UNIVERSITAT DE BARCELONA

Treball final de grau

GRAU D'ENGINYERIA INFORMÀTICA

Facultat de Matemàtiques i Informàtica
Universitat de Barcelona

Implementación de la arquitectura segura de red de una empresa

Autor: Juan Cámara

Director: Raúl Roca
Realitzat a: Departamento de Matemátiques e Informática

Barcelona, 21 de junio de 2020

Abstract

A transport company, which currently works with an obsolete IT infrastructure, seeks to open up to the international market. In order to compete with the other companies in the sector, they plan to carry out a digital transformation project for all their infrastructure.

Because more offices are being opened and new employees are recruited, an analysis of the current state of the company must be made and a design that assembles all the necessities should be also created. Besides that, a system that is easily scalable, fast and secure for the entire organization must be implemented and prioritized.

At the end, an infrastructure that meets their requirements has been designed and a small simulation has been carried out to show how such implementation would be done.

Resumen

Una empresa de transporte que actualmente trabaja con una infraestructura IT obsoleta busca abrirse al mercado internacional. Para poder competir con las demás empresas del sector, plantean hacer un proyecto de transformación digital de toda su infraestructura.

Debido a la apertura de nuevas oficinas y contratación de nuevo personal, se debe hacer un análisis de la situación actual de la empresa y crear un diseño que cumpla con sus nuevas necesidades. Aparte de esto, se debe implementar y priorizar un sistema que sea fácilmente escalable, rápido y seguro para toda la organización.

Finalmente se ha diseñado una infraestructura que se ajusta a sus requisitos y para ello se ha realizado una pequeña simulación donde se demuestra como se haría dicha implementación.

Agradecimientos

“A mis padres, a mi hermano y a toda mi familia, gracias a quienes soy quien soy y hacia quienes solo puedo expresar mi más sincero agradecimiento por apoyarme en todo momento durante toda mi etapa académica”

“A mis amigos y compañeros de la universidad, por ser mi principal fuente de energía para afrontar todos esos obstáculos que me han ido apareciendo durante el día a día”

“A mis amigos desde el colegio, por ser mi motivación y mis referentes en la vida”

“A mi profesor de Ciberseguridad y tutor de TFG, por su acompañamiento, su energía y su apoyo durante todo este último curso académico”

“A mi jefe, por ser el mejor compañero de trabajo que he podido tener durante estos últimos años y ser mi principal referente en el mundo de la informática”

Índice general

Introducción

Contexto

Internet se podría decir que es lo mejor y al mismo tiempo, lo peor que le ha sucedido al ser humano. Actualmente, cada vez son más los dispositivos que requieren de conexión a internet para hacer más sencilla la vida de las personas. Hace años era impensable que desde un dispositivo tan pequeño como son los actuales teléfonos móviles o smartphones se pudiera utilizar como por ejemplo de GPS. Hoy en día el smartphone es considerado un ordenador pequeño portátil desde el que puedes enviar mensajes hasta controlar toda la instalación eléctrica de un domicilio. Todo esto es posible gracias al boom tecnológico de los últimos años más bien conocido como Internet of Things (IoT).

Lamentablemente, este fenómeno del IoT también ha afectado a que aumente el número de ataques cibernéticos del día a día. Aunque esto suponga un problema de cara a los usuarios que utilicen esta clase de dispositivos para almacenar toda su información, el verdadero sector crítico son las empresas.

Normalmente las compañías que llevan abiertas varios años siguen utilizando equipos antiguos. Esto es debido a que una gran parte del software que actualmente utilizan solo está soportado en versiones antiguas de operativo.

Como actualizar toda la infraestructura que utilizan, normalmente supone una inversión muy grande, estas deciden la mayoría de las veces seguir trabajando con el equipo actual. Ignorando así, el peligro que tiene utilizar un software y un hardware obsoleto, refiriéndonos en términos tanto de rendimiento como de seguridad.

Motivación

Los sistemas de la información y el mundo de la seguridad han sido la principal motivación para llevar a cabo esta investigación.

El hecho de poder realizar un proyecto enfocado en la transformación digital de toda una organización, se ha visto como una oportunidad para investigar y aprender nuevas nociones sobre la funcionalidad de los sistemas IT a nivel empresarial y profundizar en los mecanismos de seguridad que estos utilizan.

Gracias a haber tenido contacto con diversas infraestructuras IT de distintas organizaciones, se ha podido comprender la metodología de trabajo de los empleados y qué elementos son necesarios para implementar un diseño seguro.

Objectivo principal

El objetivo principal de este trabajo es realizar el análisis, el diseño, la implementación y una pequeña demostración sobre la transformación digital de una empresa, tanto desde el punto de vista de la seguridad como a nivel de funcionalidad.

Objectivos específicos

El objetivo principal es desglosa en los siguientes objetivos específicos:

- **Estudiar el funcionamiento de una organización:** Para poder diseñar la infraestructura de una organización, se deberá conocer que tipo de hardware utiliza, que protocolos de trabajo existen y si existe algún tipo de seguridad en una empresa en función del volumen de empleados.

- **Diseñar una infraestructura:** Se deberá diseñar todo lo que se conoce como una infraestructura IT. Desde definir el tipo de conexión que se va a establecer hasta el tipo de hardware que se va a utilizar.

- **Implementar el diseño virtualizado:** Se deberá conocer a fondo el funcionamiento de la red y crear un dominio para la organización. Además, se deberá crear una plataforma digital corporativa.

Planificación

La planificación del proyecto se puede dividir en 3 grandes bloques de tareas:

Para estudiar el funcionamiento de una organización, se dedicará todo el mes de Enero, ya que para crear un buen diseño se debe analizar las infraestructuras de empresas distintas para ver a nivel de infraestructura que elementos y metodologías tienen en común y en que difieren.

Plantear un diseño seguro llevará todo el mes de Febrero y la mitad del mes de Marzo. Un diseño es la base de toda infraestructura, por esa razón, plantear un buen diseño evitará corregir problemas durante la implementación. Además, se deberá hacer un estudio de mercado sobre el material que se requerirá para llevarlo a cabo.

Finalmente, la parte de la simulación virtualizada es la que llevará más tiempo, desde mediados de Marzo hasta finales de Mayo. Hará falta ver el rendimiento de las VM en función de la versión de SO, diseñar e implementar las comunicaciones entre ellas y crear un dominio para la organización.

Tareas	Fecha inicio	Duración	Fecha final
Estructuración del proyecto	enero	7	15-ene
Planteamiento de un proyecto real	enero	4	20-ene
Búsqueda de información sobre diseño seguro	enero	10	31-ene
Diseño de la infraestructura	febrero	14	15-feb
Estudio de mercado sobre el hardware	febrero	14	1-mar
Documentarse sobre los diferentes tipos de servidores	marzo	14	16-mar
Planificar la parte práctica	marzo	21	7-abr
Autoformación en Windows Server 2012 R2	abril	21	29-abr
Autoformación en GNS3	abril	14	8-may
Creación de una plataforma digital	mayo	5	14-may
Configurar el dominio	mayo	20	31-may

Figura 1: Planificación del proyecto.

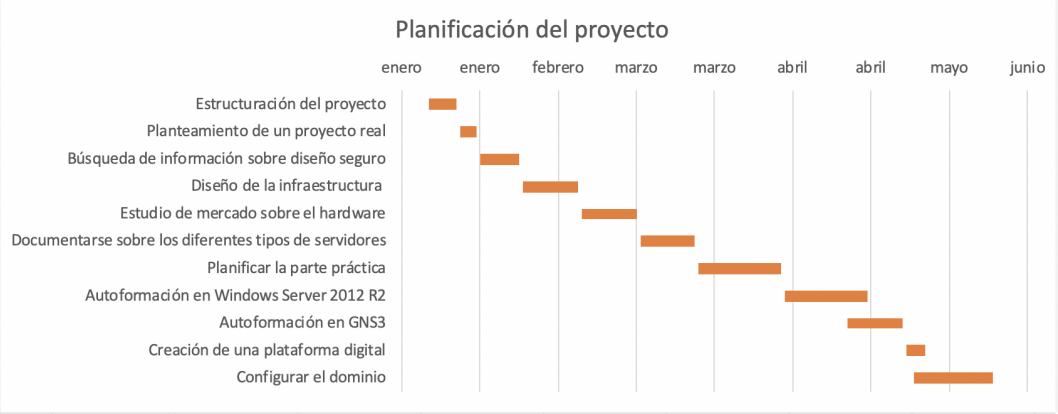

Figura 2: Diagrama de Gantt.

Costes del proyecto

A continuación se adjunta los presupuestos referidos al material que se ha utilizado para el diseño y el coste de implementar las distintas tareas:

Material	Especificaciones	nº unidades	Precio u/€	Total €
Firewall Fortigate Serie 500	- Puertos GE, GE SFP y 10 GE SFP - Incorpora servicios de Firewall, VPN, IPS	3	6.150,00 €	18.450,00 €
UniFi Switch PRO 48 PoE	- 48 ports GE PoE+ - 10 puertos GE SFP+	7	970,00 €	6.790,00 €
UniFi AC LR	- Doble banda simultanea de 5GHz y 2,4GHz - 183 metros de alcance	10	121,00 €	1.210,00 €
Servidor HPE ProLiant DL380 Gen10	- 2 Discos SSD de 480 GB - 128 GB de RAM - 2 Procesadores Intel Xeon (16 núcleos) - Tarjeta de fibra 40 Gbps	2	10.500,00 €	21.000,00 €
Servidor HPE ProLiant DL360 Gen10	- 2 Discos SSD de 480 GB - 32 GB de RAM - 1 procesador Intel Xeon (8 núcleos) - tarjeta de fibra 40 Gbps	3	3.800,00 €	11.400,00 €
Cabina de discos HP MSA 2040	- 24 bahías	1	5.950,00 €	5.950,00 €
	- Discos SSD 480 GB	24	850,00 €	20.400,00 €
Librería robotizada de cintas HPE StoreEver MSL3040	- Capacidad para 40 cintas	1	2.700,00 €	2.700,00 €
	- Cintas de 30 TB	4	150,00 €	600,00 €
Xerox VersaLink C7000	- A3 y A4 - Cola de retención de impresión - 35 ppm	10	841,00 €	8.410,00 €
Microsoft Open Value	- Activaciones ilimitadas para los últimos SOs	1	30.000,00 €	30.000,00 €
Equipo terminal	- Procesador AMD Ryzen 5 2600 3.4 GHz - 8 GB de RAM 2400 DDR4 - Disco SSD 250GB SATA	200	500,00 €	100.000,00 €
Armario Rack sede principal	- 800x1200x2100 mm	1	1.033,82 €	1033,82
Armario Rack sede secundaria	- 600x800x1600 mm	2	368,99 €	737,98 €
SAI APC Smart-UPS	- 10.000V	3	8.775,00 €	26.325,00 €
Presupuesto			Total:	255.006,80 €

Figura 3: Presupuesto del material.

Tareas	Total €
Plantear el diseño definitivo	5.000,00 €
Instalación, configuración y parametrización del dominio - Instalación controladores de dominio - Creación del dominio - Asignación de los diferentes roles	8.000,00 €
Instalación y configuración clúster de servidores de ficheros - Instalación servidores de ficheros - Agregarlos al dominio - Crear clúster - Montar la cabina de discos - Configurar la unidad compartida	15.000,00 €
Creación de los usuarios, grupos y GPOs del dominio	15.000,00 €
Instalación y configuración del servidor de copias de seguridad	5.000,00 €
Instalacion y configuración de switches y Firewalls	6.000,00 €
Configuración del entorno de trabajo de los usuarios - Instalación de la ISO corporativa - Agregar los equipos al dominio	40.000,00 €
Presupuesto	94.000,00 €

Figura 4: Presupuesto de la implementación.

Los gastos contemplados suman un presupuesto total de 349.005,80 €. En todo proyecto existe elementos que no se contemplan en el presupuesto, como, por ejemplo: los metros de cable de red necesarios. Esto es debido a que suelen ser un factor difícil de calcular una aproximación y por lo tanto varían mucho del presupuesto planteado al presupuesto final.

Organización del documento

La estructura de esta memoria se desglosa en los siguientes capítulos:

- **Introducción:** El capítulo de la Introducción tiene el objetivo de contextualizar el proyecto y explicar cuales van a ser los objetivos de este.
- **Análisis:** El capítulo de Análisis definirá la situación actual de la empresa y sus objetivos.
- **Diseño e Implementación:** En el capítulo de Diseño e Implementación se describe los patrones a seguir para crear un diseño seguro y explica como se implementa la transformación digital de una empresa.
- **Simulación de la infraestructura mediante servicios de virtualización** Este capítulo pretende demostrar de forma práctica como se implementa una nueva infraestructura en una empresa.

- **Conclusiones y trabajo futuro:** En este se detallan las conclusiones y una serie de mejoras que se implantarían en el proyecto de cara al futuro.
- **Anexos:** En este último capítulo se explican más a fondo terminos que se han ido mencionando a lo largo del proyecto.
- **Apéndice: Manual Técnico:** En el Manual Técnico se describe los elementos necesarios para ejecutar el proyecto y los pasos a seguir para el funcionamiento de este.

Capítulo 1

Análisis de la empresa

1.1. Introducción

Una empresa dedicada al sector del transporte consta con alrededor de 50 vehículos para el envío y recogida de paquetes y una única oficina situada en el distrito 22@ de Barcelona. Actualmente se encuentran con un total de 150 empleados en la plantilla, de los cuales 50 de estos trabajadores son los encargados del trasporte y el resto se encuentran divididos entre cinco departamentos en la oficina de Barcelona. Entre dichos departamentos se encuentran:

- **Departamento de administración:** el encargado de administrar y gestionar los bienes de la empresa. Además, se ocupa de gestionar los diferentes tipos de documentación.

- **Departamento de gerencia:** el encargado de toma de decisiones en la empresa.

- **Departamento de recursos humanos:** el encargado de las tareas referentes al personal de la empresa.

- **Departamento de desarrolladores:** el encargado de crear y mantener la aplicación web del transporte de paquetes, la base de datos de los envíos, etc.

- **Departamento de SI/TI:** el encargado de solucionar las averías en los equipos de la empresa y llevar el mantenimiento de la red.

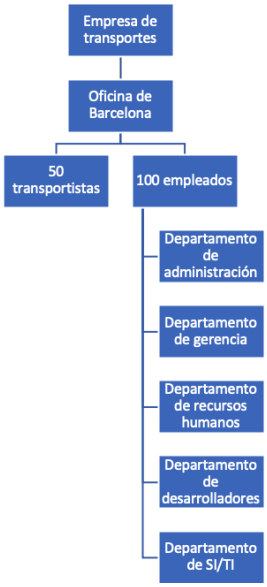

Figura 1.1: Plantilla actual.

A raíz del crecimiento lineal del número de empleados durante estos últimos años y debido a las dimensiones del local actual, pretenden expandirse y así abrirse al mercado europeo. Por esa razón, pretenden abrir una nueva sucursal tanto en Madrid como en Francia.

Debido a dar el salto a un mercado mucho más amplio, se encuentran que no pueden competir a nivel tecnológico contra las demás empresas del sector, ya que la manera actual de trabajo no es la más optima ni la más segura. Se encuentran en un punto donde el sistema actual se ha quedado obsoleto y no es el más adecuado para el volumen de personal que tienen.

Por ello, para poder optimizar su sistema de gestión y competir con las empresas de nivel internacional, buscan diseñar un plan de transformación digital para su infraestructura tecnológica IT actual.

1.2. Equipo utilizado

Todos los dispositivos que se utilizan actualmente llevan instaladas versiones de Sistemas Operativos (SO) que han llegado al final de su vida útil, por lo que no van a poder actualizarse y así parchear las nuevas vulnerabilidades que vayan apareciendo.

A la hora de trabajar, cada usuario tiene todos los documentos necesarios guardados en su ordenador a nivel local y sin tener un dominio implementado. Para la compartición de documentos, utilizan una Network Attached Storage (NAS) doméstica con capacidad suficiente como para utilizarse de servidor de ficheros. Además, cuentan con otra NAS para hacer copias de seguridad o *backup* del servidor de ficheros.

Al realizarse las copias de seguridad solo del servidor de ficheros y no a nivel de equipo local, si por alguna razón algún ordenador dejase de funcionar, todos los documentos no guardados en el servidor se perderían, además de tener que configurar el nuevo equipo de 0 a mano.

A nivel de comunicaciones de red, actualmente utilizan *switches* limitados a 100 Mbps por puerto, lo que hace que la conexión a internet sea muy lenta. El cableado de red que se utiliza esta formado por una mezcla de cables UTP Cat 5E y Cat 6.

1.3. Plan de futuro

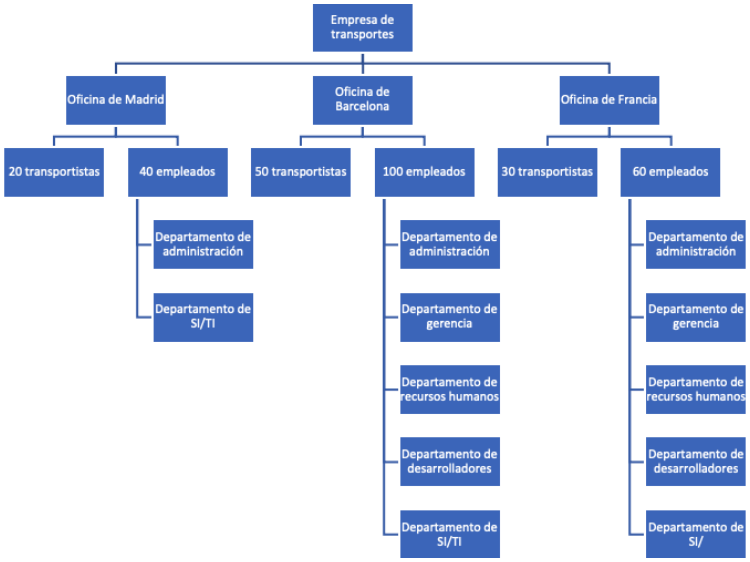

Figura 1.2: Futura plantilla.

Tienen la idea de crecer hasta ser un total de 200 trabajadores en oficinas, dejando de lado al número de transportistas. De estos 200 trabajadores, 100 de ellos pertenecerían a la sucursal de Barcelona, 40 a Madrid y los 60 restantes a Francia.

Por ello, la empresa busca una solución de transformación digital para todas las oficinas. Donde se pretende unificar las infraestructuras de las 3 sucursales, con el fin de que los empleados de todas ellas puedan acceder y compartir información de forma rápida y segura.

Capítulo 2

Disseño e Implementación

2.1. Esquema de una infraestructura segura

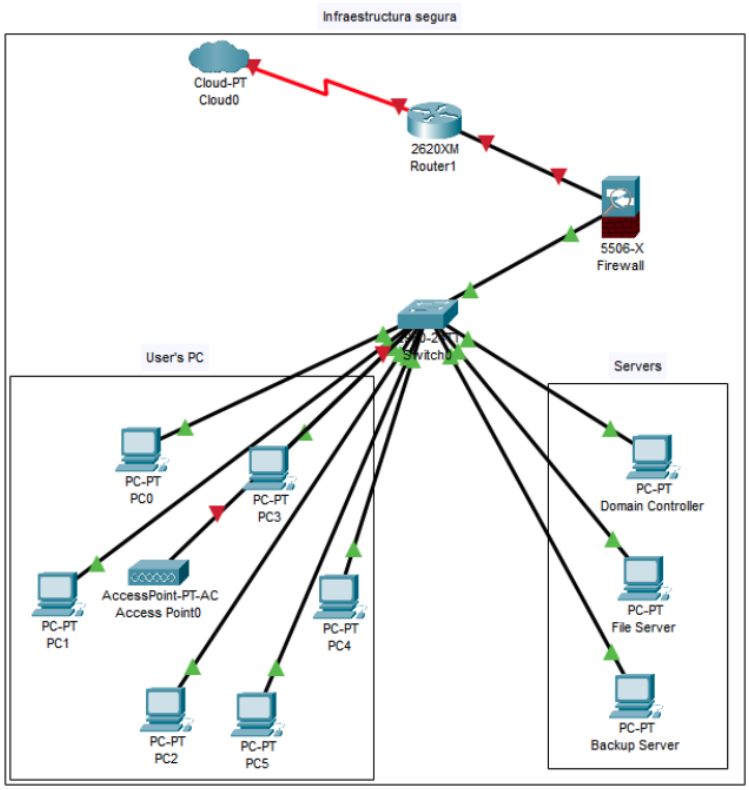

Figura 2.1: Infraestructura básica basada en un diseño seguro.

En la figura 2.1 se muestra un diseño creado con la herramienta de “Cisco Packet Tracer”, nombrando los diferentes elementos que debe tener toda infraestructura a nivel empresarial para así, trabajar de manera una forma menos insergura. Esto es debido a que fallos de seguridad van a existir siempre y por lo tanto es importante dar una solución que mitigue el mayor número de vulnerabilidades posibles y dismnuya el impacto que produciría la explotación de alguna de ellas.

Cuando se habla de que elementos debe contener el sistema IT de una empresa para así aumentar su protección, se refiere a dispositivos como el cortafuegos o *Firewall*, un *Intrusion Prevention System* (IPS), un *Intrusion Detection System* (IDS) y/o Honeypots. Aunque este tipo de hardware no pueda mitigar el 100 % de los agujeros de seguridad de una organización, hace que la seguridad de esta aumente bastante.[27]

Con esto se quiere dar a entender que tener instalado un *firewall* no evita el 100 % de las intrusiones, ya que existen mecanismos para saltar los controles de seguridad y así tener acceso a la información que navega por la Red de área local (LAN).

Cuando se habla de los diferentes equipos que pueden formar la organización, siempre se debe tener en cuenta el número de equipos terminales que hay activos, el número de dispositivos móviles o tabletas que utilicen los usuarios, que métodos de conexión utilizan estos equipos y si existe algún dispositivo que se encargue de dicha conexión. Esto son datos imprescindibles en el diseño para hacer una aproximación de los elementos que hay que proteger y que medidas de seguridad se deben tomar para el uso de ellos.

Como último punto, la gran mayoría de los activos de una empresa residen en los servidores. Suelen ser la fuente de servicios en una empresa. Por esa razón, toda organización debería tener un mínimo de 3 tipos de servidores: Un controlador de dominio o *Domain Controller* (DC), un servidor de ficheros o *File Server* (FS) y un servidor de copias de seguridad o *Backup Server* (BKP). Los cuales ninguno de estos debe estar expuesto a internet.

Se aconseja separar los servidores según la tarea que vayan a realizar. Utilizar un servidor dedicado para cada tarea tiene la desventaja de que los gastos son mucho mayores, ya que el número de servidores aumenta, pero la ventaja es que, si uno de estos servidores cae, los servicios restantes pueden seguir utilizándose independientemente.

2.2. Diseño e implementación del proyecto

Para diseñar e implementar cualquier proyecto de transformación digital, se debe tener en cuenta una serie de puntos clave para tomar las decisiones al respecto:

- Cumplir los requisitos mínimos para que el nuevo sistema funcione todo al menos igual que hasta la fecha.
- Conocer el número de usuarios.
- Tener visión de crecimiento futuro, para hacerse una idea del volumen de usuarios que se puede llegar a tener en un futuro y así crear una infraestructura que lo soporte.

- Analizar el método de trabajo actual, para concienciar a los empleados de un buen hábito de trabajo y estudiar la complejidad que les va a suponer la nueva forma de trabajar respecto a la actual.
- Analizar la infraestructura actual, para saber si existe algún tipo de hardware que se pueda reaprovechar.

Un diseño sencillo proporciona organización, permite añadir mejoras a posteriori sin tener que alterar la estructura e incluso facilita la tarea a la hora de solucionar problemas. En un diseño donde cada dispositivo hace única y exclusivamente su función se pueden detectar fallos más fácilmente, como, por ejemplo, si el fallo le ocurre a un único usuario, el problema reside en la configuración del equipo. En cambio, si falla a un colectivo, se debe revisar el problema solamente en el servidor encargado de realizar la tarea, sin tener que afectar al resto de servicios.

Plantear un diseño fácilmente escalable tiene la desventaja de que suele requerir una gran inversión inicial, pero la ventaja de que cualquier tipo de ampliación que se haga a posteriori va a ser muchísimo más barata.

Ejemplo: Un problema muy habitual que ocurre sobretodo en empresas pequeñas, empiezan a ampliar el volumen de trabajo, pero no tienen espacio para almacenarlo, por esa razón necesitan instalar una NAS para almacenar la información. Para el caso que se necesite instalar una cabina con capacidad para 2 TB, existen varias soluciones:

- La solución que escogen muchas de ellas es comprar una NAS pequeña de 2 bahías, ya que es la solución más barata, y hacer *Redundant Array of Independent Disks* (RAID) 1 de 2 TB (2 discos de 2 TB donde uno se replica con el otro, por lo tanto, el volumen final es lo mismo que tener un solo disco). De esta forma cubren sus necesidades, sin embargo, si por lo alguna razón sigue creciendo el volumen de trabajo, la manera para ampliar el espacio es comprando otros 2 discos de más capacidad y sustituyéndolos. Esta es una mala solución ya los discos antiguos no se usan para nada.
- Si se pensara con visión de futuro, la mejor opción sería comprar una NAS más grande, de 4 o 5 bahías, y se agregar solamente 2 discos. De esta manera, aunque sea un gasto inicial mayor ya que la cabina es más grande, en el caso de tener que ampliar el espacio, basta con agregar más discos en esas bahías libres. Optar por esta solución, a largo plazo sale mucho más a cuenta, ya que los discos tienen una capacidad máxima, llegado a ese límite se tendrá que cambiar el sistema entero para poder seguir ampliando. Esta la opción más rentable a largo plazo si se pretende escalar el volumen de trabajo.

Por esa razón, es muy importante configurar las prestaciones de los servidores siempre contando con una visión de crecimiento, ya que, en los proyectos de este tipo, donde se espera ser como mucho 100 usuarios, luego se alcanzan más de los esperados.

Para diseñar y llevar a cabo el proyecto de transformación digital, se ha basado en el diseño de la figura 2.1, ya que es un diseño sencillo, fácilmente escalable y con elementos dedicados cada uno a su propia función.

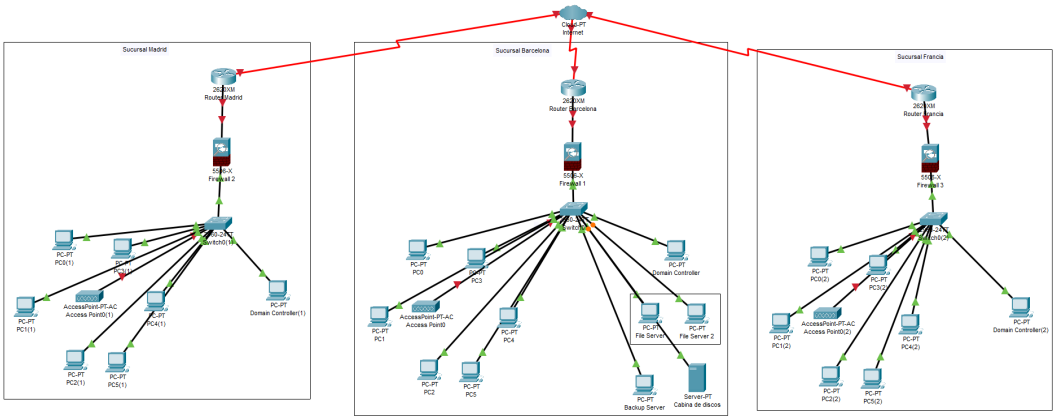

Figura 2.2: Diseño final.

Se ha creado un diseño basado en la centralización de la información, donde se requerirá de una oficina principal, que en este caso es la de Barcelona, y el resto de oficinas secundarias se conectaran a esta para acceder a la información. Crear un diseño de este estilo evita la replicación de la información en cada una de las oficinas. De tal forma que los cambios importantes a nivel de servidores o almacenamiento solo se realicen en un único punto y así, facilitar la implementación en caso de abrir nuevas oficinas. Para abrir una nueva oficina y que los usuarios puedan conectarse a la sede principal, solo es necesario instalar los equipos terminales de los empleados y un controlador de dominio.

Las soluciones más comunes a la hora de diseñar una infraestructura de tal magnitud son plantear un sistema totalmente centralizado o un sistema basado en replicación. Debido a que ambos diseños tienen sus ventajas y desventajas, después de estudiar las necesidades de los usuarios, se ha decidido crear un diseño que implemente características de ambos.

Al crear un diseño donde todos los usuarios se van a conectar al servidor de ficheros de Barcelona, es de vital importancia evitar cuellos de botella, tanto en la parte de conectividad como en la concurrencia de usuarios al acceso de la información. El objetivo es intentar buscar el termino medio entre tener un buen rendimiento y realizar las conexiones de manera segura.

En este proyecto se va a establecer 2 tipos de diseño:

- La sucursal de Barcelona va a ser la sede principal, ya que es la primera oficina que se ha abierto y donde más usuarios van a haber.
- La sucursal de Madrid y Francia, van a tener el mismo perfil tecnológico.

La justificación de que materiales se necesitarán en cada sucursal y porque se han escogido esos en concreto, se desglosará en 3 bloques: un bloque destinado a explicar la parte de redes y comunicaciones, otro bloque destinado a los servidores y por último los equipos finales.

2.3. Comunicaciones LAN y multisede

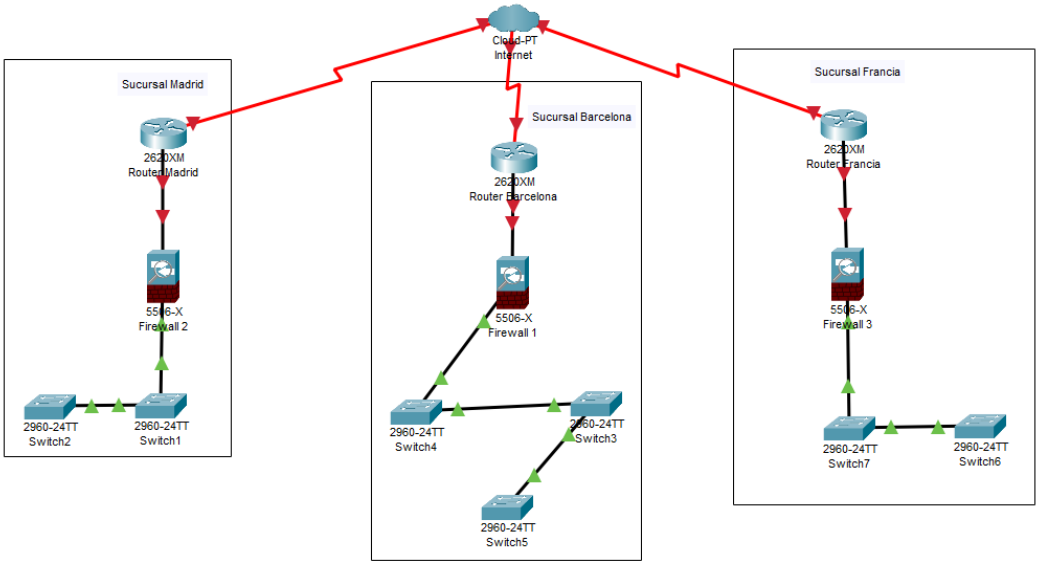

Figura 2.3: Configuración a nivel de red.

Al decidir que la mejor solución para sus necesidades es utilizar un sistema basado en centralizar los servicios en un único lugar, uno de los puntos a tener en cuenta a la hora de diseñar la infraestructura es cómo se van a comunicar las distintas sucursales entre ellas.

Existen varias soluciones de comunicación a nivel geográfico, como por ejemplo la conexión *Frame Relay* [18] [19], una MacroLAN [22] o una conexión **VPN**. Se denomina una conexión a nivel geográfico cuando la distancia entre los 2 puntos es mayor a la que se puede llegar con un cable directo, que en el caso de un cable UTP de red es de un alcance máximo de 100 metros.

Existen muchos servicios de VPN distintos, como por ejemplo OpenVPN y Forticlient. Debido a que la distancia entre las distintas oficinas es de cientos de KM y se prioriza que la transferencia de la información este protegida, se ha decidido que para realizar la conexión entre sucursales se implementará el servicio VPN de Forticlient. Forticlient es el cliente VPN de la empresa Fortinate, uno de los grandes referentes alrededor del mundo en lo que se refiere al tema de los *firewalls* por su fiabilidad y seguridad dentro de las organizaciones.

Otro factor muy importante a la hora diseñar una infraestructura es tener en cuenta los elementos básicos que hagan del sistema uno más robusto, flexible y seguro. Entre ellos se encuentra hardware como los son el **Firewall**, un **IPS**, un **Honeypot**, etc. No olvidar que también existen mecanismos de seguridad a nivel de software, como son los antivirus o sistemas de monitorización de recursos.

El *Firewall* es el elemento básico en cuanto se refiere a la seguridad perimetral de una organización, ya que va a ser el encargado de separar la red interna, los equipos del dominio en este caso, de los equipos fuera de esta red, en este caso internet. Actúan como barrera central o filtro, ya que implementan la función de control de acceso de los servicios y paquetes que se ejecutan tanto en el interior de la red (LAN) como en el exterior de la red (WAN). Por esa razón, la principal función de un *firewall* es evitar ataques del exterior contra los equipos o cualquier tipo de acceso no permitido al interior de nuestra red.

2.3.1. Hardware de conexión WAN

Para el hardware encargado de realizar la función de filtraje de paquetes que circulen por la red y de servidor VPN se ha decidido utilizar un modelo de *firewall* Fortigate Serie 500E en cada sucursal. La ventaja que implementan estos *firewalls* es que a parte de ser muy rápido el intercambio de paquetes gracias a los puertos SFP+ de 10GE, estos implementan muchos servicios dentro de sí mismos además del clásico cortafuegos, como por ejemplo el servicio de VPN, IPS, antivirus y seguridad **antibotnet** contra ataques de **Distributed Denegation of Services** (DDoS).

Se configurará el *firewall* de la sucursal de Barcelona para que realice la función de servidor VPN donde, cada una de las máquinas del dominio fuera de la red interna, se van a conectar a él para acceder al servidor de ficheros y al servidor DNS principal.

Un gran volumen de conexiones simultaneas implica el clásico problema del cuello de botella o problema de concurrencia, donde el servicio puede llegar a ir lento o incluso caer en función del número de usuarios concurrentes. Cuando suceden estos casos significa que se ha instalado un hardware que no es el apropiado. De ahí la elección de los firewalls de Fortinet, que tienen bajo control el problema de la concurrencia, ya que están enfocados para usarse a nivel profesional.

2.3.2. Hardware de conexión LAN

Los problemas de concurrencia no solo pueden aparecer a nivel de comunicación WAN. En cualquier infraestructura IT pueden aparecer problemas de concurrencia en los *switches* a nivel de LAN, en los equipos terminales donde los usuarios van a trabajar y en los servidores donde se ejecutarán los servicios principales.

Para el tema de las redes LAN internas de cada sucursal, se ha optado por coger el modelo de switch UniFi Switch PRO 48 PoE y colocar 2 en cada una de en la sucursales secundarias y 3 en la principal. De esta manera se cubre el número de dispositivos conectados por cable que se calcula que va a haber. Aunque en la oficina de Madrid habrá alrededor de 40 equipos terminales, no hay que olvidarse de dispositivos como las impresoras, los Puntos de acceso o Acces Point (AP), el DC, etc. Por esa razón se ha optado por instalar dos *switches* en vez de solo uno y así evitar problemas por disponibilidad de puertos ethernet. De esta forma también se previene comprar hardware nuevo, aunque en un futuro haya nuevos usuarios en la oficina.

UniFi es una empresa muy reconocida en el tema de conexiones LAN, lo que viene siendo controladoras de dispositivos, puntos de acceso y *switches*. Por esa razón, se ha escogido este modelo de *switch* en concreto ya que, a parte de tener muy controlado el tema de la concurrencia, dispone de 48 entradas Gigabit Ethernet (GE) Power over Ethernet (PoE). A diferencia de otros modelos de *switches*, este gestiona los 48 GE reales. Aunque estas entradas hay que comprarlas como extra, este *switch* admite la instalación de 4 puertos SFP+ de 10 GE , los cuales van a permitir que la comunicación vertical entre dos *switches* sea de entre 20 y 40 GE. Por último, recalcar la importancia de que sea un *switch* configurable PoE y no otro.

La idea es que la señal *wifi* se distribuya por toda la oficina gracias a unos AP también de la marca UniFi. Estos requieren de un cable de red y un inyector que de corriente al dispositivo. Esa es la ventaja de utilizar el *switch* escogido anteriormente, ya que se podrá configurar los puertos que vayan a ir conectados a los AP para que sean PoE y así evitar el uso de los inyectores.

Tener una buena conexión a nivel de *switch* permitirá que los usuarios tanto de la oficina principal como de las oficinas secundarias y usuarios conectados por VPN, tengan más velocidad a la hora de trabajar en el servidor de ficheros. El *firewall* a parte de ejercer la función de filtro de los paquetes que entran y salen del router, tiene conexión directa con el *switch*, por lo que de esta forma se pueda acceder a los servidores desde fuera.

2.3.3. Rangos de red

Para establecer las clases de red que se utilizarán a nivel local se ha decidido que la mejor opción sería configurar redes de tipo C y rangos correlativos. Usar IPs de clase A (10.0.0.0), de clase B (172.0.0.0) o clase C (192.0.0.0) no dejan de ser diferentes estándares enfocados a grandes redes (multinacionales), redes medianas como las de una PYME o redes pequeñas o domésticas. Por mucho que la organización se abra al mercado internacional, si las oficinas van a tener como máximo 100 empleados, con 253 IPs tienen más que suficiente. No se considera una mala praxis utilizar IPs de clase C donde, al ser correlativas, en Barcelona puede establecerse la red 192.168.50.0 y Madrid puede establecerse la red 192.169.51.0.

2.3.4. Conclusiones

Optar por usar el hardware de dos grandes empresas del sector de las telecomunicaciones va a permitir cumplir con uno de los objetivos **CIA** de la ciberseguridad a nivel de conexiones, como es el caso de la **disponibilidad** de la información.[26] El firewall de Fortinet y los *switches* de UniFi asegurarán un acceso fiable y a tiempo a la información.

Gracias a este diseño, se va a poder trabajar lo más rápido posible a través de internet y desde la misma red interna. Además, va a dar estabilidad y seguridad a la conexión en todo momento, ya que pretende ser el objetivo de hacer el diseño de esta forma.

2.4. Servidores

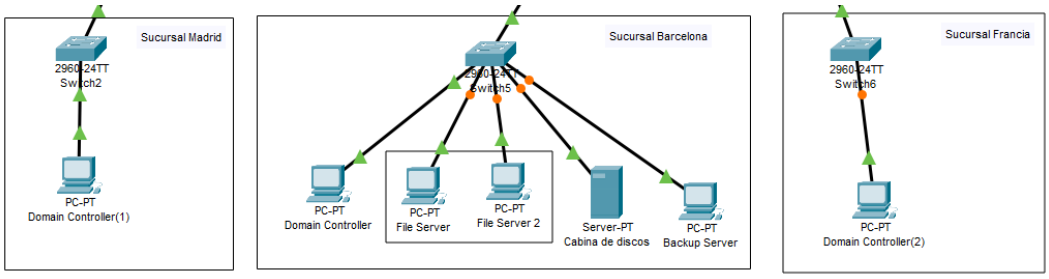

Figura 2.4: Estructura de servidores.

Siguiendo el diseño basado en la centralización de servicios mixtos, el cual comparte características con el diseño basado en la replicación, se puede apreciar que, a pesar de que la mayor parte de los servidores están en la sucursal de Barcelona, se ha agregado un controlador de dominio extra en cada sucursal.

2.4.1. Controlador de dominio

Un servidor que se le asigna el rol de controlador de dominio es el encargado de administrar los diferentes usuarios, grupos y equipos que forman de manera conjunta el dominio de una organización. También se encarga de validar el inicio de sesión de los usuarios que pertenezcan realmente al dominio.

A la hora de configurar un equipo dentro de un dominio, se requiere que el servidor DNS principal de la tarjeta de red del equipo apunte a la IP de este controlador de dominio, ya que cuando a un servidor se le asigna el rol de controlador de dominio, es obligatorio que corra el rol de servidor DNS. Esto es debido a que el servidor DNS será el encargado de resolver las peticiones dentro de un dominio.

Como la principal función de un controlador de dominio es validar los inicios de sesión de los usuarios y además se ha visto que todas las oficinas tienen habilitada una conexión VPN con Barcelona, ¿por qué se ha decidido poner un DC en cada sucursal si con solo tener el DC de Barcelona los usuarios podrían iniciar sesión igualmente?

Tiene sentido ya que, como se ha explicado con el tema de las comunicaciones, la concurrencia de usuarios es un problema muy habitual que también se encuentra en los servidores. Si se piensa como un usuario, se inicia sesión una media de 2 y 3 veces al día (cuando llega a la oficina, después del almuerzo y después de comer). A estas horas se las conocen como horas punta en cuanto nos referimos a trafico de red en el DC. Si un solo servidor se encargara de validar todos los inicios de sesión, en función del volumen de usuarios, podría hacer que el servidor se colgase y finalmente cayera. Eso dejaría a todas las oficinas sin acceso al servidor de ficheros.

Una manera de evitar el problema de concurrencia en las horas punta, es instalar un servidor de DC en cada sucursal, de tal forma que ya no es un único servidor el que

se encarga de todas las validaciones, sino que cada usuario se validaría en el DC que le corresponda. Además, se configuraría estos DC para que se repliquen en todo momento y así tanto tener disponibles las modificaciones relacionadas con los usuarios, grupos o políticas a tiempo real.

Para los DC de la figura 2.4, se ha decidido optar por servidores HPE ProLiant DL360 Gen10, con 2 unidades de disco SSD de 480 GB utilizando un sistema de replicación RAID 1, 32 GB de RAM y un Intel Xeon de 8 núcleos (16 hilos). HP son líderes en lo que viene a ser los equipos y servidores a nivel empresarial, tanto en rendimiento como en seguridad.

Es muy importante proteger el DC, ya que este servidor contiene toda la base de datos del directorio activo, es decir, la base de datos de todos los usuarios y grupos de un dominio. Para prevenir que la información se pierda a causa de algún fallo en el disco duro, se ha decidido agregar un disco duro idéntico adicional. La causa de que se añada un segundo disco de 480 GB no es por un tema de almacenamiento, sino más bien para hacer un RAID 1 de la información del árbol del dominio. Un RAID 1 (mirror) se utiliza para replicar información entre dos discos. De esta manera se previene que, en caso de que uno de los dos discos falle, el sistema pueda seguir funcionando.

2.4.2. Servidor de ficheros

El nuevo protocolo de trabajo que deberán seguir todos los usuarios del dominio es: SIEMPRE trabajar en el servidor de ficheros. De esta manera se consigue que en caso de que el equipo de un usuario falle, este sea reemplazado y no se pierda la información que, al fin y al cabo, es el principal activo que le da valor a una empresa.

Se podría decir que el servidor de ficheros es uno de los principales elementos de esta infraestructura, ya que es el punto común donde más concurrencia de usuarios se va a tener. Desde la visión de un usuario que tenga cierta noción sobre el funcionamiento de los sistemas IT, se podría llegar a pensar que tener un servicio centralizado para toda una empresa puede ser tanto una ventaja como una vulnerabilidad.

Tener un único FS, implica que la disponibilidad sea muy alta. Todo el mundo va a requerir de conexión con el FS para realizar cualquier tarea y, si este servidor cae, automáticamente la empresa queda parada. Desde el punto de vista de la seguridad, a un atacante siempre le va a interesar obtener esos activos que le dan valor a una empresa. Pero contra menos puntos vulnerables tenga la organización, más difícil será el acceso a la información.

Al plantear el diseño teniendo en cuenta prioritariamente la seguridad de la empresa se ha decidido dejar el servidor de ficheros en una única oficina, además de aportar una solución al problema de la disponibilidad. Por esa razón se ha decidido crear un clúster de servidores de ficheros y además agregar una cabina de discos.

Un clúster de servidores de ficheros no aumenta la velocidad de acceso a la información ya que no trabajan en paralelo, sino que en este caso el clúster se crea a modo de fallo. Si por alguna razón un FS ficheros cae, el clúster será el encargado redirigir a los usuarios de un FS al otro. De esta manera, el usuario no notará ningún cambio y podrá seguir trabajando igualmente. [5]

Como este servidor va a tener a todos los usuarios conectados durante toda la jornada laboral al mismo tiempo, este debe tener mejores especificaciones respecto al DC. En este caso, se ha optado por instalar 2 servidores HPE ProLiant DL380 Gen10 en clúster, con 2 unidades de disco SSD de 480 GB utilizando un volumen de replicación RAID 1 para el tema del SO, 128 GB de RAM para aumentar la velocidad de acceso a los ficheros que utilicen los usuarios, 2 procesadores Intel Xeon de 16 núcleos y además se le ha agregado una tarjeta de fibra a 40 Gbps para que la comunicación con la cabina de discos sea la más rápida posible. Este servidor solo va a ser el encargado de correr el SO, toda la información va a estar almacenada en la cabina de discos.

La cabina de discos es un hardware también en formato RACK, y su única función es de almacenar información. Requiere de un servidor aparte para poder gestionarlo, por esa razón se instala un FS. Para ello se ha escogido el modelo HP MSA 2040 de 24 bahías, ya que en base a la experiencia y el perfil de empresa que tienen, no van a trabajar con ficheros muy pesados, por lo que la configuración que se establecería seria la de agregar 24 discos SSD de 480 GB y hacer un volumen de replicación RAID 5 o RAID 6.

Los RAID son distintos formatos de repartición de los datos entre las unidades de disco, de tal manera que la información esté más o menos replicada. Es muy útil, ya que, en función del grado de replicación de los datos entre los discos, podrán fallar más o menos discos y aun así conservar todo el volumen de información.

2.4.3. Servidor de copias de seguridad

Por último, para lo que viene siendo el servidor de copias, se ha optado por una solución no tan común que proporcionará velocidad y seguridad a estas. Para el servidor de copias se ha decidido instalar una biblioteca robotizada o librería de cintas. Esta, a diferencia de un servidor de discos normal, da una velocidad de escritura muchísimo mayor que la que puede dar un servidor de discos normal. Además, el espacio de almacenaje para copias que pone a disposición es muchísimo mayor en el mismo tamaño físico. Cuando se piensa en un disco duro, se piensan en capacidades máximas de entre 8 o 12 TB, pero una cinta tiene aproximadamente las mismas dimensiones que un disco duro y en cambio puede almacenar hasta 56 TB.

2.4.4. Conclusiones

Este diseño de servidores proporciona la seguridad de utilizar las últimas versiones de SO, como es el caso de Windows Server 2019 Datacenter. De esta forma se evitará los fallos de seguridad de las versiones anteriores. Además, este sistema proporciona una alta disponibilidad de la información, soluciones en caso de caída de los servicios, más velocidad y mejora del rendimiento en las máquinas para que los usuarios no tengan problemas a la hora de trabajar.

2.5. Equipos terminales y hardware necesario a nivel de usuario

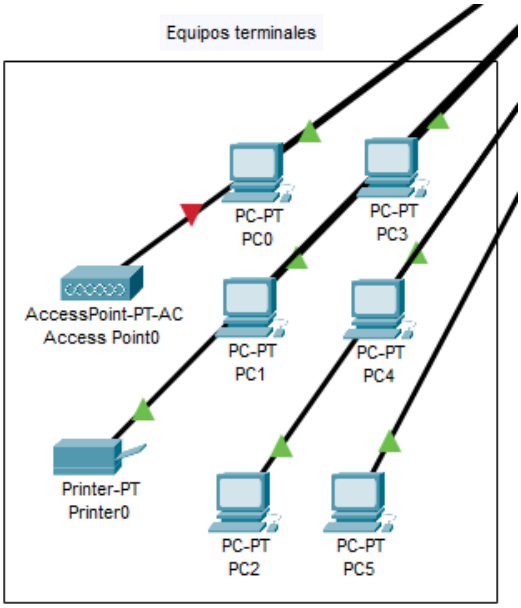

Figura 2.5: Equipos terminales.

2.5.1. Equipos terminales y plataforma digital

En empresas grandes, donde es inviable la gestión de los equipos de los usuarios de forma individual, se creó el concepto de plataforma digital. Una plataforma digital es una imagen ISO corporativa de un SO donde ya viene incluido todos los programas que el usuario va a necesitar, actualizaciones, configuraciones de red, etc. De tal forma que agilice muchísimo la instalación de nuevas máquinas y solo sea necesario agregarlas al dominio para que los usuarios puedan empezar a trabajar.

Aunque las consultas de la información se hagan sobre el FS, los programas y el cómputo se va a ejecutar a nivel local. Por lo que para un perfil general de usuario se ha pensado que todos deberían tener un equipo mínimo con 8 GB de RAM y un disco duro SSD de 250 GB para que la experiencia de usuario sea fluida. Cuando se habla de implementar la transformación digital de una empresa y utilizar una plataforma digital para los equipos del dominio, significa que todos los equipos excepto los servidores deberían ser idénticos, para que así ninguno tenga configuraciones especiales y cualquier cambio se pueda hacer a nivel global para todos con herramientas de actualización distribuida.

Si existe el caso de que algún usuario requiere del uso de un portátil, como todos los equipos van a pertenecer al dominio, dentro de la empresa no va a tener ningún

problema. En cambio, fuera de ella, los portátiles solo se van a poder utilizarse de manera local, y así, evitar acceder al servidor de ficheros fuera del espacio habilitado.

2.5.2. Licencias

Microsoft lanzó hace años un paquete relacionado con el licenciamiento por volumen para equipos de una organización. A este paquete se le conoce por el nombre de Microsoft Open Value. Cuando se abre una empresa y se tiene un número considerable de usuarios, para evitar comprar un gran número de serials distintos, Microsoft lanzó este paquete de serial único con el que se puede activar e instalar en todos los equipos de una empresa las últimas versiones de Windows. Este serial es válido tanto para licencias de equipos terminales (Windows 10 pro) como para las versiones de los servidores (Windows Server 2019).

Es la solución por la que se suele optar en empresas con muchos equipos, ya que en estas es muy habitual que vayan cambiando los ordenadores que van dejando de funcionar con el tiempo. De esta forma, basta con cambiar el equipo defectuoso por otro, instalar la plataforma digital y activarla con el serial corporativo.

2.5.3. Puntos de acceso e impresoras

En todas las empresas hay empleados que utilizan el teléfono móvil como herramienta de trabajo, y para ello se requerirá conexión. Por esa razón, se ha decidido instalar los AP UniFi AC LR, para dar así cobertura por toda la oficina. Además, estos AP se configurarían de tal forma que den señal de dos redes Wifi distintas. De esta forma si algún cliente requiere de conexión cuando este en alguna oficina, no podrá ver las IP de los equipos y además se le restringirá la velocidad de navegación para no hagan un uso indebido de la red ni perjudiquen al resto de usuarios.

Para no sobrecargar un único AP con todos los usuarios de cada oficina se ha planteado que, con una buena distribución, lo ideal sería instalar un AP por cada 20 usuarios. Por esa razón 2 AP se instalarán en la oficina de Madrid, 5 en la de Barcelona y los 3 en la de Francia.

Por último, como en todas las empresas se requiere del uso de impresoras, se ha decantado por utilizar el modelo de Xerox C7000. Se trata esta de una impresora de la gama profesional que, aparte de imprimir una buena cantidad de hojas por minuto y poder enviar documentos vía Wifi, incorpora la opción de impresión retenida. Este tipo de impresión funciona insertando un código para imprimir los documentos y no que se mezclen con los del resto de usuarios.

2.6. Conceptos de seguridad a nivel empresarial

Al implementar un dominio se pueden crear políticas tanto a nivel de usuario como a nivel de equipo. El uso de estas es muy importante ya que, regular las acciones lega-

les que los usuarios podrán realizar sobre el sistema suele ser un factor que aumenta bastante la seguridad de una organización.

Existen políticas de todo tipo, desde establecer configuraciones de red predeterminadas para los usuarios del dominio hasta definir que fondo de pantalla van a tener cuando inicien sesión. Muchas de estas políticas aumentaran la seguridad de la organización, como, por ejemplo:

- Establecer un servidor DNS predeterminado para los usuarios del dominio puede filtrar a que sitios web se pueden conectarse. De esta forma evitamos que se conecten a sitios potencialmente peligrosos de donde malintencionadamente descarguen software malicioso.
- Definir los permisos de las carpetas a las cuales los usuarios van a poder acceder en función del departamento al que pertenezcan. Establecer correctamente los permisos nos va a permitir cumplir los 2 objetivos CIA restantes de la ciberseguridad: Confidencialidad e Integridad. [26]
- Inhabilitar el uso de las entradas USB para evitar introducir hardware o software malicioso en los equipos.

Definir una jerarquía segura en el FS significa que cada usuario solo va a tener acceso a la información que necesite. Optar por este diseño evita la mayor parte de los problemas relacionados con la filtración de información. Que los principales activos de una organización tengan integridad es lo que le da valor y reputación a esta. Por esa razón es muy importante dar los permisos mínimos y necesarios a los usuarios, ya que de esta forma se suelen evitar problemas debido a una indebida modificación o destrucción de la información.

Según fuentes de IBM, entre el 60-70 % de los incidentes dentro de una empresa es debido a *insiders*, personal interno de la organización. Debido a ello, las empresas tienen que tomar más medidas de seguridad sobre la información a la que pueden acceder los usuarios. [20]

Los **ciberdelincuentes** utilizan varias técnicas de ataque para obtener información de la empresa, como por ejemplo: técnicas de **ingeniería social**, ***Phishing***, **compromiso de correo corporativos** (BEC) o simplemente técnicas de **fuerza bruta** para obtener credenciales de acceso. Por mucho que el equipo de TI aplique diseños de seguridad o protocolos de trabajo para prevenir estos ataques, nunca se van a prevenir el 100 % de ellos. Esto es debido a que el factor que es más vulnerable siempre es el humano.

Por esa razón es muy importante enseñar al personal de la empresa metodologías de trabajo seguro y conceptos de seguridad. Existen consejos muy sencillos que disminuyen mucho el riesgo de ser atacados en un futuro, como, por ejemplo: realizar copias de seguridad de los equipos, cambiar las contraseñas con frecuencia, establecer un protocolo de acción para evitar ataque de ingeniería social y mantener actualizados todos los dispositivos. Actualizar los equipos suele corregir los agujeros de seguridad de las nuevas vulnerabilidades que van apareciendo. Hay que recordar que mantener la seguridad de los equipos no es suficiente. Cualquier dispositivo que se conecte a la

red de la organización o contenga alguna credencial relacionada con el dominio, puede ser un factor de amenaza. [1]

Cuando las empresas tienen un departamento de ciberseguridad, se suele hacer uso de *Honeypots* y equipos de monitorización. Un *Honeypot* es un equipo vulnerable a propósito que no contiene información valida de la empresa. A su vez, este suele estar conectado a un equipo de monitorización, que analizará en todo momento la existencia de anomalías tanto en el *Honeypot* como en la LAN. Utilizar estos equipos es una buena técnica para prevenir ataques. Mientras que los atacantes están perdiendo el tiempo con el *Honeypot*, al departamento de ciberseguridad de la empresa le da tiempo a aplicar contramedidas. [24]

Capítulo 3

Simulación de la infraestructura mediante servicios de virtualización

En este capítulo se tratará de demostrar como sería crear una simulación real dentro de las posibilidades que ha brindado el hardware disponible.

3.1. Definición de los objetivos y del hardware disponible

El objetivo de esta simulación ha sido aprender a diseñar un entorno seguro e implementar todas las funcionalidades necesarias para que se asemeje a una infraestructura IT real. Por esa razón, se ha diseñado un entorno más limitado donde habrá 2 sucursales y 4 departamentos por sucursal.

Para realizar el experimento, se requirió aprender conceptos de subnetting para así crear todo el sistema de red, hizo falta introducirse en el mundo de los servidores de dominio y los diferentes roles que puede ejercer un servidor [9], se ha creado y diseñado la estructura de un árbol de dominio, y finalmente se han aplicado conceptos de seguridad para proteger a todo el personal y equipos de la organización.

El entorno de emulación se ha realizado sobre un portátil personal con un i7 de séptima generación y 16 GB de memoria RAM. Para ello, se ha utilizado la herramienta GNS3 para la emulación de las conexiones de red y el programa VirtualBox para ejecutar las distintas máquinas virtuales de la organización.

3.2. Emulador GNS3 para diseño de red

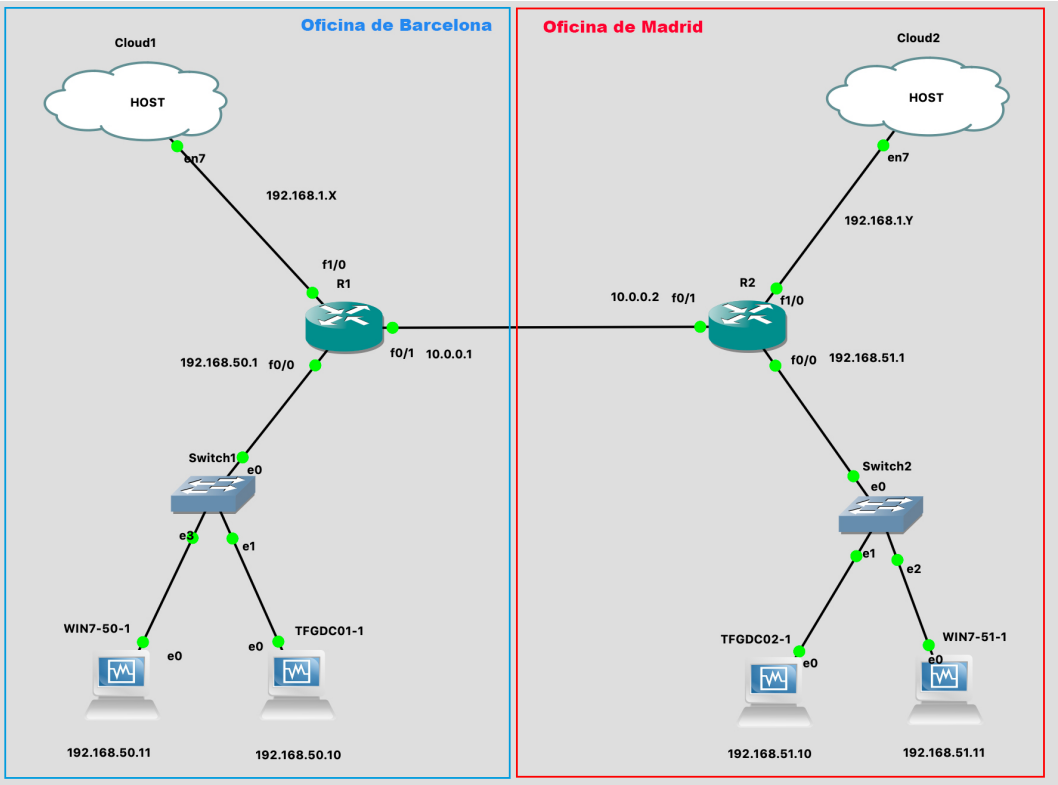

Figura 3.1: Diseño general de las comunicaciones mediante el GNS3.

GNS3 es un emulador de sistemas y telecomunicaciones creado por la compañía Cisco Systems. A diferencia del simulador Cisco Packet Tracer, este permite trabajar con hardware físico, como son el caso de tarjetas de red personales o incluso máquinas virtuales que se tengan instaladas en el equipo.

El software GNS3 crea a nivel de aplicación un servidor de entorno virtual. Aquí es donde se ejecutarán toda clase de máquinas virtuales, routers, *switches*, etc. Siempre sobre el puerto 3080 del equipo donde se realice el experimento. Uno matiz ha tener en cuenta es el elemento Cloud del emulador, el usuario debe entenderlo como el equipo host que ejecuta el servidor de entorno virtual. En este caso, el elemento Cloud se entiende como un equipo portátil con 2 tarjetas de red físicas.

La realidad es que la mayoría de oficinas suelen estar separadas geográficamente, lo que supone conectar las oficinas mediante el uso de una VPN o contratar una MacroLAN. Como para realizar el experimento se han podido ejecutar máximo 4 VM al mismo tiempo, no se ha podido dedicar una máquina extra en la oficina de Barcelona para crear un servidor VPN.

Por esa razón el experimento se ha realizado a nivel de Campus. Esto significa que la distancia horizontal entre las 2 redes no supera los 100 metros, por lo que podremos interconectar los routers mediante un cable UTP o hacer uso de un cable de Fibra Óptica. Se ha considerado hacerlo de esta forma, ya que para la parte práctica se ha profundizado más en la implementación de un dominio que en la conexión entre las redes.

Al tratarse de un emulador hay dispositivos que no están disponibles en el software, como es el caso de un Firewall o un IPS. Debido a ello, se ha decidido aplicar conceptos de seguridad solamente a nivel de equipos.

3.2.1. Configuración Cloud

El software GNS3 permite emular las tarjetas de red físicas del equipo. Al encontrarse una incompatibilidad con la tarjeta de red wifi integrada del equipo. Se optó por adquirir un adaptador de red USB-C to Ethernet compatible con el simulador para así poder dar salida a internet a las VM. [2]

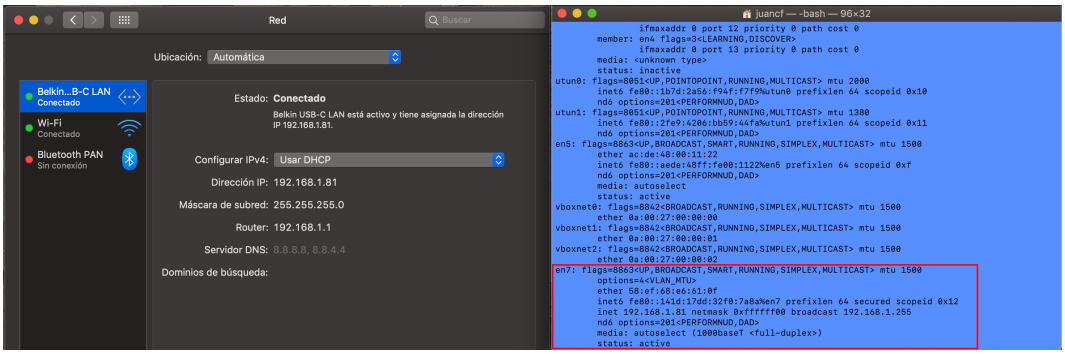

Figura 3.2: Adaptador de red.

Como se muestra en la figura 3.1, se puede observar que existe una conexión por cable entre el dispositivo Cloud, que utiliza el puerto Ethernet Network 7 (e7), y ambos routers, que utilizan el puerto FastEthernet 1/0 (f1/0). Este adaptador e7 equivale a la tarjeta de red que proporciona el adaptador Belkin. A través de esta entrada se asignará una IP dinámica, la 192.168.1.81 en este caso, mediante DHCP al equipo host.

3.2.2. Configuración del router

Modelo de router

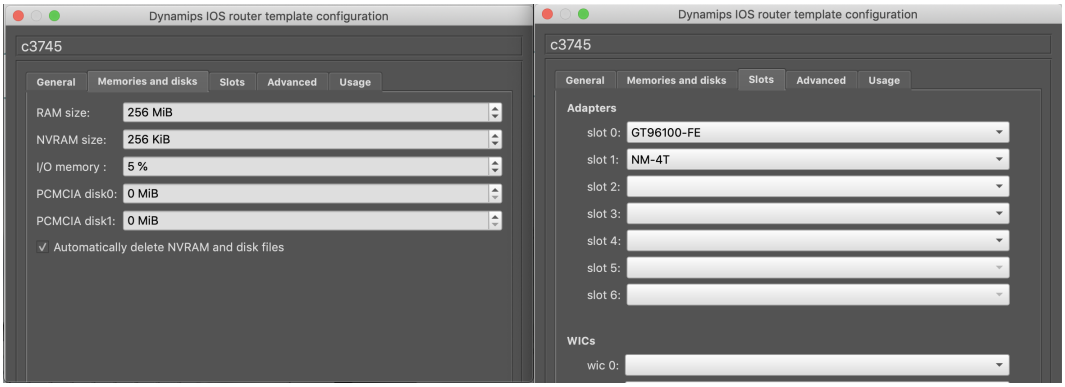

Figura 3.3: Configuración del router Cisco C3745.

GNS3 admite compatibilidad con un gran número de modelos de routers distintos. Debido a que todas las imágenes ISO de estos modelos son de pago, únicamente se pudo obtener las imágenes de los modelos C3745 y C7200.

Aunque inicialmente se empezó a construir el laboratorio utilizando el modelo C7200 para ambos routers, debido a problemas relacionados con los ficheros de configuración y experimentar un retraso excesivo al utilizar la consola de comandos, se optó por sustituir los routers C7200 por el modelo C3745.

Para la configuración de este modelo se decidió agregar 2 tarjetas de red:

- La GT96100-FE en el slot 0, ofrecía 2 entradas FastEthernet. Estas entradas se utilizaron para comunicar las redes LAN de ambas oficinas. Esta tarjeta de red, además, viene predeterminada ya con la imagen del modelo C3745.
- La NM-1FE-TX en el slot 1, ofrecía la entrada ethernet restante para que así, los equipos pudiesen salir a internet.

Para el diseño de red se decidió utilizar para las redes LAN de cada oficina la interfaz fa0/0, donde se han establecido las redes 192.168.50.0 y 192.168.50.51. Se ha escogido estos rangos de red para diferenciarlos de los rangos clásicos que proporcionan los proveedores de servicios por defecto, como es el caso de las redes 192.168.1.0 de Movistar y 192.168.0.0 de Vodafone. Al ser un número redondo hace que recordar la red a la que se pertenecen los usuarios sea de recordar.

Configuración de las redes

Los routers de gama profesional, a diferencia de los domésticos, suelen utilizar un único puerto único por red. Por esa razón, en el diseño planteado se ha utilizado 3 redes

distintas: la red 192.168.1.0 utilizada en el puerto f1/0 será la que permita a los equipos salir a internet, la red 192.168.50.0 y 192.168.51.0 utilizadas en el puerto f0/0 serán las redes LAN de cada oficina respectivamente, y finalmente la red 10.0.0.0 utilizada en el puerto f0/1 se ha utilizado para establecer el enrutamiento entre routers.

La red ***192.168.1.0*** será la encargada de proporcionar internet a los usuarios del dominio. Al ser Movistar el proveedor de servicios que se ha utilizado es el rango de red que utilizarán los dispositivos que quieran conectarse a internet.

Como los dispositivos R1 y R2 van a utilizarse de pasarela para salir a internet, la IP que se asigne a los routers en el puerto f1/0 no es importante. Siempre y cuando la IP asignada pertenezca al rango de red que tenga salida a internet. Por esa razón, se ha optado por asignar la IP mediante el servidor DHCP del router de Movistar.

Ambos routers realizarán la función de *Gateway* en el puerto f 0/0 para las redes correspondientes a los rangos ***192.168.50.0*** y ***192.168.51.0***. Para la asignación de IPs dentro de las redes LAN se han configurado los routers para que implementen la función de servidor DHCP, encargándose así de asignar las IPs de forma dinámica a los equipos que pertenezcan a la LAN.

Para simular un ejemplo real, se decidió que en cada red hubiese un grupo o pool de 10 IPs reservadas y otro pool 243 IPs de asignación dinámica. De esta forma se podía asignar IPs estáticas a equipos que su dirección nunca debiera cambiar, como por ejemplo el *gateway* o el DC, y IPs dinámicas para demás equipos del dominio, en este caso los equipos terminales.

Cuando se crea un servidor de DHCP, se debe establecer el servidor DNS que deberán usar los equipos que se les haya asignado el direccionamiento IP de forma dinámica. Es muy importante indicar en este ejemplo práctico que el servidor DNS fuese justamente la IP del DC de la LAN correspondiente. De esta forma se podrán agregar los equipos al dominio.

Por último, se ha requerido especificar el tipo de *Network Address Translation* (NAT) que utilizaría el pool de IPs que se había establecido previamente. Existen diferentes tipos de NAT, por ello, se decidió implementar NAT *override* sobre la IP pública que asigne el proveedor de servicios para así, poder navegar por internet. [8]

Por norma general, una buena práctica a nivel de seguridad es que el controlador de dominio nunca debe esta expuesto a internet, para así evitar ataques como el famoso *ransomware WannaCry*. Con esto se quiere dar a entender que el equipo puede tener acceso a internet, pero nunca se debe publicar un servicio de este. [21]

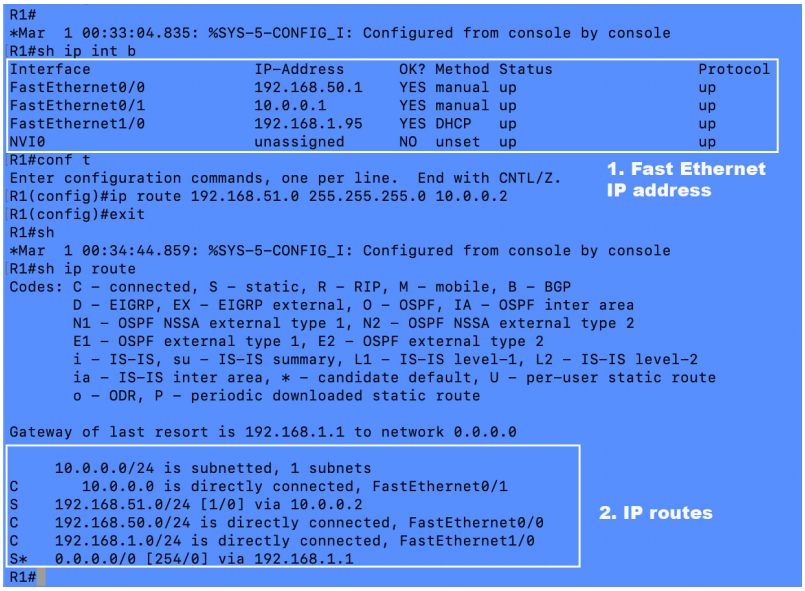

Figura 3.4: Establecer IP route.

Para que un equipo de la red de Barcelona pudiese tener comunicación con otro equipo de la red de Madrid, no basta con comunicar los routers. Se ha requerido definir el salto que debe tomar la conexión para llegar al destino.

Para ello, se ha decidido utilizar la red de clase A ***10.0.0.0*** para conexiones a nivel de router como podemos observar en la figura 3.4. De esta forma es más fácil diferenciarla de las conexiones a nivel de equipos en LAN, donde se han utilizado redes de clase C. Para configurar la conexión entre routers se han utilizado los puertos f0/1 de ambos routers para establecer una conexión por cable directa y se ha asignado la IP 10.0.0.1 al R1 y la IP 10.0.0.2 al R2 de forma manual.

Es indispensable crear las rutas estáticas de salto cuando se establecen conexiones manualmente, como es el caso de estos routers. Observando la figura 3.1 puede plantearse la idea de que el router automáticamente ya sabe por que puerto debe salir simplemente consultando la red del destinatario. Pero esto es falso, hay que indicárselo manualmente.

Suponiendo que el equipo de Barcelona con IP 192.168.50.11 quiere enviar un PING al equipo con la IP 192.168.51.11. Para ello, deberá seguir un recorrido:

1. El dispositivo con la ip 192.168.50.11 envía el protocolo ICMP (ping) al *Gateway* de su red, en este caso es el router R1 con la IP 192.168.50.1.

2. El R1 consulta por que interfaz de red debería mandar el mensaje, finalmente verifica que ha de salir por el puerto f0/1 como la IP 10.0.0.1.

3. El R2 recibe la señal y consulta en la trama el destinatario. Una vez verificado, lo transmite por el f0/0 hasta llegar al dispositivo destino que, en este caso, tiene la IP 192.168.51.11.

4. Una vez recibido el mensaje, este devuelve la trama de respuesta haciendo el mismo recorrido, pero a la inversa, así hasta llegar otra vez al dispositivo origen.

Es extraño que el R1 transmita la trama por la interfaz f0/1, cuando esta, está utilizando un rango de red distinto al del destinatario (10.0.0.0 != 192.168.51.0). Esto es posible gracias a establecer rutas de salto estáticas o también llamadas IP Routes.

Establecer una IP Route significa agregarle un camino al router para resolver consultas que directamente no sabe como realizarla. [7] Como se aprecia en la figura 3.4, en la parte de abajo se muestra claramente que para resolver peticiones sobre la red 192.168.51.0 debe preguntar a la IP 10.0.0.2.

Como el protocolo PING no se completa hasta que el emisor no recibe la respuesta verificada del destinatario, es muy importante que se realicen las IP Routes necesarias en cada router para que pueda completarse la comunicación bidireccional entre ellos.

3.2.3. Resultados

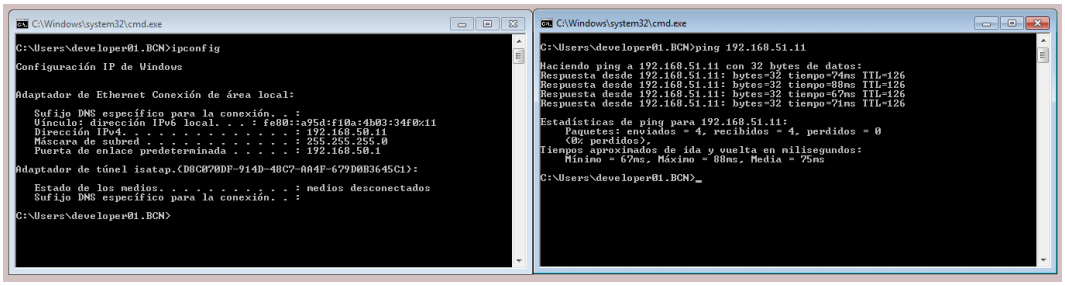

Figura 3.5: Ping desde la sede de Barcelona a la sede de Madrid.

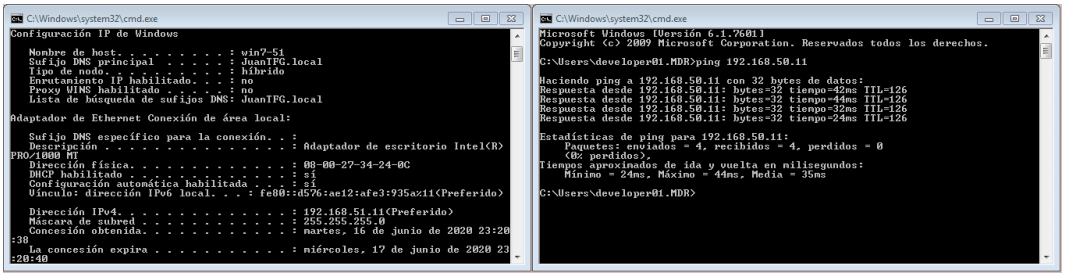

Figura 3.6: Ping desde la sede de Madrid a la sede de Barcelona.

Una vez establecidas todas las configuraciones en ambos routers y agregado las IP Routes necesarias para establecer conexión multisede, estará habilitada la conexión con los equipos de la otra oficina.

Como se puede observar tanto en la figura 3.5 como en la figura 3.6, si se realiza una petición PING entre los equipos con las IP 192.168.50.11 y 192.168.51.11, se puede

ver claramente un 100 % de éxito en los paquetes recibidos. Este valor y el tiempo de latencia de las respuestas sirve de referencia para comprobar la estabilidad de la conexión que se ha establecido.

Un detalle que se debe remarcar en la figura 3.6, es que en la primera ventana de la consola se puede apreciar que ambos equipos están agregados al dominio. Por esa razón justifica aún más la conexión entre oficinas.

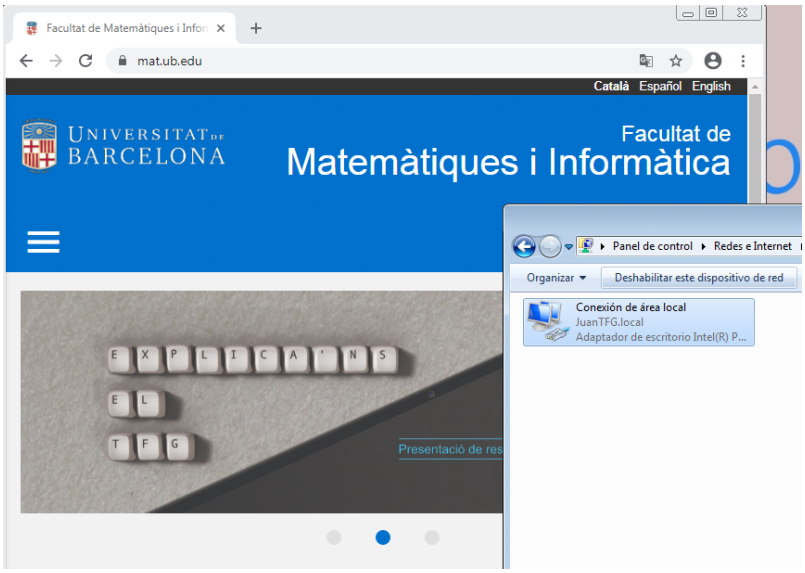

Figura 3.7: Conexión a internet desde la red LAN.

Para finalizar las pruebas, la figura 3.7 muestra como un equipo del dominio que utiliza solamente una interfaz de red, es capaz de llegar a la LAN de la otra oficina y además navegar por internet. Esto es debido a que se ha realizado correctamente las conexiones entre ambos routers del emulador.

3.3. Virtualización de los servidores

Debido a la falta de recursos a la hora de realizar el proyecto, con tal de maximizar la semejanza con el proyecto real, se ha tomado la decisión de implementar solamente el DC de cara a los servidores, para así poder mostrar la funcionalidad de un dominio con una VM de un equipo terminal.

3.3.1. Controlador de dominio

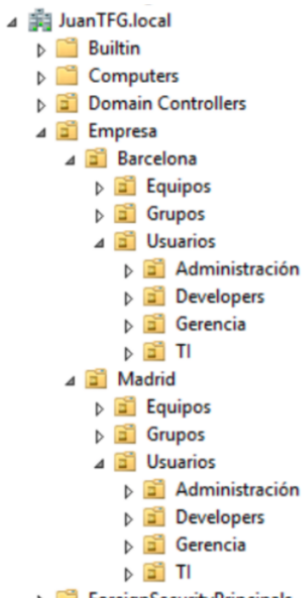

Figura 3.8: Árbol de dominio.

Para la gestión de los usuarios y los grupos de la organización, se ha creado el dominio **JuanTFG.local**. Cuando se instala el rol de DC a un servidor, este solicitará agregar el equipo a un dominio existente o crear un bosque. Se conoce como bosque al dominio raíz de un directorio activo, el dominio del cual nacerán todos los otros dominios. En este caso al tratarse de un dominio totalmente nuevo, se estableció **JuanTFG.local** como nombre del bosque o árbol de dominio.

La nomenclatura estándar para definir el nombre del dominio es utilizar *"NombreEmpresa.local"*. Esto se hace para que el servidor DNS diferencie el nombre de dominio corporativo utilizado para los equipos de la organización del dominio web. Cuando una empresa decide unificar bajo el mismo nombre de dominio todos los servicios, como por ejemplo el dominio web, las cuentas de correo, etc. Se utiliza un nombre de dominio sin el *".local"*, ya que será un único servidor DNS el que indique la IP de cada servicio.

Las unidades organizativas (OU) son contenedores que se crean dentro de un Directorio Activo o *Active Directory* (AD) para organizar objetos. Se conoce como objetos a los usuarios, grupos y equipos de que pertenecen a un dominio.

En este caso ambas sedes pertenecen a la misma empresa. Para facilitar la gestión y tener una estructura organizada, se ha decidido crear una OU Empresa global y crear distintas OU para las distintas sucursales dentro de esta. De esta forma se podrá aplicar políticas de grupo o *Group Policy Objects* (GPOs) distintas en cada oficina si fuese necesario.

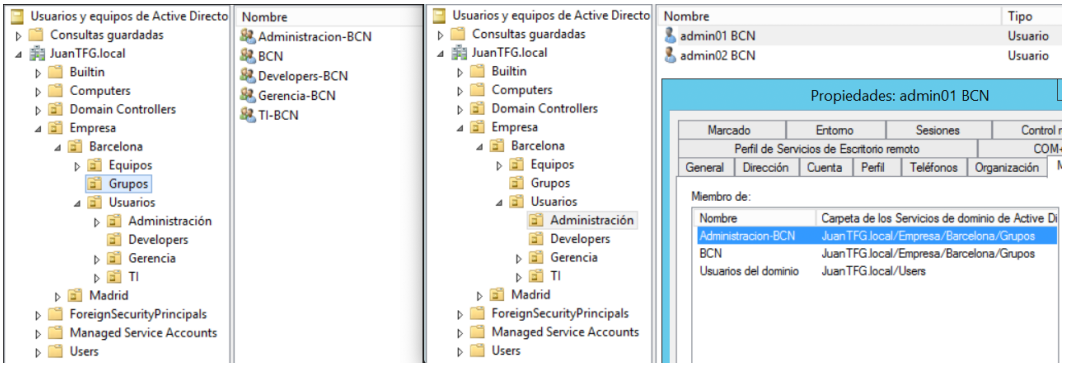

Figura 3.9: Frupos del Active Directory.

Para cada oficina se ha creado las distintas OU referente a los equipos físicos del dominio, los grupos que se van a utilizar para restringir permisos y los diferentes usuarios que la forman. En este caso se ha creado 2 OU referentes a las oficinas de Madrid y Barcelona. Donde habrá en ambos casos 4 departamentos:

- Departamento de Administración.
- Departamento de Gerencia.
- Departamento de Desarrolladores.
- Departamento de Personal de TI.

Para la nomenclatura de los grupos se ha utilizado el "*NombreDepartamento-Oficina*", además de crear un grupo genérico para cada oficina.

Cuando se refiere a los usuarios, se busca una nomenclatura que no relacione ninguna persona física con un nombre de usuario. De esta forma se estandariza un protocolo de trabajo en función del departamento al que pertenece el usuario. Para dicha nomenclatura se ha utilizado "*NombreDepartamento+ID-oficina*" siguiendo un poco la estructura de los grupos. En la figura 3.9 se puede observar como el usuario **admin01.BCN** es miembro de los grupos **Administración-BCN** y **BCN**.

Crear y gestionar los grupos a los que van a pertenecer los usuarios es muy importante. Implementar un buen diseño puede evitar la mayoría de las fugas de información por parte de *insiders* [20], haciendo que cada usuario solamente pueda tener acceso a la carpeta que le corresponde por su departamento.

3.3.2. Servidor de ficheros

Aunque en la idea original se planteó crear un servidor de ficheros en la sede de Barcelona para que, desde cualquier oficina los usuarios se conectaran y compartiesen ficheros. A la hora de crear las conexiones de red con el software GNS3 y ver lo insostenible que era tener tantas VM levantadas al mismo tiempo, se decidió prescindir de tener un servidor de ficheros dedicado.

Debido a ello, se decidió optar por implementar una solución más práctica y elegante que simulara el mismo resultado cara a los usuarios, la cual fue reducir el volumen de espacio de la VM TFGDC01 y crear una unidad de disco nueva para los datos.

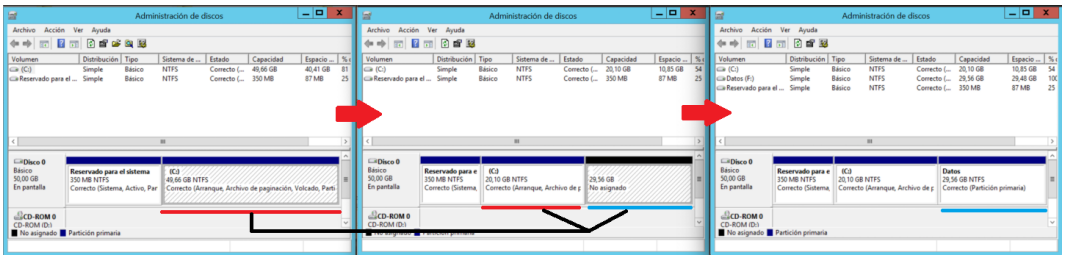

Figura 3.10: Simulación de servidor de ficheros.

Con el administrador de discos, se decidió coger el disco C que originalmente tiene disponible 50 GB y reducir una parte de ese espacio para orientarlo al volumen compartido de los usuarios. Una vez se reduce el volumen, esta parte pasa a ser un "volumen no asignado". Finalmente creas un nuevo volumen simple en ese espacio y le asignas una letra, que, en este caso, se conoce como volumen F (Datos).

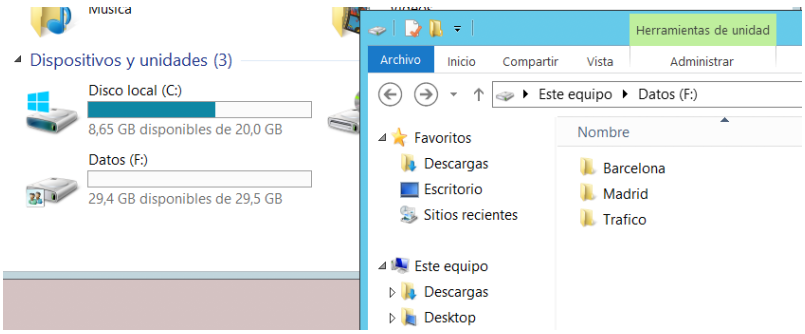

Figura 3.11: Unidad de datos compartida.

Por último, se estableció en las propiedades de seguridad de la unidad compartida que únicamente pudiesen tener acceso los miembros del dominio. Dentro de esta, se ha creado tres carpetas: dos de estas carpetas están destinadas a las diferentes oficinas de forma independiente y la carpeta Trafico esta orientada a compartir ficheros entre todas ellas. Es muy importante establecer que grupos van a tener acceso a cada carpeta.

Los permisos de seguridad de las carpetas utilizan el mismo mecanismo de herencia que los objetos en programación. Hay casos que interesa que un grupo acceda a una profundidad determinada pero no a la profundidad máxima del directorio.

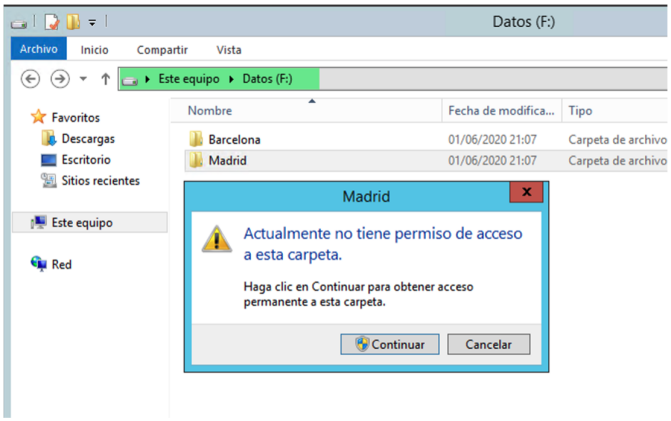

Figura 3.12: Acceso regulado con permisos.

Al realizar la prueba con el usuario **admin01.BCN**, se ve en la figura 3.12 al intentar acceder a la carpeta de Madrid almacenada en la unidad F, no tiene permisos para hacerlo. De esta forma se evita filtraciones de información. Normalmente las empresas que trabajan de forma departamental, donde la información de ese departamento es independiente al del mismo departamento en otra oficina. Por esa razón, a un usuario no le debe interesar que se hace en otros departamentos.

3.3.3. Automatización de las configuraciones para los usuarios del dominio

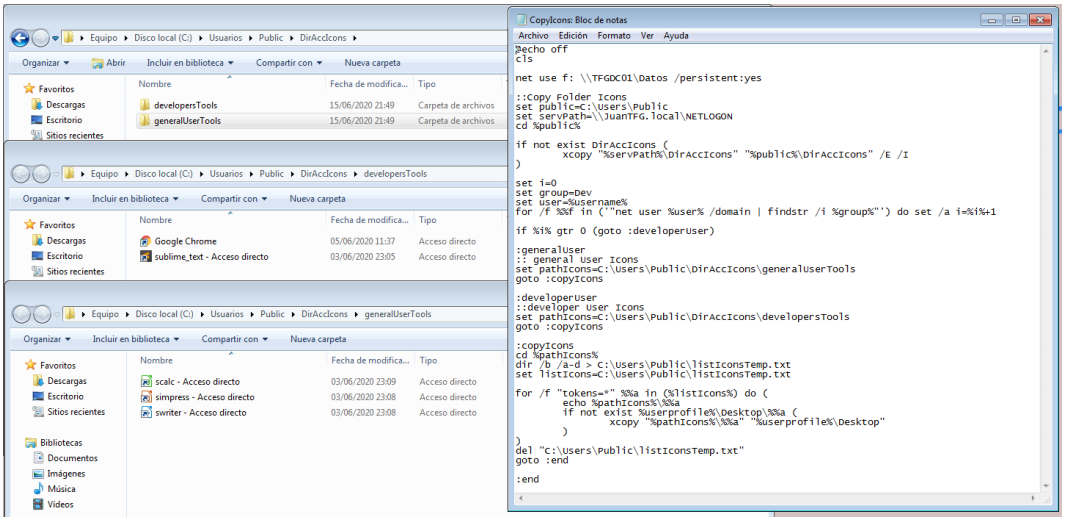

Figura 3.13: Script de accesos directos.

Para automatizar la configuración de las herramientas que debe tener un nuevo usuario para empezar a trabajar, se ha creado un script que se ejecuta al inicio de sesión

del usuario gracias a una GPO. Este script mapeará la unidad de Datos (F:) compartida del servidor TFGDC01 para que el usuario tenga acceso. Además, copiará una serie de Accesos Directos en el escritorio en función del grupo al que pertenezca el usuario. [4] Aparte de esto, se ha decidido crear otra GPO para establecer un fondo de escritorio común para todos los usuarios del dominio.

3.4. Creación de una plataforma digital

Una plataforma digital es una ISO corporativa común para todos los equipos terminales del dominio. Esto quiere decir que contiene las ultimas actualizaciones de un SO, todos los parches de seguridad reportados hasta la fecha, todos los programas que cualquier usuario del dominio pueda necesitar, etc. Existen herramientas como BartPE o PEBuilder que permiten la creación de una ISO personalizada, donde se selecciona de una lista de programas disponibles los que la imagen instalará al inicio. Simulando esta plataforma digital, se ha creado una VM de Windows 7 con la última versión de SO disponible, el navegador Google Chrome, el programa SublimeText para los desarrolladores y el LibreOffice para los demás usuarios del dominio.

Con esta VM previamente configurada, basta con clonar la VM, agregarla a la red que le corresponde en el software de GNS3 y agregar ese equipo al dominio. De esta forma se simula la instalación una ISO corporativa a un equipo y agregarlo finalmente al dominio.

3.5. Resultados de la simulazión virtualizada

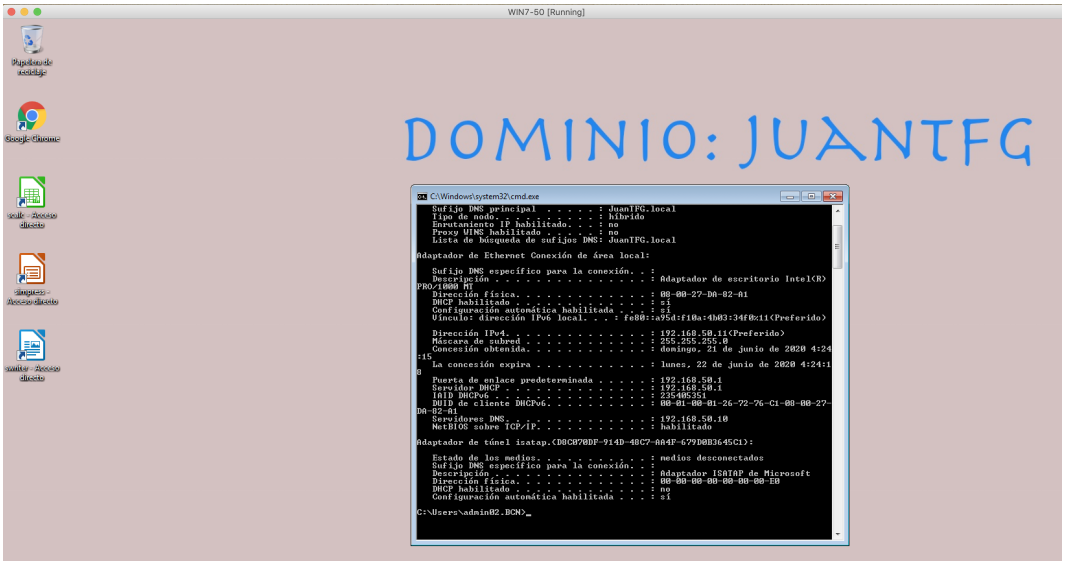

Figura 3.14: Entorno de escritorio del usuario Admin02.BCN.

En la figura 3.14 se puede observar que el usuario admin02.BCN ha iniciado sesión en el equipo Win7-50, el cual pertenece a la red LAN de Barcelona. Vemos que este usuario ha podido iniciar sesión en el dominio gracias a que el servidor DNS que le ha predefinido la configuración de red del software GNS3 le ha asignado la IP del equipo TFGDC01.

Además, se puede apreciar que se han establecido una serie de iconos en función del grupo al que pertenece el usuario. Por último recalcar que la GPO encargada de establecer el fondo de escritorio común para todos los usuarios del dominio funciona correctamente.

Figura 3.15: Entorno de escritorio del usuario Developer01.MDR.

En la figura 3.15 se puede observar que el usuario developer01.MDR ha iniciado sesión en el equipo Win7-51, el cual pertenece a la red LAN de Madrid. A diferencia de la figura 3.14, en este caso el servidor DNS que se ha establecido ha sido la IP del equipo TFGDC02. Al tratarse de un usuario que pertenece al grupo de desarrolladores, el script de inicio le ha asignado unos iconos de acceso directo distintos al del usuario admin02.BCN.

Gracias a estas imágenes se ha podido comprobar como se diseña y se implementa una infraestructura IT de entorno empresarial desde 0, totalmente funcional. Donde un usuario va a poder trabajar desde un equipo que pertenezca al dominio y va a poder guardar y modificar ficheros desde su respectiva carpeta departamental del servidor de ficheros y además va a tener acceso a Internet.

Por esa razón, se podría decir que la simulación del proyecto de transformación digital virtualizado se ha realizado correctamente.

Capítulo 4

Conclusiones y Trabajo futuro

4.1. Conclusiones

En esta sección se analizará si se han cumplido los objetivos que se establecieron al inicio del proyecto.

El objetivo de **estudiar el funcionamiento de una organización** se ha cumplido en el tiempo estimado. El principal inconveniente que se encontró a la hora de cumplir este objetivo fue que toda la información referida a metodologías de trabajo era muy enfocada a protocolos que normalmente utilizan empresas con miles de empleados, pero realmente no había ejemplos orientados a empresas más pequeñas.

Gracias al haber podido ver empresas de diferentes sectores de cerca, se ha podido estudiar diferentes protocolos de trabajo más reales y analizar que ventajas y que desventajas que tiene trabajar de una forma o de otra.

El objetivo de **diseñar la infraestructura IT de una empresa** se ha cumplido en un poco menos del tiempo estimado. Para este objetivo se encontró un gran inconveniente debido a la protección personal de las empresas. Ninguna empresa va a documentar al 100 % como esta montada su infraestructura ya que eso le pondría en riesgo de ser un objetivo vulnerable.

Toda la información adquirida de varias fuentes recalcaba la importancia de separar los servidores por servicios y la implementación de un firewall. Gracias a la información recogida sobre como es un diseño genérico de una infraestructura, los conocimientos adquiridos realizando el primer objetivo de estudiar los mecanismos de trabajo de una organización y la posibilidad de ver los equipos de varias empresas de cerca, se ha podido dar una solución que sea fácilmente escalable, rápida y segura.

Por último, el objetivo de **implementar una infraestructura IT completa virtualizada** llevo un poco más del tiempo previsto, lo que al haber tardado un poco menos en el diseño teórico, se compensó el tiempo total estimado del proyecto.

Al querer llevar a cabo un proyecto originalmente muy ambicioso, donde se pretendía virtualizar todos los equipos básicos de una empresa sobre la VM que ofrece el

propio software GNS3, debido a incompatibilidades con el software y las limitaciones del equipo, se vio obligado a reestructurar la dimensión de la infraestructura.

4.2. Trabajo futuro

Como trabajo futuro se implementaría un sistema de redirección de perfiles móviles o *User Folder Redirection*. El cual permitirá a los usuarios acceder al contenido de su carpeta de escritorio y documentos desde cualquier equipo de la organización. Para ello se requiere la instalación de un servidor de perfiles móviles el cual se encargará de presentar la carpeta perfil del usuario donde se inicie sesión.

Además, se implementaría un sistema de monitorización que analice lo que esté pasando en el FS en todo momento, para así evitar ataque tipo **Ransomware**. Y se agregará una serie de equipos que realicen la tarea de *Honeypot*. De esta forma se podrán detectar indicios de ataques y ejecutar las contramedidas a tiempo.

Capítulo 5

Anexos

Este capítulo se va a centrar en profundizar en conceptos que se han ido nombrando a lo largo del proyecto

5.1. Conceptos sobre redes y telecomunicaciones

5.1.1. ¿Que es una IP y un servidor DNS?

IP

El protocolo de internet o Internet Protocol (IP) actúa como identificador de dispositivo dentro de una red. Este identificador o IP puede ser asignado mediante un dispositivo externo, el que por norma general suele ser el router o *Gateway* o especificado por el mismo dispositivo de forma manual.

Un *Gateway* es el dispositivo por el cual pasará todo el trafico de una red y suele ser el encargado de asignar estas IPs a los dispositivos. La asignación de estas IPs suele ser mediante el *Dynamic Host Configuration Protocol* (DHCP) de forma dinámica.

Existen 2 tipos de IPs:

- Las IPs estáticas son asignadas de forma manual. Suelen ser utilizadas para dispositivos de red que siempre deben tener el mismo identificador, como, por ejemplo, la IP del servidor del DC, la IP del servidor de *backup* o las impresoras).

- Las IPs dinámicas se pueden ver como pool o una lista de direcciones IP que se van repartiendo en el momento que un dispositivo nuevo quiere entrar en la red. En una red podrá haber tantos dispositivos como direcciones IP (o direcciones de host) haya disponibles. En una red de tipo C, la clásica red local doméstica con direccionamiento 192.168.1.0 o 192.168.0.0 por defecto, hay 253 direcciones host disponibles.

Entender como funciona el direccionamiento y la identificación de dispositivos en una red es vital a la hora de crear el diseño de red en una empresa. Plantear un mal diseño o no conocer los mecanismos de resolución puede provocar que los usuarios haya días que pierdan el acceso a los recursos de la red.

Para solucionar este asunto, se suele utilizar el pool de IPs reservadas para asignar a estos equipos una IP estática o resolver por nombre de dispositivo (NETBIOS). Ambas soluciones son igual de válidas. [23]

Servidor DNS

Una IP no deja de ser un identificador dentro de una red. Cada URL apunta a la dirección IP de un servidor web. Por esa razón, cuando se escribe en un navegador la IP 172.217.16.238 este lleva a la web de Google.

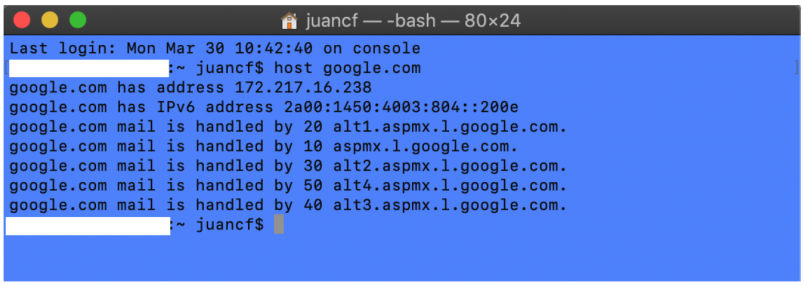

Figura 5.1: Obtener dirección IP de un dominio web.

Los servidores de resolución de nombres o *Domain Name Server* (DNS) se crearon para facilitar el acceso a estas páginas para los usuarios, ya que es mucho más sencillo recordar un nombre que una dirección IP.

Lo que para un usuario es buscar en un navegador la web de www.Google.com, los equipo lo traducen a preguntar a los servidores DNS de internet qué IP tiene ese nombre asignado en la tabla de direcciones.

5.1.2. Virtual Private Network (VPN)

Una VPN es una conexión tunelizada y encriptada punto a punto que permite crear una red local sin necesidad de que los usuarios de dicha red estén físicamente conectados entre sí, sino a través de Internet. Este tipo de conexiones son muy útiles ya que permiten al usuario obtener las ventajas de la red local y una mayor flexibilidad. [25]

El teletrabajo es el principal uso de este tipo de conexiones, ya que mediante el algoritmo de cifrado AES permite establecer una conexión segura entre el equipo del usuario y la red privada de la organización. Durante este periodo de confinamiento ha sido vital el uso de este servicio para que los empleados pudieran trabajar como si estuviesen sentados en la misma oficina.

Este tipo de conexión suele utilizarse además para evitar la censura y bloqueos geográficos de contenido, ya que es muy común que en determinados países cierto contenido o información este prohibido.

5.1.3. Network Address Translation (NAT)

Debido al *Internet Protocol versión 4* (IPv4) que se utiliza hoy en día para navegar por internet, existe un número limitado de IPs públicas. El organismo internacional de primer nivel, la AINA (*Internet Assigned Numbers Authority*), repartió el último bloque libre en enero de 2011. [3]

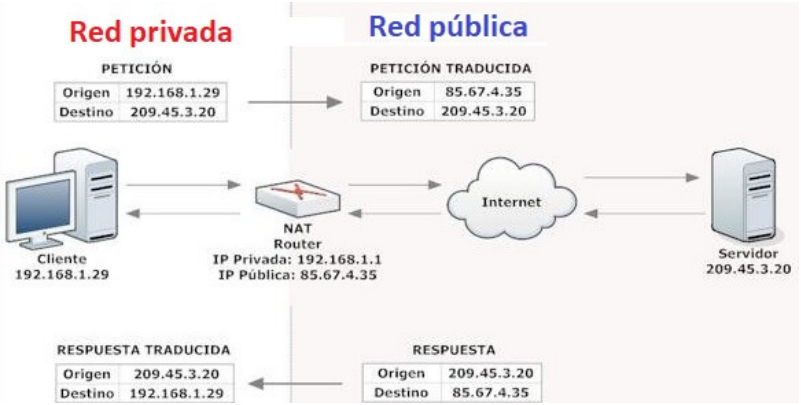

Figura 5.2: Network Address Translation.

Por esa razón, hoy en día no existen un número suficientemente grande de IPs públicas para el número de dispositivos que existen. Debido a ello se plantearon diferentes soluciones al respecto y finalmente se decantó por implementar el protocolo NAT. Este protocolo se propuso como una solución para que todos los dispositivos de una misma red pudiesen navegar por internet, utilizando una o un grupo muy reducido de IPs públicas para ello.

Las redes domésticas utilizan una única IP pública establecida por el proveedor de servicios para salir a internet, y es el Gateway el encargado de hacer las traducciones de IP privada a IP pública y viceversa. [6]

Existen 3 tipos de NAT:

Tipos de NAT	Descripción
Nat estática	Se mapea una dirección IP privada con una dirección IP pública de forma estática, de manera que una IP privada siempre deberá estar casada con una IP pública.
Nat dinámica	Mejora varios aspectos respecto la NAT estática, ya que ahora no casaremos una dirección IP privada con una IP pública, sino que tendremos disponibles un pool de IP públicas para direccionar un pool de IP privadas de forma dinámica y a demanda. Ejemplo: si tenemos 5 IPs públicas y 10 IPs privadas, las 5 primeras máquinas que quieran conectarse a internet podrán hacerlo, y el resto deberá esperar hasta que se libere alguna IP pública del pool de IPs.
Nat con sobrecarga (PAT o Port Address Translation)	Es el caso de NAT más utilizado, sobretodo en los hogares, en este caso no dispondremos de un pool de IPs públicas, sino que tendremos 1 única IP pública para mapear todas las IPs privadas. Esto funciona de la manera que requiere del uso de puertos de conexión, así podremos mantener conexiones simultaneas mapeando a distintos puertos de conexión.

Figura 5.3: Tabla de los tipos de NAT.

5.2. Conceptos sobre sistemas IT

5.2.1. Diseño basado en duplicación vs basado en replicación

Un sistema centralizado se basa en que todos los usuarios se conectan a un único punto para utilizar un servicio, como, por ejemplo: iniciar sesión en un dominio o acceder a un servidor de datos compartido. Un sistema basado en replicación implica que cada oficina tenga la misma configuración a nivel de servidores.

Tipo	Ventajas	Desventajas
Centralización	• Facilitar la gestión de la información. Hacer un cambio a nivel de dominio, AD, etc. Se realiza en un único punto. • Permite ahorrar costes a nivel de servidores y almacenamiento. • Evitar duplicar la información y puntos de amenaza.	• Tener los servicios unificados en un mismo punto hace que la disponibilidad sea indispensable. Si el servidor que ejecuta el servicio cae, dejará sin trabajar a todos los usuarios. • Mayor consumo del ancho de banda. • Existe un único punto donde se almacena los activos de la empresa.
Replicación	• Mejora de rendimiento respecto a la centralización. • Reducción del consumo del ancho de banda. • Previene en cierta manera la perdida de información.	• Costes muchos mayores al tener que replicar la infraestructura de servidores. • Aumenta el número de puntos de amenaza.

Figura 5.4: Ventajas y desventajas de los modelos.

5.2.2. Nomenclatura estándar a nivel de servidor

A nivel de servidor, se suele asignar el nombre al equipo en función del rol que vaya a desarrollar. Para ello, se suele utilizar una nomenclatura estándar:

(Empresa)(Servidor)(id del servidor)

Estos son los identificadores de los servidores más utilizados:

- DC ->Domain Controller
- FS ->File Server
- SQL ->SQL Server
- BKP ->Backup Server
- RDP ->Remote Desktop Server

5.2.3. Diferencias entre una OU y un grupo en Active Directory

Una Unidad Organizativa (OU) es un contenedor donde se almacenan los objetos típicos que se encuentran dentro de un AD, como por ejemplo usuarios, grupos de usuarios, equipos u otras OU del dominio. Estas OU se utilizan para agrupar y organizar objetos para así, delegar derechos administrativos sobre ellos y aplicar *Group Policy Object* (GPOs) en cada OU. [15]

Un grupo es un conjunto de usuarios en los cuales se puede definir una serie de permisos específicos. Los permisos básicos son de escritura, lectura y ejecución.

Tanto una OU como un grupo sirve para agrupar usuarios, pero básicamente la diferencia es que agrupar estos usuarios en OU sirve para aplicar GPOs concretas para el contenedor al que pertenecen, en cambio, un grupo sirve para dar ciertos privilegios a un conjunto de ellos.

Ejemplo: Una GPO del dominio definirá que a todos los usuarios del dominio se les defina el mismo fondo de escritorio, mientras que, el grupo de desarrolladores no tendrá acceso a las carpetas de Administración.

5.3. Vocabulario básico sobre seguridad

Durante toda la memoria se han utilizado términos relacionados con la seguridad, por esa razón se ha adjuntado una serie de conceptos con su correspondiente significado:

- **Firewall:** Sistema de hardware que separa nuestra red interna de la red externa y se encarga de hacer filtraje de paquetes y aceptar las conexiones entre los puertos de conexión de 2 equipos.
- **IPS:** Intrusion Prevention System. Hardware que hace de barrera entre el router y el *Firewall* para prevenir ataques a nuestra red interna.
- **IDS:** Intrusion Detection System. Hardware que hace de barrera entre el router y el *Firewall* para prevenir ataques a nuestra red interna.
- **Botnet:** Una red de equipos zombi o *bots* los cuales han sido infectados previamente y tienen el objetivo que en cuanto el equipo líder de la orden, realizar un ataque de DDoS.
- **DDoS:** (*Distributed Denegation of Services*) Un ataque de denegación de servicios consiste en hacer peticiones de solicitud a una web o servicio en masa con el objetivo de que el equipo no pueda gestionar todo el tráfico de golpe y finalmente acabe haciendo caer el sistema.
- **CIA:** Las siglas de los 3 objetivos de la ciberseguridad (Confidentiality, Integrity and Avaiability).
- **Insider:** Personal interno de la empresa que filtra información fuera de ella sin autorización o provoca problemas dentro de una organización. Se considera amenaza máxima dentro de una empresa.
- **Ransomware:** Es un software malicioso que tiene el objetivo de encriptar los datos de un equipo para pedir un rescate por la clave de desencriptación.

Apéndice A

Manual técnico

A.1. Requerimientos para la ejecución del proyecto virtualizado

Para la ejecución de la parte virtualizada del proyecto, se ha utilizado la versión 2.2.7 del emulador GNS3[16], juntamente con la versión 6.1 del software de virtualización VirtualBox[17].

Para este proyecto se requerirá la descaga y la instalación previa de las siguientes VM:

- VM Windows 7 - 50 [12].
- VM Windows 7 - 51 [13].
- VM Windows Server 2012 R2 - TFGDC01 [10].
- VM Windows Server 2012 R2 - TFGDC02 [11].
- Proyecto GNS3 [14].

A.2. Como ejecutar

Per ejecutar el proyecto se deberá seguir una serie de pasos:

1. Descarregar los ficheros adjuntos en la sección anterior.
2. Importar las 4 VM al VirtualBox.
3. Mover el contenido del archivo zip GNS3 descomprimido a la carpeta donde se tenga instalado el software. Por defecto la ruta en OSX es /Users/user/GNS3 y en entorno Windows es C:\Users\user\GNS3.
4. Abrir el proyecto de GNS3 y ejecutar todos los elementos disponibles.

A.3. Nota

En el caso de querer iniciar sesión dentro del dominio, se adjunta una lista con los usuarios disponibles:

- administrador - Patata123456
- admin01.BCN - Patata123456
- admin02.BCN - Patata123456
- gerente01.BCN - Patata123456
- gerente02.BCN - Patata123456
- developer01.BCN - Patata123456
- developer02.BCN - Patata123456
- TI01.BCN - Patata123456
- TI02.BCN - Patata123456
- admin01.MDR - Patata123456
- gerente01.MDR - Patata123456
- developer01.MDR - Patata123456
- TI01.MDR - Patata123456

Aunque establecer la misma contraseña para todos los usuarios del dominio vaya contra las reglas básicas de la ciberseguridad para la protección de la información, se ha decidido configurar los usuarios de esta forma para así facilitar la ejecución de la parte virtualizada.

Bibliografía

[1] *15 consejos de seguridad informática para el día a día*, https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/.

[2] *Adaptadoro usb-c to ethernet*, https://www.amazon.es/Belkin-F2CU040btBLK-Adaptador-Gigabit-Ethernet/dp/B014FBQ738/ref=sr_1_3?__mk_es_ES=ÅMÅ\begingroup\let\relax\relax\endgroup[Pleaseinsert\PrerenderUnicode{Åi}intopreamble]~O~N&dchild=1&keywords=ethernet+belkin+usb+c&qid=1590670525&sr=8-3.

[3] *Agotamiento de las direcciones ipv4*, https://openwebinars.net/blog/agotamiento-de-las-direcciones-ipv4/, Autor: Alberto Molina.

[4] *Checking ad group membership from a batch file*, https://slecluyse.wordpress.com/2011/05/15/checking-ad-group-membership-from-a-batch-file/, Autor: Slecluyse.

[5] *Clúster servidor de archivos*, https://www.jmsolanes.net/es/cluster-servidor-de-ficheros/, Autor: Josep Ma Solanes.

[6] *Configurar red nat*, https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/, Autor: Leandro Di Tommaso.

[7] *Configure static route - gns3*, https://www.9tut.com/configure-static-route-gns3-lab.

[8] *Connect gns3 to lan and internet*, https://www.youtube.com/watch?v=BA1oubidWbU, Autor: Jared Swets.

[9] *Curso de windows server 2012 r2*, https://www.youtube.com/watch?v=fY2948ZFlqc&list=PLn5IkU1ZhgiZtUlWXcCfzHp61NIf8coQ5&index=1, Autor: JGAITPro.

[10] *Descargar ova tfgdc01*, https://mega.nz/file/66wRkTKD#tvnzaMNTNIBk5aqSXsiSGG8TV0RofxAvA4kJnwxdDYk.

[11] *Descargar ova tfgdc02*, https://mega.nz/file/z7olXJRa#qsKEpIpSD4wtaHAYkapTJuiRGkxO85hUNMETgWcOqXU.

[12] *Descargar ova win7-50*, https://mega.nz/file/LzphBYSC#c3kmxeEBb6zZ8ObtAXGe72R3G5BCrPKKVmF1RYNcwEY.

[13] *Descargar ova win7-51*, https://mega.nz/file/LuxR3Z6L#boNRU6jbhKrJGdYpExH-heHBxFrspcOtRhAfhECfu94.

[14] *Descargar proyecto gns3*, https://mega.nz/file/7ygzkaTY#JXUOeFErlkwrZt8Yhg8khn1sjOOFnH013qCRYynWSLc.

[15] *Diseño de las unidades organizativas*, https://www.adrformacion.com/knowledge/administracion-de-sistemas/definicion_de_unidades_organizativas_en_un_servidor.html, Autor: Jose Mª Rodríguez.

[16] *Download gns3 2.2.7*, https://www.gns3.com/software/download.

[17] *Download virtualbox 6.1*, https://www.virtualbox.org/wiki/Downloads.

[18] *Frame relay*, http://informatica.uv.es/iiguia/AER/Tema9.pdf, Autor: Estudiante de informática de la UV.

[19] *Frame relay configuration*, https://www.packettracernetwork.com/tutorials/framerelay.html.

[20] *La amenaza de los insiders en ciberseguridad*, https://medium.com/@Fernando_Mateus/la-amenaza-insider-en-ciberseguridad-riesgo-percibido-vs-riesgo-real-af80053e7c Autor: Fernando Mateus.

[21] *ransomware wannacry*, https://www.kaspersky.es/resource-center/threats/ransomware-wannacry.

[22] *Redes corporativas para grandes empresas*, https://www.movistar.es/grandes-empresas/soluciones/fichas/wan-lan/.

[23] *Resolución de nombres netbios*, https://windowserver.wordpress.com/2011/03/18/resolucin-de-nombres-de-mquina-dns-wins-etc/, Autor: Guillermo Delprato.

[24] *What is a honeypot?*, https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot.

[25] *What is a vpn*, https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/, Autor: Chris Hoffman.

[26] National Research Council, *Computers at risk: Safe computing in the information age*, Technology to Achieve Secure Computer (1991), 75–84.

[27] Joel Thomas Langill Eric D. Knapp, *Industrial network security*, Chapter 10 - Implementing Security and Access Controls (2015), 283–322.