UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería de Telecomunicación

Implementación de un sistema de monitorización y gestión de un centro de datos

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

AUTOR/A: Palomares Salvador, Diego

Tutor/a: León Fernández, Antonio

CURSO ACADÉMICO: 2022/2023

Resumen

Toda la tecnología que conocemos ha avanzado y sigue avanzando de una forma muy rápida, lo que ha requerido que todos nosotros estemos a la altura y nos adaptemos a todos los cambios que han surgido en nuestras vidas. Una parte importante se les atribuye a las empresas, que también han tenido que cambiar su forma de trabajar para ser accesible a todo el mundo y llegar al máximo número posible de personas. Estas empresas han tenido que adaptar su manera de influir en nuestro mundo cambiando algunos medios y tecnologías dentro de ellas.

Un claro ejemplo son los centros de datos que tienen las empresas y la importancia de la organización dentro de ellas. Una forma muy cómoda para tener todo bajo nuestro control es virtualizando toda la información. Para ello, el monitoreo de los diferentes elementos y dispositivos en una empresa puede llegar a ser vital para su organización, de forma que, viendo sólo una pantalla, puedas saber qué está fallando entre todas tus pantallas, puertos, cableados u otros dispositivos monitoreables y cómo arreglarlos de una forma rápida, efectiva y segura.

Resum

Tota la tecnologia que coneixem ha avançat i continua avançant d'una forma molt ràpida, la qual cosa ha requerit que tots nosaltres estiguem a l'altura i ens adaptem a tots els canvis que han sorgit en les nostres vides. Una part important se'ls atribueix a les empreses, que també han hagut de canviar la seua manera de treballar per a ser accessible a tothom i arribar al màxim nombre possible de persones. Aquestes empreses han hagut d'adaptar la seua manera d'influir en el nostre món canviant alguns mitjans i tecnologies dins d'elles.

Un clar exemple són els centres de dades que tenen les empreses i la importància de l'organització dins d'elles. Una forma molt còmoda per a tindre tot sota el nostre control és virtualizando tota la informació. Per a això, el monitoratge dels diferents elements i dispositius en una empresa pot arribar a ser vital per a la seua organització, de manera que, veient només una pantalla, pugues saber què està fallant entre totes les teues pantalles, ports, cablejats o altres dispositius monitoreables i com arreglar-los d'una forma ràpida, efectiva i segura.

Abstract

All the technology we know has advanced and continues to advance in a very fast way, which has required all of us to keep up with and adapt to all the changes that have arisen in our lives. An important part of this is attributed to companies, which have also had to change the way they work in order to be accessible to everyone and reach as many people as possible. These companies have had to adapt their way of influencing our world by changing some of the means and technologies within them.

A clear example is the data centers that companies have and the importance of the organization within them. A very comfortable way to have everything under our control

is virtualizing all the information. For this, the monitoring of the different elements and devices in a company can become vital for your organization, so that, seeing only one screen, you can know what is failing among all your screens, ports, wiring or other monitorable devices and how to fix them in a fast, effective and safe way.

Índice

Capítulo 1. Introducción

En este primer punto se desarrollará una breve introducción al proyecto, exponiendo una base que sirva de contexto para una mejor comprensión del proyecto realizado, además de listar los objetivos y explicar la estructura que hemos seguido en la memoria.

Este proyecto ha sido realizado en coexistencia con mi periodo de prácticas extracurriculares en el departamento de redes de la empresa Nunsys SA (Figura 1), situada en el Parque Tecnológico de Paterna, una empresa especializada en la implantación de soluciones integrales de tecnología. Realiza proyectos de Transformación Digital, Ciberseguridad, Industria 4.0, Comunicaciones, Sistemas, Software, Audiovisuales y Formación, dirigidos tanto a empresas privadas como a entidades públicas.[1]

Figura 1. Edificio HQ de Nunsys en el Parque Tecnológico de Paterna

La globalización del mercado, el desarrollo de nuevas tecnologías, el crecimiento de la empresa, la organización y necesidades que debe tener una empresa de estas características… Debido a estas y más razones, un proyecto que resulta bastante interesante en esta empresa es el monitoreo de su centro de datos, precedido de un correspondiente estudio que nos permita realizar el proyecto de la manera más adecuada posible y que una vez se haya finalizado el trabajo, los propios empleados de la empresa puedan utilizarlo sin ningún problema y de una forma relativamente sencilla. Dicho proyecto fue elegido debido a que podría ser una ayuda considerable tanto en el avance y desarrollo de Nunsys como en el trabajo diario de oficinistas y técnicos, además de favorecer un buen clima de trabajo. Ya no será necesario buscar y recopilar información y anomalías en el estado de los dispositivos que tenemos a nuestra disposición manualmente, si no que podremos detectar todo esto de una forma rápida y automática que nos permitirá ahorrar tiempo y, en ocasiones, dinero y problemas que puedan surgir al no encontrar estos posibles fallos.

1.1 Contexto

Es indudable que durante los últimos años las empresas del sector tecnológico han experimentado un notable desarrollo tanto en su hardware como en su software. Este hecho ha puesto de manifiesto la necesidad de crear un sistema de organización que permita a todos los trabajadores de estas empresas realizar sus tareas diarias de la forma más sencilla, dinámica y eficiente posible, teniendo en cuenta factores como el tiempo del que dispone cada uno de ellos y exprimiendo todas las posibilidades que nos ofrece la tecnología hoy en día. Debido a esto, se deben buscar soluciones y alternativas que fomenten el crecimiento de la empresa, colaborando con personas que ayuden a este desarrollo de una forma favorable y productiva.

Para ello, se ha llevado a cabo este proyecto que consta en el monitoreo del Centro de Procesamiento de Datos (‘CPD’) de la empresa Nunsys SA. A continuación, vamos a explicar ciertos conceptos que pueden resultar poco habituales para las personas que no se dediquen a este sector y que son necesarias para entender el desarrollo de este trabajo.

Aprovechando que este proyecto se basa principalmente en el propio **monitoreo** procederemos a dar significado a este término. Su origen se encuentra en ‘monitor’, un aparato que toma imágenes de instalaciones filmadoras o sensores y que permite visualizar algo en una pantalla. [2]

Según la RAE, monitorear es ‘observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías’. Una conceptualización más adecuada dentro del contexto en el que se encuentra este trabajo (teniendo en cuenta que está enfocado en el Centro de Procesamiento de Datos de la empresa Nunsys) sería la que define el monitoreo como ‘el proceso continuo y sistemático mediante el cual se verifica la eficiencia y la eficacia de un proyecto a través de la identificación de sus logros y debilidades y, en consecuencia, se recomiendan medidas correctivas para optimizar los resultados esperados del proyecto’. [3]

Una vez sabemos el significado y contexto de la palabra en la que se basa el proyecto vamos a dar otra definición que puede resultar algo desconocida para ciertas personas que no estén familiarizadas con este sector. Se trata del Centro de Procesamiento de Datos, el CPD (Figura 2).

Prácticamente todas las empresas, ya sean públicas o privadas, tienen su centro de datos, bien propio o alojado en un tercero. Pero ¿qué es exactamente un CPD?

Como resumen, un **CPD** es la instalación que centraliza las operaciones y la infraestructura de TI de una organización, en la que se almacenan, procesan, tratan y difunden datos y aplicaciones. [4]

Un centro de datos suele reunir muchos servidores, tanto de procesamiento como de almacenamiento y redes, y suele tener algunos de los activos más críticos e importantes de una organización. Estas grandes instalaciones consumen mucha energía y, al reunir tantos equipos en tan poco espacio, necesitan de unos buenos sistemas de ventilación y refrigeración para mantener unas óptimas condiciones de trabajo.

Figura 2. Imagen ejemplo de Centro de Procesamiento de Datos

Según María Coppola [5], desarrolladora de la estrategia SEO para el contenido de HubSpot en español, y su blog en dicha página, los centros de datos se pueden clasificar en cuanto a su tamaño y número de instalaciones. Sin embargo, cada uno se compone por los siguientes elementos que constituyen su estructura y funcionamiento:

I. Computación

En la mayoría de las ocasiones es suministrada por servidores de alta gama y se compone por la memoria y la potencia, que favorece la ejecución de las aplicaciones del CPD.

II. Seguridad

El principal objetivo en un data center es garantizar que la información de la empresa no sea accesible a terceros a causa de desastres naturales o incendios, accesos no autorizados por la misma empresa o robos de información. Por lo tanto, la seguridad es un elemento clave.

III. Almacenamiento

Toda la información y los datos de una empresa quedan almacenados dentro del CPD. Sin embargo, no todas las entidades aseguran su información de forma física, sino que optan por un almacenamiento en la nube que cuenta con la ventaja del guardado de copias de seguridad para poder recuperar los datos cuando tienen lugar situaciones como las que se han mencionado en el apartado anterior. No obstante, el transporte de datos de esta modalidad, por lo general, es menos rentable que un almacenamiento físico.

IV. Redes

Dispositivos como enrutadores, switches o conmutadores, entre otros, son elementos que hacen referencia a las interconexiones entre los componentes del data center y el entorno exterior.

V. Software de análisis

Un software de análisis es una herramienta que, a través de funciones como el análisis predictivo, es capaz de realizar estudios estadísticos que permitan tomar mejores decisiones de cara al futuro y, por lo tanto, nos ofrece una mayor seguridad de nuestros datos.

Los centros de datos pueden ser relativamente pequeños y ocupar una sala u oficina, pero también pueden ser gigantes ocupando espacios especialmente destinados para este fin. En todos ellos la seguridad (física y lógica) y confiabilidad son dos de los aspectos más importantes y cruciales para su operación y mantenimiento [6].

A continuación, mostraremos diferentes formas de clasificar los data center atendiendo a cuestiones como su utilidad o dónde y cómo estén situados y abordaremos la cuestión de la seguridad de estos espacios [5] [7].

Esta clasificación ha sido estructurada según su nivel de disponibilidad:

Tier 1 o infraestructura básica

Este nivel de infraestructura es el más básico de todos, ya que tiene una disponibilidad de un 99,7%, esto supone un tiempo de inactividad máximo de alrededor de 28 horas anuales. Por lo tanto, podemos decir que es sensible a interrupciones, planificadas o no, que pueden afectar al flujo de datos.

Tier 2 o infraestructura de capacidad redundante

Su porcentaje de disponibilidad es del 99,74 % y ofrece una mejor protección que el nivel anterior, aunque también puede presentar interrupciones inesperadas. El componente redundante hace referencia a que cuenta con un sistema de piso elevado y generadores auxiliares.

Tier 3 o infraestructura simultánea

Este nivel de instalación no afecta al funcionamiento cuando la interrupción es planificada, sin embargo, puede haber problemas en las ocasiones no previstas y presentar paradas para mantenimiento. Su disponibilidad es del 99,98%.

Tier 4 o infraestructura tolerante a fallas

Este nivel de data center es el más alto en cuanto disponibilidad (99,99%) siendo interrumpido únicamente una vez al año durante aproximadamente 26 minutos. Este es el más resistente a fallos o contra eventos físicos

Además de esta clasificación, también podemos diferenciarlos de la siguiente forma [5]:

- **Data Center empresarial**

Este data center se encuentra localizado en un área concreta dentro de la empresa, ya que su funcionamiento se debe exclusivamente a necesidades de la misma, como el almacenamiento o la seguridad de los datos. Este tipo de data center es del que dispone la empresa con la que se ha trabajado en este proyecto.

- **Data center de colocación**

Este tipo de data center es una solución a empresas que puedan tener espacio o recursos limitados ya que permite alojar toda la infraestructura informática en las instalaciones ofrecidas por un proveedor.

- **Data Center de servicios administrativos**

Este tipo es similar al anterior con la diferencia de que además de ofrecer el espacio físico, el proveedor de este servicio se encarga también de toda la operación y mantenimiento del mismo.

- **Data Center en la nube**

La principal diferencia con los tres anteriores es que no tiene una infraestructura física, sino que todos los datos se almacenan en un espacio conocido como ‘nube’ que, por lo general, pertenece a un proveedor externo.

Aparte de toda la seguridad que requiere un CPD anteriormente mencionada y que, de alguna forma, podemos obviar, también es importante atender a este tipo de cuestiones:

Seguridad perimetral

Este tipo de seguridad hace referencia a una barrera tanto física (controles vehiculares o la propia edificación de la compañía), como tecnológica (ciberseguridad) que protege a la empresa en general.

Seguridad en instalaciones

Este tipo de seguridad es específica de la empresa en su totalidad. Se refiere al acceso a sus instalaciones por parte del personal y de otros técnicos o especialistas y, por tanto, también es un área importante de proteger antes de llegar al propio data center.

Seguridad en sala de ordenadores

Este se refiere a un sistema de seguridad más enfocado en el área exacta en la que se encuentra el propio data center para evitar el acceso no permitido y, por tanto, cualquier daño accidental o intencional. Para ello se usan sistemas de identificación y verificación.

En Nunsys, por ejemplo, se accede con un sistema de seguridad de huella biométrica, por lo que solo tienen acceso ciertas personas.

Seguridad en racks

Es la última capa de seguridad propiamente física a cubrir. Se trata del armario en el que se encuentran los dispositivos que conforman el data center. Los sistemas más utilizados para proteger esta zona van desde la videovigilancia hasta, como se ha mencionado anteriormente, la seguridad biométrica.

Una vez puesto en contexto el lugar donde llevaremos a cabo todo el proceso del proyecto, monitorizaremos todos los dispositivos y cableado que se encuentren dentro para poder examinar cuándo se detecta alguna anomalía en alguno de ellos, o incluso ver si se localiza algún contratiempo con algún cable que los una o forme parte de ellos. De esta manera, podremos resolver el problema de una forma rápida y efectiva, podremos descubrir de qué se trata exactamente con un simple vistazo a nuestra pantalla de monitoreo y ahorrar tiempo.

1.2 Objetivos

En este apartado, listaremos los objetivos planteados para lograr un proyecto realista, útil y viable, señalando también la motivación que ha ocasionado este propósito.

El objetivo principal (y sus consecuentes secundarios) son:

- Proporcionar a la empresa una herramienta que permita a los empleados detectar los dispositivos de la red corporativa de Nunsys, así como sus posibles fallos y anomalías.
    - Encontrar el software más indicado para las necesidades del proyecto a través de la búsqueda y comparación de las opciones disponibles.
    - Conocer y familiarizarnos con las características que nos brinda el software que hemos elegido

- Detectar y cubrir las necesidades que requería la empresa, tal como crear diferentes sensores para cada dispositivo que permitan conocer la disponibilidad de este en cada momento, entre otras.

Por otra parte, también me gustaría hacer mención de los objetivos personales que me he marcado durante la realización del proyecto:

- Adquirir la experiencia de trabajar para una empresa real manipulando los datos de una entidad especializada en el sector de las telecomunicaciones.
- Aprender a establecer tareas y organizar el tiempo de una forma eficiente y realista de acuerdo con el plazo límite establecido para la entrega de este trabajo.
- Aplicar mi conocimiento adquirido tanto en el grado como en las prácticas para proponer mi primer proyecto de la mano de la empresa con la que he estado trabajando durante los últimos meses, Nunsys SA.

1.3 Estructura de la memoria

Una vez introducidos el contexto y los objetivos del proyecto, procederemos a fijar la estructura que seguirá la memoria. Esta está comprendida por 6 capítulos, de los cuales, a continuación, se expone una breve descripción:

Capítulo 1. Introducción: En lo que respecta a este apartado, se introduce y se incluye todo lo necesario para dar pie a un mejor entendimiento de todo el proyecto, ayudando a comprender y contextualizar el desarrollo completo, adjuntando además la estructura de la memoria y su metodología, donde se explica la distribución de las tareas junto al famoso diagrama de Gantt.

Capítulo 2. Estudio y explicación del software empleado. Conceptos teóricos/básicos. En este capítulo se explican las herramientas utilizadas durante el proceso, cómo se han estudiado los diferentes softwares posibles que permitiesen la elaboración del proyecto y por qué se ha elegido el software correspondiente, realizando una tabla comparativa de las características principales que ofrecen estos programas.

Capítulo 3. Disposición, configuración y organización en PRTG: En este capítulo se explica de una forma más detallada la forma en la que nosotros hemos usado PRTG, cuál es la disposición del software y algunas configuraciones que han sido de utilidad para nuestro proyecto, profundizando en la interfaz.

Capítulo 4. Red de monitoreo del proyecto. En esta sección se visualiza cómo hemos organizado la red que hemos monitorizado, mostrando resultados y explicando algunas cuestiones importantes para el desarrollo de la monitorización. Además, se exponen diferentes aspectos del software que hemos optimizado con el objetivo de facilitar el trabajo y el uso de la monitorización a la empresa. Se ilustra también el entorno en el que hemos trabajado durante estos meses.

Capítulo 5. Conclusiones y propuesta de trabajo futuro: Este apartado comprende las conclusiones que hemos obtenido tras la completa realización del proyecto, además de las posibles mejoras e implementaciones a aplicar en futuros desarrollos. También se recogen algunas mejoras que hemos obtenido tras declarar los principales objetivos y que hemos podido añadir tras el trabajo realizado durante todo el proceso.

Capítulo 6. Bibliografía: Para finalizar, en esta sección se han listado las referencias empleadas durante la realización de todo el proyecto, ya sean artículos de prensa, documentos oficiales y otras fuentes de rigor.

1.4 Metodología

A continuación, describiremos la planificación que hemos seguido para la realización de este proyecto. Por un lado, veremos la distribución inicial del proyecto y, por otro, el esquema de tiempos con los periodos asignados a cada actividad propuesta.

1.4.1 Gestión del proyecto

Desde el primer momento, y debido a que este proyecto ha sido realizado dentro de una empresa, se ha necesitado el cumplimiento de algunos plazos estrictamente. Esto ha implicado reuniones constantes con Javier Furió, empleado de Nunsys que me ha ayudado y guiado en este proyecto para revisar los objetivos fijados y la evolución del proyecto.

Cabe destacar que ha sido necesaria una distribución de tareas previa a la elaboración del proyecto de tal forma que el tiempo queda dividido en: una **fase de análisis** dónde se estudian las posibles exigencias que podremos encontrarnos a lo largo del proceso; una **fase de planificación** en la que marcamos los plazos establecidos o fechas clave y metas para realizar el trabajo; una **fase de diseño** en la que comenzamos a revisar todos los objetivos necesarios para el proyecto aportando nuevas ideas que lo enriquezcan; una **fase de desarrollo** que incluye tanto la documentación previa en la materia como el estudio de software y todo el trabajo posterior, y una **fase de conclusión**.

También es importante comentar que este proyecto ha sido desarrollado con materiales y dispositivos proporcionados por la empresa, como el ordenador portátil, los dispositivos utilizados para hacer todas las pruebas previas y, obviamente, el centro de datos de Nunsys junto con todo el edificio HQ sobre el que hemos trabajado.

1.4.2 Distribución de tareas

Como podemos observar en el diagrama temporal recogido en la Figura 3, la elaboración de este proyecto se ha comprendido entre las semanas discurridas entre los meses de septiembre y febrero de 2022. En este diagrama hemos diferenciado cinco fases: Propuesta y análisis, Planificación, Diseño, Desarrollo y Conclusión. A continuación, se recoge la explicación de cada una de ellas, dando una descripción sobre su distribución, su desarrollo y el tiempo dedicado.

El periodo de tiempo entre los últimos días de septiembre y las primeras dos semanas de octubre corresponde a la **fase de Propuesta y Análisis,** durante la cual se acudió a la empresa para buscar una idea clara de proyecto. Para ello, se hizo un análisis superficial de las demandas del departamento con el fin de establecer unos objetivos a cumplir, así como en qué condiciones y con que herramientas se iba a poder trabajar en la consecución del proyecto.

Durante las siguientes dos semanas aproximadamente tuvo lugar la **fase de Planificación**. Es decir, una vez tuvimos operacionalizado todo el trabajo a realizar, se llevó a cabo una planificación temporal mediante la fijación de pequeñas metas, reuniones de control y plazos límites para organizar todo el trabajo de los siguientes meses.

La **fase de Diseño** transcurrió durante los últimos días de octubre y las primeras dos semanas de diciembre, cuando empieza el verdadero desarrollo de la estructura del proyecto. En este periodo comenzamos con una lluvia de ideas o "brainstorming" donde se revisaron los objetivos establecidos en la primera fase, se plantearon problemas, soluciones y nuevas implementaciones que permitiesen un mejor trabajo posterior. Después, se reajustaron todas las metas necesarias, los tiempos y la forma de trabajo hasta que finalmente dimos con un guion definitivo a partir del cual empezar a movernos.

La fase con más tiempo de dedicación, con un total de casi dos meses y medio, es la **fase de Desarrollo.** Durante este periodo se llevó a cabo, en primer lugar, el trabajo de documentación. Este paso es de gran importancia ya que necesitábamos obtener cierta información previa a la utilización del programa para comprender y contextualizar todos los datos que íbamos a manejar posteriormente. Una vez habíamos comprendido el material con el que íbamos a trabajar, se realizó un estudio de software para ajustar todas las funciones y herramientas que este nos brindaba a las necesidades de la empresa. A continuación, tuvo lugar la parte de pruebas y desarrollo de software, que podemos decir que es la etapa más complicada y trascendental de todo el proyecto. Esta subfase comprende todo lo relacionado con hacer monitorizables todos los dispositivos del data center, asignando sus direcciones IP dentro del software y comprobar que todo está implementado correctamente para un funcionamiento adecuado. Este trabajo está acompañado de una validación final que nos permite comprobar que todo funciona correctamente, no hay ningún fallo en el proyecto y, por lo tanto, hemos conseguido proporcionar a la empresa las facilidades que nos habíamos propuesto en los objetivos.

Para finalizar, tenemos la **fase de Conclusión**, que corresponde al último mes de trabajo y pone punto final al proyecto con las últimas correcciones por parte del tutor de la universidad. En este apartado realizamos una revisión final de todo el proyecto con los responsables de la empresa, asegurándonos que todos los objetivos han sido cumplidos e informar de algunas mejoras añadidas a estas pautas. Tras todo esto, ya es posible que los trabajadores de la empresa que lo necesiten puedan disponer de este beneficio. Solo queda hacer las correcciones necesarias en el trabajo para depositarlo en la fecha establecida.

En lo que respecta a la elaboración de la memoria podemos decir que su creación comienza desde las primeras etapas del proyecto. Desde la fase de Propuesta y análisis, ya comenzamos a escribir mientras paralelamente se proseguía con su propia realización. Mientras nos informábamos sobre todo el contexto, decidíamos los objetivos o pensábamos una metodología ya podíamos ir escribiendo según íbamos avanzando, ayudándonos de esquemas y resúmenes que contribuían al progreso del trabajo.

Por otra parte, también ha sido necesaria la creación de un fichero PowerPoint para la exposición del proyecto ante el tribunal. Este periodo se sitúa alrededor de las últimas semanas de la Conclusión y posteriores.

1.4.3 Diagrama temporal de Gantt

En este apartado se adjunta el diagrama temporal de Gantt (Figura 3). En él podemos observar el tiempo dedicado a cada una de las fases del proyecto además de contemplar las dependencias y coexistencias entre tareas.

Aunque he estado en Nunsys como estudiante de prácticas desde el pasado mayo de 2022, no fue hasta septiembre de ese mismo año cuando nos pusimos de acuerdo en realizar mi TFG en esta empresa. Desde estas fechas y hasta febrero de este mismo año con un total de 6 meses he estado realizando mi proyecto de monitorización en la empresa.

En este diagrama se ha optado por dejar únicamente el cronograma, ya que ya hemos descrito las diferentes fases en el apartado anterior. De esta forma, el lector podrá apreciar lo explicado anteriormente de una manera sencilla, clara y visual:

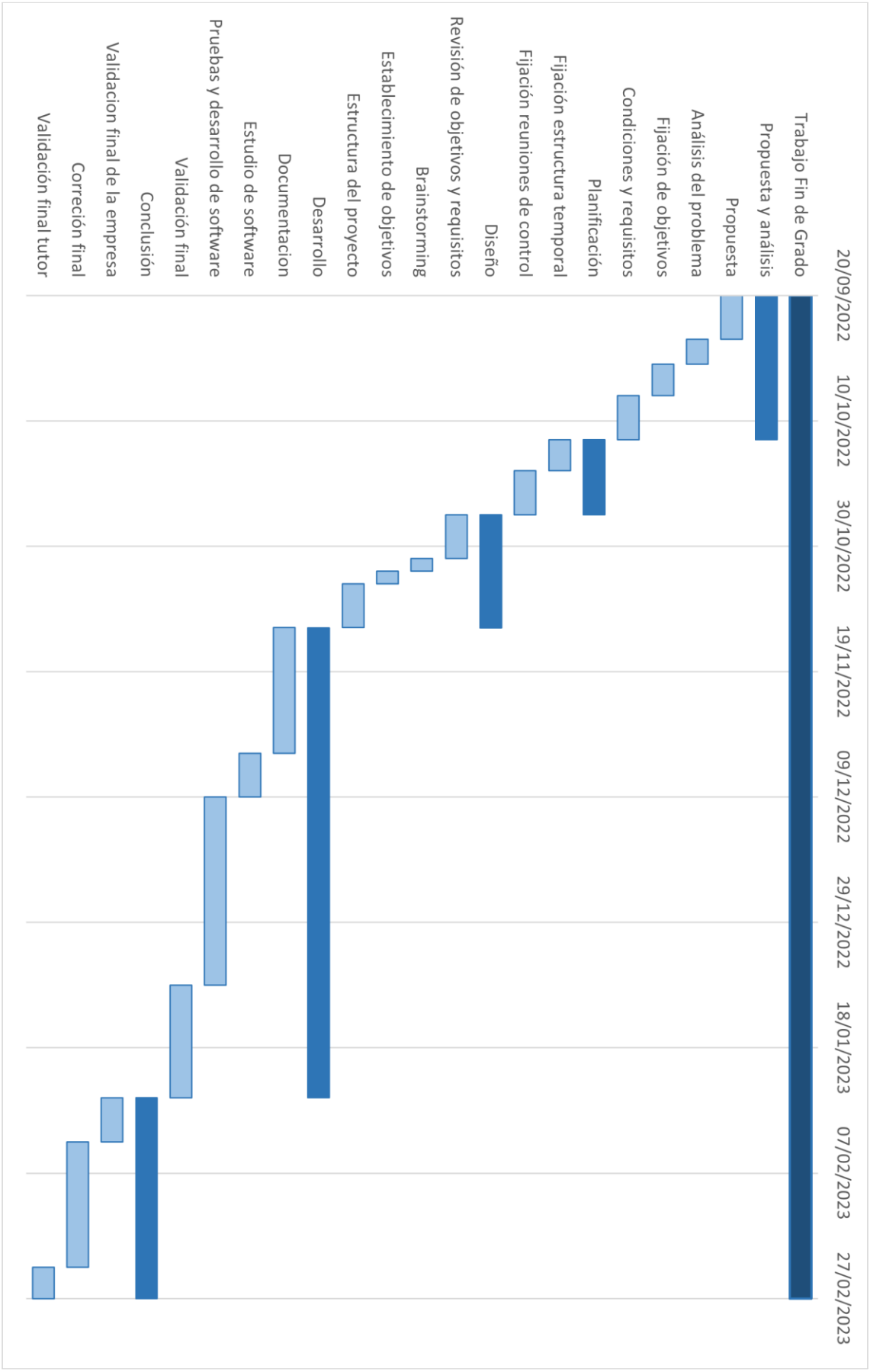

Figura 3. Diagrama temporal de Gantt sobre el tiempo empleado en cada actividad del proyecto

Capítulo 2. Estudio y descripción del software empleado. Conceptos teóricos/básicos.

Atendiendo a nuestras necesidades, requeríamos de un software que fuese capaz de gestionar las IP y administrar la infraestructura del data center de la empresa. Para nosotros, un sistema de gestión basado en IPAM era imprescindible.

'La gestión de direcciones IP' o 'IP Address Management' (IPAM) es la metodología que nos permite gestionar todo lo relacionado con IP. Todo lo que engloba el universo lógico del modelo TCP/IP. Con un IPAM puede administrar IPv4, IPv6, VLAN, Subredes, IP. Además, para cada una de estas opciones podemos asignar tags y roles junto a muchas otras opciones. [8]

En pocas palabras, IPAM es un medio para planificar, rastrear y administrar el espacio de direcciones del Protocolo de Internet (IP) utilizado en una red.

De una forma un poco más coloquial, el IPAM se puede explicar como un sistema de gestión de direcciones IP dentro de un contexto corporativo, que permite la organización, el seguimiento y el ajuste de la información relacionada con el espacio de direcciones IP.

En este capítulo describiremos cómo ha sido el proceso que hemos seguido para la elección y el estudio del software que utilizaremos durante el proyecto. Explicaremos las razones por las que lo hemos elegido por delante de otros que, aparentemente, tienen la misma función, elaborando una tabla comparativa en la que podemos observar las características que nos han hecho decantarnos por el software que finalmente hemos elegido. Además, daremos una explicación de este software, dando ejemplos, aclarando su uso y la forma en la que trabajaremos con él.

Cabe decir que estos tipos de software pueden llegar a ser muy similares en cuanto a sus características principales, pero si nos fijamos bien, los estudiamos y vemos sus utilidades dentro del objetivo general del proyecto, podemos observar que entre ellos hay diferencias que pueden llegar a ser cruciales para nuestro avance y desarrollo, con una variedad inmensa de características que en principio pueden parecer insignificantes; una vez nos iniciamos en el proyecto nos damos cuenta de que influyen más de lo que podíamos pensar. Por lo tanto, debemos saber qué software nos conviene utilizar antes de comenzar el proyecto para evitar que nuestro trabajo se quede atrás y elaborarlo de una manera eficiente.

Aunque bien es cierto que no existe el software de monitorización perfecto, sí que podemos elegir entre los más convenientes para los objetivos planteados y seleccionar el óptimo para nuestro propósito, estudiando diversos factores que puedan llegar a ser de utilidad durante la realización del proyecto. Esto nos lleva al estudio del software que emplearemos y las distintas posibilidades y elecciones de las que disponemos.

En un principio, contemplamos varios que podían encajar con nuestras necesidades tales como Netbox, PRTG, Manage Engine, OP Manager o algunos otros que finalmente decidimos descartar tras un primer vistazo. Una vez tuvimos el conocimiento necesario sobre todas estas opciones que se nos planteaban comenzamos a estudiarlas más a fondo para ver exactamente cuál se ajustaba de una forma más clara a nuestras condiciones, viendo a qué alternativa podríamos sacarle más partido.

Una de las primeras opciones que consideramos fue **Manage Engine OP Manager (Figura 4).** Este software nos proporciona muchas de las ventajas que ya podíamos

encontrar en otros que habíamos analizado anteriormente, pero las buenas valoraciones que tiene y los premios y reconocimientos que se le ha proporcionado hicieron que estuviese dentro de nuestras principales elecciones.

Algunas de las características que nos presenta Manage Engine OP Manager son: monitorización de redes en tiempo real, monitorización de servidores físicos y virtuales, umbrales multi-nivel, dashboards personalizados y monitorización de links WAN (Figura 5). Estas características principales son con las que ya contábamos y, debido a que este era un software desconocido para nosotros y del que no contábamos con la licencia, preferimos optar por otras alternativas que nos fuesen más prácticas. [9]

Figura 5. Logo comercial de Manage Engine OpManager

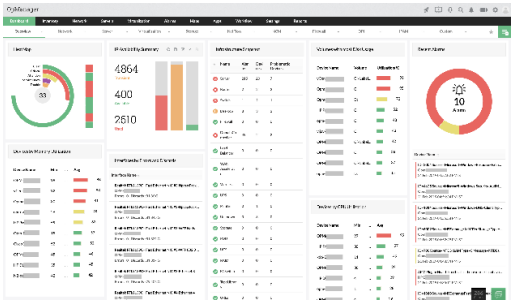

Figura 4. Captura de pantalla de un ejemplo de interfaz gráfica de Manage Engine OpManager

Otra opción que tuvimos en cuenta fue **Netbox (Figura 6)**. Esta es una herramienta de código abierto que utiliza la licencia Apache 2.0. Desde un principio ya fue un fuerte candidato para nuestro proyecto debido a sus múltiples opciones de gestión basadas tanto en DCIM como en IPAM. Netbox se basa en el enormemente popular marco Django para el lenguaje de programación Python, que ya es uno de los favoritos entre los ingenieros de redes. Los usuarios pueden aprovechar sus habilidades existentes de codificación de herramientas de Python para incrementar la funcionalidad ya amplia de Netbox a través de complementos y scripts personalizados. [8]

En un primer estudio de los posibles softwares a elegir, Netbox iba a ser la herramienta utilizada para nuestro proyecto debido a sus amplias características y las funcionalidades que nos ofrece (Figura 7), pero debido a nuestro conocimiento de Paessler PRTG nos decantamos por esta otra opción, sobre la que hablaremos más detalladamente a continuación.

Figura 6. Logo comercial de Netbox

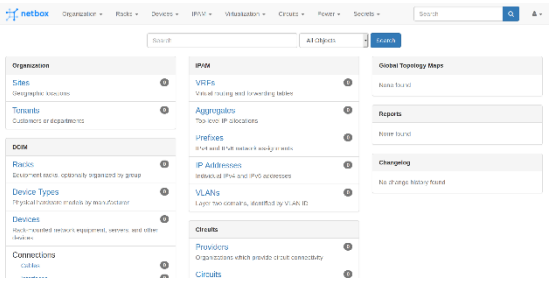

Figura 7. Captura de pantalla de ejemplo de interfaz gráfica en Netbox

Por último, y como hemos mencionado, tenemos **Paessler PRTG Network Monitor,** el software que finalmente hemos escogido para la realización del proyecto:

Tras un estudio detallado sobre qué programa podría ser una mejor opción para este trabajo y para la propia empresa decidimos que sería el Paessler PRTG Network Monitor. Esta elección se debió a diversas ventajas que presenta esta opción en nuestra situación. En un primer momento, era solamente una alternativa más, ya que el estudio realizado y las funciones y ventajas que posee lo colocaban como una de las principales alternativas. Tras seguir contemplando cual podía ser la mejor elección llegamos a la conclusión de que este sería el software que íbamos a utilizar, ya que cumplía con todas las capacidades que buscábamos y además ya era conocido tanto por mí, como por la empresa, lo que ayudó a la elección del mismo por mis supervisores en Nunsys.

Mi conocimiento sobre PRTG venía de un trabajo anterior en Nunsys mientras ayudaba y apoyaba a distintos empleados de la empresa que usaban este software. Todo esto sumado a las características que nos presenta nos convenció de tal forma que fue el elegido para nuestro proyecto.

La tabla que se muestra a continuación es una comparativa con algunos aspectos que nos han ayudado a decantarnos por este software frente a otras posibles opciones (Tabla 1).

	PRTG Paessler	**OP Manager**	**Netbox**
Conocimiento previo	La empresa ya había trabajado con PRTG. Yo había indagado un poco anteriormente.	Ni la empresa ni yo teníamos conocimiento de este software.	Nunsys sabía la existencia del software, pero nunca habían trabajado con él.
Facilidad de instalación	Gran facilidad de usar, instalar y visualizar.	Facilidad a la hora de descargar e instalar.	No se puede instalar en Windows, se necesita una máquina virtual en Linux y descargarlo e instalarlo requiere un alto nivel de complejidad.
Intuición y facilidad de uso	Facilidad a la hora de utilizar el software. Interfaz muy intuitiva y sencillez de uso.	No tan intuitivo, interfaz un poco escasa.	Software no tan intuitivo al utilizarlo por primera vez, una vez acostumbrados la facilidad de su

			uso aumenta considerablemente.
Funcionalidades	Software bastante completo en cuanto a su funcionamiento general incluyendo muchas opciones.	Programa no tan completo a la hora de monitorizar una red.	Software muy completo, incluye funcionalidades muy útiles.
Licencias	Nunsys ha adquirido la licencia más grande del software.	La empresa no dispone de ninguna licencia correspondiente a OP Manager.	Nunsys no tiene comprada ninguna licencia de Netbox.

Tabla 1. Tabla comparativa de algunas características útiles ante nuestras necesidades

Ahora describiremos más detalladamente todo lo relacionado con cuestiones técnicas que nos puedan ayudar a una mejor comprensión de las funcionalidades que nos ofrece PRTG

Como ya sabemos y para resumir todo lo relacionado con este software, **Paessler PRTG** es un software de monitorización proactiva de red capaz de monitorizar en tiempo real sistemas, dispositivos y aplicaciones. Cuando los umbrales críticos establecidos por el cliente se sobrepasan, o se produce un error, PRTG genera una alerta, creando un informe de estado completo de la infraestructura TI.

Aparte, volvería a destacar que la monitorización PRTG permite anticiparse a los problemas y resolverlos antes de que se hagan grandes. PRTG Network Monitor es una solución NMS (Network Management System) para monitorizar toda la infraestructura TI de una compañía, permitiendo tener una visión general del rendimiento y estado de la red, asegurando que todos los componentes importantes de la infraestructura IT que puedan afectar a la empresa estén disponibles. Un sistema de gestión de red o NMS, es una aplicación o conjunto de aplicaciones que permite a los administradores de red administrar los componentes independientes de una red dentro de un marco de administración de red más grande.

PRTG garantiza rendimiento, disponibilidad y el correcto uso del ancho de banda en una red IT**.** A través de la monitorización proactiva de la red, el administrador puede intervenir de forma rápida y eficaz de forma remota si el administrado no se encuentra en el lugar en el que se está produciendo el problema [10].

Las **principales ventajas** que ofrece la monitorización con PRTG y con las que hemos podido beneficiarnos en este trabajo son:

- Monitorización de ancho de banda para controlar el flujo de datos de la empresa.

- Interfaz fácil de usar (Figura 8) y configurar, incluye graficas en tiempo real (Figura 9) y reporting personalizado.

- Detección y anticipación de problema: notificación de caídas por correo electrónico o SMS.

- Amplia selección de sensores (más de 200 tipos), puede llegar a gestionar 100 sensores con la versión gratuita.

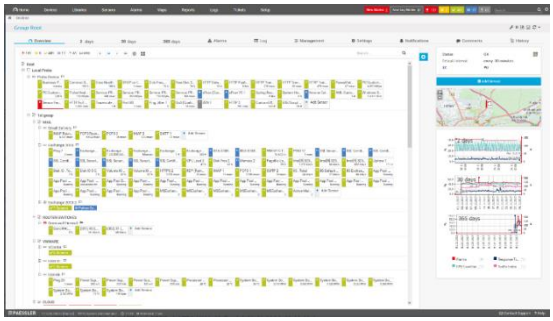

Figura 8. Ejemplo de interfaz en PRTG Paessler Network Monitor con sensores programados

Figura 9. Ejemplo de gráficas PRTG Paessler Network Monitor

Otras ventajas que resultan igual de interesantes son la administración remota a través de navegador web o dispositivos móviles y el soporte de todos los métodos comunes de adquisición de datos de utilización, como el servicio SNMP.

En el caso de Nunsys, la empresa tiene contratada la licencia más grande que nos ofrece el software, con la que no nos tenemos que preocupar nunca de la cantidad de dispositivos o sensores que monitorizamos. Ya no solamente para ellos mismos, sino que también “alquilan” estos sensores para empresas cliente que los necesitan.

Nunsys tiene un servidor local con el que puede administrar equipos que se encuentren en otra empresa. Es por esto por lo que la entidad cubre los servicios de monitorización de otros negocios que actúan como cliente, gestionando sus dispositivos mediante una sonda remota que permite el acceso a estos equipos (Figura 10).

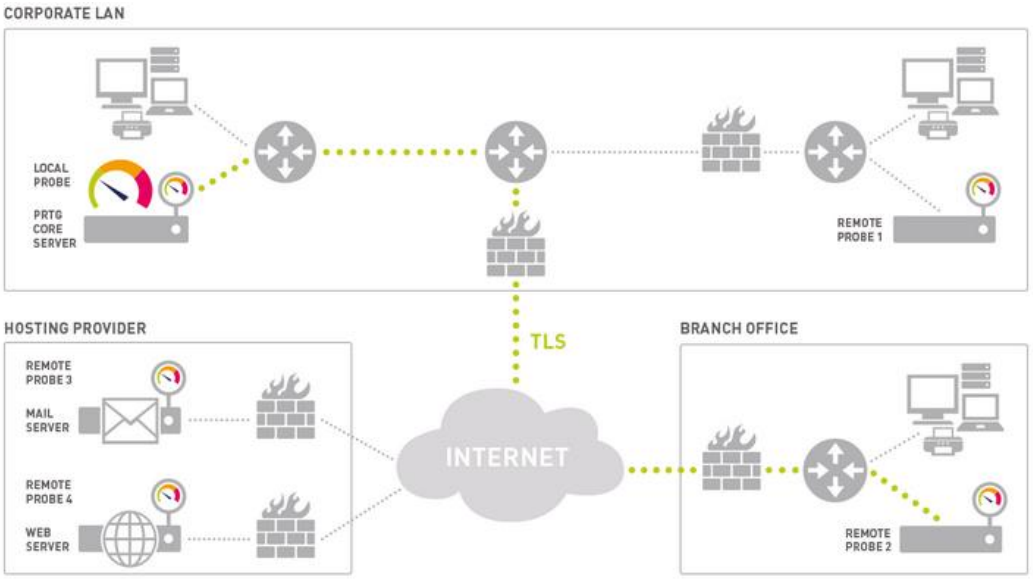

Figura 10. Esquema de sondas locales y remotas administradas por un servidor principal

Para una monitorización de cada dispositivo son necesarios sensores con lo que podamos visualizar el tipo, el estado y algunas características de estos dispositivos. Un sensor puede monitorizar un servicio de red, una URL, un puerto de un switch, la memoria de un disco o la ocupación de una CPU, entre otras muchas opciones. Así, si el software detecta alguna anomalía en alguno de estos nos avisará mediante las alarmas configuradas.

En el siguiente capítulo, pasaremos a explicar más detalladamente todo lo relacionado con PRTG y nuestra configuración dentro del software.

Capítulo 3. Disposición, configuración y organización en PRTG

En este capítulo describiremos cómo funciona la configuración en PRTG y veremos además como hemos organizado la interfaz en base a nuestras necesidades mientras mostramos con ejemplos prácticos a modo de tutorial básico la forma que hemos tenido de organizar ciertas opciones que nos ofrece Paessler en su software.

3.1 Descubrimiento automático de PRTG

En primer lugar, vamos a hablar sobre la opción de descubrimiento automático que ofrece PRTG nada más abrir el programa. Esta es una herramienta útil que nos permite escanear un rango específico de direcciones IP y agregar automáticamente los dispositivos que encuentra a su supervisión. Una vez termine este proceso, podemos modificar la lista, agrupar dispositivos o crear mapas de red fáciles de leer. Esta opción permite también programar el descubrimiento automático para que se repita cada cierto tiempo, según la frecuencia y el tipo que decidamos (Figura 11).

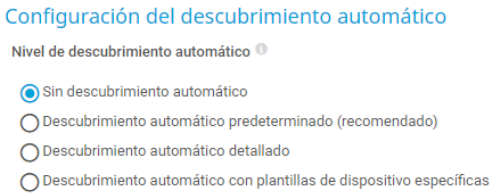

Figura 11. Cuadro de selección de tipo de descubrimiento automático

PRTG también cuenta con paneles de control personalizables que clasifican sus dispositivos de red en listas ordenadas automáticamente. Esto puede llegar a ser útil en el propio descubrimiento automático ya que, una vez terminado, clasifica los dispositivos según su tipo, procedencia o sistema operativo. Puede clasificar ordenadores, distinguiendo además entre su sistema operativo, impresoras, servidores, etc. Una vez hemos realizado el descubrimiento automático, la interfaz se muestra de la siguiente forma en nuestra pantalla (Figura 12).

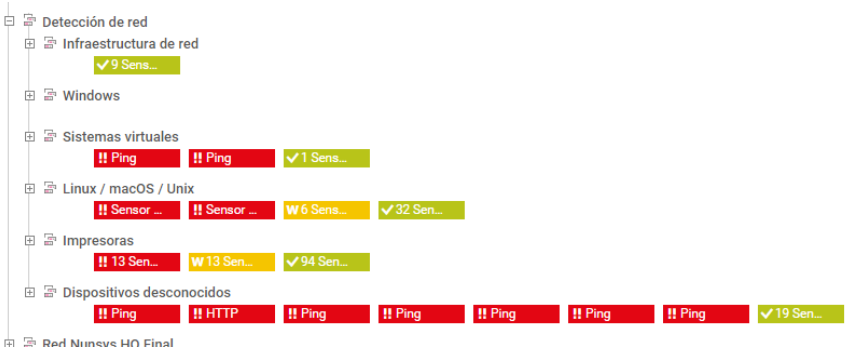

Figura 12. Clasificación de los dispositivos de nuestra red tras el descubrimiento automático

Como podemos ver en la imagen anterior, este descubrimiento se añade con el nombre de 'Detección de red', clasificando los diferentes dispositivos que detecta en grupos adaptados para cada uno de ellos. En nuestro primer descubrimiento automático el

resultado ha sido este, pero la empresa nos pidió algo un poco más elaborado y con unas características propias.

3.2 Disposición de PRTG

En este apartado hablaremos de todo lo relacionado con la disposicion general que presenta PRTG y como podemos movernos por la interfaz. Veremos gran parte de las opciones de configuración de las que disponemos mientras mostramos con ejemplos propios del proyecto cómo hemos configurado algunas de estas funcionalidades.

A continuación, explicaremos brevemente las pestañas más importantes de la interfaz del software.

3.2.1 Página principal

Nada más entrar con nuestro usuario y contraseña nos aparece la Página Principal (Figura 13). Lo que más nos llama la atención es la información general de todos los sensores que tenemos activos, estén en estado de fallo, advertencia, en pausa o en estado de OK, creando una gráfica que nos ayuda a echar un vistazo rápido de todo nuestra red. También nos crea otra gráfica automáticamente de los sensores que nos están dando algún tipo de problema (Figura 13).

Además, en la parte superior, podemos observar una fila con diferentes ubicaciones en las que clickar, de la que destacan, mirando de izquierda a derecha, 'Dispositivos', 'Sensores', 'Mapas'y 'Configuración'.

Figura 13. Página principal y gráficas estado de los sensores

3.2.2 Dispositivos

En esta pestaña podemos observar todos los dispositivos que hemos encontrado o que hemos añadido a nuestra red con sus respectivos sensores. Aquí podemos encontrar la información necesaria para saber cuáles están en funcionamiento y cuáles están dándonos algún tipo de error.

En este apartado también tenemos un símbolo '+', con el que, clicando sobre él podemos ver cinco opciones más donde podemos añadir: una sonda remota, un grupo en el que se añaden los dispositivos y sensores manualmente, un grupo automático en el que se hace

un descubrimiento sobre un rango de IPs que se indique, un nuevo dispositivo o un sensor (Figura 14).

Por defecto, esteremos en la parte de 'Resumen'. A su derecha podemos ver diferentes pestañas que muestran gráficas en base a diferentes periodos de tiempo que han estado activos los dispositivos.

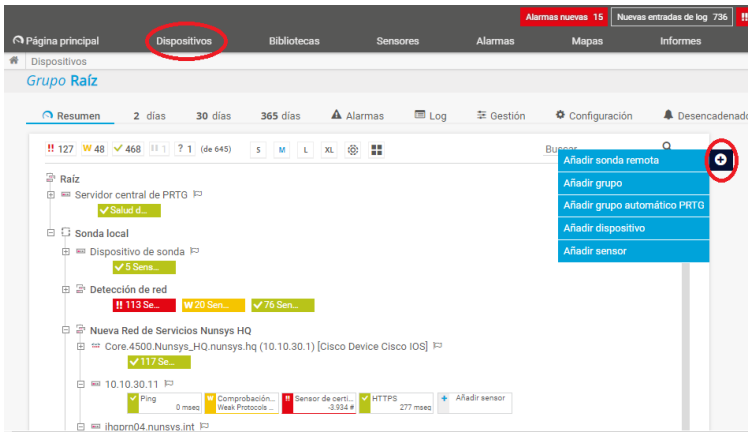

Figura 14. Vista general de la pestaña Dispositivos

3.2.3 Sensores

Si pinchamos en la pestaña de 'Añadir sensor' encontramos todos los tipos de sensores con los que podemos trabajar. Lo primero que nos aparece en pantalla son tres preguntas que nos pueden servir como orientación sobre qué sensor queremos elegir (Figura 15). Estas cuestiones nos sirven de orientación, pudiendo responder a todas ellas o solamente a las que consideremos según cual sean nuestras necesidades. Después, el propio software nos lleva hacia unos sensores u otros. Esto puede ser útil para cuando estamos empezando y no tenemos claro qué nos puede venir bien en cada caso y en cada dispositivo.

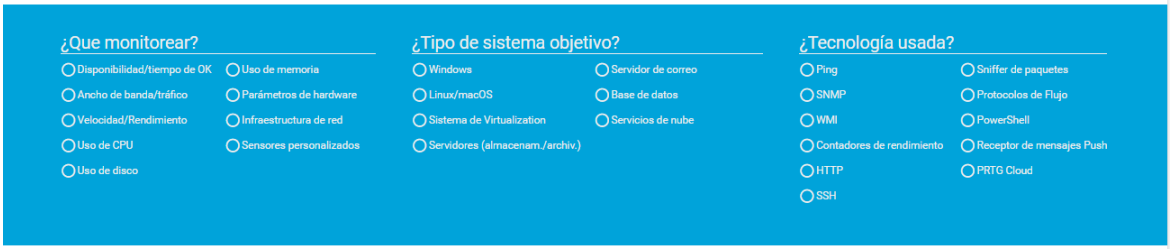

Figura 15. Preguntas de orientación sobre los sensores*

Una vez PRTG nos haya guiado a partir de las preguntas mencionadas anteriormente o bien hayamos buscado un sensor por nuestra cuenta, nos aparecen todas las opciones con una breve descripción y marcándonos el nivel de impacto al rendimiento que tendrá si lo añadimos a nuestra red, yendo de verde a rojo de una forma bastante intuitiva (Figura 16).

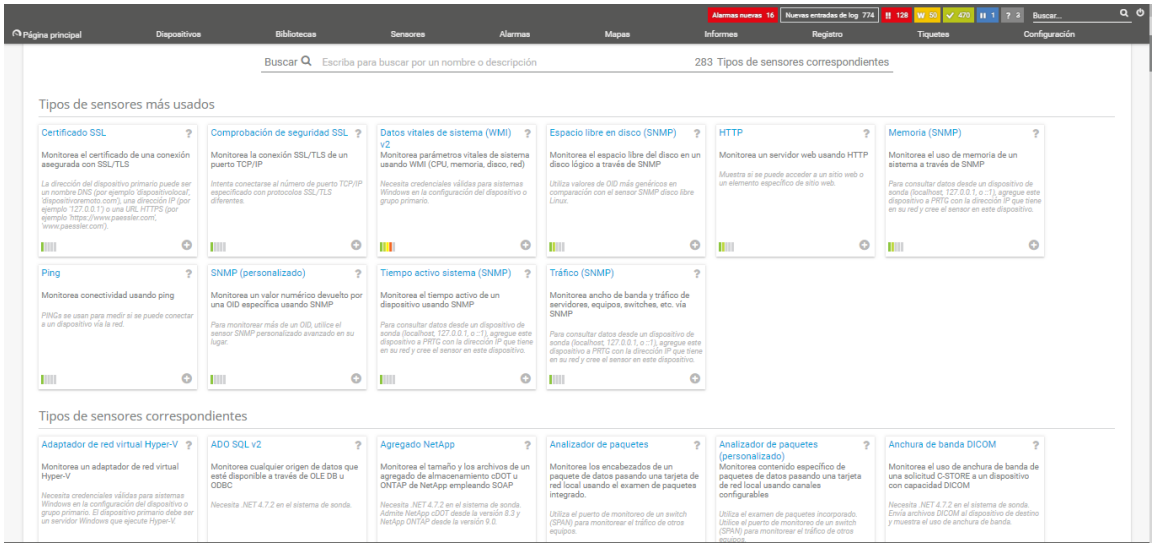

Figura 16. Vista general de los sensores disponibles

3.2.4 Mapas

Un poco más a la derecha, siguiendo la línea de las pestañas principales, tenemos la parte de 'Mapas'. En esta sección podremos ver o crear mapas a nuestro antojo con los que podremos veremos nuestra red de una forma más clara y visual. Podemos añadir u ordenar como prefiramos la forma en la que se muestran nuestros dispositivos, crear gráficas que nos ayuden a visualizar nuestra red o mostrar cómo están conectados estos dispositivos. Antes de crear ningún mapa, nos aparecen dos ejemplos que son generados automáticamente, de esta forma podemos hacernos una idea de todas las posibilidades que tenemos.

Figura 17. Magic Map generado automáticamente

Este mapa (Figura 17) es un mapa generado automáticamente por PRTG. Se corresponde con una proyección solar de los estados de los sensores de la red. Dentro de estos mapas puedes insertar cualquier tipo de imagen con la que apoyarte para realizar mapas más útiles y versátiles. Algunas de las opciones más interesantes que podemos encontrar dentro del creador de mapas son: anillos de estado, listas top 10 de características que pueden llegar a ser importantes conocer para ciertos aspectos, gráficos correspondientes a 2, 30 o 365 días de sensores que nosotros elijamos, entre otras.

3.2.5 Configuración

En la pestaña de 'Configuración' (Figura 18) podemos encontrar un gran número de opciones entre las que destacan la configuración para el envío de notificaciones, configuración de horarios (donde podemos gestionar programaciones para realizar pausas en el monitoreo) o la información de licencia (donde podemos ampliar la nuestra en el caso que se requiera).

El resto de configuración es bastante accesible ya que cada opción nos ofrece una breve descripción de su uso.

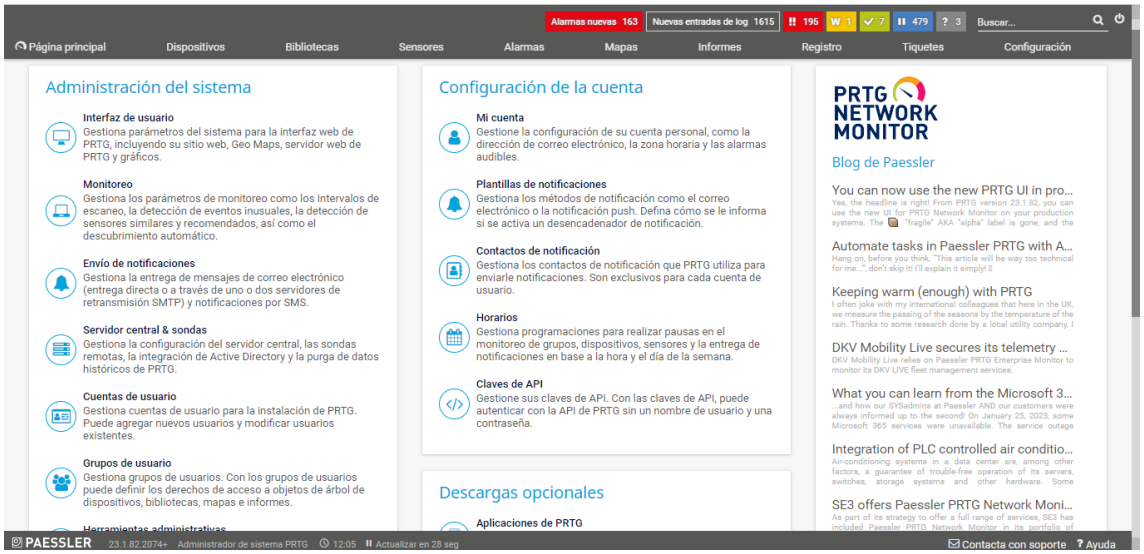

Figura 18. Vista general de la pestaña Configuración

3.2.6 Alerta y notificaciones

En PRTG también existe un sistema de alertas que nos permite configurar y personalizar cómo y por qué queremos recibir alertas. Podemos crear alertas sobre todos los sensores y todos los dispositivos que tenemos en nuestra red eligiendo cuál queremos que sea el desencadenante del fallo, durante un tiempo que nosotros determinemos y qué tipo de notificación queremos recibir. Además, podemos programarlo para que según cual sea el fallo, el sensor se quede en un estado u otro. Más adelante explicaremos más detalladamente el funcionamiento de estas y pondremos un ejemplo dentro de nuestra red.

Capítulo 4. Red de monitoreo del proyecto

En este capítulo procederemos a describir cómo es la red que hemos utilizado para la monitorización. En mitad de la realización del proyecto, el departamento de redes de Nunsys se trasladó a un nuevo edificio que no contaba con un Centro de Procesamiento de Datos, por lo que la monitorización se llevó a cabo en un edificio situado a escasos metros que pertenece a la misma empresa.

Este punto está dividido en dos secciones. Por una parte, comentaremos nuestro entorno en el que hemos trabajado para después explicar todo lo referente a la propia monitorización.

4.1 Nuestro entorno de trabajo

Durante este apartado vamos a mostrar cuál y cómo ha sido el entorno en el que hemos desarrollado nuestro proyecto. Este se ha centrado en el edificio HQ de Nunsys (Figura 1) situado en el Parque Tecnológico de Paterna. Este edificio cuenta con 2 plantas habitables en las que se da conexión a múltiples dispositivos de la empresa y donde gran cantidad de empleados los utilizan para hacer su labor a diario.

Nosotros hemos estado trabajando en la sala de comerciales situada en la primera planta (Figura 19), desde donde hemos realizado la monitorización completa.

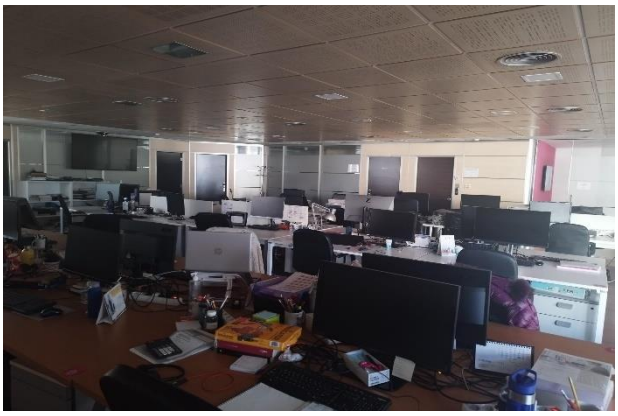

Figura 19. Imagen de la sala central de trabajo

Además de monitorizar remotamente los dispositivos necesarios y que posteriormente veremos detalladamente, también necesitábamos trabajar desde los armarios en los que se encuentran los switches monitorizados. De esta forma, podíamos ver físicamente los dispositivos con los que estábamos trabajando.

A continuación, mostramos el pequeño CPD de la planta de comerciales (Figura 20). En este tipo de salas se requiere siempre una normativa estricta que proteja y ayude al correcto funcionamiento de los componentes de los que disponemos en su interior. Esta normativa se corresponde con el estándar TIA 942, que proporciona una serie de recomendaciones y directrices para la instalación de una infraestructura de este tipo.

En esta normativa se recogen algunas directrices, entre las que podemos destacar la climatización dentro de la sala o la prevención y solución ante posibles incendios [7]. De

esta forma, y cumpliendo la normativa, contamos en esta sala con un aire acondicionado que no podemos modificar y un extintor regulado por la normativa.

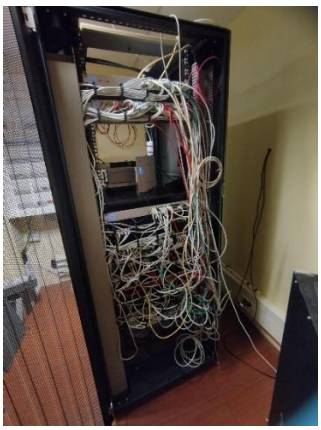

Figura 20. Imagen del armario de la sala de comerciales

4.2 Nuestra configuración y organización

El desarrollo del proyecto comienza cuando nos conectamos a la red corportativa de Nunsys para empezar a monitorizar con Paessler. El primer paso fue utilizar la herramienta de descubrimiento automatico que se muestra a continuación (Figura 21). En nuestro caso, debido a las necesidades que nos demanda Nunsys y a las características de la red, nos decantamos por el nivel de descubrimiento automático detallado, llevado a cabo una vez (sin repeticiones) y con un método de escaneo mediante dirección IP y subred (queremos un rango de IP de 512 direcciones).

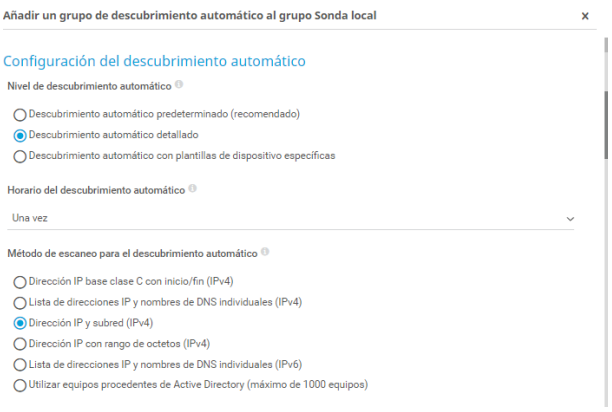

Figura 21. Imagen 1 de las opciones para nuestro descubrimiento

El rango de estas direcciones lo indicamos a continuación, escribiendo la IP y la subred.

El nombre de los dispositivos que queremos que nos aparezcan es su nombre DNS. Esto ha sido elección personal nuestra para tener una mejor visión de qué dispositivos estamos detectando. La otra opción es utilizar las direcciones IP.

Como ya hemos hecho un primer descubrimiento automático y queremos volver a detectar todos los dispositivos posibles, debemos seleccionar la opción en la que también descubrimos dispositivos que nuestro programa ya conoce. Estas otras 3 opciones las podemos obsevar en la Figura 22.

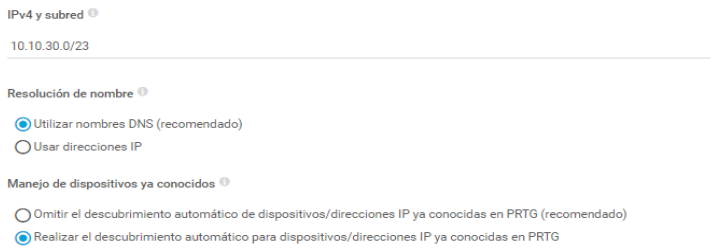

Figura 22. Imagen 2 de las opciones para nuestro descubrimiento

Por último, tenemos las opciones que tienen que ver con las credenciales del software. En nuestro caso queremos que todas estas se hereden de la sonda local. (Figura 23)

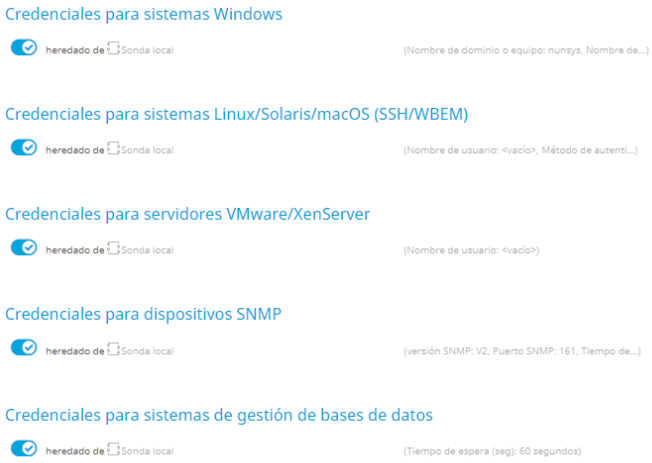

Figura 23. Imagen 3 de las opciones para nuestro descubrimiento

Cabe decir que no todos los dispositivos son detectados automáticamente, ya que algunos pueden corresponderse con un rango de red diferente al que hemos indicado. Por lo tanto, pregunté a algunos superiores de la empresa para saber qué dispositivos eran importantes para monitorizarlos y sobre cuáles de ellos querían tener una monitorización más estricta para empezar a trabajar en ello. Estos eran, principalmente, los dispositivos que tienen relación con las comunicaciones dentro del edificio, tales como switches y AP que debían estar en nuestra monitorización debido a la importancia de estos en la conexión de la red dentro de nuestro edificio. Tras contactar con los encargados que podían proporcionarme estas IP, me puse manos a la obra para añadirlos de forma manual a la red de monitorización en nuestra lista de dispositivos de PRTG.

Una vez tuvimos registrados todos los dispositivos que la empresa necesitaba monitorizar, nos dimos cuenta de que no teníamos acceso a algunos sensores por SNMP, como es el caso de las impresoras. Por tanto, las credenciales para estos dispositivos SNMP debían cambiarse.

Al tratarse de una red de una empresa privada, y debido a que nuestra intención es localizar los dispositivos y la mayoría de los sensores por SNMP, cambiamos las credenciales para los mismos. Esto supone que podamos localizar todos los sensores posibles de los dispositivos que no son accesibles desde el exterior. Es como si se necesitase una contraseña para poder ver los sensores (Figura 24).

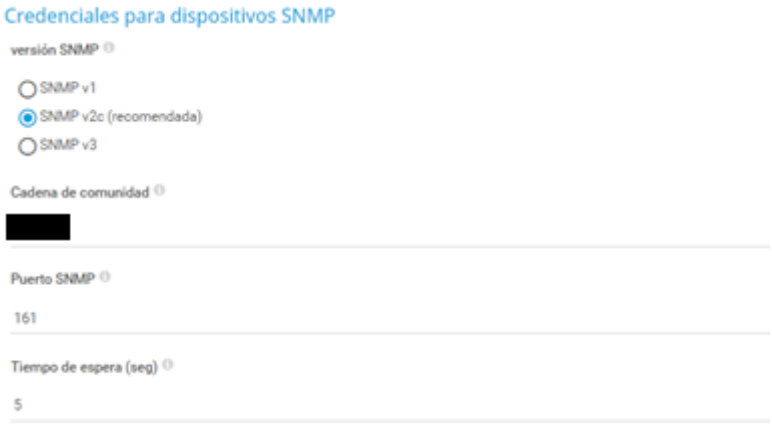

Figura 24. Cambio de credenciales de SNMP para dispositivos en Nunsys

Una vez teníamos todo configurado con los dispositivos que habíamos encontrado y los que añadimos manualmente, procedimos ordenar los diferentes dispositivos en categorias según la empresa nos fuese indicando. Gracias a la herramienta que nos ofrece el programa de añadir nuevos grupos (Figura 25) para separar los dispositivos y establecer categorias de la forma más adecuada según las necesidades demandadas.

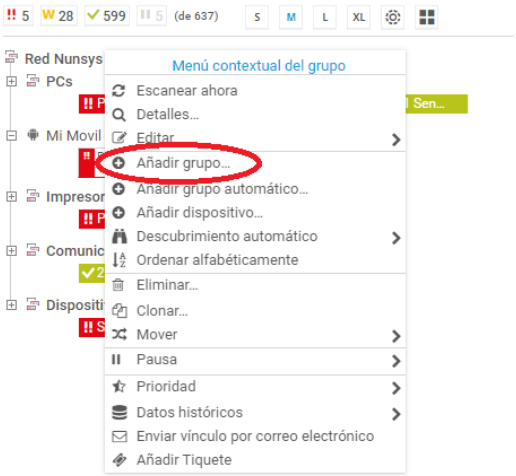

Figura 25. Añadir grupo en PRTG

En nuestro caso, y debido a las requisitos que Nunsys tenía para esta monitorización, configuramos y organizamos el software con la siguiente disposición:

En primer lugar tenemos los **ordenadores** (Figura 26) que están conectados a la red y los que PRTG ha detectado automáticamente. En Nunsys estos ordenadores están

denominados de una forma específica, por lo que podemos identificarlos fácilmente y añadirlos al grupo de PCs correspondiente. Para estos dipositivos el único sensor realmente necesario es el de Ping, con el que identificamos si está conectado a la red o no. En una monitorización de estas características no es necesario saber si estos tienen conexión a internet, la carga de procesador, etc. En nuestro caso tuvimos una excepción, ya que en nuestra red se encontraba un ordenador que sí queríamos monitorizar de una forma más específica. Para ello, aparte de añadir otros sensores como la carga del procesador, el espacio del disco, la memoria o el volumen de entrada y salida (Figura 27) dentro del PC, también añadimos desencadenantes de estado y volumen en sus alarmas.

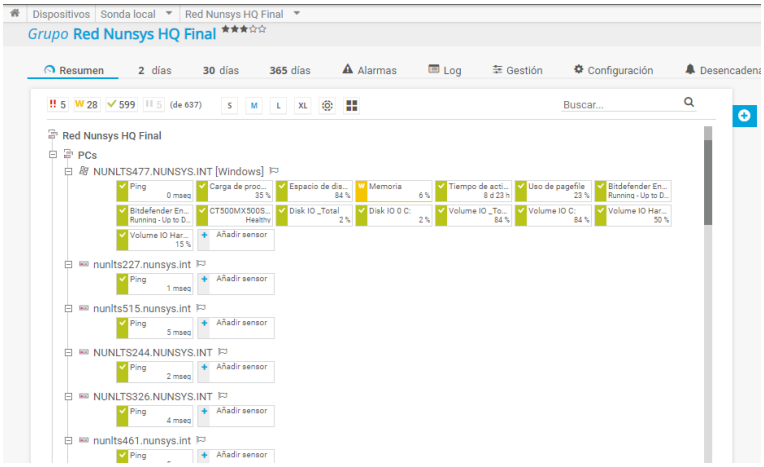

Figura 26. Disposición de PCs detectados por PRTG

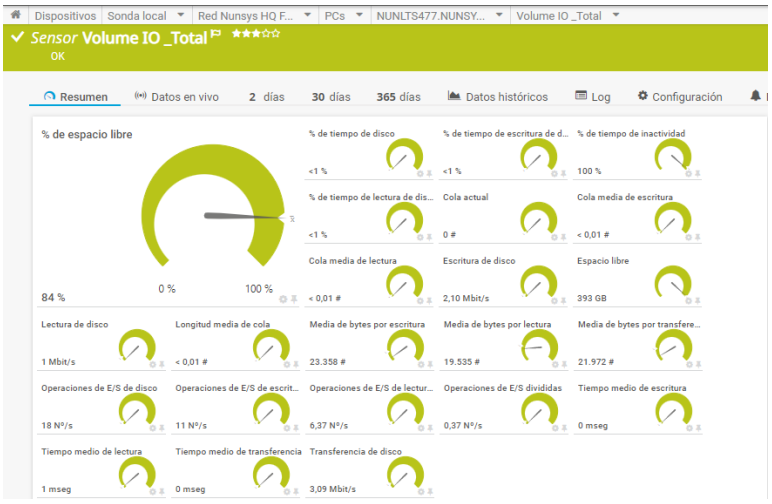

Figura 27. Diferentes sensores de un PC

Por otra parte, tenemos las **impresoras** de la oficina que están conectadas a la red corporativa de Nunsys y que son detectadas con PRN en su nombre, lo que se identifica con 'printer'. Gracias a esta nomenclatura podemos saber que se correspoden con impresoras de la empresa. Para estos dispositivos los sensores con más importancia a la hora de hacer una monitorización sobre ellos son los de HTTP y HTTPS para comprobar de esta forma si pueden acceder a internet y así poder seguir imprimiendo desde la

distancia. Además, añadimos sensores que pueden llegar a resultar muy interesantes como el estado del hardware, el estado de memoria, el tiempo de actividad o la carga de CPU, entre otros (Figura 28).

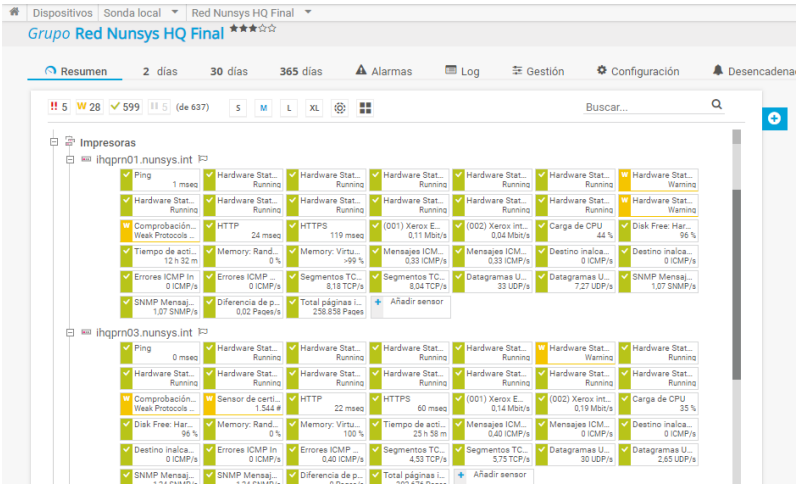

Figura 28. Disposición de las impresoras en PRTG

Por otra parte, nos encontramos con el grupo de **comunicaciones** (Figura 29), posiblemente la parte más importante en cuanto al monitoreo de toda la red de Nunsys. Los dispositivos de este grupo los hemos dividido en varios subgrupos ordenados por su localización física. De esta forma podremos visualizarlos limpiamente, sabiendo dónde podemos encontrar cada uno.

En primer lugar contamos con un Switch CISCO Core 4500 que corresponde a la puerta de enlace de la red; está situado en el edificio adyacente (Nunsys Cloud) al que nos encontrábamos nosotros.

Comenzando con los grupos propiamente dichos nos encontramos con el CPD de la planta de comerciales. Este, cuenta con tres switches de Unifi que nombramos como 01, 02, y 03 siguiendo el orden en el que están colocados físicamente de arriba a abajo en el armario; además, encontramos un AP al que se conectan los dispositivos de la zona de comerciales del edificio.

A continuación tenemos el grupo que corresponde con el CPD de la planta baja del edificio. En él podemos ver cinco switches nombrados por la sala a la que corresponde cada uno.

El último subgrupo de comunicaciones es el Aula Formación, donde encontramos un switch correspondiente a este aula y un AP para dar conexión a los dispositivos que se encuentran en ella.

Para terminar el grupo de comunicaciones tenemos tres AP distribuidos por diferentes salas del edificio; uno para la zona de Administración, otro para la sala de Escuelas Conectadas y otro para la sala de Gestión Documental.

Todos estos dispositivos son de vital importancia, ya que son los que realmente dan la conexión a los demás dispositivos que encontramos en la red. Sin ellos, o simplemente con algún fallo en su hardware, el trabajo de la empresa se veria perjudicado. De esta

forma, configuramos todos los sensores que nos permitían tener algo de informción sobre ellos.

Todo este grupo ha sido organizado de esta forma para clarificar y facilitar el trabajo futuro, contribuyendo a la creación de mapas que nos ayuden a visibilizar la monitorización del edificio que veremos más adelante. Además, en cada uno de los dispositivos añadimos un desencadenador de estado, activando que nos llegase un email a nuestro correo corporativo cada vez que el ping de cada uno de ellos falle. Como es obvio, no hemos podido hacer pruebas con este desencadenante ya que si lo forzamos a fallar podemos perjudicar el trabajo de la empresa. Más adelante, veremos un ejemplo de como hemos añadido un desencadenante y cómo funciona una alarma de este tipo de una forma práctica; esta la hemos probado en 'mi teléfono móvil', donde sí hemos podido realizar esta prueba.

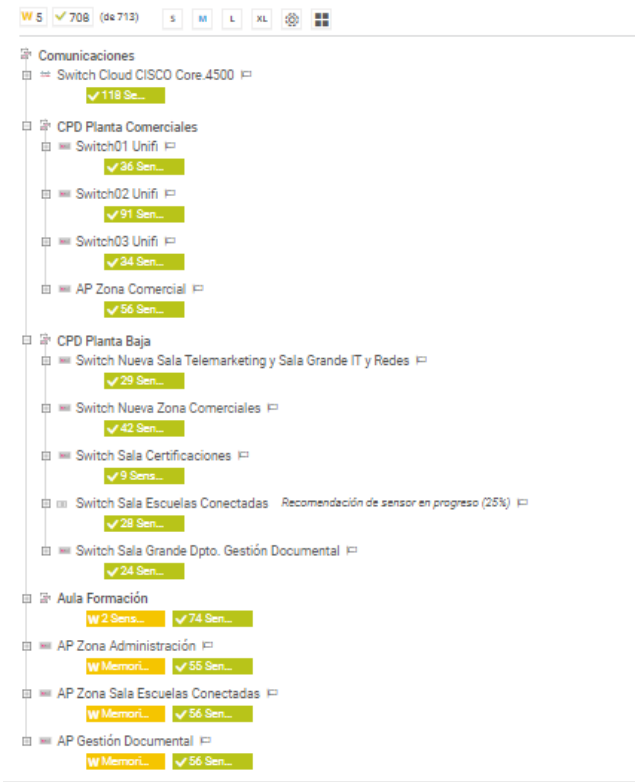

Figura 29. Disposición del grupo de comunicaciones dentro de PRTG

Entre los sensores más importantes se encuentran: el sensor del ping, por supuesto, todos los puertos Ethernet que tienen una conexión con otro dispositivo y que deben estar permanentemente activos, la salud del sistema, el estado de los firewall o los host disponibles, entre otros.

A continuación, veremos el ejemplo del switch que actúa como puerta de enlace, junto con los sensores que nos puede proporcionar para obtener toda la información posible (Figura 30). Se trata de un Cisco Core 4500.

Figura 30. Cisco Core 4500 en PRTG y sus sensores disponibles

A continuación veremos el ejemplo del armario que tenemos en la planta de comerciales, cómo están conectados cada uno de los switches que nos encontramos en él. En ellos podemos ver las conexiones que presentan, qué puertos tiene activos y cómo quedan reflejados en los sensores que vemos en el software.

En primer lugar tenemos el 'Switch01 Unifi' (Figura 31). Este es un switch de 24 puertos que se corresponde con un Ubiquiti UniFi USW-PRO-24-POE (Figura 32).

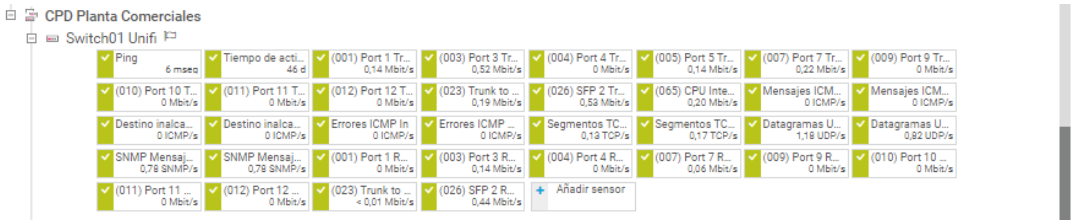

Figura 31. Switch nº1 del armario de comerciales en PRTG

Figura 32. Switch nº1 del armario de comerciales

En segundo lugar nos encontramos con el 'Switch02 Unifi' (Figura 33), un switch de 48 puertos, que se corresponde con un Ubiquiti UniFi US-48-500W (Figura 34).

Figura 33. Switch nº2 del armario de comerciales en PRTG

Figura 34. Switch nº2 del armario de comerciales

Por último podemos ver el 'Switch03 Unifi' (Figura 35). Al igual que el primero, este es un switch de 24 puertos que también se corresponde con un Ubiquiti UniFi USW-PRO-24-POE (Figura 36).

Figura 35. Switch nº3 del armario de comerciales en PRTG

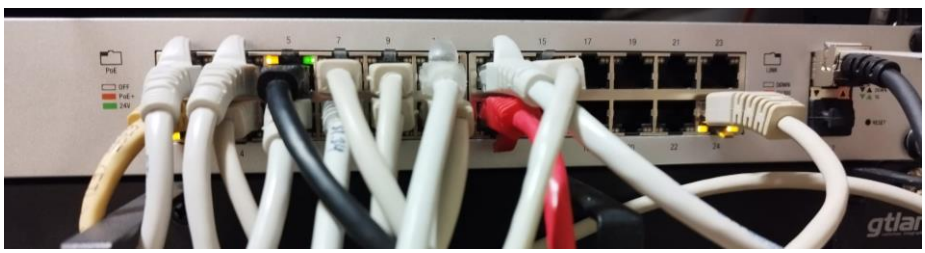

Figura 36. Switch nº3 del armario de comerciales

Con el permiso de ciertos responsables de la empresa, ya que no se deben conectar dispositivos personales a la red corporativa de Nunsys, el único dispositivo suelto que nos encontramos en nuestra red es **mi teléfono móvil** (Figura 37), en el que hemos configurado el sensor Ping para tener la información de cuándo está conectado a la red de Nunsys y cuándo no. Este dispositivo nos ha servido sobretodo para realizar las pruebas necesarias de que nuestro sistema en PRTG de la red de Nunsys actúa correctamente y, de esta forma, cuando haya un fallo real en cualquier dispositivo todo funcione de una manera adecuada.

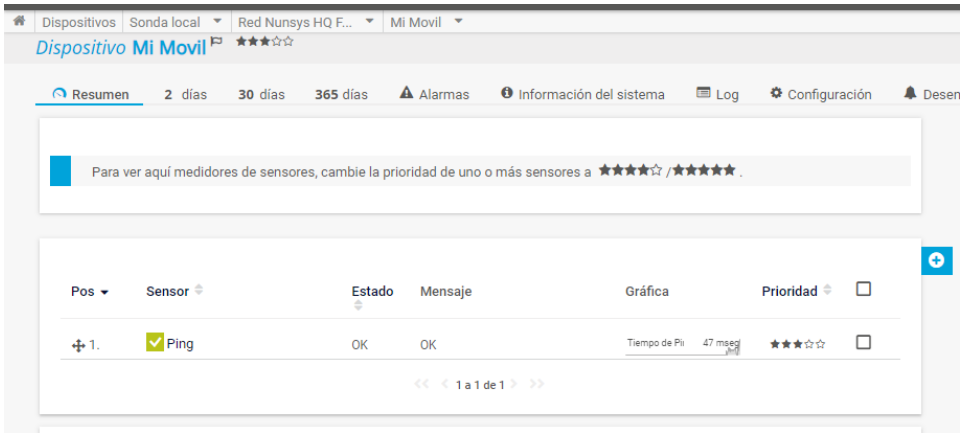

Figura 37. Mi teléfono móvil en PRTG

Para añadir mi teléfono móvil a nuestra red de PRTG hemos forzado a mi teléfono a conectarse a la red de Nunsys siempre con la misma IP (en vez de por DHCP, que sería lo normal en un teléfono). De está forma, siempre que entre y salga de Nunsys, mi teléfono se conectará con la dirección IP que hemos añadido en nuestro programa.

A continuación, y como ya hemos mencionado anteriormente, mostraremos con diferentes capturas de pantalla dentro de PRTG, una demostración de cómo hemos creado una alerta para el dispositivo 'Mi móvil'.

En primer lugar, debemos elegir qué tipo de desencadenador y sobre qué dispositivo lo queremos añadir según nuestras necesidades y qué nos resulte de mayor importancia en nuestra red (Figura 38).

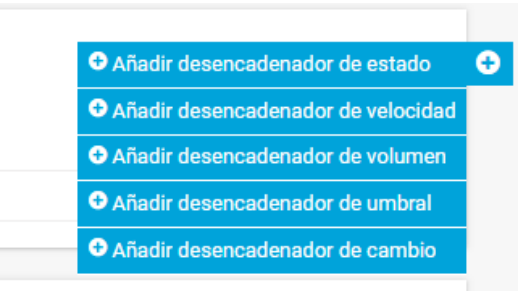

Figura 38. Captura de tipos de desencadenadores para alarmas

En nuestro caso elegiremos un desencadenador de estado ya que nuestro objetivo es recibir una notificación por correo electrónico una vez el ping esté en estado de fallo durante más de 20 segundos (Figura 39).

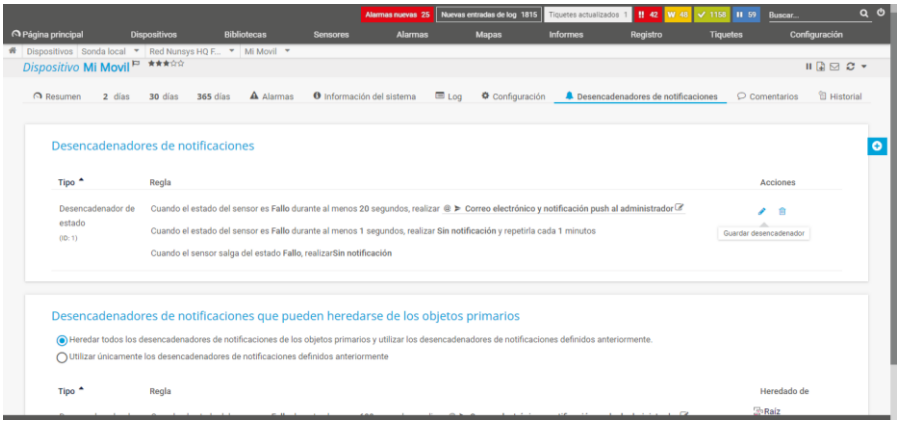

Figura 39. Captura de las opciones para desencadenar una notificación

De esta forma hemos configurado la alarma que queríamos, de forma que PRTG nos avisará con un correo cada vez que surja dicho problema (Figura 40).

Figura 40. Captura al recibir la notificación por correo electrónico

Aparte de esta configuración también podemos añadir otros desencadenadores como el de velocidad, en que podemos añadir una alerta cada vez que la velocidad sea menos a unos kbit/segundo que nosotros determinemos o el de volumen, con el que podemos añadir una alerta cada vez que el tráfico sea mayor a una cantidad que también podemos personalizar nosotros.

Por último, disponemos de los **dispositivos desconocidos** (Figura 41) que ha detectado el descubimiento de PRTG. Debido a que no se corresponden con ningún nombre DNS, no podemos identificarlos de una forma exacta. Una forma de poder intuir de qué dispositivo se trata es mirando qué tipo de sensores recoge automáticamente. En nuestro caso, y viendo los tipos de sensores que ha registrado, es muy probable que estos dispositivos que vemos se correspondan con equipos de final de usuario como un portátil

personal o un teléfono móvil. A pesar de nuestras intuiciones, los dejamos como dispositivos desconocidos.

Figura 41. Disposición de los dispositivos desconocidos en PRTG

Esta es la disposición que, tras algunas reuniones con diversas personas de la empresa, hemos decidido que sería óptima para nuestro caso. Finalmente, una vez hemos visto cada grupo organizado por separado, vamos a ver cómo ha quedado dentro del software la organización general de la red que hemos monitorizado (Figura 42):

Figura 42. Disposición final de nuestra red en PRTG

Por último, pasaremos a hablar de los mapas que hemos creado para ver la red monitorizada de una forma completamente visual. En nuestro caso hemos creado algunos que pueden ser de gran utilidad en la empresa según las peticiones de los trabajadores que

manifestaban principalmente la falta de organización en la visualización del estado de cada dispositivo.

En primer lugar tenemos dos mapas facilitados por la empresa que se corresponden con el plano cenital de cada una de las plantas del edificio HQ en el que hemos trabajado. En ellos hemos añadido los dispositivos monitorizados en el lugar que se encuentran. Por un lado tenemos el plano de la planta baja (Figura 43), donde podemos encontrar el CPD de esta planta, el AP que da conexión a la sala de Gestión Documental, el que la da a la Sala de Escuelas Conectadas y el grupo que incluye los dispositivos del Aula de Formación.

Figura 43. Mapa de la planta baja del edificio HQ de Nunsys

Por otro lado tenemos el plano de la primera planta del edificio (Figura 44). En él nos encontramos con el CPD de la planta de comerciales (de la que veremos a continuación un poco más detenidamente) y el AP que encontramos en la zona de Administración.

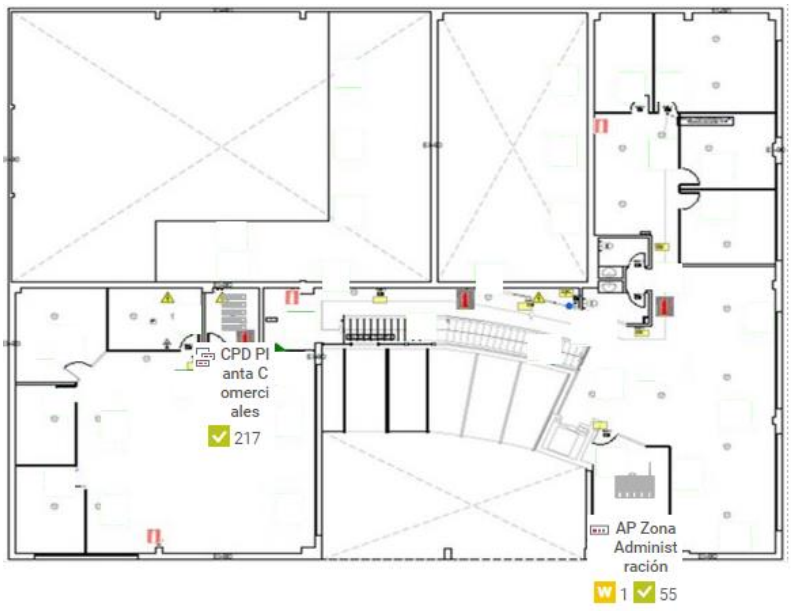

Figura 44. Mapa de la primera planta del edificio HQ de Nunsys

Como hemos mencionado anteriormente, también tenemos un mapa con el plano cenital del entorno de trabajo; la planta de comerciales, desde donde hemos estado desarrollando el proyecto la gran parte del tiempo durante estos meses. En la figura 45 podemos observar que disponemos de 3 largas mesas en las que diferentes trabajadores realizan sus funciones con su ordenador. Además, contamos con cuatro pequeños despachos a los que podemos acceder donde se sitúan dos ordenadores más a monitorizar. En cada puesto, hemos colocado su ordenador correspondiente por IP para saber qué ordenador está disponible en cada momento. Los que en el momento de la realización de la captura de pantalla del mapa estaban apagados, no tienen conexión a internet y no conseguimos llegar a ellos con un ping, aparece su sensor en rojo. Por el contrario, los que estaban activos y conectados a la red de Nunsys aparecen sus sensores en verde.

Como podemos observar, en este mapa también hemos añadido la sala de CPD con los 3 switches de Unifi dentro de ella y el anteriormente mencionado switch de CISCO que se encuentra en la planta baja del edificio. Así, cuando uno de los sensores de estos cuatro indispensables dispositivos falle, se pondrá en rojo y simplemente visualizando este mapa y pinchando en él podremos detectar qué switch ha sido y, más específicamente, qué sensor es el que está dando problemas.

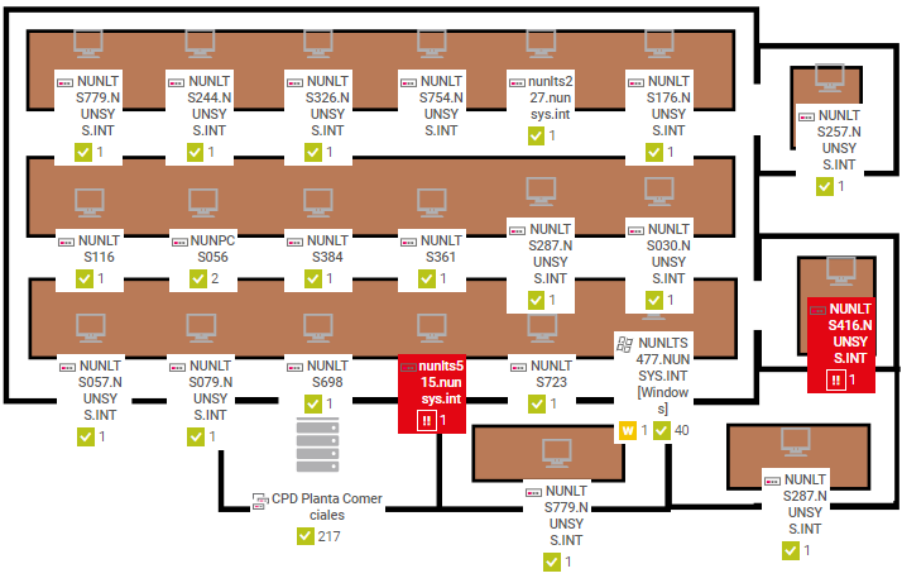

Figura 45. Mapa del plano de la oficina de comerciales

A continuación veremos otro de los mapas que hemos creado para facilitar el trabajo a los trabajadores de la empresa. Debido a que el grupo de las comunicaciones, en el que se encuentran los switches de la empresa, es el más importante en cuanto a su disponibilidad y no podemos dejar que algún sensor no esté disponible durante mucho tiempo, hemos decidido crear un mapa que se dedique a este grupo en concreto. En él podemos ver un anillo correspondiente a todo el grupo de comunicaciones y otros dos más pequeños que se corresponden con los dos CPD que tenemos en nuestra red (Figura 46).

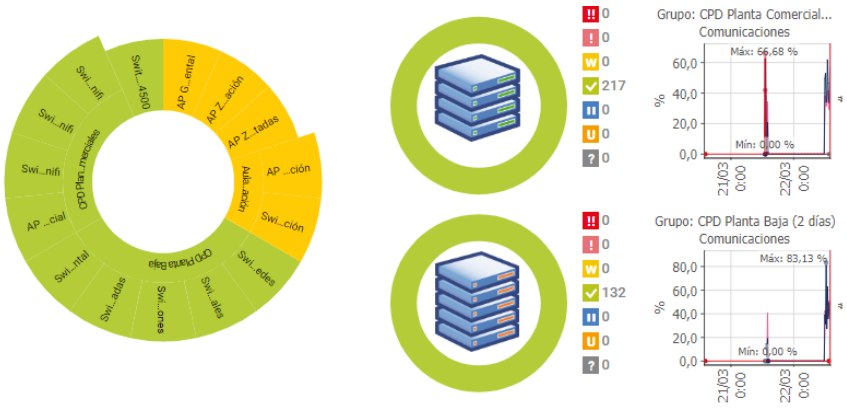

Figura 46. Mapa de anillos centrado en el grupo de comunicaciones

Otra opción que podía resultar de utilidad para ver la monitorización de la red era realizar el siguiente mapa (Figura 47). En él podemos observar una proyección solar de los sensores de los dispositivos de la red del edificio HQ de Nunsys, acompañada de un árbol de los dispositivos monitorizados. Con un simple vistazo a este mapa, podemos darnos cuenta de qué dispositivo está fallando en ese preciso instante dentro de nuestra red.

Figura 47. Mapa de proyección solar de todos los dispositivos

Otra alternativa a la proyección solar de la figura anterior es este mapa donde vemos también todos los dispositivos ordenados de una forma distinta. En él también podemos ver qué dispositivos no se encuentran activos en cada momento pero mediante una disposición de estos muy diferente. (Figura 48)

Hemos considerado hacer estas dos opciones debido a que no siempre será la misma persona la que esté atenta a la monitorización, de forma que cada una que la revise pueda elegir la forma en la que se encuentre más cómoda visualizando el estado de la red.

Figura 48. Mapa de visualización de todos los dispositivos

Por último, hemos creado un mapa en el que podemos ver toda la red de una manera un poco más detallada, viendo cada uno de los grupos que hemos creado por separado. Hemos añadido cuatro proyecciones solares con su árbol de dispositivos que hace referencia a los cuatro grupos creados (Figura 49).

Figura 49. Mapa de proyecciones solares de cada grupo creado

Capítulo 5. Conclusiones y propuesta de trabajo futuro

En este quinto y último apartado pasaremos a estudiar las conclusiones que hemos obtenido tras la realización del proyecto. Tras comentar nuestras propias valoraciones, mencionaremos los objetivos cumplidos que nos habíamos propuesto para este desarrollo. Para finalizar, también mencionaremos nuevas implementaciones con las que podemos seguir avanzando nuestro proyecto en un futuro.

5.1 Conclusiones

Gracias a un estudio previo, y teniendo en cuenta las exigencias de esta empresa, logramos encontrar un software que se amoldaba a nuestras necesidades y a los requisitos que habían sido propuestos al comienzo del proyecto. Tras haber terminado y probado nuestro sistema con la empresa, podemos decir que se ha cumplido el objetivo principal por el cual se plantea la realización de este trabajo: realizar una monitorización de la red en tiempo real de una empresa y, de esta forma, ofrecer el contenido a esta misma para facilitar la labor de los empleados de Nunsys.

Con esta monitorización tratamos de plasmar en un software la red que encontramos en el edificio HQ de Nunsys en el Parque Tecnológico de Paterna. De forma que si se diese la situación en la que se produce un fallo en alguno de los dispositivos monitorizados, podamos darnos cuenta al instante de qué está ocurriendo en nuestra red y así reducir daños que puedan causar a la empresa. Los dispositivos más importantes que podemos encontrar en el edificio HQ de Nunsys y que hemos podido detectar son: switches que conectan otros equipos de la red, AP que dan conexión a usuarios finales, PCs con los que se trabaja dentro de la empresa o impresoras conectadas a la red local.

Una de las razones por las que la empresa demandaba esta solución era la falta de organización de todos los datos de los equipos del edificio previa al proyecto y que consistían en métodos menos eficientes como el registro de estos datos en hojas de documentos Excel.

Buscábamos proyectar el conocimiento adquirido durante el grado y el periodo de prácticas sobre una empresa real, simplificándoles el trabajo diario a personas que se encuentran dentro de Nunsys y tras su conclusión, podemos decir que hemos conseguido lo que en un principio nos habíamos propuesto.

Pese a haber cumplido con todos los objetivos personales y marcados por la empresa que se plantearon al inicio del proyecto, han ido surgiendo ciertas dificultades que merecen la pena mencionar:

- Debido al gran volumen de trabajo de esta empresa, los empleados que podían ayudarme con las dudas que iban surgiendo en el desarrollo de mi trabajo, no siempre tenían disponibilidad para atenderme. Debido a esto, en algunas ocasiones debía pasar a otro punto antes de poder continuar con la tarea que me estaba generando problemas.
- Al poco tiempo de comenzar el proyecto el departamento de redes tuvo un cambio de oficina. Este hecho no nos afectó demasiado, pero la planificación que teníamos para la monitorización del primer edificio ya no nos resultaba de gran utilidad. Ya no contábamos con algunos dispositivos que también eran interesantes de monitorizar, como alarmas o sensores, pero mantuvimos la esencia

del proyecto debido a que queríamos ajustarnos a las necesidades y esto era lo que la empresa necesitaba de nosotros en ese momento.

Por otra parte, también nos hemos encontrado con muchas facilidades que nos han ayudado a optimizar y agilizar el trabajo de monitorización, como son:

- La buena acogida que ha tenido este proyecto por parte de Nunsys durante todo el proceso, la amabilidad de las personas que trabajan aquí y la predisposición a ayudar en todo momento. Además, cabe mencionar la ayuda de Javier Furió, quien siempre que ha podido ha estado pendiente y revisando mi trabajo dentro de la empresa.
- La suerte de poder combinar mi periodo de prácticas con la realización de este trabajo a demanda de la empresa con la que estuve colaborando, me ha permitido desarrollar un gran interés por este ámbito de las telecomunicaciones, lo que a su vez me ha impulsado a aprender y formarme para que el proyecto fuera lo más útil posible para Nunsys y sus trabajadores.

5.2 Futuras implementaciones

El trabajo ya contiene funcionalidades firmes y concretas en base a los objetivos propuestos y los requerimientos de la empresa. A pesar de ello, somos conscientes de algunas de las limitaciones que tiene este proyecto. Estas se pueden deber a que el proyecto ha sido realizado en calidad de alumno de prácticas, por lo que el acceso a algunas instalaciones y conocimiento de los datos era limitado.

Una pequeña mejora que habría dado más empaque a este proyecto podría haber sido tener la posibilidad de añadir imágenes de los diferentes CPD y dispositivos que hemos monitorizado. En nuestro caso, solo hemos tenido acceso físico al CPD de la zona de comerciales, ya que el acceso al que podemos encontrar en la planta baja y el que tenemos en el edificio de Nunsys Cloud, contaban con acceso restringido.

Otra posible mejora que podría ayudar a nuestro proyecto es la creación de más mapas dentro del software. Este es un avance que podría aportar un mayor apoyo a los trabajadores que usarán este trabajo en el trabajo de su día a día. Una vez que estas personas trabajasen con este proyecto y supiesen qué más necesitan y cómo podrían beneficiarse aun más de esta monitorización, podrían aportar ideas de cómo creen que un nuevo mapa podría optimizar su trabajo y qué tipo de mapa podría ayudar más a su propia experiencia con nuestra monitorización.

Una elección más personalizada de los sensores para cada dispositivo también podría ayudar a una mejora de la monitorización. En nuestro caso, hemos elegido una gran cantidad de sensores para cada equipo que nosotros creemos que pueden ser de gran utilidad para los trabajadores, con ayuda de diferentes personas que usarán este software. La posible mejora puede residir en la optimización de estos sensores, ya que una vez se pongan manos a la obra, pueden darse cuenta de que, en la práctica, algunos pueden llegar a ser más indispensables que otros que, en un principio, podía parecer que no iban a tener la misma importancia dentro de la monitorización.

Las alarmas personalizadas son de gran utilidad para el trabajo diario y para una monitorización de este estilo. En este proyecto, las alarmas que nosotros hemos añadido se encuentran en el sensor del ‘ping’ de cada uno de los equipos de comunicaciones. Otra posible futura mejora está en una mayor cantidad de alertas donde las personas que

trabajarán con esta monitorización se encuentren cómodas. Esto debe ser controlado, ya que una cantidad masiva de alertas puede llegar a molestar.

También cabe recordar que la monitorización se ha realizado solo en el edificio HQ por lo que no solo no hemos podido abarcar todas las instalaciones, sino que ahora los edificios cuentan con sistemas de organización diferentes.

Por tanto, otras recomendaciones para mejorar el proyecto podemos encontrarlas tanto en desarrollar la misma monitorización en otros edificios de Nunsys, realizando la misma organización dentro de ella, como en unificar todas las posibles monitorizaciones creando un grupo para todas ellas. De esta forma podríamos ver todos los dispositivos en un mismo grupo de PRTG que está conectado al servidor raíz de Nunsys.

De ser así, un ejemplo de como quedarían repartidos los grupos de PRTG sería de la siguiente forma (Figura 50), teniendo en cuenta una posible futura monitorización del edificio Nunsys Cloud, donde dentro de cada grupo, se encontrarían cada uno de los dispositivos monitorizados.

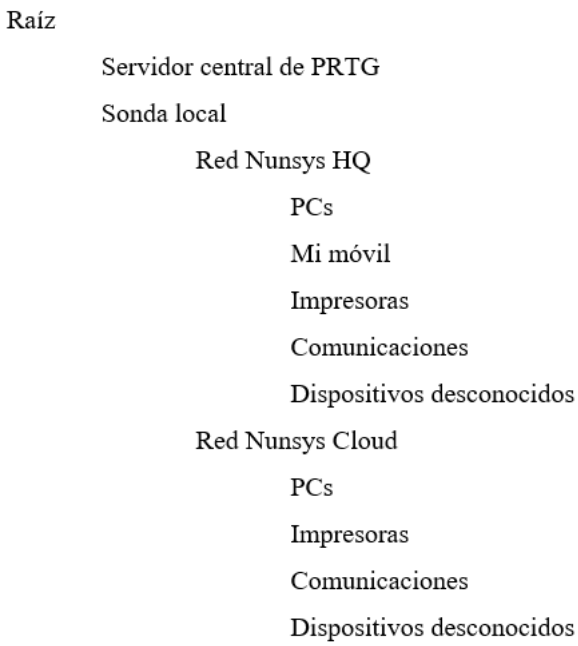

Figura 50. Ejemplo de grupos tras la unificación de monitorizaciones de Nunsys HQ y Nunsys Cloud

Capítulo 6. Bibliografía

[1] «Nuestra cultura», Nunsys. https://www.nunsys.com/personas/nosotros/nuestra-cultura/ (accedido 4 de marzo de 2023).

[2] «Definición de monitoreo - Definicion.de», Definición.de. https://definicion.de/monitoreo/ (accedido 4 de marzo de 2023).

[3] «Monitoreo y evaluación - Mapa conceptual | OIT/Cinterfor». https://www.oitcinterfor.org/general/monitoreo-evaluaci%C3%B3n-mapa-conceptual (accedido 4 de marzo de 2023).

[4] A. Herranz, «CPD: qué es un centro de procesamiento de datos y cómo funciona», Xataka, 17 de mayo de 2021. https://www.xataka.com/pro/cpd-que-centro-procesamiento-datos-como-funciona (accedido 4 de marzo de 2023).

[5] M. Coppola, «Qué es un data center o centro de datos, tipos e implementación». https://blog.hubspot.es/marketing/data-center (accedido 4 de marzo de 2023).

[6] E. G. Novelec |, «Claves de seguridad para el diseño de un centro de datos», Grupo Novelec. https://blog.gruponovelec.com/redes-vdi/claves-de-seguridad-para-el-diseno-de-un-centro-de-datos/ (accedido 4 de marzo de 2023).

[7] «Data Center: El Estándar TIA 942 | Grupo COFITEL». https://www.c3comunicaciones.es/data-center-el-estandar-tia-942/ (accedido 4 de marzo de 2023).

[8] G. S. D. Connectivity, «¿Qué es Netbox y para qué sirve Netbox?» https://golesuite.com/ (accedido 4 de marzo de 2023).

[9] «Software empresarial para la gestión de redes - ManageEngine OpManager Plus». https://www.manageengine.com/es/it-operations-management/network-monitoring.html (accedido 4 de marzo de 2023).

[10] PanelNunsys, «PRTG: Monitorización y supervisión de red», Nunsys, 1 de agosto de 2012. https://www.nunsys.com/monitorizar-permite-detectar-problemas-y-resolverlos/ (accedido 4 de marzo de 2023).