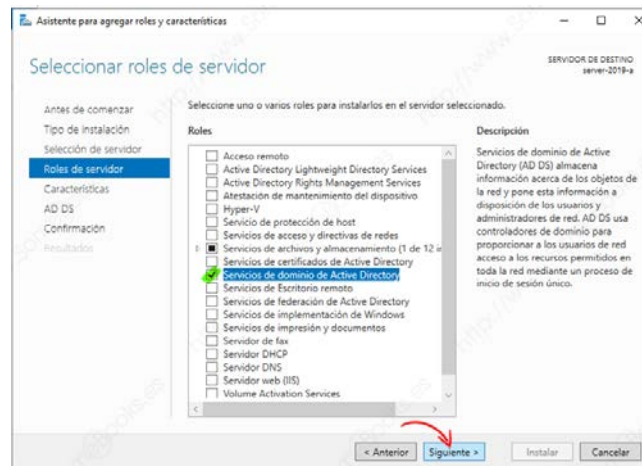


Figura 6.5.2.8 Lista de roles seleccionados para instalar.

Dar click sobre el botón *Siguiente* para continuar. Después de seleccionar los roles, el asistente ofrece la posibilidad de instalar características, figura 6.5.2.9. En versiones anteriores, se aprovechaba para instalar *Administración de directivas de grupo*. El objetivo era centralizar, en una sola herramienta, las directivas de grupo de toda la instalación. Sin embargo, en *Windows Server 2019*, ya se encuentra instalada de forma predeterminada.

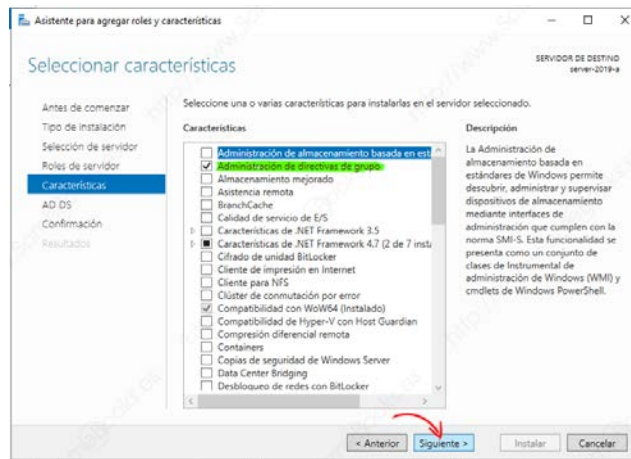


Figura 6.5.2.9 Selección de características a instalar.

Limitarse a hacer click sobre el botón *Siguiente*. Se define el concepto de *rol* como un servicio que el equipo ofrece a los clientes de la red. Por el contrario, una *característica* es una función que usa el servidor para llevar a cabo su propia labor.

Después de esto, aparece una pantalla informativa, figura 6.5.2.10, que se sugiere leer atentamente. Quizás uno de los aspectos más interesantes de esta ventana es la recomendación de instalar al menos dos controladores de dominio para un determinado dominio, con el fin de aumentar la disponibilidad de la infraestructura de red. Y haciendo caso a esta recomendación, se implementan dos servidores, uno será el controlador de dominio principal, y el segundo, el controlador de dominio secundario. Este esquema es con el fin de que en caso de que alguno de los dos llegase a fallar, el que queda en funcionamiento pueda hacerse cargo de la administración de la red o del dominio, por el tiempo necesario mientras se prepara un equipo más como servidor de dominio principal o controlador de dominio secundario.

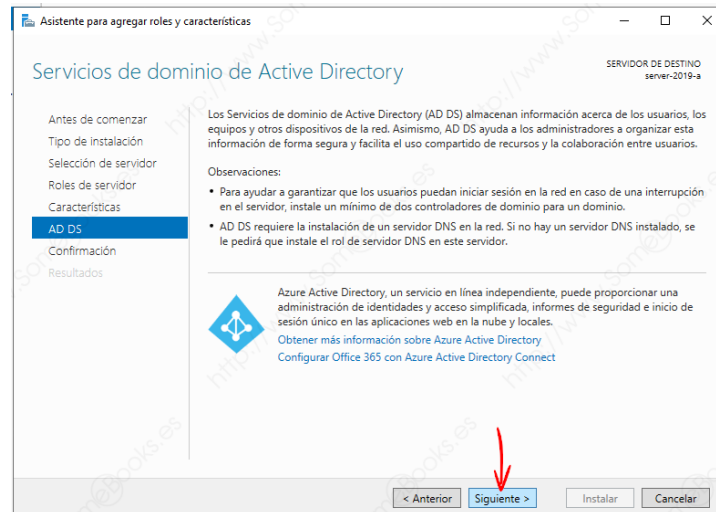


Figura 6.5.2.10 Servicio de Active Directory y recomendaciones de la instalación de otras características.

También se recuerda la necesidad de disponer de un servidor *DNS* y se informa que se instalará el servicio de espacio de nombres y los de replicación, que son necesarios para el servicio de directorio. Cuando se tenga la seguridad de haber entendido toda la información, hacer click en el botón *Siguiente*.

Antes de proceder con la instalación, se tiene la oportunidad de marcar la opción *Reiniciar automáticamente el servidor de destino en caso necesario*, como muestra la figura 6.5.2.11. Esto facilita el reinicio del sistema incluso cuando se esté administrando un equipo remoto. Recordar que, en pasos anteriores, figura 6.5.2.5, se pudo haber elegido otro servidor que estuviese accesible a través de la red.

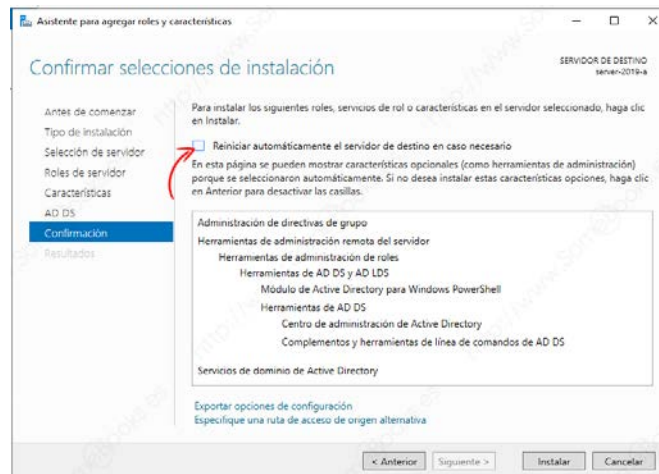


Figura 6.5.2.11 Confirmar selecciones de instalación.

De cualquier modo, dar click sobre la opción. Al hacerlo aparece un cuadro de diálogo que advierte de que, al marcar la opción, pueden producirse reinicios sin notificaciones previas.

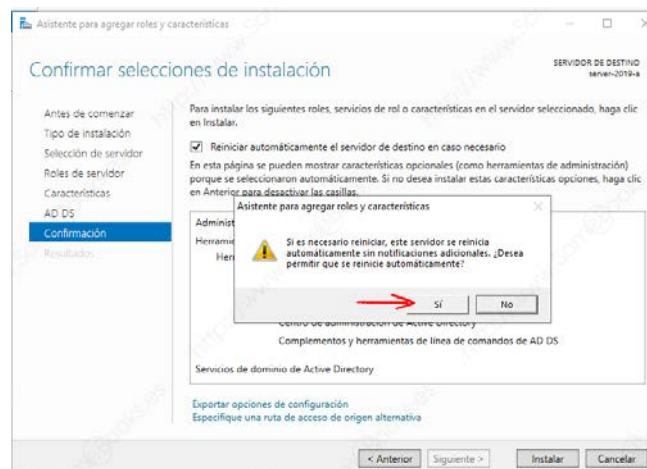


Figura 6.5.2.12 Advertencia de reinicios sin notificaciones previas.

Para este caso, dar click sobre el botón *Sí*. Figura 6.5.2.12.

Por último, en la pantalla que resume la instalación, se pueden comprobar los distintos roles y características que van a instalarse. Como es habitual, si se observa algún error, se tiene la opción de usar el botón *Anterior* para retroceder hasta el paso adecuado y realizar las modificaciones pertinentes o necesarias. Figura 6.5.2.13.

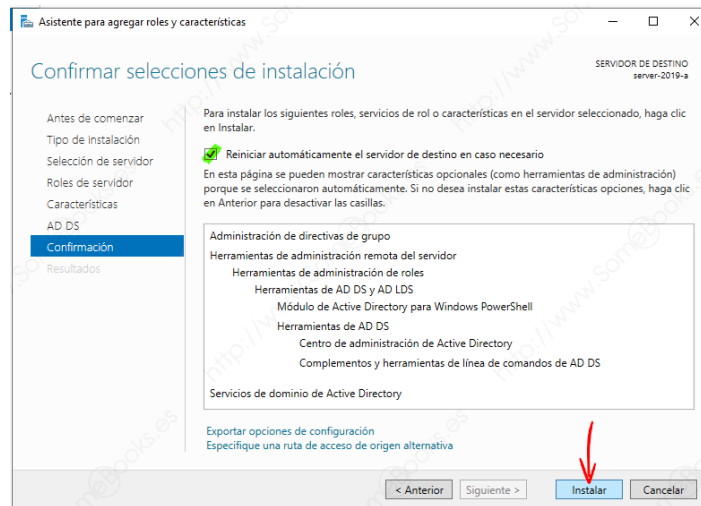


Figura 6.5.2.13 Confirmar y aceptar el reinicio automático de la instalación.

Sin embargo, si todo es correcto, dar click sobre el botón *Instalar*. A partir de aquí, en la parte superior de la ventana se podrá ver una barra de progreso que informa del avance de la instalación. Figura 6.5.2.14.

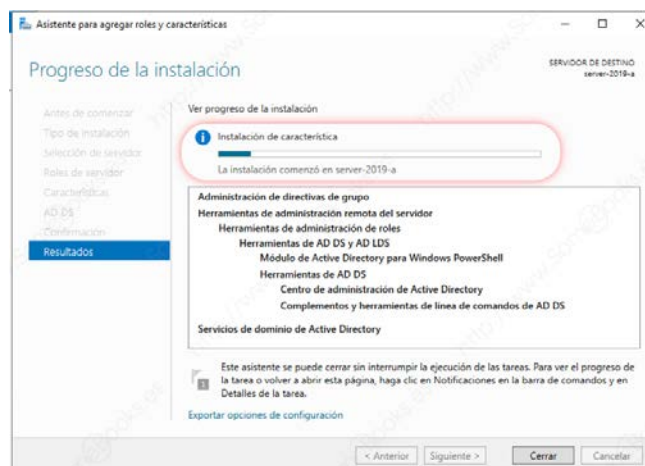



Figura 6.5.2.14 Progreso de la instalación.

Observar que ya es posible cerrar el asistente y el proceso de instalación no se interrumpirá. Si se hace, se podrá consultar el avance de la tarea o abrir la ventana

del asistente usando el icono  que aparece en la parte superior del *Administrador del servidor*. Para el caso que nos ocupa, limitarse a esperar.

Cuando termine la instalación, se presenta un recuadro con un enlace con el texto *Promover este servidor a controlador de dominio*. Figura 6.5.2.15.

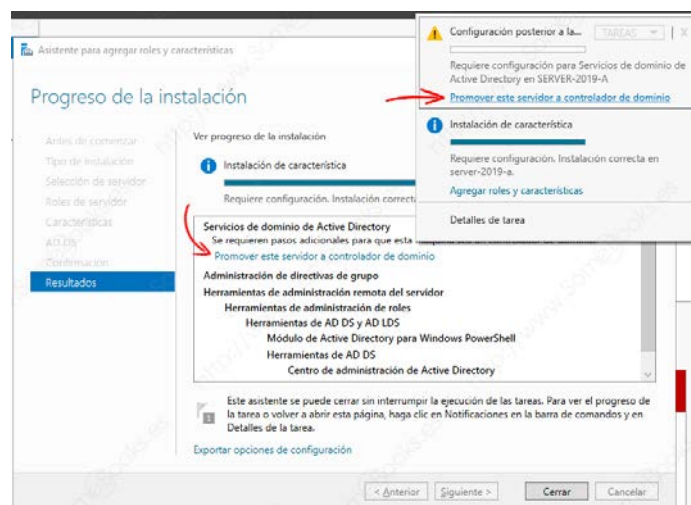


Figura 6.5.2.15 Opción de promover este servidor a controlador de dominio.

También se puede utilizar el icono de notificación que aparece en la parte superior del *Administrador del servidor*. Al hacer click sobre él, también aparece el enlace que permite *Promover este servidor a controlador de dominio*.

Dado que el objetivo es disponer de un controlador de dominio (DC) para administrar los recursos de la infraestructura de red, hasta este momento, se tiene ya instalado el rol *Servicios de dominio de Active Directory* y algunas características suficientes para poder ser un controlador de dominio, sin embargo, se tiene que hacer algo más con estas características y roles para lograrlo. De este punto en adelante, es el momento de promocionar el servidor para convertirlo en un *controlador de dominio*.

Bastaría, en este momento, con hacer click sobre el enlace *Promover este servidor a controlador de dominio* de la última pantalla del asistente. Así se iniciaría la promoción del equipo a *Controlador de Dominio*.

Al hacerlo, se abre la ventana del Asistente para configuración de *Servicios de dominio de Active Directory*. En la primera pantalla, se debe indicar el tipo de operación que se quiere implementar:

- Agregar un controlador de dominio a un dominio existente.
- Agregar un nuevo dominio a un bosque existente.
- Agregar un nuevo bosque.

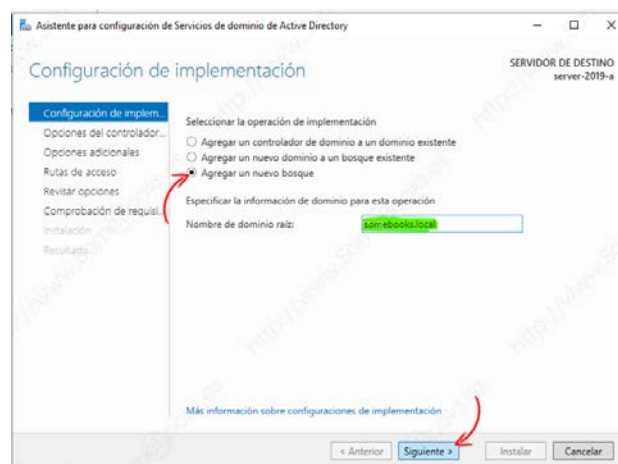


Figura 6.5.2.16 Especificando el nuevo dominio.

Como en este caso se parte de una situación en la que no se dispone de infraestructura previa, la opción que se debe elegir es la última, *Agregar un nuevo bosque*. Figura 6.5.2.16.

Al hacerlo, en la parte inferior se solicita el dominio raíz para el nuevo bosque. Si se dispone de un dominio registrado en Internet, aquí se incluiría el nombre de dicho dominio. Cuando se haya escrito el nombre, dar click en *Siguiente*.

En el siguiente paso, *Opciones del controlador de dominio*, indicar el nivel de funcionalidad del controlador. Si no se tiene en la red controladores de dominio que ejecuten versiones más antiguas de *Windows Server*, se debe elegir *Windows Server 2019*, que será el valor predeterminado.

También se puede elegir un nivel de funcionalidad con una versión anterior, como *Windows Server 2008*, *2012* o *2016*, en caso de llegar a añadir este tipo de controladores posteriormente. Figura 6.5.2.17.

Cuanto más antiguo sea el nivel de funcionalidad que se elija, más limitadas se verán las prestaciones del árbol de dominios.

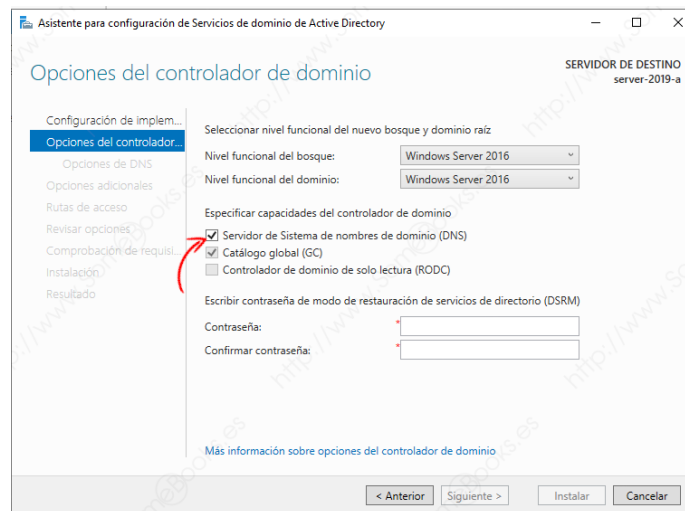


Figura 6.5.2.17 Seleccionar nivel de funcionalidad del nuevo bosque y dominio.

Bajo la leyenda *Especificar capacidades del controlador de dominio*, indicar que el equipo también actuará como *Servidor de nombres de Dominio (DNS)*. Además, aparecerán dos opciones más: *Catálogo global (GC)* y *Controlador de dominio de solo lectura (RODC)*. Figura 6.5.2.17.

Microsoft recomienda que todos los controladores de dominio sean también *servidores DNS* para asegurar que *Active Directory* esté siempre disponible.

El primero aparecerá seleccionado de forma obligatoria porque todo dominio debe tener un catálogo global y se está instalando el único controlador que hay hasta el momento en la red. Del mismo modo, dado que el servidor actual es único, no puede ser de sólo lectura.

Por último, es necesario proporcionar y escribir la contraseña del *modo de restauración de servicios de directorio (DSRM)*. Como es habitual, se escribe por duplicado para evitar errores tipográficos. Figura 6.5.2.18. Y para finalizar esta parte, dar click en el botón *Siguiente*.

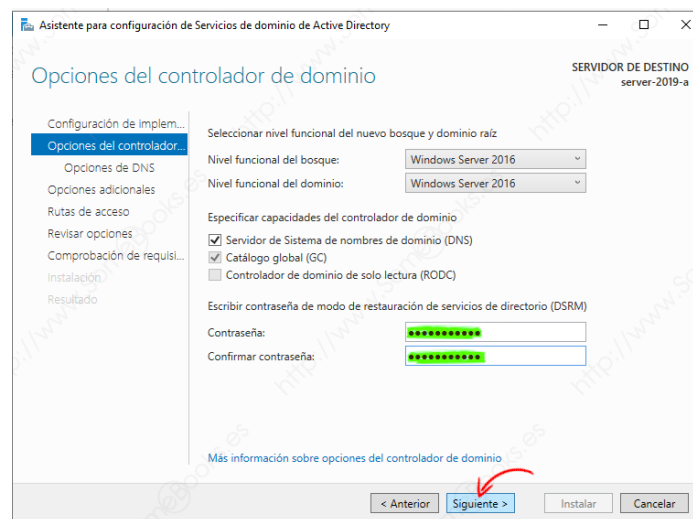


Figura 6.5.2.18 Contraseña de modo de restauración de servicios de directorio (DSRM).

En el siguiente paso, *Opciones de DNS*, si se dispusiera de una infraestructura *DNS* anterior a la instalación del dominio, se debería especificar si se desea crear en dicha infraestructura una delegación para el *servidor DNS* que se va a instalar. Sin embargo, como no se cuenta con un *Servidor DNS principal*, Windows Server muestra un aviso indicando que *No se puede crear una delegación para este*

servidor DNS porque la zona principal autoritativa no se encuentra. Como se puede ver en la figura 6.5.2.19.

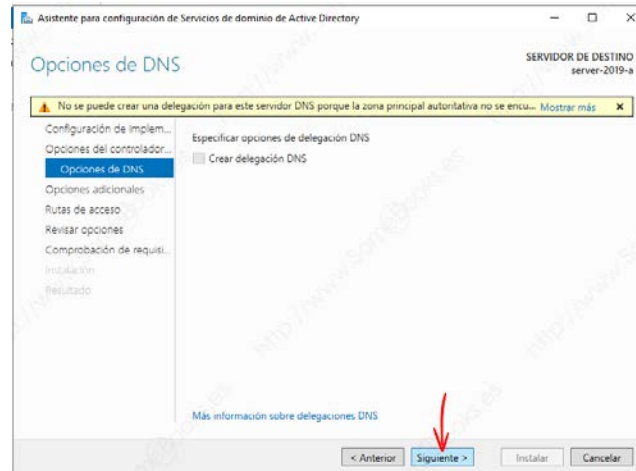


Figura 6.5.2.19 Especificar opciones de delegación DNS.

A continuación, en el paso *Opciones adicionales*, el asistente sugiere un nombre *NetBIOS* para el dominio raíz del bosque. Lógicamente, se puede aceptar el nombre que se propone o indicar cualquier otro. Ver figura 6.5.2.20. El nombre *NetBIOS* puede tener hasta 15 caracteres formado por letras (mayúsculas o minúsculas), dígitos o guiones ('-'), aunque no puede ser enteramente numérico. Para seguir, dar click sobre el botón *Siguiente*.

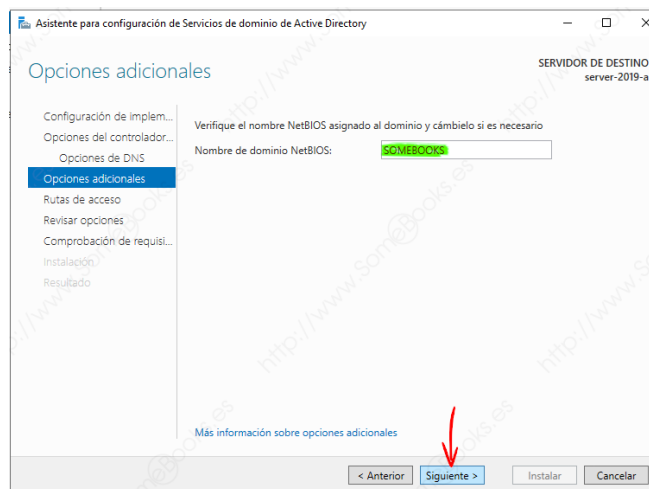


Figura 6.5.2.20 Nombre de dominio NetBIOS.

Después de esto, en el apartado *Rutas de acceso*, el asistente pregunta dónde se desea almacenar los archivos de trabajo de *Active Directory* (la base de datos, los archivos de registro y la carpeta SYSVOL). Los *archivos de registro* también suelen llamarse *archivos log*. Ver figura 6.5.2.21.

Puede ser una opción interesante pero sumamente útil que los archivos de registro y la base de datos se almacenen en volúmenes separados. De esta forma mejoraría el rendimiento (ya que se podrá acceder a ambos archivos de forma simultánea) y las posibilidades de recuperación de los datos si se producen problemas.

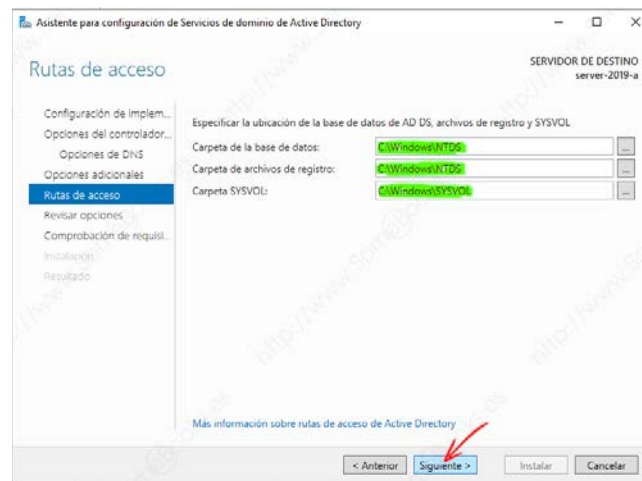


Figura 6.5.2.21 Rutas de acceso de las bases de datos y archivos de registro.

A pesar de todo, en la ventana aparece de forma predeterminada una ubicación de la unidad C. El motivo es muy sencillo: no se tiene otra. Por lo tanto, limitarse a hacer click en *Siguiete*.

En el apartado *Revisar opciones*, el asistente muestra un resumen del proceso de instalación. Como se muestra en la figura 6.5.2.22. Revisarlo para asegurarse de que no se han cometido errores en los pasos anteriores. Como es habitual, se dispone del botón *Anterior* para resolver cualquier error en el que se haya podido incurrir.

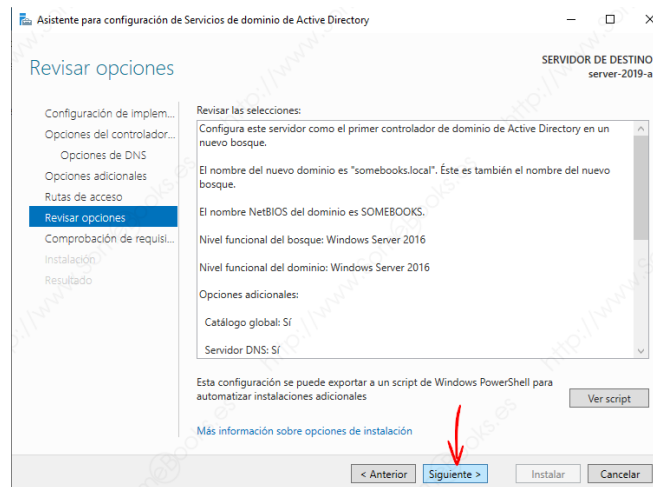


Figura 6.5.2.22 Resumen de opciones de instalación.

Se dispone también del botón *Ver script*, figura 6.5.2.23, que permite obtener un script de *PowerShell* para automatizar una instalación como ésta sin tener que volver a introducir de nuevo todos los datos.

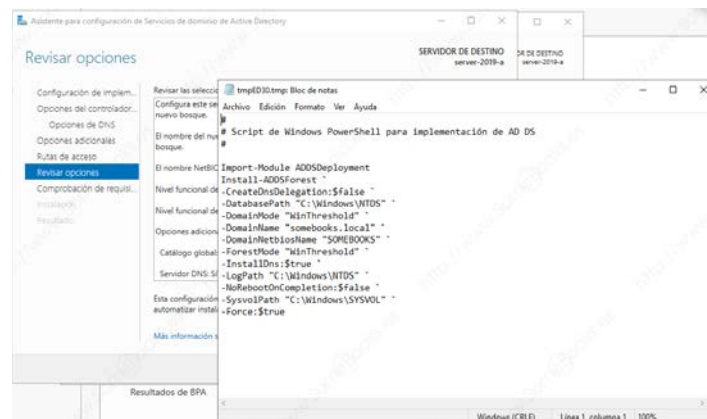


Figura 6.5.2.23 Script de Windows Power Shell de la instalación.

Por último, en el apartado *Comprobación de requisitos*, se verifica que el sistema cumpla todas las condiciones para convertirse en un controlador de dominio.

Como se puede observar en la imagen siguiente, figura 6.5.2.24, pueden aparecer algunos avisos, como el que informa de que no puede crearse una delegación para el servidor DNS que se está a punto de instalar (ya se comentó esta circunstancia anteriormente). También pueden aparecer errores que impidan la instalación del controlador de dominio. En estos casos, no se podrá continuar hasta que no se hayan resuelto.

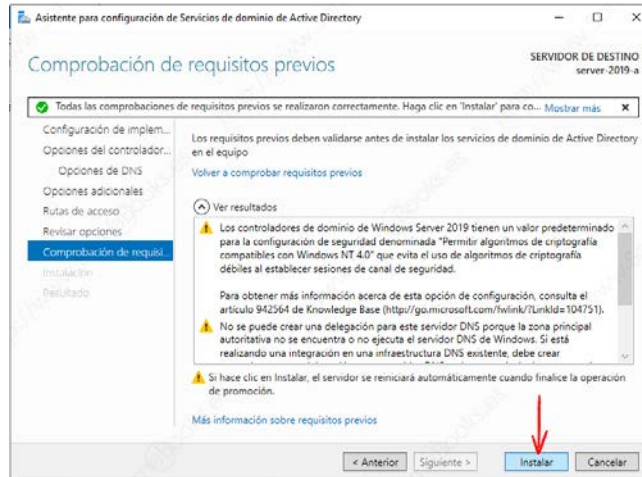


Figura 6.5.2.24 Comprobación de requisitos previos.

Si no se presentan errores, dar click sobre el botón *Instalar* para completar la operación. Durante el proceso de instalación seguirán apareciendo mensajes informativos que se deberán tener en cuenta para una futura configuración del servidor. Cuando termine la instalación, el servidor se reiniciará automáticamente.

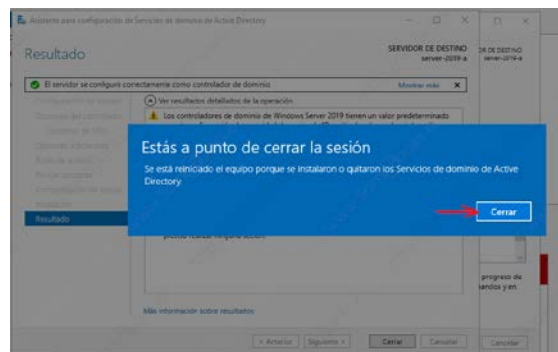


Figura 6.5.2.25 Reinicio por instalación de Servicios de Active Directory.

Cuando aparezca el mensaje, se hace click sobre el botón *Cerrar*, figura 6.5.2.25. Al hacerlo, comienza el proceso de reinicio. Sólo esperar a que se complete. El proceso puede durar un tiempo considerable porque se está completando la configuración del sistema. Al iniciar, se presenta la pantalla de bienvenida. Pulsar las teclas Ctrl + Alt + Supr para autenticarse.

Cuando finalmente se solicite la contraseña de la cuenta *Administrador*, se debe observar que la cuenta aparece precedida del nombre *NetBios* del dominio. Esta es la primera constatación de que todo el proceso de instalación ha sido correcto. Figura 6.5.2.26.

Si durante el proceso de instalación, la contraseña que se definió para iniciar en modo de restauración es diferente de la contraseña para la cuenta del usuario *Administrador*, hay que tener presente que la contraseña que se definió NO ES la misma que se usará para iniciar en el modo de restauración.

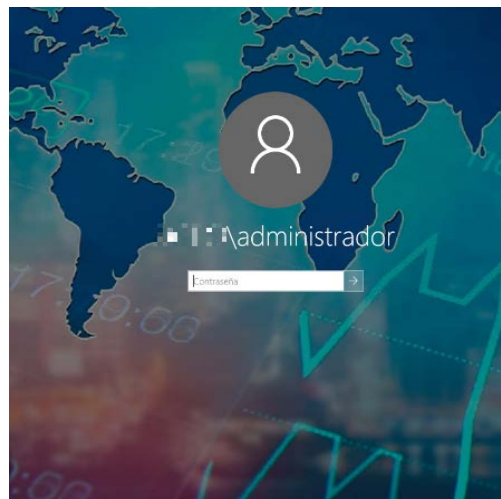


Figura 6.5.2.26 Primer inicio de sesión.

La primera vez que se inicie sesión con la cuenta *Administrador*, observar que tarda bastante más tiempo del normal. El motivo, de nuevo, es que el rol que tiene esta

cuenta dentro del sistema también ha cambiado y dichos cambios se aplicarán en este momento.

Para finalizar, debe asegurarse de que todo el proceso ha sido correcto, observar la pantalla de propiedades del equipo. Una de las formas más sencilla de conseguirlo consiste en abrir la ventana del Explorador de archivos. Figura 6.5.2.27. Una vez en ella, dirigirse al panel izquierdo de la ventana y hacer click, con el botón derecho del ratón, sobre el elemento *Este equipo*.

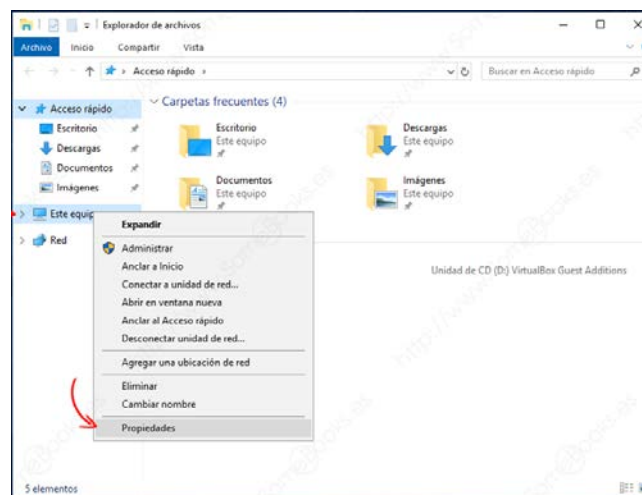


Figura 6.5.2.27 Propiedades del equipo.

Al hacerlo, se consigue que se muestre la ventana *Sistema*. En ella se puede comprobar que los valores de los campos *Nombre completo del equipo* y *Dominio* son correctos. Figura 6.5.2.28.

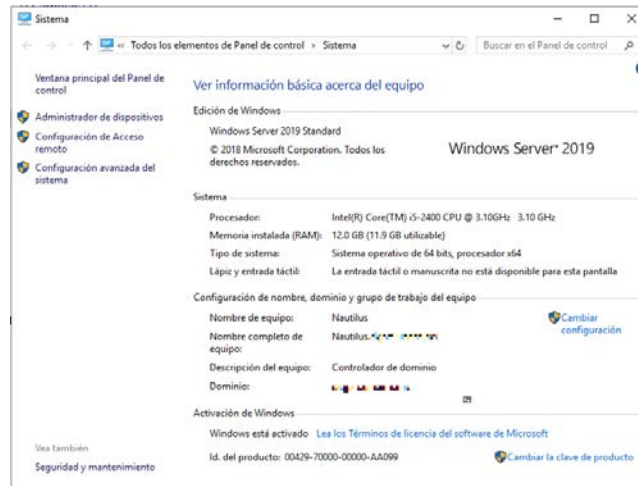


Figura 6.5.2.28 Propiedades del servidor. Nombre completo del equipo y dominio.

Una vez realizada la comprobación, cerrar la ventana y con esto, se da por terminada la instalación del controlador de dominio principal.

6.5.3 Añadiendo un segundo controlador de dominio para el dominio existente

La decisión de contar con un segundo controlador de dominio, es debido a que se cuenta con instalaciones de la DGPO en la Zona Cultural del campus. Y ya que se decidió implementar un dominio que controle y administre la infraestructura de red de la dependencia, también se decide agregar la estructura de red, usuarios y equipos del edificio en la Zona cultural. Por lo tanto, se implementa un segundo servidor Windows Server 2019 como controlador de dominio secundario que estará físicamente en dicho edificio administrando la red y en contacto con el controlador de dominio principal.

La principal ventaja de añadir un segundo controlador de dominio, para un dominio que ya existe, es que se puede mantener una réplica constante del primero.

Esto permite alcanzar dos objetivos:

- Aumentar la confiabilidad de la instalación, ya que ésta seguirá dando servicio incluso cuando falle uno de los dos servidores, el controlador de dominio que ya se instaló y el que se va a instalar e incorporar al dominio. Esta característica suele llamarse tolerancia a fallos.
- Distribuir la carga de los clientes entre ambos servidores. Al hacerlo, los clientes tendrán una reacción más rápida del sistema.

En este caso, se instalará Windows Server 2019 en un nuevo equipo, se configurará y se promocionará como controlador del dominio secundario. También se tendrá que configurar el primer controlador para que se sincronice con éste. En concreto, los pasos que se van a seguir son los siguientes:

1. Configurar el *Servidor DNS* del controlador de dominio principal.
2. Configurar las características de red del equipo nuevo.
3. Unir el nuevo equipo como cliente del dominio.
4. Añadir el rol *Servicios de dominio de Active Directory* al nuevo equipo.
5. Promocionar el nuevo equipo como controlador de dominio del bosque.
6. Ajustar la configuración de red.
7. Comprobar los servidores DNS.
8. Replicar los controladores de dominio.
9. Comprobar la replicación.

6.5.4 Configurar el servidor DNS del controlador de dominio principal

El primer paso, es configurar el servidor DNS del primer controlador de dominio, el único que se tiene hasta ahora, para que atienda las solicitudes del rango de direcciones IP que conforman la red.

Más adelante, se muestra cómo poder configurar también los reenviadores para que los nombres que no sean conocidos, los que no estén definidos en la red, se consulten en un servidor DNS de nivel superior, en este caso, y a modo de ejemplo, se podrían utilizar los servidores de Google.

Lo primero que se hace es abrir el *Administrador del servidor* y, en el menú *Herramientas*, hacer clic sobre la opción *DNS*. Como se muestra en la figura 6.5.4.1.

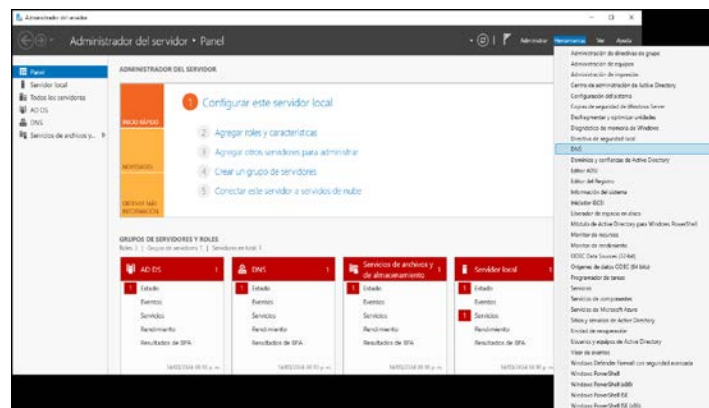


Figura 6.5.4.1 Accediendo al Servidor DNS del controlador de dominio principal.

Se abre la ventana *Administrador de DNS*. En ella, se debe desplegar, si no lo está, la entrada con el nombre del servidor que se está configurando, que es la correspondiente al controlador actual. En el árbol, dar click con el botón derecho del ratón sobre la entrada *Zonas de búsqueda inversa*. Como se muestra en la figura 6.5.4.2. Y, finalmente, en el menú de contexto que aparece, elegir *Zona nueva*...

Figura 6.5.4.2 Administrador DNS para crear una Nueva zona inversa.

Al hacer esto, se abrirá el *Asistente para nueva zona*. Como lo deja ver la figura 6.5.4.3. Con ella, se traducen los nombres *DNS* que sean conocidos por el servidor en sus correspondientes *IPs*.

Figura 6.5.4.3 Asistente para nueva zona inversa.

En el siguiente paso, se indica la pretensión de crear una zona principal y que se va a guardar en el *directorio activo*. Figura 6.5.4.4.

Figura 6.5.4.4 Elegir tipo de zona para la nueva zona inversa.

Después, indicar el ámbito en el que se va a replicar, copiar, la nueva *zona*. Indicamos también, que se replique en todos los *servidores DNS* del dominio, de modo que se incluya el *servidor DNS* del nuevo controlador, una vez que se haya creado. Figura 6.5.4.5.

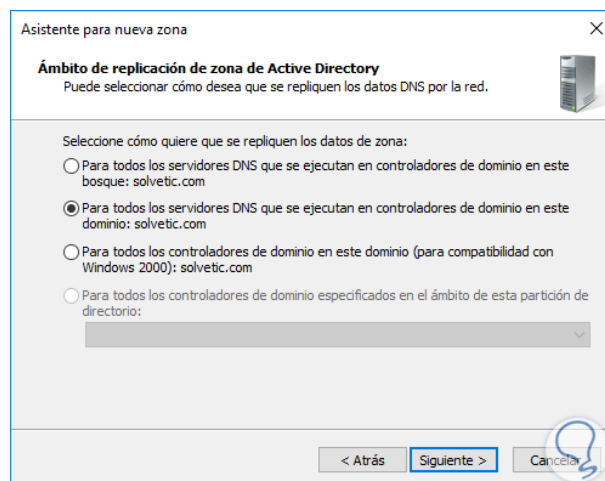


Figura 6.5.4.5 Ámbito de replicación de zona de Active Directory.

Lo siguiente es indicar si se desea crear la *zona de búsqueda inversa* para direcciones *IPv4* o *IPv6*. Como se muestra en la figura 6.5.4.6. Observar que sólo se

puede elegir una de las dos, por lo que, si en nuestra red vamos a utilizar ambos protocolos, se debería crear dos zonas de búsqueda inversa independientes, una para cada versión de IP. No obstante, recordar, que se desactivó el protocolo *IPv6* en la sección anterior, por lo que sólo se necesitará *IPv4*.

Figura 6.5.4.6 Elegir crear búsqueda inversa para IPv4 o IPv6.

A continuación, indicar el *id. de red*, es decir, el rango de direcciones que podrán beneficiarse de los servicios de la nueva *zona DNS*. En este caso, escribir *192.168.1*, lo que repercutirá en que sean atendidas todas las computadoras de la red que se encuentre en el rango de direcciones desde *192.168.1.1* hasta *192.168.1.255*. Ver la figura 6.5.4.7.

Figura 6.5.4.7 Establecer el rango de red que será atendido por el servidor DNS.

En el siguiente paso, indicar el tipo de actualización dinámica que debe permitir la zona DNS. Figura 6.5.4.8. El objetivo de las actualizaciones dinámicas es que los equipos cliente puedan registrarse en la zona y actualizar los registros relativos a sus propios recursos, cada vez que se produzca un cambio.

Figura 6.5.4.8 Elegir tipo de actualización dinámica.

En este caso, sólo permitir actualizaciones que provengan de equipos que estén integrados en el directorio activo.

En el último paso, obtenemos un resumen de todas las características que se han establecido en los puntos anteriores. Como se puede ver en la figura 6.5.4.9. Por supuesto, es muy recomendable leerlo con atención para asegurarse de que todo es correcto. Si se observara algún error o anomalía, utilizar el botón *Atrás*, para volver al paso donde se produjo dicho error y resolverlo.

Figura 6.5.4.9 Finalización del asistente para nueva zona.

Si todo es correcto, sólo queda hacer click sobre el botón *Finalizar*. La figura 6.5.4.10 muestra la nueva zona creada.

En este momento, ya se ha conseguido que el controlador de dominio resuelva los nombres relativos a nuestra infraestructura de red. Sin embargo, si en los equipos cliente se había configurado la dirección IP del controlador de dominio como *servidor DNS* único, se observará que la red funciona correctamente, pero que los clientes no pueden navegar por Internet.

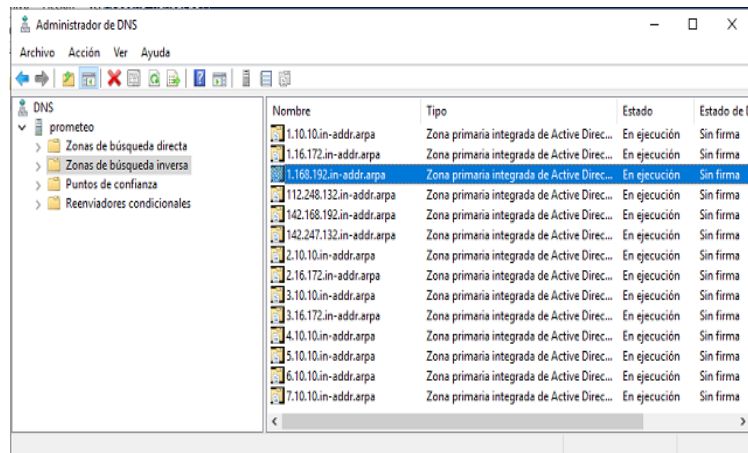


Figura 6.5.4.10 Zona de búsqueda inversa creada.

Esto se debe a que, cuando un cliente aporte un nombre que no pertenezca a la red local, el *servidor DNS* no lo conocerá y, por lo tanto, no sabrá resolverlo. Para evitar esta contingencia, se configuran los *reenviadores*, es decir, las *direcciones IP* que hacen referencia a otros *servidores DNS* a los que se debe recurrir cuando no se conozca la dirección que se le está solicitando.

6.5.5 Configuración de reenviadores

Para comenzar, en la ventana *Administrador de DNS*, que ya se había abierto en la sección anterior, hacer click con el botón derecho del ratón sobre el nombre del controlador de dominio.

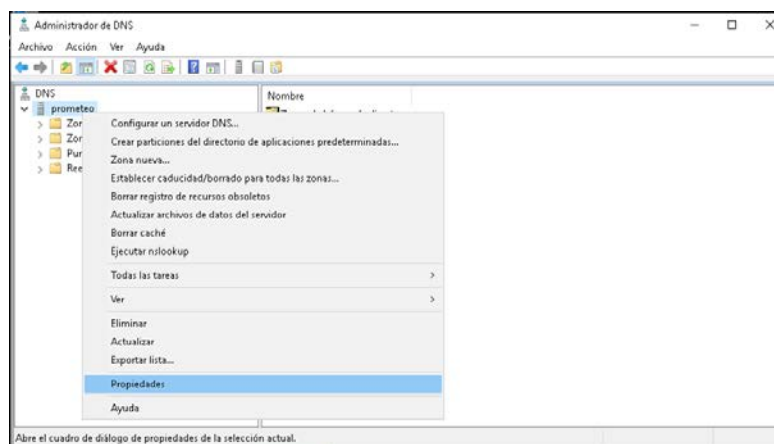


Figura 6.5.5.1 Propiedades del dominio en el servidor DNS

En el menú de contexto que aparece, elegir la opción *Propiedades*. Como se muestra en la figura anterior 6.5.5.1. Aparecerá la ventana *Propiedades* del Servidor. En ella, dirigirse a la pestaña *Reenviadores*. Aquí se observa que, en este caso, ya se tienen definidas algunas de las IPs de otros *DNS a los que se recurrirá cuando el DNS que se tiene no conozca las direcciones solicitadas*.

Puede definirse también, además de las que se muestran, la dirección 1.1.1.1, que está catalogada, como el servidor DNS más rápido de Internet, y que se ofrece como una colaboración de Cloudflare, Inc. Figura 6.5.5.2.

Esto significa que, para este caso, el problema ya está resuelto. Sin embargo, para ilustrar su funcionamiento, se puede añadir uno de los servidores DNS de Google, concretamente, la dirección 8.8.8.8.

Lógicamente, si no hubiese ninguna dirección definida, y se quisiera añadir ambas, sólo se tendría que repetir el proceso siguiente dos veces. Por supuesto, el proceso funcionará exactamente igual con la dirección IP de cualquier servidor DNS público.

Figura 6.5.5.2 Reenviadores en el servidor.

Comenzar por hacer click en el botón *Editar*. En la ventana *Editar reenviadores*, figura 6.5.5.3, se observa la lista con las direcciones IP definidas hasta el momento. En la lista, la primera línea aparece en azul y contiene el texto *<Haga clic aquí para agregar una dirección IP o un nombre DNS>*.

Figura 6.5.5.3 Editar reenviadores.

Hacer click en la primera línea, observando también, que, si se elige cualquier otra línea, se puede eliminar la IP que se haya elegido o cambiarla de orden. Esto último permite otorgar preferencia a unos servidores DNS sobre otros.

También se puede elegir el número de segundos que esperará el sistema antes de enviar la solicitud al siguiente servidor. Cuando sea todo correcto, hacer click sobre el botón *Aceptar*. La siguiente figura 6.5.5.4. muestra el proceso ya realizado.

Figura 6.5.5.4 Direcciones IP de los servidores DNS de reenvío.

De vuelta en la ventana de *Propiedades*, se puede comprobar que todo ha sido correcto cuando la columna *FQDN del servidor* aparece rellena, constatando que el servidor ha sido encontrado en Internet e identificado correctamente.

Ya sólo queda hacer click sobre el botón *Aceptar*. Y, para terminar, se incluye una tabla con otros *servidores DNS* públicos y gratuitos, tabla 6.5.5.1., que se pueden utilizar en lugar de los propios de *Google*.

Tabla 6.5.5.1 Servidores DNS públicos y gratuitos.

Servidores DNS		
Proveedor	Servidor DNS principal	Servidor DNS secundario
OpenDNS	208.67.222.222	208.67.220.220
Level3	209.244.0.3	209.244.0.4
Verisign	64.6.64.6	64.6.65.6
SmartViper	208.76.50.50	208.76.51.51
OpenNIC	192.95.54.3	192.95.54.1
Norton ConnectSafe	199.85.126.10	199.85.127.10
Dyn	216.146.35.35	216.146.36.36
FreeDNS1	37.235.1.174	37.235.1.177
SafeDNS	195.46.39.39	195.46.39.40
DNS.WATCH	84.200.69.80	84.200.70.40
Alternate DNS	198.101.242.72	23.253.163.53
Comodo Secure	8.26.56.26	8.20.247.20
Hurricane Electric	74.82.42.42	

6.5.6 Configurar las características de red del nuevo servidor

En este punto, lo primero, es que ya se cuenta con un nuevo equipo que incorpora un sistema operativo *Windows Server 2019* instalado. Una vez superado este aspecto, es importante asegurarse de que la configuración de la red es correcta.

Siguiendo el criterio que se aplicó para la instalación y configuración del controlador de dominio principal, asegurarse de que está deshabilitado el *protocolo IPv6* y, para el protocolo *IPv4*, seguir el siguiente criterio:

- Asignar una *IP estática* que se encuentre libre en la red. Para este caso, la **192.168.142.8**. Ya que se encuentra en una red distinta y físicamente, en la Zona Cultural Universitaria.
- Añadir la máscara de red adecuada para la configuración, que en este caso es la 255.255.255.0.
- Incluir la puerta de enlace que se esté utilizando en el resto de equipos. En este caso, la **192.168.142.1**.

- Y, por último, aunque probablemente lo más importante, como *Servidor DNS* preferido, indicar la dirección IP del servidor principal.

6.5.7 Unir el nuevo servidor como cliente del dominio

La forma más fácil de que funcione correctamente la posterior promoción del servidor nuevo como segundo controlador del dominio, es convertirlo antes en un nuevo equipo cliente del dominio. Así, se puede asegurar que todas las configuraciones son correctas antes de comenzar la promoción.

Para lograrlo, sólo se tienen que seguir las indicaciones de *Unir un cliente Windows 10 a un dominio Windows Server 2019*, ya que el proceso es idéntico y que se detalla posteriormente en la sección 6.5.14.

Para este caso, aunque no es obligatorio, se recomienda cambiar el contenido del campo *Descripción del equipo* para que tenga un nombre descriptivo (en este caso, *Controlador de dominio secundario*, que es el rol que tendrá cuando se termine el proceso).

También cambiar el nombre del equipo, *nombre_servidor* y, sobre todo, elegir *Dominio* en la parte inferior y escribir el nombre del dominio del que se va a formar parte. Figura 6.5.7.1.

Una vez completada la operación, se observará un mensaje indicando que el equipo cliente se ha unido correctamente al dominio.

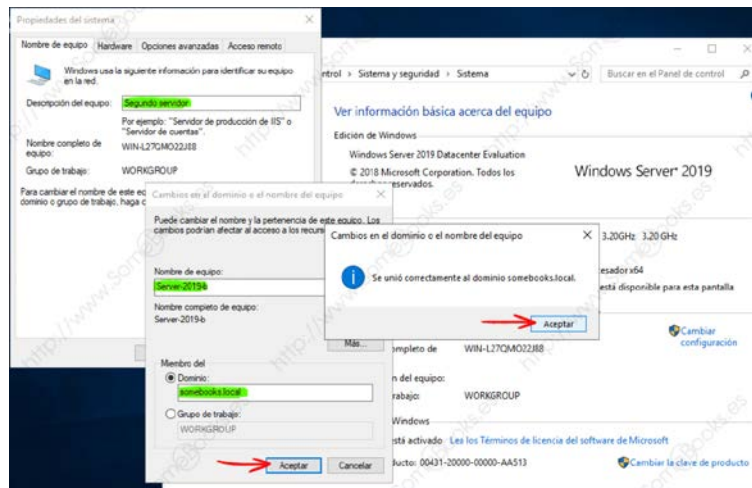


Figura 6.5.7.1 Unión del nuevo servidor al dominio.

Al terminar, sólo faltará reiniciar el equipo para que los cambios se hagan efectivos. Si no se produce ningún error durante el proceso, no será realmente necesario, pero podemos realizar una última comprobación. En el equipo que actúa como controlador de dominio actual, es decir, el servidor *nombre_servidor*, asegurarse de que este equipo cliente, el que será en el futuro controlador de dominio secundario, ha sido incorporado satisfactoriamente al dominio.

Para lograrlo, sólo abrir la ventana *Usuarios y equipos de Active directory* y elegir la entrada *Computers* (en este caso *Controladores de dominio*) en el panel de la izquierda se observarán los equipos agregados recientemente. Esto se puede visualizar en la figura 6.5.7.2.

En ese momento, comprobar, en el panel de la derecha, que ya aparece el nombre del equipo nuevo.

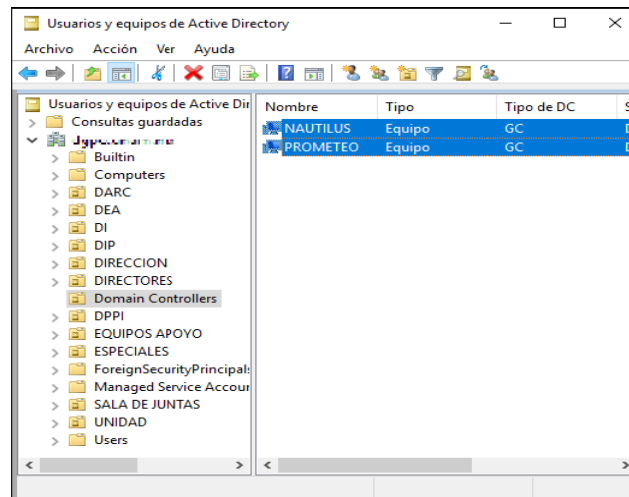


Figura 6.5.7.2 Computadoras y DC unidos al dominio.

6.5.8 Añadir el rol Servicios de dominio de Active Directory al nuevo servidor

Como ya se dijo al principio, el siguiente paso consiste en promocionar el nuevo servidor para que actúe como segundo controlador del dominio. La promoción es muy similar a la que ya se vio para el servidor controlador de dominio principal. Sin embargo, como existen algunas diferencias importantes, se va a explicar nuevamente y así evitar posibles errores.

Lo primero es iniciar sesión en el nuevo servidor con la cuenta *Administrador* del dominio. Sin embargo, tener cuidado porque el sistema ofrece, de forma predeterminada, la cuenta del *Administrador* local, la del propio equipo, no la del dominio. Como lo muestra la figura 6.5.8.1.

Para cambiar el comportamiento predeterminado, sólo es necesario hacer click sobre el elemento *Otro usuario* en la pantalla de autenticación.

A continuación, debe autenticarse con la cuenta *Administrador* del dominio. Algo tan sencillo como escribir el nombre DNS completo de la cuenta, en este caso, *dominio\administrador* o [administrador@dominio.com](#). Escribir el nombre de la cuenta y la contraseña correspondiente.

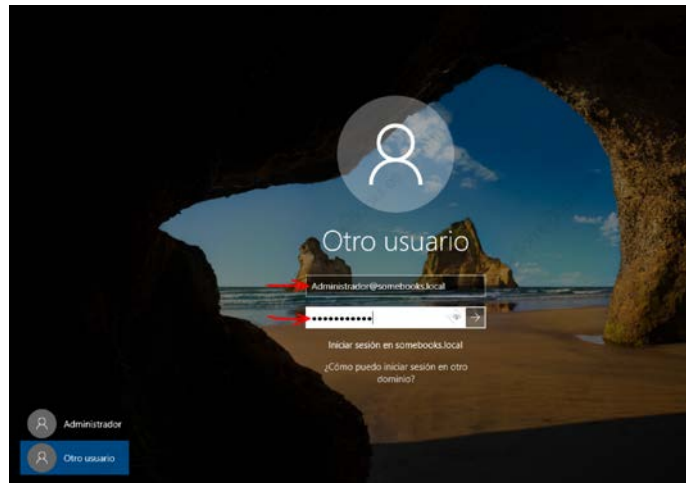


Figura 6.5.8.1 Autenticación al dominio del DC secundario.

Se puede utilizar cualquier cuenta válida en el dominio, que tenga privilegios para llevar a cabo la promoción. También se puede utilizar el nombre *NetBios* de la cuenta en lugar de su nombre *DNS*. Es decir, *dominio/administrador* en lugar de *administrador@dominio.com*, y el resultado será el mismo. El objetivo ha sido ilustrar que esta opción también es viable y que ambas son equivalentes.

Una vez autenticados, se está listo para iniciar la tarea de añadir el rol *Servicios de dominio de Active Directory* al nuevo servidor de dominio secundario.

Dado que el procedimiento es el mismo que se describió para la instalación y configuración del controlador de dominio principal, sólo se describirán los pasos a seguir y se expondrán algunas pantallas del procedimiento, sobre todo, donde sea importante y haya diferencia.

Iniciar por elegir *Agregar roles y características* en el menú *Administrar* del *Administrador del servidor*. Como se muestra en la figura 6.5.8.2.



Figura 6.5.8.2 Agregar roles y características del DC secundario.

El asistente muestra las recomendaciones habituales en cuanto a asegurarnos de que la contraseña de la cuenta de *administrador* es segura, que la configuración de red es correcta, que disponemos de direcciones IP estáticas y que hemos instalado las últimas actualizaciones de seguridad en el sistema operativo.

Una vez que todo sea correcto, dar click en el botón *Siguiente*. Al igual que para el servidor DC principal, se hará una *Instalación basada en características o en roles*. Elegir dicha opción y hacer click sobre el botón *Siguiente*.

En la página *Seleccionar servidor de destino*, marcar la opción *Seleccionar un servidor del grupo de servidores* y en la lista de servidores, asegurarse de que se encuentre seleccionado el controlador actual, que será el único que aparezca. A continuación, hacer click sobre el botón *Siguiente*.

En el siguiente paso, se tiene que elegir el servicio o servicios que se desea instalar. Recordar que la instalación de *Active Directory* conlleva, para su correcto funcionamiento, la instalación implícita de un *Servidor DNS*. Se podría pensar que en este caso no sería necesario porque se tiene uno instalado en el controlador de

dominio principal, pero, como el objetivo es instalar un controlador de reemplazo, que pueda asumir las tareas del controlador principal cuando sea necesario, se necesita que también actúe como *servidor DNS*. En cualquier caso, el asistente no nos permite elegir y lo instala de forma predeterminada. Por lo tanto, marcar la casilla *Servicios de dominio de Active Directory*. Como se observa en la figura 6.5.8.3.

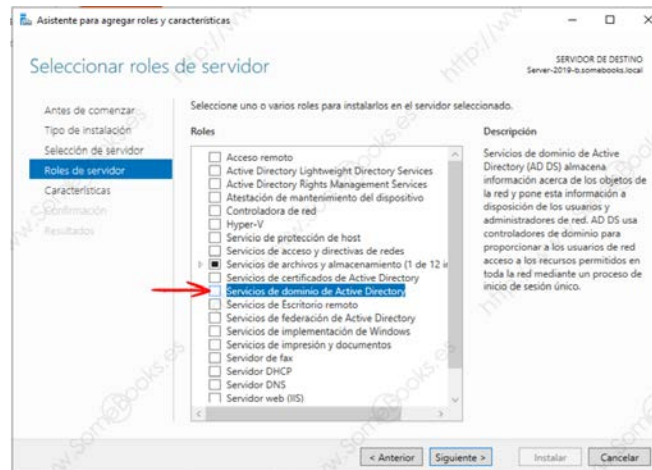


Figura 6.5.8.3 Rol de Servicios de dominio de Active Directory a instalar.

Al hacerlo, el asistente muestra un aviso indicando que los servicios elegidos dependen de otros roles y características que necesitan ser instalados también de forma complementaria. Nos limitamos a dar click sobre el botón *Agregar características*.

Al hacerlo, se comprueba que la línea *Servicios de dominio de Active Directory* ya aparece seleccionada. Para continuar, dar click sobre el botón *Siguiente*.

Después de seleccionar los roles, el asistente ofrece la posibilidad de instalar características. Asegurarse de marcar la casilla correspondiente a la característica *Administración de directivas de grupo* para centralizar en una sola

herramienta las directivas de grupo de toda la instalación. Una vez elegida la característica, dar click sobre el botón *Siguiente*.

Después de esto, aparece una pantalla informativa sobre los *Servicios de dominio de Active Directory* que se recomienda leer atentamente. Quizás uno de los aspectos más interesantes de esta ventana es la recomendación de instalar al menos dos controladores de dominio para un determinado dominio, con el fin de aumentar la disponibilidad de la infraestructura de red. Precisamente, ese es el objetivo hasta este momento.

También, le recuerda al usuario la necesidad de disponer de un servidor DNS y nos informa de que se instalará el servicio de espacio de nombres y los de replicación, que son necesarios para el servicio de directorio. Para continuar, dar click sobre el botón *Siguiente*.

Antes de iniciar la instalación, se puede marcar la opción *Reiniciar automáticamente el servidor de destino en caso necesario*. Al hacerlo aparece un cuadro de diálogo que advierte que, al marcar la opción, pueden producirse reinicios sin que se dé aviso alguno. Como lo muestra la siguiente figura 6.5.8.4.

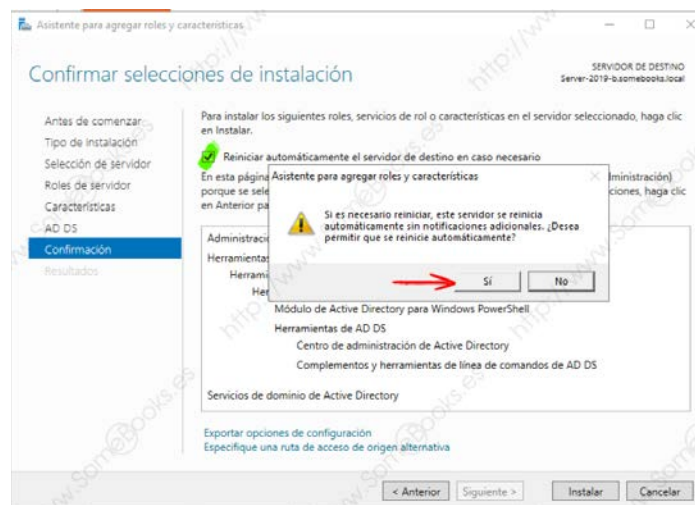


Figura 6.5.8.4 Confirmar selecciones de instalación.

Finalmente, comprobar cada uno de los *roles y características* que van a instalarse. Como es habitual, si se observa algún error, se puede usar el botón *Anterior* y retroceder hasta el paso adecuado para realizar las modificaciones. Sin embargo, si todo es correcto, dar click sobre el botón *Instalar*.

A partir de aquí, en la parte superior de la ventana se podrá observar una barra de progreso que informa del avance de la instalación. Se puede cerrar el asistente y el proceso de instalación no se interrumpirá. En nuestro caso, nos limitamos a esperar.

Cuando termine la instalación, aparecerá un enlace con el texto *Promover este servidor a controlador de dominio*. Bastará con hacer click sobre el enlace para iniciar el paso siguiente.

6.5.9 Promocionar el nuevo servidor como controlador de dominio secundario

El último paso del apartado anterior nos enlaza con el verdadero objetivo de todo este proceso: promocionar el nuevo servidor para que actúe como segundo controlador del dominio.

En términos generales, la promoción es muy similar a la que ya se describió para instalar un dominio con Windows Server 2019 en el DC principal. Sin embargo, como existen algunas diferencias importantes, vamos a volver a explicarlo de una forma detallada con el fin de evitar posibles errores.

Al hacer click sobre el enlace *Promover este servidor a controlador de dominio*, se abre el *Asistente para configuración de Servicios de dominio de Active Directory*.
Figura 6.5.9.1.

Para comenzar, se debe indicar el tipo de controlador de dominio que se está implementando. En este caso, vamos a añadir un nuevo controlador de dominio en un dominio que ya existe.

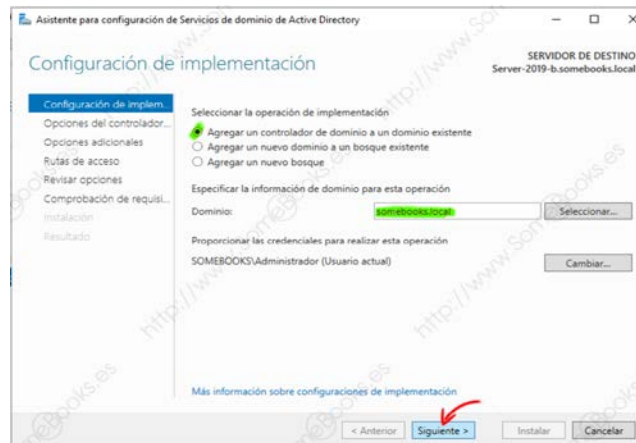


Figura 6.5.9.1 Uniendo el nuevo DC a un dominio existente.

Justo debajo, se debe indicar el nombre del dominio principal del bosque en el que vamos a añadir el controlador de dominio que se está configurando, *nombre_dominio.com*. También se tendrá que indicar la cuenta, con privilegios adecuados en el dominio, la que se va a utilizar para llevar a cabo la tarea. Como antes se configuró el equipo como cliente del dominio y se ha iniciado sesión con las credenciales de la cuenta *Administrador*, ahora se ofrece utilizar estas credenciales de forma predeterminada. Si se decide utilizar una cuenta diferente, sólo habría que hacer click sobre el botón *Cambiar*. Una vez completada la información, hacer click sobre el botón *Siguiente*.

En la página *Opciones del controlador de dominio*, figura 6.5.9.2, el asistente ya da por hecho que el equipo actuará como *Servidor de nombres de dominio, DNS*. Además, aparece marcada la opción para convertirlo en un *Catálogo global (GC)*. También se debe indicar el *Sitio* en el que se ubicará el controlador de dominio.

Cuando se instala por primera vez el *Directorio Activo*, en la base de datos se crea un nuevo objeto llamado *Default-First-Site-Name* donde se ubica el primer controlador de dominio.

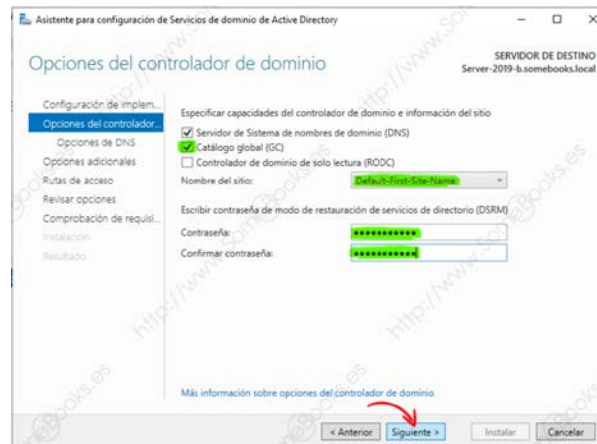


Figura 6.5.9.2 Opciones del controlador de dominio secundario.

Después de esto, el asistente solicitará la contraseña de *Administrador* para cuando se necesite iniciar el sistema en el *modo de restauración de servicios del directorio (DSRM – Directory Service Restore Mode)*. Esta contraseña no es la misma de la cuenta *Administrador* del dominio, aunque, si se quisiera, se puede utilizar la misma. En cualquier caso, se recomienda que sea una contraseña segura. Por último, dar click en el botón *Siguiente*.

En el siguiente paso, *Opciones de DNS*, aparece un aviso de que no se puede crear una delegación para este *servidor DNS*. No preocuparse, ya que el problema quedará resuelto más adelante.

Si se desea, se puede obtener más información haciendo click sobre el enlace *Mostrar más*. Aunque es más que suficiente con dar click sobre el botón *Siguiente*.

En la página *Opciones adicionales*, elegir el controlador desde el que queremos que se realice la replicación inicial. Obviamente, sólo podemos elegir el nombre del servidor que se muestra, porque es el único que se tiene y es el controlador de dominio principal.

En cuanto a la opción *IFM (Install From Media)*, está indicada para situaciones en las que se trata de replicar un controlador remoto, que almacena una infraestructura compleja, al que se accede a través de un ancho de banda escaso. Para evitar problemas de conexión, se podría transportar la información de *Active Directory* en un medio de almacenamiento externo y utilizarlo en este punto de la instalación.

En cualquier caso, *IFM* no sustituye a una conexión de red, porque hay datos que no pueden replicarse por este medio.

El siguiente paso consiste en indicar las ubicaciones donde se guardarán, de forma local, los datos relativos al controlador de dominio secundario que se está configurando. Lo más frecuente es utilizar las ubicaciones predeterminadas. Por lo tanto, limitarse a dar click sobre el botón *Siguiente*.

En la página *Revisar opciones*, como cabe esperar, el asistente muestra un resumen del proceso de instalación. Revisarlo para asegurarse de que no se han cometido errores en los pasos anteriores. Como es habitual, se dispone del botón *Anterior* para resolver cualquier error que pudo haberse cometido. Si todo es correcto, dar click sobre el botón *Siguiente*.

Por último, en el apartado *Comprobación de requisitos previos*, se verifica que el sistema cumple las condiciones para convertirse en un controlador de dominio.

Pueden aparecer algunos avisos, como el que informa que no puede crearse una delegación para el *servidor DNS* que se va a instalar, ya se comentó esta situación

anteriormente. También pueden aparecer errores que impidan la instalación del controlador de dominio. En estos casos, no se podrá continuar hasta que se resuelvan. Como en este caso representativo no hay errores, solo dar click en el botón *Instalar*. Después de esto, se observa cómo se desarrolla el proceso de instalación. Cuando termine, se presenta un aviso de que se va a cerrar la sesión, que realmente significa, es que se va a reiniciar el equipo.

6.5.10 Ajustando la configuración de red del nuevo controlador de dominio secundario

Aunque no es imprescindible, después de reiniciar, se recomienda ajustar la configuración del *Protocolo de Internet versión 4 (TCP/IPv4)*, figura 6.5.10.1, o, en su caso el de la versión 6 para que cada servidor haga referencia como *servidor DNS preferido* al equipo contrario y como *Servidor DNS alternativo*, a él mismo.

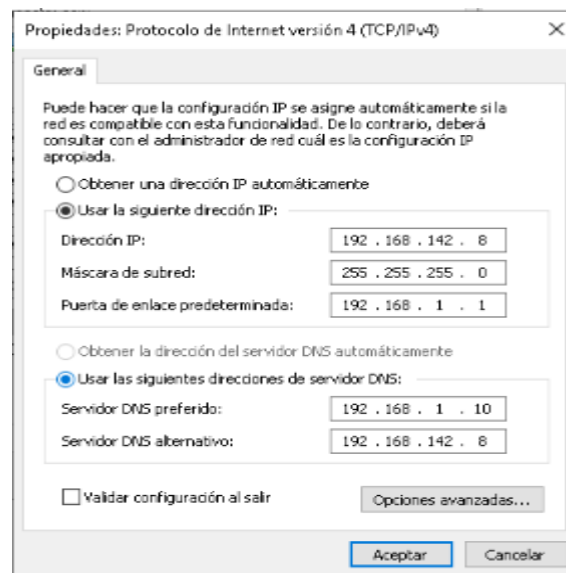


Figura 6.5.10.1 Ajuste de la configuración del protocolo TCP/IPv4 del nuevo DC secundario.

Es decir, el servidor principal, con IP 192.168.1.10, hará referencia a la IP 192.168.142.8, del servidor secundario como servidor DNS preferido. Y el servidor

secundario, con IP 192.168.142.8, hará referencia a la IP 192.168.1.10, del servidor principal como servidor DNS preferido.

6.5.11 Comprobar los servidores DNS

Lo siguiente por hacer es asegurarse de que la configuración predeterminada de los *servidores DNS* se ha producido de forma correcta. Para ello, se puede comenzar por la configuración del servidor secundario.

Elegir la opción *DNS* dentro del menú *Herramientas* del *Administrador del servidor*. En el panel izquierdo de la ventana *Administrador de DNS*, desplegar la entrada que representa al equipo DC secundario, en su interior, *Zonas de búsqueda directa*. Por último, desplegar la entrada correspondiente al nombre del dominio del que forma parte.

En el panel derecho se podrán observar varios datos:

- Los dos controladores de dominio se encuentran registrados como *Servidores de nombre (NS)*.
- Que el *Inicio de autoridad (SOA, del inglés Start of Authority)* hace referencia al servidor secundario.
- Que ambos controladores de dominio están registrados, tanto el principal como el secundario. Como puede observarse en la figura 6.5.11.1.

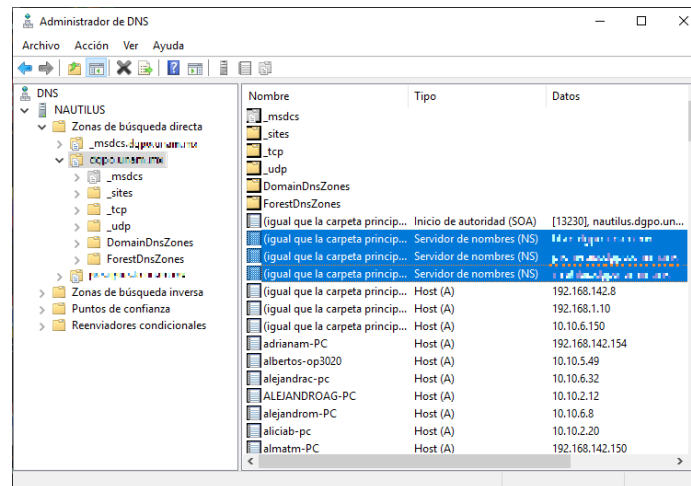


Figura 6.5.11.1 Configuración del Servidor DNS del DC principal.

Y si se desea, se puede hacer la misma comprobación en el servidor DC principal. En él, también abrir el *Administrador de DNS*, desplegar la entrada que representa al servidor principal y, en su interior, *Zonas de búsqueda directa*. Por último, desplegar la entrada correspondiente al nombre del dominio al que pertenece.

En el panel derecho se pueden observar varios datos:

- Los dos controladores de dominio se encuentran registrados como *Servidores de nombre (NS)*.
- Que el *Inicio de autoridad (SOA, del inglés Start of Authority)* hace referencia al servidor principal.
- Que ambos controladores de dominio están registrados.

6.5.12 Replicar los controladores de dominio

Durante los siguientes minutos, el controlador de dominio principal se estará replicando sobre el nuevo controlador de dominio secundario, pero, como la creación de los objetos de conexión puede ocupar bastante tiempo, se crearán manualmente y así comprobar de inmediato que todo funciona correctamente.

Para comenzar, elegir la opción *Sitios y servicios de Active Directory* dentro del menú *Herramientas* del *Administrador del servidor*.

Figura 6.5.12.1 Comprobando la existencia de los dos controladores de dominio.

En el panel izquierdo, desplegar *Sites, Default-First-Site-Name* y después *Servers*. En su interior, observar los dos controladores de dominio que se tienen. Como lo muestra la figura 6.5.12.1.

Desplegando cada uno de los servidores, se tendrá acceso a la configuración de *NT Directory Services* (NTDS Settings). Sin embargo, si no se ha dado tiempo a que se creen los objetos de conexión, puede que en el panel derecho solo se vea el mensaje *No hay elementos disponibles en esta vista*.

Si este fuera el caso, se puede forzar la creación de los objetos haciendo click sobre cada entrada *NTDS Settings* con el botón derecho del ratón y eligiendo, en el menú de contexto que aparece, la opción *Todas las tareas*, y a continuación, elegir *Comprobar la topología de replicación*.

Al hacerlo, aparece un mensaje informativo como el de la figura 6.5.12.2, informando de que la comprobación se ha realizado y que, en este caso, **el servidor principal** está viendo al **servidor secundario**, cuando se haga en el **servidor**

secundario, el mensaje será, al contrario. También avisa de la necesidad de realizar la replicación.

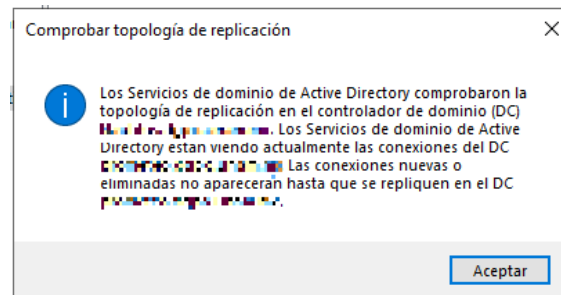


Figura 6.5.12.2 Comprobando la replicación entre los dos DC.

Después de esto, probablemente se deba actualizar la información del árbol para que se muestre actualizada. Para lograrlo, hacer click con el botón derecho del ratón sobre *Sites*. Y, en el menú de contexto que aparece, elegir la opción *Actualizar*. Figura 6.5.12.3.

Figura 6.5.12.3 Actualizar sitios y Servicios de Active Directory.

Ahora, sólo queda hacer efectiva la replicación. Para eso, dirigirse de nuevo a cada una de las entradas *NTDS Settings* y comprobar que al hacer click sobre ellas aparecen los objetos de conexión en el panel derecho.

Lo siguiente será hacer click con el botón derecho del ratón sobre los objetos de conexión de cada servidor. Y en el menú de contexto que aparece, elegir *Replicar ahora*. Figura 6.5.12.4.

Figura 6.5.12.4 Generando la replicación entre los DC.

Cuando se complete la replicación, aparecerá el mensaje, *Los servicios de dominio de Active Directory replicaron las conexiones*, informando de que el proceso se ha completado.

6.5.13 Comprobando la replicación

Para comprobar que, efectivamente, desde el controlador de dominio secundario, se tiene acceso a todos los datos del dominio, abrir la herramienta *Usuarios y equipos de Active Directory* desde el menú *Herramientas del Administrador* del Servidor. Cuando se abra la ventana *Usuarios y equipos de Active Directory*, en el panel izquierdo desplegamos la entrada correspondiente al dominio. Después, hacer click sobre *Computers*. Se observará, en el panel de la derecha, que aparecen los equipos que actúan como clientes del dominio. Se observa que los dos DC aparecen en el apartado *Domain Controllers* y en el apartado *Users* se pueden observar todos los usuarios y grupos de usuarios del dominio. Lo que se está comprobando aquí es que

el segundo controlador ya conoce los clientes del dominio. Como se puede constatar en la figura 6.5.13.1.

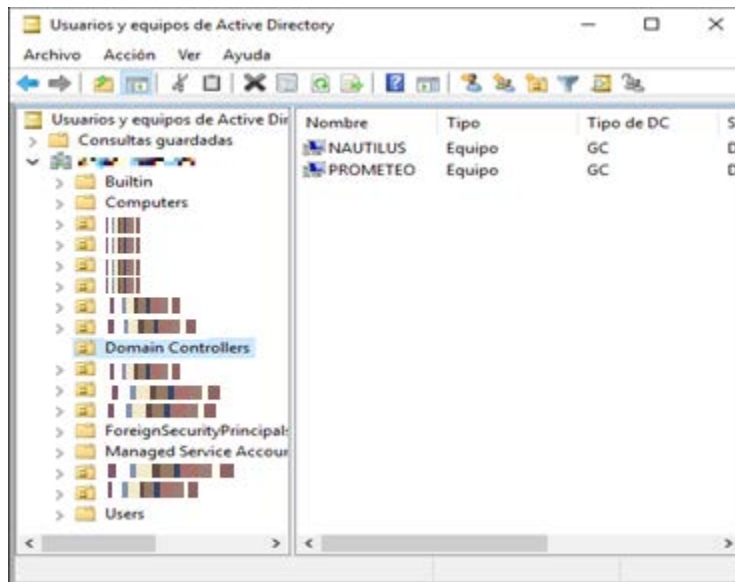


Figura 6.5.13.1 Comprobando la replicación entre los dos DC.

6.6 Unir un cliente Windows 10 al dominio

El primer paso, para comenzar a utilizar los recursos que ofrece un dominio, consiste en añadir a dicho dominio los equipos que puedan actuar como clientes. En este caso, comenzar por un equipo que está ejecutando Microsoft Windows 10. Básicamente, el proceso consistirá en realizar los siguientes pasos:

- Establecer las características de red, para que coincidan con las necesidades del dominio.
- Ajustar el nombre del equipo cliente.
- Unir el equipo al dominio.

Al final del proceso, iniciar sesión en el equipo cliente usando una cuenta de usuario de las que ya se tengan definidas en el dominio. Con esto se comprobará que el proceso se ha realizado correctamente.

6.6.1 Configurando la red del equipo cliente

Para conseguir que un cliente pueda unirse a un dominio, antes asegurarse de que las características de su configuración de red sean coincidentes con las necesidades del dominio.

Aquí, se puede dejar habilitada la asignación automática de IP, pero asegurarse de que el Servidor DNS preferido haga referencia a la dirección IP del controlador del dominio. Aunque para mayor seguridad, es mejor declarar una dirección IP estática para el equipo Windows 10 que se pretende unir al dominio.

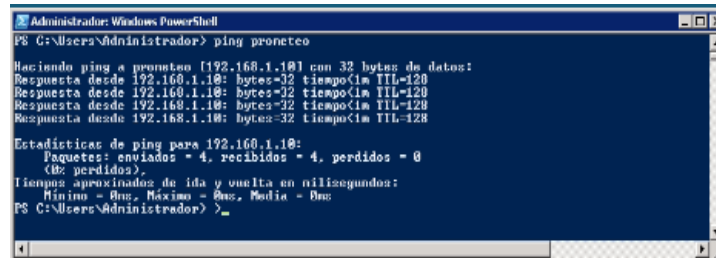
6.6.2 Comprobación de que la configuración de red es correcta

Asegurarse de que no se ha cometido ningún error. Esto es tan sencillo como abrir una ventana de comandos y hacer un ping al Servidor. Si se utiliza el nombre del servidor en lugar de su dirección IP, no sólo se estará comprobando que el equipo cliente está en la misma red que el servidor. También se comprobará que la configuración DNS del cliente es correcta y que el servidor DNS del controlador de dominio está funcionando adecuadamente.

Si la respuesta no es correcta, se deberán repasar las últimas acciones realizadas. Para comenzar, dar click, con el botón derecho del ratón, sobre el botón Inicio. En el menú que aparece, elegir la opción *Windows PowerShell*. Una vez que se abra la ventana de *PowerShell*, teclear la siguiente orden:

```
Ping nombre_servidor
```

Si todo es correcto, el servidor responderá y la salida será parecida a lo que muestra la figura 6.5.14.2.1.



```
Administrador: Windows PowerShell
PS C:\Users\Administrador> ping pronetco

Haciendo ping a pronetco [192.168.1.10] con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo=1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo=1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo=1m TTL=128
Respuesta desde 192.168.1.10: bytes=32 tiempo=1m TTL=128

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos)
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\Administrador>
```

Figura 6.5.14.2.1 Comprobación de la correcta configuración de red del cliente.

6.6.3 Cambiar el nombre del equipo y unirlo al dominio

El siguiente procedimiento de cierta manera ya se trató cuando se unió el servidor de dominio secundario. Pero se vuelve a tocar para un equipo con Windows 10.

El procedimiento consiste en asignarle un nombre al equipo. Puede ser que describa o dé una pista de donde se encuentra el equipo o de que usuario se trata, tal vez el nombre del área donde se encuentra. Al indicar el nombre del dominio, el sistema procederá a establecer el vínculo.

Una manera es abrir el explorador de archivos de Windows. En el panel izquierdo, dar click con el botón derecho del ratón sobre *Este equipo*, y elegir *Propiedades*. De la ventana que se abre, en el panel derecho elegir la opción *Cambiar el nombre de este equipo (avanzado)*. Al hacerlo, aparecerá la antigua ventana que muestra la descripción, figura 6.5.14.3.1, y el nombre del grupo de trabajo o dominio al que pertenece.

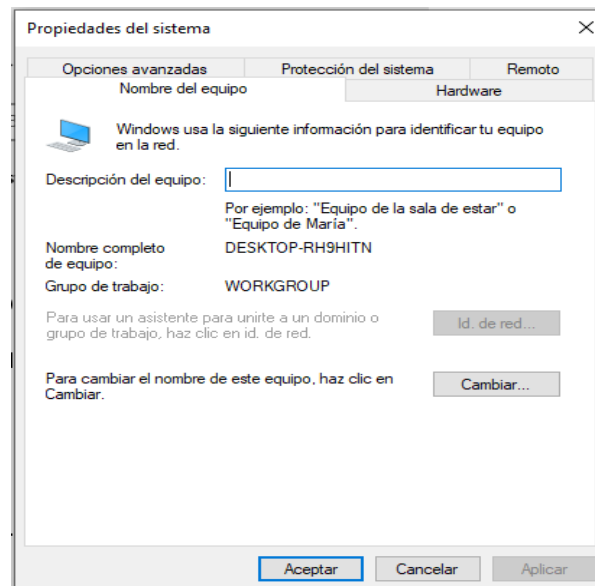


Figura 6.5.14.3.1 Cambiar nombre al equipo cliente.

En la imagen se puede observar que, en estos momentos, el nombre del equipo es el que la instalación le asignó, o bien el que ya le hayamos asignado. Además, también vemos que pertenece al grupo de trabajo predeterminado (*WORKGROUP*), que se asigna a todos los equipos con Windows desde hace innumerables versiones. Para cambiar estos datos, sólo hay que hacer click en el botón *Cambiar...* para escribir el nuevo nombre del equipo, si es el caso, y el nombre del dominio al que se va unir.

Esto se hace en la ventana que aparece a continuación, figura 6.5.14.3.2. En el campo *Nombre de equipo*, asignarle un nombre al equipo. Además, en el área *Miembro del*, elegir la opción *Dominio* y debajo escribir el nombre del dominio al que se desea unir el equipo. Cuando los datos sean correctos, dar click en *Aceptar*.

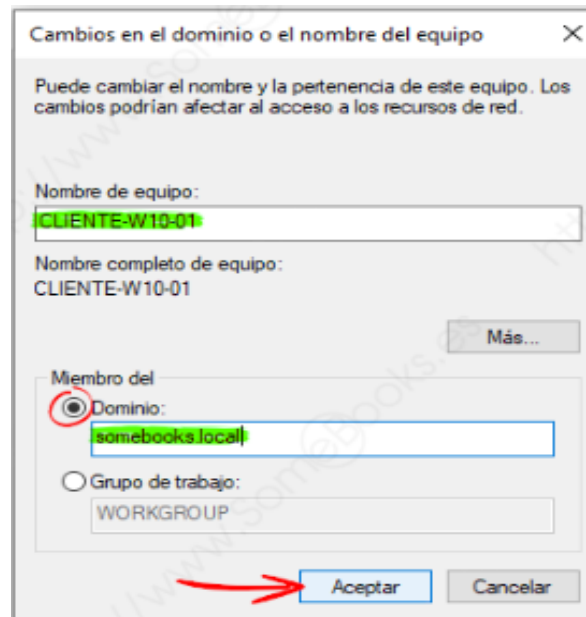


Figura 6.5.14.3.2 Cambio de pertenencia de grupo de trabajo a dominio del nuevo equipo cliente.

En ese momento, Windows 10 busca en la red el dominio especificado. Si no lo encuentra, aparecerá un mensaje de aviso. Probablemente se habrá cometido algún error en los datos introducidos.

Si lo encuentra, se deberá escribir un nombre de usuario y una contraseña, perteneciente al dominio, que tenga privilegios suficientes para unir el equipo cliente. La ventana de autenticación se cierra y en su lugar aparece un mensaje indicando que el equipo se ha unido correctamente al dominio. Si se cometió algún error en el nombre de usuario o en la contraseña, en lugar del mensaje *Se unió correctamente al dominio nombre_dominio.com*, aparecerá uno de error y se tendrá que volver a intentar.

A continuación, aparece una nueva ventana informativa indicando que se debe reiniciar el equipo para que se apliquen los cambios, pero que antes se deben cerrar todos los programas y guardar todos los archivos que se tengan abiertos. Hacer click sobre *Aceptar*. Cuando se haya concluido el reinicio, se procede a iniciar sesión con una de las cuentas de usuario del dominio.

6.7 Creando Unidades Organizativas y asignarles contenido


Una *Unidad Organizativa*, del inglés, *Organizational Unit* o, simplemente, *OU*, es un contenedor del *Directorio Activo* que puede contener *usuarios, equipos, grupos* y otras *unidades organizativas*.

Una vez creada una *Unidad Organizativa*, se le pueden otorgar valores de configuración de directiva de grupo o se puede delegar sobre ella una parte de la autoridad administrativa. Así, un usuario puede tener autoridad para administrar una determinada unidad organizativa y no tenerla para el resto.

En definitiva, actuarán como contenedores que ayudan a representar la organización lógica de nuestra red y/o de la dependencia.

6.7.1 Crear una nueva unidad organizativa

Primeramente, se debe comenzar por abrir la herramienta *Usuarios y equipos de Active Directory*. Se puede llegar a esta opción de dos maneras diferentes:

1. Desde el menú *Herramientas* del *Administrador del Servidor*.
2. Ejecutando la orden **dsa.msc** desde la ventana *Ejecutar* que se puede abrir usando la combinación de teclas 

A continuación, ubicar el puntero del ratón sobre el nombre del dominio y dar click con el botón derecho. En el menú de contexto que aparece, elegimos *Nuevo* y a continuación, *Unidad organizativa*. Como se muestra en la figura 6.5.16.1.

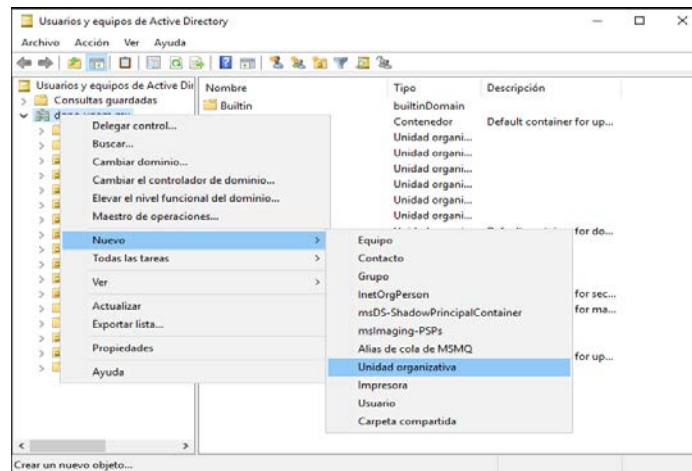


Figura 6.5.16.1 Crear una Unidad Organizativa.

Si lo que se quiere es crear la *Unidad Organizativa* dentro de otra que ya existe, en lugar de dar click con el botón derecho del ratón sobre el nombre del dominio, figura 6.5.16.2, hacerlo sobre la *Unidad Organizativa*, dentro de la cual se creará otra *Unidad Organizativa*.

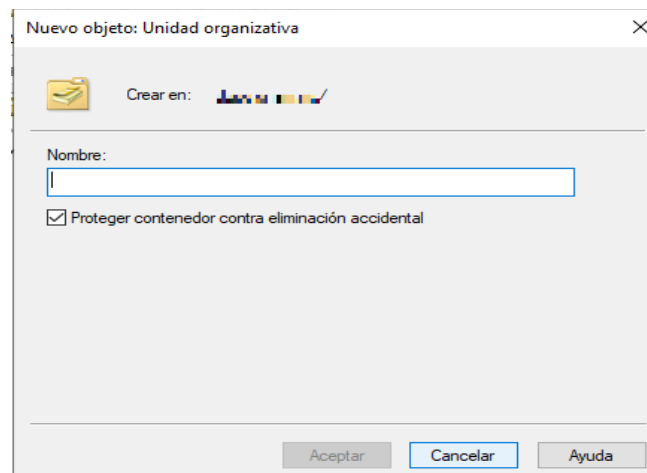


Figura 6.5.16.2 Asignándole nombre a la nueva Unidad Organizativa.

A continuación, escribir el nombre que se desee o describa a la *UO*. También se puede dejar marcada la opción *Proteger contenedor contra eliminación accidental*. De esta forma, el sistema impedirá que se elimine la *Unidad Organizativa* por error.

Para finalizar, dar click en *Aceptar*. Repitiendo el proceso anterior, se pueden crear las *UO* que se necesiten.

6.8 Crear cuentas de usuario en el dominio

La herramienta que permite administrar usuarios del dominio se llama *Usuarios y equipos de Active Directory*. Para ejecutarla, sólo necesitamos acceder al menú *Herramientas* del *Administrador del Servidor*, y cuando se muestre el menú, dar click sobre la opción *Usuarios y equipos de Active Directory*.

Se abre la ventana *Usuarios y equipos de Active Directory*, figura 6.5.17.1. En ella se dispone de un panel a la izquierda donde se puede ver el dominio *nombre_dominio.com* y, dentro, los diferentes contenedores de los que se dispone. Entre ellos, se encuentran *Builtin* y *Users*, los contenedores predeterminados para grupos y usuarios.

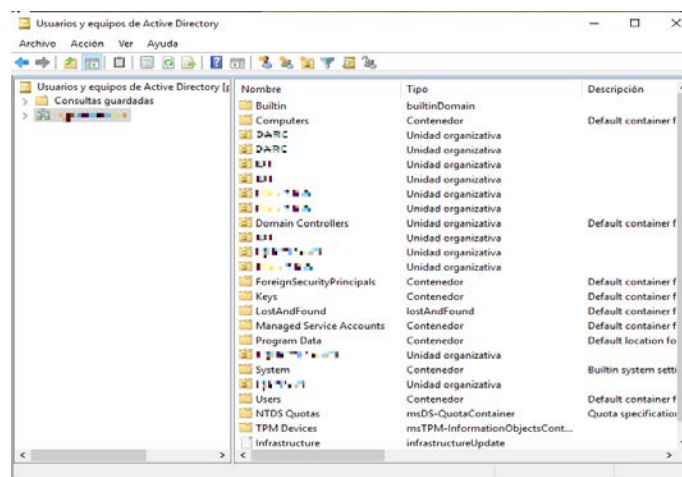


Figura 6.5.17.1 Unidades Organizativas del dominio sobre las cuales se pueden crear usuarios.

Si se tuviera acceso a más de un dominio, también aparecerían en el panel izquierdo.

Una vez elegido el contenedor donde se almacenará el nuevo *usuario*, para crearlo, se tiene que dar click con el botón derecho del ratón sobre él. En el menú de contexto que aparece, elegir *Nuevo* y, a continuación, *Usuario*.

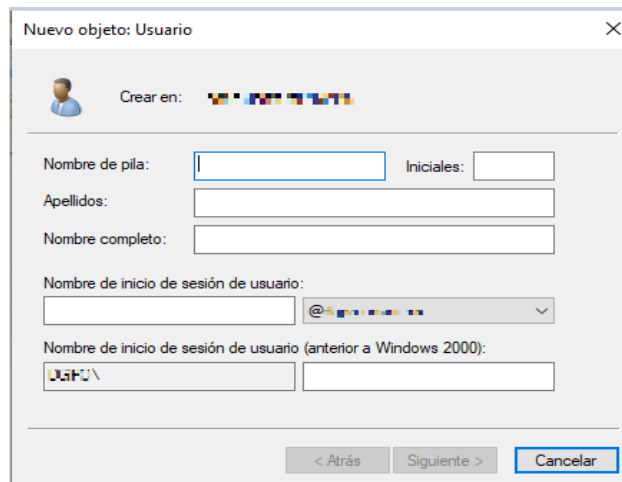


Figura 6.5.17.2 Creando un nuevo usuario en una UO.

Al hacerlo, aparece una nueva ventana titulada *Nuevo objeto: Usuario*. Es el asistente de creación de *usuarios*. Figura 6.5.17.2. En el primer paso, se tendrá que rellenar los datos del usuario: Su *Nombre*, *Apellidos* e *Iniciales*. Con ellos se formará el campo *Nombre completo*, aunque si no es del agrado el resultado, se puede editar.

A continuación, escribir el *Nombre de inicio de sesión de usuario* que, en realidad, se compone de dos partes: el nombre propiamente dicho y el sufijo, que se elige de una lista desplegable. Si se dispone de varios dominios en la red, en la lista aparecerá una entrada por cada uno de ellos.

Por último, el campo *Nombre de inicio de sesión de usuario (anterior a Windows 2000)* tiene como objeto permitir que se conecten al dominio clientes que ejecuten Windows 95, Windows 98 o Windows NT. Cuando se haya concluido de dar toda

esta información, dar click sobre *Siguiente*. A continuación, se tiene que proporcionar una contraseña para el nuevo usuario, la cual deberá cumplir con los requerimientos de complejidad del sistema operativo.

Además, en la parte inferior de la ventana se dispone de cuatro opciones:

- *El usuario debe cambiar la contraseña en el siguiente inicio de sesión:* Si se marca, opción por defecto, se obliga al usuario a cambiar la contraseña que se le está definiendo, la próxima vez que inicie sesión en el dominio. De esta forma, el usuario estará seguro de que nadie más conoce su contraseña.
- *El usuario no puede cambiar la contraseña:* Al contrario que la anterior, esta opción impide que el usuario pueda cambiar su contraseña en ningún momento. Esta opción puede resultar interesante para que el administrador mantenga el control total sobre alguna cuenta temporal o de invitado.
- *La contraseña nunca expira:* hace que la contraseña no expire en el plazo que establezca el sistema operativo.
- *La cuenta está deshabilitada:* Mientras esta opción esté marcada, el usuario no podrá iniciar sesión en el sistema.

Cuando se hayan completado los datos necesarios en este paso, dar click sobre el botón *Siguiente*.

Como es habitual en todas las herramientas de configuración de Windows Server 2019, el asistente muestra un resumen de los datos introducidos antes de crear la cuenta de manera efectiva. Si todo es correcto, dar click sobre el botón *Finalizar*. De lo contrario, utilizaremos el botón *Atrás*.

En este momento, si la contraseña que se ha elegido no cumpliera las condiciones de complejidad predeterminadas que se han comentado, aparecería un mensaje de aviso y se tendría que volver atrás para resolver el problema. No obstante, si todo

es correcto, la ventana *Nuevo objeto – Usuario* se cerrará y volvemos a ver la ventana *Usuarios y equipos de Active Directory*.

Seguir este procedimiento para crear todos los usuarios que sean necesarios. Se pueden crear dentro del contenedor *Usuarios*, o bien, en cada una de las UO que ya se hubieran creado, para así asignar los usuarios a su respectiva UO. El procedimiento es el mismo. Del mismo modo, se pueden crear grupos de usuarios. Estos servirán para cuando se tenga que aplicar sobre ellos alguna política de seguridad.

6.8.1 Operaciones frecuentes sobre cuentas de usuario de un dominio Windows Server 2019

Normalmente se pueden llevar a cabo algunas acciones sobre las cuentas de usuario del dominio, en particular, las siguientes:

- Modificar valores generales de las cuentas.
- Establecer horas de inicio de sesión.
- Limitar los equipos desde los que un usuario puede iniciar sesión.
- Averiguar de qué grupos es miembro un usuario.
- Recuperar contraseñas.
- Deshabilitar una cuenta de usuario.
- Hacer que un usuario sea miembro de un grupo.
- Copiar cuentas de usuario.
- Eliminar una cuenta de usuario.
- Entre otras acciones más.

Todos estos ajustes se realizan desde la herramienta *Usuarios y equipos de Active Directory*.

6.9 Directivas de grupo (GPO)

Dentro de las tareas básicas, pero fundamentales, para mantener las mejores prestaciones del controlador de dominio, está el asignar, editar o eliminar permisos y acciones tanto a los usuarios como a los equipos de la dependencia. Si esto se hiciera de forma individual implicaría demasiado tiempo de modo que *Microsoft* ha desarrollado *las directivas de grupo (GPO)* con el fin de que cualquier cambio u orden que sea creada, esta se replique de forma automática a todos los equipos de la unidad organizativa donde se creó dicha GPO o bien en todo el dominio.

Cuando se configura un equipo, hay que configurar decenas, de parámetros y opciones. Es necesario decidir en donde accederá el usuario, a qué carpetas tendrá acceso, que impresoras podrá usar, cuál será su fondo de escritorio, su página de inicio, qué configuración de firewall tendrá, qué programas podrá usar o incluso si podrá instalar programas. Una cantidad muy grande de configuraciones que puede ser tedioso en un solo equipo, pero que puede ser una tarea casi titánica en caso de hacerlo en cientos o incluso miles de ellos.

Desde que apareció Windows Server 2000, la característica de *Directivas de Grupo* o GPO, los administradores de sistemas *Microsoft* han podido definir configuraciones centralizadas para desplegarlas sobre el parque de equipos, usuarios y servidores.

6.9.1 Definiendo Directiva de grupo o GPO

Una GPO (Group Policy Object – Objeto de Políticas de Grupo), es una colección virtual de diversas configuraciones de políticas que pueden ser aplicadas tanto a elementos como equipos o usuarios del dominio. Cada GPO tiene un nombre único el cual se conoce como GUID.

Con este ambiente, todos los equipos cuyo sistema operativo sea Windows, contarán con un GPO local, ya sea que este equipo forme parte o no de un entorno de Active Directory. Todas las GPO locales siempre se procesan porque los GPO basados en Active Directory tienen prioridad mucho más alta que las demás por sus prestaciones en el dominio.

La mayor ventaja que proporciona este modelo es que al implementarlas, las políticas de grupo o GPO's, de manera centralizada para posteriormente desplegarla sobre los equipos y usuarios, la interacción del administrador con los usuarios y equipos finales es mínima, por lo que se consigue un considerable ahorro de tiempo de administración.

Pero esta no es la única ventaja; ya que el establecer configuraciones centralizadas que se propagan a los equipos y servidores bajo demanda, también ayudan a eliminar fallos de implementación, ya que es mucho más normal cometer un error cuando se despliega cien veces una configuración que cuando se despliega una única vez.

Otra ventaja, es que en caso de tener que hacer modificaciones posteriores, se realizarán una única vez, propagándose los cambios al resto de la explotación sin que esto revierta en un gran volumen de trabajo y en un nuevo riesgo de error.

Cuando se decide aplicar *Directivas de Grupo*, o *Políticas de Grupo o GPO*, se puede definir también el ámbito en el que van a tomar efecto dichas configuraciones. Se puede definir que afecte a toda la dependencia, o a una parte de ella, llegando a una gran granularidad, en la que se defina, por ejemplo, que solo afecte a los usuarios de una oficina, a los de un departamento o incluso a un solo usuario y aquí se encuentra otro de los puntos fuertes de las *GPO*.

6.9.2 Instalar la Consola de Administración de Directivas de Grupo

Para instalar la consola de *Administración de Directivas de Grupo* en *Windows Server 2019*, figura 6.5.19.2.1, ir a la utilidad *Administrador del servidor* y allí usar alguna de las siguientes opciones:

- Ir al menú *Administrar > Agregar roles y características*.
- Pulsar en la línea *Agregar roles y características* ubicada en el panel central del administrador.
- En la ventana desplegada, se debe ir a la sección *Características* y allí activar la casilla *Administración de directivas de grupo*. Pulsar en *Siguiente* y seguir los pasos del asistente.

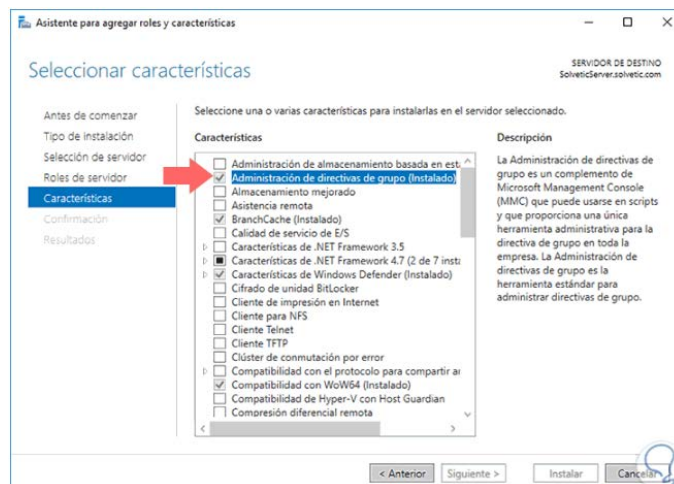


Figura 6.5.19.2.1 Instalando la característica Administración de directivas de grupo.

Ya instalada, para abrirla se cuenta con dos alternativas que son:

- Ir al menú *Herramientas* y allí seleccionar la opción *Administrador de directivas de grupo*.
- Usando la combinación de teclas:

Tecla Windows + **R**

Ahora ejecutar el comando, figura 6.5.19.2.2:

gpmmc . msc

Pulsar *Enter* o *Aceptar*.

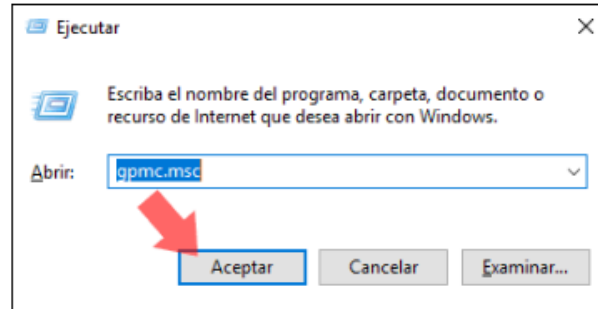


Figura 6.5.19.2.2 Abrir consola de Administración de Directivas de Grupo desde la ventana Ejecutar.

Normalmente, cuando se habla de las *Directivas de Grupo*, muchas veces se suele pensar en las configuraciones básicas, en los mapeos de unidad de red o de impresoras y en algunos casos, también de los despliegues de programas de manera automática, pero la aplicación de las *Políticas y Preferencias* puede llegar mucho más allá.

6.9.3 Ejemplo de implementación de una GPO.

Cuando se habla de *Políticas o Directivas de Grupo*, se debe saber que el elemento más básico que se tiene es la *Configuración de Directiva Individual*, que suele conocerse como *directiva o política*, y que es la encargada de definir un cambio de configuración concreta. Por ejemplo, una que impide que el usuario pueda abrir el *Panel de Control*, Ver la unidad C:, usar los USB o instalar un programa.

Tal como se ha dicho previamente, las políticas se aplican sobre usuarios o equipos por lo que se debe tener en cuenta que existen dos tipos de directivas en función de a quien tienen que aplicarse:

-
- Cuando afectan a un equipo se habla de *Directivas de Ajuste de Configuración de Equipo*. Estos ajustes se realizan cuando la máquina inicia o actualizando de manera automática cada 90-120 minutos, empezando a contar desde el momento del inicio de la máquina.
 - Cuando afectan a un usuario se habla de *Directivas de Configuración de Usuario*. Estos ajustes se realizan cuando se inicia la sesión o actualizando de manera automática cada 90-120 minutos, empezando a contar después del inicio.

El mayor problema que pueden presentar las *GPO* no es la complejidad de planificación y creación ni la complejidad de administración y mantenimiento, es el uso de la herencia de las *GPO*, ya que existen distintos niveles a los que pueden aplicarse, y estas pueden “pisarse” unas a otras si no se les planifican correctamente.

Por esta razón, es muy importante conocer los niveles a los que puede vincularse una *GPO* y la forma en la que interactúan unas con otras, para así evitar comportamientos indeseados, como se muestra en la figura 6.5.19.3.1. Ya que, cuando se vincula una *GPO*, esta quedará aplicada al contenedor de nivel superior, pero se propagará hacia los niveles inferiores.

Tener claro que las *GPO* pueden desplegarse a los siguientes niveles:

- Nivel de Dominio.
- Nivel de Sitio.
- Nivel de OU (Unidad Organizativa).
- Nivel local.

Sin embargo, el orden de aplicación es el siguiente:

- GPO Locales.
- GPO a nivel de Sitio.
- GPO a nivel de Dominio.
- GPO a nivel de OU.



Figura 6.5.19.3.1 Representación del orden de procesamiento de las GPO.

Dentro de las múltiples tareas que en muchas ocasiones se deben realizar como administrador, está la de impedir que algunos o todos los usuarios tengan o no acceso a diferentes aplicaciones o programas dentro de la organización con el fin de mejorar la seguridad de la misma.

Uno de las principales utilidades que encontramos en todas las versiones de Windows, no solamente a nivel de servidores, está relacionada con el **Panel de control** ya que desde allí se gestionan múltiples parámetros de todo el equipo y del sistema y un uso indebido del mismo puede afectar todo el rendimiento tanto del equipo como de las aplicaciones que deben ser ejecutadas.

En este ejemplo se muestra cómo se puede impedir al acceso a los usuarios creando una política de grupo.

Primeramente, abrir *el Administrador de Directivas de Grupo*, figura 6.5.19.3.2, mediante una de las dos maneras descritas en el apartado anterior.

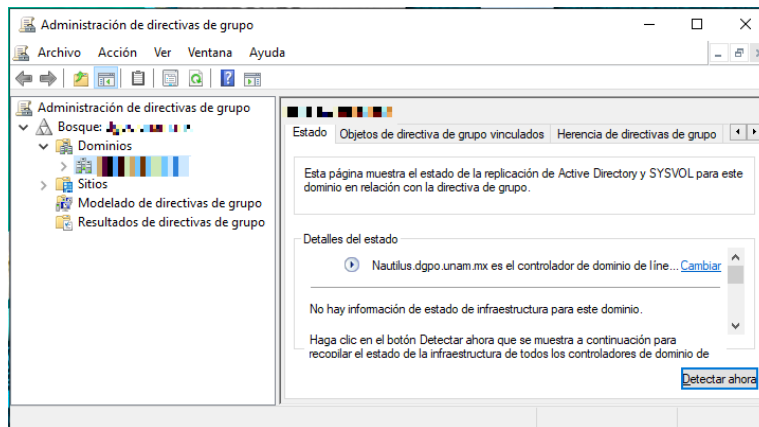


Figura 6.5.19.3.2 Consola Administración de Directivas de Grupo.

Crear la política de grupo. Cuando se crea una política de grupo se cuenta con dos opciones:

- Crear una política de grupo a nivel general para todos los usuarios seleccionando la opción *Default Domain Policy*.
- Crear una política a un grupo determinado de usuarios seleccionando la *unidad organizativa* en particular.

Para este ejemplo, se crea la política en la unidad organizativa Usuarios Solvetic por lo cual se debe desplegar el dominio y dar click derecho sobre dicha OU y elegir la opción *Crear GPO en este dominio y vincularlo aquí*. Ver la figura 6.5.19.3.3.

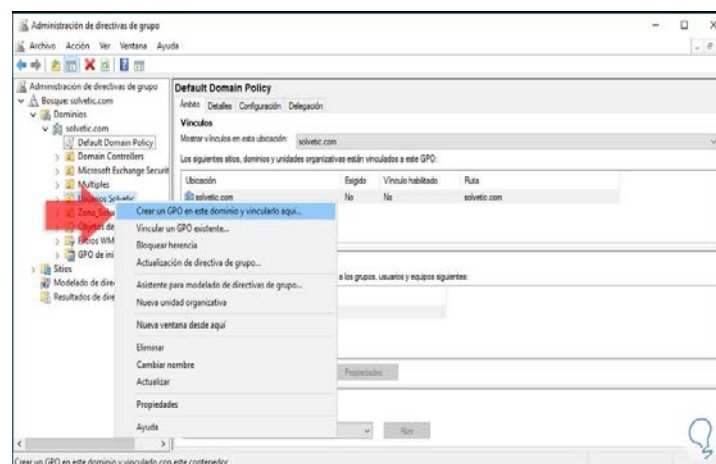


Figura 6.5.19.3.3 Crear una GPO y vincularla.

En la ventana desplegada, asignar un nombre a la política, como se muestra en la figura 6.5.19.3.4.



Figura 6.5.19.3.4 Asignándole un nombre a la nueva GPO.

Pulsar *Aceptar* y observar que la política ha sido creada de manera correcta. Ahora, dar click derecho sobre la política y seleccionar la opción *Editar*. En la ventana desplegada, figura 6.5.19.3.5, ir a la siguiente ruta:

- Configuración de usuario.
- Directivas.
- Plantillas administrativas.
- Panel de control.

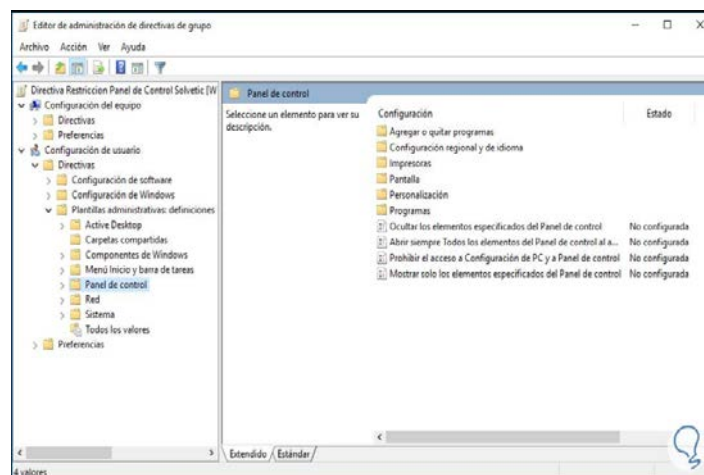


Figura 6.5.19.3.5 Configurando las acciones de la política de grupo.

En el panel derecho, configurar la política con el nombre *Prohibir el acceso a Configuración de PC y a Panel de control*. Dar doble click sobre ella y se observará que por defecto no está configurada. Basta con marcar la casilla *Habilitada* para que la restricción sea efectiva. Figura 6.5.19.3.6.

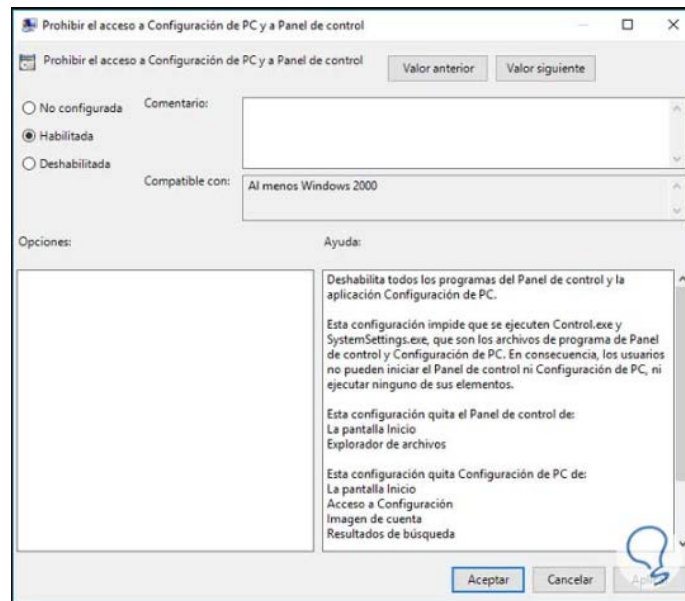


Figura 6.5.19.3.6 Habilitando la Política elegida para que tenga efecto sobre la UO deseada.

Pulsar *Aplicar* y luego *Aceptar* para guardar los cambios. Se puede observar que la política ha sido configurada de manera correcta.

Para comprobar que todo ha sido configurado de manera correcta, intentar abrir el panel de control desde uno de los equipos de alguno de los usuarios que pertenecen a la unidad organizativa sobre la cual, se creó la GPO y se podrá observar que el resultado es el siguiente, figura 6.5.19.3.7:

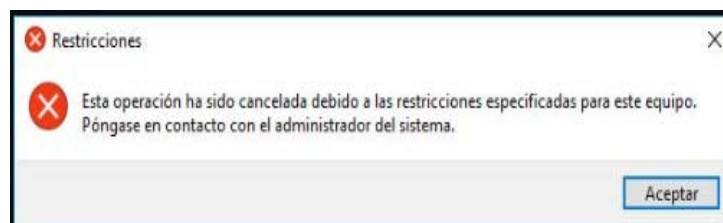


Figura 6.5.19.3.7 Mensaje indicando que no es posible la acción solicitada debido a la aplicación de una política.

Como se puede dar cuenta, de esta manera se ha restringido el acceso al Panel de control y por ende se evita que algún usuario inexperto o con malas intenciones ejecute cambios no autorizados en el equipo.

Con esto se tiene un panorama amplio y claro para darse cuenta de lo que se pretende llevar a cabo o implementar para sustituir la actual infraestructura de red con la que cuenta la DGPO. De los varios servidores con los que se cuenta actualmente, algunos de ellos son servidores como tal, pero también los hay de equipos personales a los que se les instaló Windows Server 2019 para que funcionen como servidores. Obviamente, con las limitaciones que todo esto conlleva.

Capítulo 7

Conclusiones

Se determinó que el esquema de dominio con Windows Server 2019 es factible en lo técnico o tecnológico, operativo y administrativo para su implementación en la DGPO debido a todas las bondades y ventajas que ofrece comparado con el esquema de servidores independientes que se tenía.

La disponibilidad y conectividad que garantiza este esquema de dominio con dos controladores, es esencial para la DGPO ya que, en algún fallo en cualquiera de los dos, la disponibilidad de información y recursos, continúa. Evitando así la paralización y/o retrasos en las actividades normales de la dependencia.

La planeación y el uso de la replicación entre los dos servidores, determinó que se está muy cerca de lograr una alta disponibilidad en el sistema de información de la dependencia.

Debido a varios cierres de la dependencia por parte de estudiantes, y el tener uno de los dos servidores fuera de la misma, se ha garantizado la continuidad de las actividades.

El esquema permite también, estandarizar los entornos de trabajo de cada equipo de los usuarios, permitiendo también limitar o controlar los accesos y usos de los recursos.

Brinda un apoyo en el ahorro de tiempo para realizar las actividades de los usuarios, ya que los limita a realizar cambios no autorizados por la dependencia la cual puede generar pérdida de horas de trabajo, pérdida de información, retraso en las

actividades diarias, con un esquema de dominio se garantiza la estabilidad de los sistemas internos de la dependencia.

El dominio permite que todos los usuarios se puedan crear, eliminar, bloquear, cambiar y esto se actualice en todos los equipos del dominio lo cual ayuda al administrador a tener el control de los permisos y accesos. Es decir, permite la administración centralizada de usuarios.

Los usuarios se pueden restringir para que únicamente tengan acceso al uso del equipo y a la hora de intentar realizar la instalación de una aplicación, una configuración del sistema, necesite la autorización del administrador, brindando a los administradores de red, mejor control y estabilidad.

Los equipos al pertenecer a un dominio se puede controlar la seguridad de las carpetas y unidades de red compartidas, permitiendo y denegando accesos por usuarios o grupos de usuarios, por ejemplo, se pueden crear unidades de red por departamento y solo los miembros de cada departamento pueden ver la información y no pueden ingresar a otras carpetas de otros departamentos.

Como era de esperarse, se presentaron en varios grupos de usuarios, la tan conocida frase, "*resistencia al cambio*". Esta aparece cuando un trabajador, departamento o empresa en general debe modificar sus rutinas o hábitos, estos últimos pueden ser buenos o malos, pero el miedo, la comodidad o la dificultad de hacerlo les bloquea o paraliza, causándoles esta resistencia al cambio. Y es que se esperaba dado que el nuevo esquema los limitaría en muchas cosas que estaban acostumbrados a hacer o llevar a cabo de una manera normal para ellos. La resistencia al cambio organizacional se define como la actitud que manifiestan los trabajadores cuando **se introducen cambios metodológicos y de procesos** que conllevan modificaciones en rutinas y/o hábitos de trabajo.

La formación recibida en la Facultad de Ingeniería fue fundamental para ponerla en práctica en la vida laboral. Las principales características y habilidades adquiridas por un ingeniero en computación a su paso por la Facultad, tales como técnicas de programación, bases de datos, redes, sistemas operativos, entre otras. Así como la capacidad para resolver problemas, desarrollar un pensamiento crítico, habilidades de comunicación y trabajo en grupo, fueron enriquecidas en el mismo desarrollo profesional y puestas en práctica con la participación en distintos proyectos. Todas estas características fueron aplicadas en los tres proyectos aquí expuestos. Gracias a los cuales, y a actualización mediante cursos, tanto en la Facultad como en el ámbito profesional, dichas habilidades y capacidades han sido altamente enriquecidas y robustecidas a lo largo de mi trayectoria profesional.

Recomendaciones

Aunque el dominio implementado con Windows Server 2019 funciona muy bien, incluso superando las expectativas, sería muy bueno actualizar y migrar a la versión de Windows Server 2022 que es la versión más nueva. Sólo sería cuestión de hacer un análisis de costeo para ver todo lo relacionado con licencias del software.

En un dominio con Windows Server, es muy recomendable tener al menos dos controladores de dominio para tener redundancia y, por ende, disponibilidad de los servicios, ya que si cualquiera de los dos falla, el que queda seguiría brindando todos los servicios y administrando los recursos de la red hasta que el segundo controlador volviera a estar en servicio. Por tanto, no estaría nada mal, de que se agregara un tercer controlador de dominio con la finalidad de redundancia y balanceo de cargas de trabajo y flujo de información en la red. Las buenas prácticas indican que como mínimo, se debería contar con dos controladores en un dominio.

Definiciones

Active directory: Directorio Activo (AD) 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.

AD DS: Active Directory Domain Services proporciona los métodos para almacenar datos de directorio y poner dichos datos a disposición de los usuarios y administradores de la red.

AD LDS = Active Directory Lightweight Domain Services = Servicios de dominio ligeros de Active Directory. Ofrece muchas de las funcionalidades del servidor AD, pero no exige la implementación de dominios ni de controladores de dominio.

Borland: Borland Software Corporation (anteriormente Borland International, Inc.) es una compañía de software, ubicada en Austin, Texas, Estados Unidos.

Broadcast: Proceso de transmisión de información a varios receptores diferentes al mismo tiempo. La difusión amplia, difusión ancha o broadcast, es la transmisión de datos que serán recibidos por todos los dispositivos en una red. Envía información a todos los dispositivos que se encuentren conectados en la misma red.

Bugs informáticos: Los bugs informáticos son errores o fallas de un programa o sistema que produce resultados inesperados, es decir, que trabaja de una forma para la que no estaba diseñado originalmente.

Clipper: Es un lenguaje de programación procedural e imperativo creado en 1985 por Nantucket Corporation y vendido posteriormente a Computer Associates, la que lo comercializó como CA-Clipper.

Cloudflare, Inc. es una empresa estadounidense que ofrece servicios de red de entrega de contenido, ciberseguridad en la nube, mitigación de DDoS y servicios de

registro de dominio acreditados por ICANN. La sede de Cloudflare se encuentra en San Francisco, California.

Conexión IAS: El Servicio de autenticación de Internet o IAS (en inglés Internet Authentication Service) es un componente del sistema operativo Windows Server que proporciona autenticaciones de usuario, autorizaciones, contabilidad y auditoría.

Conexión RDS: Conexiones de Servicios de Escritorio Remoto es un componente del sistema operativo Windows Server que proporciona conexiones remotas entre dispositivos con el sistema operativo Windows.

Conexión RRAS: El servicio de enrutamiento y acceso remoto (RRAS) es un conjunto de servicios de red de la familia Windows Server que permite a un servidor realizar los servicios de un enrutador adicional y funciones de conectividad TCP con ayuda de redes privadas virtuales (VPN) o conexiones de acceso telefónico.

Conexión SMB: Acrónimo de Server Message Block, es el método que se utiliza en funciones de red en Windows, así como el protocolo Samba en los Macs y Unix.

Controlador de dominio: Los controladores de dominio son servidores de Windows que contienen la base de datos de Active Directory (AD) y ejecutan funciones relacionadas con AD, como la autenticación y la autorización. Un controlador de dominio es cualquier servidor Windows Server que cuente con la función de controlador de dominio instalada.

dBASE: Fue el primer sistema de gestión de base de datos usado ampliamente para microcomputadoras. La gran ventaja de este sistema era la de permitir buscar un registro en una base de datos por una clave en lugar de hacerlo de manera secuencial o directa, como ocurría en lenguajes de programación como BASIC.

DNS: Sistema de nombres de dominio. Permite a los usuarios conectarse a sitios web usando nombres de dominio en lugar de direcciones IP.

Dirección IP: Es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa “protocolo de Internet”, que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.

Discos NAS: Los sistemas NAS combinan hardware y software con protocolos (o reglas) que permiten compartir archivos en la red. Si se siguen estos protocolos, cualquier computadora puede acceder sin problemas a los archivos del dispositivo NAS como si los archivos estuvieran almacenados en la propia computadora.

DMZ red: Zona desmilitarizada (demilitarized zone, DMZ) es una red perimetral que protege la red de área local (local-area network, LAN) interna contra el tráfico no confiable. El objetivo final de una DMZ es permitir que una organización acceda a redes no confiables, como Internet, a la vez que garantiza que su red privada o LAN permanecen seguras. En la DMZ, las organizaciones normalmente almacenan servicios y recursos externos, así como servidores para el sistema de nombres de dominio (Domain Name System, DNS), el protocolo de transferencia de archivos (File Transfer Protocol, FTP), correo, proxy, protocolo de voz sobre Internet (Voice over Internet Protocol, VoIP) y servidores web.

Dominio: En el contexto de una red informática, un dominio se refiere a un conjunto de servidores de red y otros equipos interconectados, que comparten una misma información de seguridad y cuentas de usuario, en las que uno o varios de ellos asumen la responsabilidad de administrar diversos aspectos de la red.

DSRM: Modo de restauración de servicios de directorio. Es un modo para reparar o recuperar Active Directory Domain Services (AD DS).

Firmware: Se define como un tipo de software embebido en la memoria de lectura de un dispositivo que se encarga de proporcionar las instrucciones sobre el comportamiento del dispositivo y suele activar las funciones básicas del mismo.

FQDN = Fully Qualified Domain Name. Se refiere a la dirección completa y única necesaria para tener presencia en Internet. Está compuesta por el nombre de host

y el de dominio y se utiliza para localizar hosts específicos en Internet y acceder a ellos mediante la resolución de nombres.

FreeBSD: Es un sistema operativo libre y de código abierto de tipo Unix que descende de la Berkeley Software Distribution, basada en Research Unix. La primera versión de FreeBSD se publicó en 1993.

GUID = El identificador único global, en inglés: globally unique identifier es un número pseudoaleatorio empleado en aplicaciones de software.

Hub: Dispositivo que conecta varios aparatos entre sí y permite que se comuniquen entre ellos.

ISP: Proveedor de servicios de internet (ISP, por las siglas de Internet Service Provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como ADSL, cablemódem, GSM, dial-up, fibra óptica, satélite, streaming, etc.

Latencia mide el retraso de un sistema. La latencia de red es el tiempo que tardan los datos en viajar de un punto a otro a través de una red. Una red con una latencia alta tendrá tiempos de respuesta más lentos, mientras que una red con una latencia baja tendrá tiempos de respuesta más rápidos.

LDAP = El protocolo ligero de acceso a directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP) hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

NAS = Un sistema NAS consiste en un dispositivo de almacenamiento de alta capacidad conectado a una red que permite a los usuarios y clientes autorizados almacenar y recuperar datos en una ubicación centralizada.

NETBIOS: Nombre de NETBIOS: Nombre de dominio que consiste en una dirección de 16 bytes para la identificación en la red de área local.

PCI: Peripheral Component Interconnect (Interconexión de componentes periféricos) o PCI es la forma más común de conectar tarjetas controladoras adicionales a la placa base de un ordenador.

PfSense: Es un sistema operativo especializado de software libre, diseñado para montar servicios de cortafuegos y seguridad del más alto nivel para tu empresa basado en FreeBSD.

QoS: (Quality of Service) Conjunto de requisitos de servicio que la red debe cumplir para asegurar un nivel de servicio adecuado para la transmisión de los datos.

RAID: Un RAID es un grupo de discos físicos independientes que proporciona un alto rendimiento al aumentar la cantidad de unidades utilizadas para guardar y acceder a los datos. Un subsistema de disco RAID mejora el rendimiento de E/S y la disponibilidad de datos.

Spyware: Es un tipo de software que se instala en el ordenador sin que el usuario tenga constancia de ello. Suele venir oculto junto a otros programas que se instalan de manera consciente, lo que lo hace muy difícil de detectar. Una vez en el ordenador, recopila información para enviarla a terceros.

SSID: Un SSID (identificador de red SSID) es el nombre público de una red de área local inalámbrica (WLAN) que sirve para diferenciarla de otras redes inalámbricas en la zona.

STP (Shielded Twisted Pair) Cable par trenzado blindado.

UEFI: Es el primer programa que se ejecuta cuando iniciamos nuestro PC, teniendo 3 fines: verificar el hardware conectado a la placa, activar los componentes y vincularlos al sistema operativo. Sus siglas se refieren a Unified Extensible Output System, que no deja de significar sistema de salida extensible unificado.

Telemática: Es la combinación de la informática y de la tecnología de la comunicación para el envío y la recepción de datos.

Topología de red: Es la forma en que están instalados, distribuidos e interconectados todos los elementos que conforman la red. El buen funcionamiento de una red informática, dependen en gran parte de su topología de red.

Turbo Pascal lenguaje de programación: Se introdujo en los años 70´s con un impresionante éxito. Fue el lenguaje de referencia para enseñar en las universidades. Lenguaje estructurado diseñado para promover un método disciplinado y elegante a la hora de programar. Con su uso se lograban desarrollar programas bien organizados, escritos con claridad y relativamente libre de errores. Orientado para cualquier tipo de computadora.

UTP (Unshielded twisted pair) Cable par trenzado no blindado.

WiFi: Es una contracción del término en inglés Wireless Fidelity (Wi-Fi o fidelidad inalámbrica), es una tecnología de redes inalámbricas que permite a los dispositivos electrónicos conectarse entre sí de manera fluida a una red mediante frecuencias de radio.

Referencias

- Universidad Internacional de la Rioja, 04/01/2022

Topología de red: Qué es y que tipos hay.

<https://ecuador.unir.net/actualidad-unir/topologia-red/>

- Juan Gómez, 12/09/2022

Topologías de red: ¡Descúbrelas!

<https://www.tokioschool.com/noticias/topologias-red/>

- Ikusi Velatia, 2024

Red informática: Todo lo que necesita saber para su empresa.

<https://www.ikusi.com/mx/blog/red-informatica-todo-lo-que-necesita-saber-para-su-empresa/>

- Black Box Explains, 2024

Diferencia entre CAT5e y CAT6

<https://www.blackbox.com.mx/mx-mx/page/46780/Recursos/Technical/black-box-explica/Copper-Cable/Categorias-5e-y-6#:~:text=Los%20cables%20CAT6%20han%20sido,y%20otra%20de%204%20carriles.>

- Thorsman by thorsmex group, 2023

¿Qué es un rack de comunicaciones?

<https://thorsmex.mx/blog/que-es-un-rack-de-comunicaciones/>

-
- Revista Seguridad 360, 03/04/2023

Desentrañando los secretos de los site de comunicaciones: Características, usos y normas

<https://revistaseguridad360.com/noticias/site-de-comunicaciones/>

- Diana Hwang, Abril 2021

Red de área local o LAN

<https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN#:~:text=Una%20red%20de%20%C3%A1rea%20local,de%20un%20%C3%A1rea%20geogr%C3%A1fica%20espec%C3%ADfica.>

- Imagar Solutions Company, Agosto 4 2022

Red LAN, qué es y cómo protegerla

<https://www.imagar.com/blog-desarrollo-web/red-lan-que-es-y-como-protegerla/>

- Christian José, Octubre 15 2021

Grupo de trabajo y dominio, ¿Qué son?

<https://informaticaconangel.com/redes/grupo-de-trabajo-y-dominio/>

- Solvetic Sistema, Septiembre 02 2021

Diferencias entre grupo de trabajo y dominio ¿Cuál elijo?

<https://www.solvetic.com/tutoriales/article/1465-diferencias-entre-grupo-de-trabajo-y-dominio-cual-elijo/>

- Imagar Solutions Company, Julio 27 2021

Ventajas y desventajas de Windows Server

<https://www.imagar.com/blog-desarrollo-web/ventajas-y-desventajas-de-windows-server/>

-
- Axarnet, Diciembre 17 2019

Windows Server: qué es y características

<https://axarnet.es/blog/windows-server#funciones>

- microsoft.com, 30/08/2023

Comparación de las ediciones Standard y DataCenter de Windows Server 2019

<https://learn.microsoft.com/es-es/windows-server/get-started/editions-comparison-windows-server-2019?tabs=full-comparison>

- DELL Technologies, Diciembre 08 2023

Comprensión de los tipos de discos duros, RAID y controladoras RAID en servidores DELL PowerEdge y chasis Blade

<https://www.dell.com/support/kbdoc/es-ec/000137374/descripci%C3%B3n-de-los-tipos-de-disco-duro-raid-y-controladoras-raid-en-los-servidores-dell-poweredge-y-chasis-del-servidor-blade#:~:text=Un%20RAID%20es%20un%20grupo,y%20la%20disponibilidad%20de%20datos.>

- netebu.com, Septiembre 16 2020

Qué es una DMZ y cómo puede ayudar a proteger tu empresa

<https://netebu.com/announcements/86/Que-es-una-DMZ-y-como-te-puede-ayudar-a-proteger-tu-empresa.html>

- Juan Ignacio Oller Aznar, 25/10/2022

Que son y para que sirven las GPO

<https://jotelulu.com/blog/que-son-y-para-que-sirven-las-gpo/#:~:text=La%20mayor%20ventaja%20que%20nos,ahorro%20de%20tiempo%20de%20administraci%C3%B3n.>

- Julio Lorenzo, 03/03/2022

¿Qué es un Access Point?

[https://www.compucentro.com.mx/noticias-ti/que-es-un-access-point-redes-y-seguridad#:~:text=Entendiendo%20los%20Access%20Point&text=Tambi%C3%A9n%20conocidos%20como%20WAP%20\(Wireless,interconectarse%20con%20otra%20red%20externa.](https://www.compucentro.com.mx/noticias-ti/que-es-un-access-point-redes-y-seguridad#:~:text=Entendiendo%20los%20Access%20Point&text=Tambi%C3%A9n%20conocidos%20como%20WAP%20(Wireless,interconectarse%20con%20otra%20red%20externa.)