Facultade de Informática
UNIVERSIDADE DA CORUÑA

TRABAJO FIN DE GRADO
GRADO EN INGENIERÍA INFORMÁTICA
MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Metodología para la implementación de la norma ANSI/TIA-942 en Centros de Datos empleando herramientas de gestión de activos

Estudante: Hadrián Peleteiro Rey

Dirección: Víctor Manuel Carneiro Díaz

A Coruña, Septiembre de 2023.

A mis padres y a mi hermano, por haberme apoyado a lo largo de estos cuatro años.

Agradecimientos

Me gustaría agradecer en primer lugar a mis padres y a mi hermano por todo el apoyo que me han brindado siempre, también a mis amigos, especialmente a aquellos que me han acompañado en A Coruña y durante toda la carrera, haciendo que la universidad se convirtiese en una etapa llena de buenos momentos, siendo mis compañeros Tony, Iago, Abel, Zambrana, Casas, Migas, Hugo, Adri y mis compañeros de piso Dani y Braga los principales artífices de esto. No me puedo olvidar tampoco de mis amigas Sonia y Laura, que igualmente han estado ahí desde el primer día hace ya cuatro años. También a mis amigos de siempre y del instituto, que ya saben ellos quienes son, por seguir juntos a pesar de estudiar todos en lugares diferentes. Por último me gustaría agradecer a todos los profesores que se han volcado para facilitar el aprendizaje durante la carrera y que han sido de gran ayuda, especialmente a mi tutor Víctor Carneiro y a Alejandro Mosteiro, por las facilidades y apoyo que me han proporcionado en el desarrollo de este trabajo.

Resumen

En este trabajo se planteará y desarrollará una metodología para la aplicación del estándar ANSI/TIA-942 en un Centro de Procesamiento de Datos (CPD), con el objetivo de facilitar el proceso de obtención de una certificación Tier por parte del mismo. Se emplearán diferentes herramientas que servirán de apoyo en la aplicación de la metodología y se probará la misma en un caso real, para estudiar los resultados obtenidos y realizar cambios en caso de ser necesario.

Abstract

In this work, a methodology for the implementation of the ANSI/TIA-942 standard in a Data Center (DC) will be proposed and developed, aiming to ease the process of obtaining a Tier certification for the center. A number of tools will be employed to support the application of the methodology, and it will be tested in a real case scenario to study the obtained results and make changes if required.

Palabras clave:

- Tier
- CPD
- Redundancia
- Metodología
- Activo
- Rack
- Servidor

Keywords:

- Tier
- DC
- Redundancy
- Methodology
- Asset
- Rack
- Server

Índice general

Índice de figuras

Capítulo 1

Introducción

En la era digital en la que vivimos hoy en día, los datos son uno de los motores más importantes que impulsan el funcionamiento de múltiples organizaciones en todo tipo de sectores. La gestión y el procesamiento de una forma eficiente de esta información se ha convertido en una prioridad para garantizar el rendimiento y la continuidad de los servicios ofrecidos. En este contexto, un Centro de Procesamiento de Datos (CPD) desempeña un papel principal brindando un entorno seguro y confiable para el almacenamiento, procesamiento y distribución de los datos.

La importancia de los CPD, radica en su capacidad para albergar y administrar grandes volúmenes de información de manera eficiente, garantizando la disponibilidad, la integridad y la confidencialidad de los datos. Estos centros representan un activo estratégico para las organizaciones, ya que aseguran el funcionamiento continuo de sus sistemas de Tecnologías de la Información (TI), así como la protección de activos digitales críticos.

Es en este contexto en el que aparece el estándar ANSI/TIA-942 [1]. Esta norma desarrollada por las entidades American National Standards Institute (ANSI) y Telecommunications Industry Association (TIA) establece los requisitos y las mejores prácticas para el diseño, la construcción y la operación de los CPD. Su objetivo principal es garantizar la disponibilidad de los servicios y la seguridad de la información en estos entornos críticos. En términos generales, la normativa define diferentes niveles de redundancia, clasificación de áreas, alimentación eléctrica, enfriamiento y seguridad física, entre otros aspectos, que permiten a las organizaciones seguir una guía para cumplir con los estándares internacionales y asegurar la continuidad del negocio.

La aplicación de la normativa ANSI/TIA-942 en los CPD proporciona beneficios de diversos tipos. En primer lugar, asegura la calidad y la fiabilidad de las instalaciones, ya que

minimiza los riesgos de interrupción de servicios y protege los datos ante posibles amenazas o desastres [2]. Además, esta normativa brinda una guía para la planificación y el diseño de los CPD, facilitando la toma de decisiones estratégicas y optimizando la eficiencia operativa.

1.1 Objeto de estudio

En este trabajo de fin de grado, nos dedicaremos a estudiar la norma mencionada anteriormente para desarrollar una metodología funcional que facilite la implementación de la misma en los CPD. En concreto, nuestra metodología se centrará en los diferentes niveles Tier en los que la norma clasifica los CPD dependiendo de sus características. Estos niveles se basan en una serie de criterios que evalúan la disponibilidad y redundancia de los sistemas, con el objetivo de asegurar la continuidad de los servicios y la protección de la información.

La clasificación Tier se compone de cuatro niveles, designados como Tier I, Tier II, Tier III y Tier IV. Cada nivel representa un grado creciente de disponibilidad y fiabilidad de los sistemas y componentes del CPD. Hablaremos más adelante de estos niveles.

1.2 Objetivos

El principal objetivo de este trabajo es el de desarrollar y probar una metodología que facilite la implementación del estándar anteriormente mencionado, para aplicarla luego de forma práctica en un CPD real. En palabras generales, una metodología proporciona un conjunto de pasos a seguir con el objetivo de formalizar el procedimiento para realizar una tarea de forma consistente. Mejorar la eficiencia en este tipo de centros, considerados ya como infraestructura crítica, supone un gran avance para la organización a la que pertenecen, por eso es importante seguir una metodología adecuada, minimizando errores y optimizando los recursos disponibles. Además, es mucho más costoso modificar partes del CPD una vez construidas para que se adapten a los requisitos de las distintas certificaciones, que construirlas de forma correcta desde un primer momento, lo cual hace que tenga especial importancia el hecho de que la organización tenga claro todos los pasos que se han de seguir, los objetivos que desea cumplir y la forma de alcanzarlos.

Introducimos aquí el concepto de calidad, que puede entenderse como hacer las cosas bien a la primera, proporcionando a los clientes externos e internos, resultados que satisfagan plenamente los requisitos acordados. La implementación de una metodología adecuada es de gran ayuda para garantizar la calidad, ya que al definir procesos claros, criterios de control y revisiones, se pueden identificar y corregir errores de manera temprana.

Otro aspecto importante es que la metodología pueda emplearse en diferentes tipos de CPD, su adaptabilidad a diferentes entornos le confiere una mayor utilidad, y también proporciona la oportunidad de observar los resultados que se obtienen al aplicarla en condiciones diferentes, para comparar resultados y llevar a cabo mejoras en la misma. Esta metodología también busca apoyar en la mejora continua de la organización, proporcionando un marco para la revisión de los procesos realizados en el CPD, pudiendo aplicarse en repetidas ocasiones con el objetivo tanto de mantener el nivel Tier del centro, como de adquirir uno mayor. También se busca facilitar el trabajo de los responsables del centro cuando se quiera obtener un determinado certificado Tier.

Además, se busca familiarizarse con herramientas tanto de descubrimiento como de gestión de activos y profundizar en el conocimiento y aplicación de la normativa ANSI/TIA-942, ya que se trata de uno de los estándares por excelencia en cuanto a este tipo de infraestructuras, empleando a nivel mundial en todo tipo de organizaciones. Otro de los objetivos es entender y experimentar el proceso de llevar a cabo un trabajo de auditoría en el CPD.

1.3 Capítulos y contenido de la memoria

Los siguientes capítulos de la memoria contendrán los resultados del trabajo realizado, en concreto contaremos con cinco capítulos: estado del arte, metodología, herramientas empleadas, caso práctico y conclusiones.

Estado del arte

Capítulo dedicado a exponer la información extraída del estándar ANSI/TIA-942, en el que se hablará del propio estándar, de la redundancia y de los diferentes niveles Tier. La parte más importante del capítulo se centrará en el análisis de los diferentes requisitos que impone el estándar para cada uno de los diferentes Tier, información que emplearemos más adelante en la metodología.

Metodología

En este capítulo, se expondrá de principio a fin la metodología desarrollada, hablando sobre cada una de las fases que la componen y explicando los pasos a seguir que contempla la

misma.

Herramientas empleadas

El contenido de está sección se centrará en nombrar y explicar las diferentes herramientas que emplearemos como apoyo para aplicar la metodología en un caso práctico. Se hablará sobre las diferentes herramientas en general y se darán ejemplos de su utilización y del aporte que nos brindan en la aplicación de la metodología. Las herramientas se han seleccionado siguiendo un criterio en base a su utilidad en cuanto a la aplicación de la metodología, así como su sencillez de uso y aprendizaje para usuarios que no cuenten con experiencia en las mismas. Por este motivo, hemos elegido para trabajar las herramientas GLPI [3], OpenVAS [4] y Nmap [5].

Caso práctico

En esta parte hablaremos de todo lo relacionado con la aplicación de la metodología en un caso real, explicando los diferentes pasos que se han seguido, la elección del CPD a estudiar y la forma en la que se realizaron las diferentes etapas de la metodología. Se expondrán las pruebas realizadas en el propio CPD empleando las herramientas mencionadas en el capítulo anterior y los resultados obtenidos en las mismas.

Conclusiones

En el capítulo final, se analizarán los resultados obtenidos durante todo el proceso, así como la experiencia general en todo el proyecto. Se tratará particularmente el comportamiento de la metodología en el caso práctico, con el fin de comprobar su utilidad y sus posibles aplicaciones en el futuro. Por último, hablaré también de mi experiencia personal sobre el trabajo.

Capítulo 2

Estado del arte

Este trabajo está notablemente influenciado por el estándar ANSI/TIA-942, por lo que este capítulo estará dedicado a recopilar la información que se ha extraído tras el estudio del estándar. Primero, hablaremos del concepto de redundancia y de los diferentes tipos que existen de la misma, para luego explicar de forma resumida las características más importantes de cada nivel Tier. Finalmente se establecerán detalladamente los diferentes requisitos que se exigen para cada uno de los niveles Tier, para los 4 subsistemas que se recogen en el mismo: telecomunicaciones, eléctrico, arquitectura e infraestructura mecánica.

Esta parte es vital, ya que nos basaremos en esta información para determinar los requisitos que cumple el CPD estudiado y diseñar el plan de cambio para nuestro CPD.

2.1 La redundancia

En un CPD, la redundancia consiste en la duplicación o multiplicación de los componentes críticos del sistema con el objetivo de garantizar la continuidad de los servicios en caso de fallas o interrupciones. La implementación de la redundancia tiene como propósito mitigar los riesgos y aumentar la disponibilidad y fiabilidad del CPD.

Puede aplicarse a diversos aspectos del centro, sistemas de alimentación eléctrica, refrigeración, computación, telecomunicaciones... A través de la redundancia, se busca garantizar la continuidad de los servicios críticos, reducir los tiempos de inactividad y proteger la integridad de los datos.

A continuación, vamos a definir los términos que se emplean en el estándar para hablar sobre los diferentes niveles de redundancia:

N - El sistema dispone de lo mínimo para satisfacer los requerimientos básicos. Cualquier fallo puede suponer pérdidas en el servicio.

N+1 - Se agrega un componente adicional al mínimo requerido, por ejemplo, si tenemos un sistema de refrigeración N, se añade uno adicional como respaldo (N+1). Soportaría el fallo o mantenimiento de cualquiera de las dos unidades sin interrumpir el servicio.

N+2 - Igual al nivel anterior pero con dos componentes adicionales, por lo que soportaría dos fallos en sus componentes.

2N - En este nivel de redundancia, se duplican todos los componentes necesarios, que funcionan como dos sistemas independientes. Esto significa que se tiene un conjunto completo de componentes en funcionamiento y otro conjunto de respaldo idéntico. Si falla alguno de los componentes principales, el componente duplicado asume la carga sin interrupciones en el servicio. Es una de las opciones más seguras, pero también más caras debido al costo de proporcionar redundancia en todos los componentes del sistema.

2(N+1) - De forma similar al anterior nivel, se duplican los componentes necesarios para el funcionamiento del CPD, pero también incluye un componente adicional de respaldo para cada componente principal. Este nivel soportaría el fallo de un sistema completo y de algún componente en el de respaldo.

2.2 Los niveles Tier

En este apartado, se describirá de forma breve estos niveles que emplea la norma para la clasificación de los CPD. Estos niveles fueron definidos inicialmente por el Uptime Institute, pero se expanden en el estándar. Cabe destacar que un CPD puede tener diferentes niveles Tier para distintas partes de su infraestructura, por ejemplo, podría estar clasificado como Tier 3 en cuanto a electricidad pero Tier II en telecomunicaciones. Sin embargo, para simplificar, si un CPD tiene todos los subsistemas con la misma certificación (p.ej. Tier II), se dice que tiene un Tier II general. En el caso de tener diferentes certificaciones en los subsistemas, se mencionarían de forma específica. Por ejemplo si hablamos de un CPD con certificación $T_2E_3A_4M_2$, este tendría las siguientes características:

- Telecomunicaciones, Tier 2.
- Eléctrico, Tier 3.
- Arquitectura, Tier 4.

- Infraestructura mecánica, Tier 2

Es importante destacar que la clasificación general del CPD se hace empleando el nivel **más bajo** de sus subsistemas, en el caso del ejemplo, el Tier general sería de 2. Se debe tener cuidado al mantener la capacidad del sistema mecánico y eléctrico en el nivel correcto a medida que la carga del centro de datos aumenta con el tiempo. Por ejemplo, un CPD puede verse degradado del nivel 3 o el nivel 4 hasta el nivel 1 o el nivel 2, si se emplea equipo destinado a la redundancia para apoyar nuevos activos de computación o telecomunicaciones.

A continuación, se realiza una descripción breve de los diferentes niveles:

Tier I - Básico: Este nivel se refiere a un CPD básico, con capacidad limitada para soportar interrupciones planificadas o no planificadas. En el caso de querer realizar mantenimientos preventivos o reparaciones, la infraestructura debe apagarse en su totalidad. Los criterios principales para la clasificación Tier I incluyen una única vía de alimentación eléctrica y refrigeración, sin redundancia en los sistemas y una disponibilidad de servicio del 99,671% (aproximadamente 28,8 horas de interrupción al año).

Tier II - Componentes redundantes: En este nivel, se incorpora una mayor redundancia para mejorar la disponibilidad del CPD. A diferencia de los Tier I, estos tienen que contar con un Sistema de Alimentación Ininterrumpida (SAI). Pueden tener componentes redundantes de alimentación eléctrica y enfriamiento, pero siguen teniendo una vía única de distribución, por lo que realizar mantenimiento requiere parar el servicio. La disponibilidad de servicio se incrementa a un 99,741% (aproximadamente 22 horas de interrupción al año).

Tier III - Mantenible de forma concurrente: Este nivel representa un CPD de nivel avanzado con una mayor disponibilidad y redundancia. Los criterios clave para la clasificación Tier III incluyen sistemas de alimentación y refrigeración con redundancia N+1 y la capacidad de realizar mantenimiento planificado sin interrupción de servicios, debido a que tiene al menos dos vías de alimentación eléctrica y de enfriamiento. Sin embargo, actividades no planificadas tales como errores en su operación o fallos espontáneos de los componentes de la infraestructura de las instalaciones aún pueden causar una interrupción del centro de datos.Se requiere una disponibilidad de servicio del 99,982% (aproximadamente 1,6 horas de interrupción al año).

Tier IV - Tolerante a fallos: Este nivel es el más alto en términos de disponibilidad y redundancia. Los criterios para la clasificación Tier IV incluyen sistemas de alimentación y refrige-

ración con redundancia 2N, lo que significa que hay dos sistemas totalmente independientes que pueden funcionar por separado. Estos CPD son completamente redundantes, por lo que pueden soportar fallos espontáneos, ya que cuentan con diferentes rutas de distribución **actuando de forma simultánea**. También se requiere la capacidad de realizar mantenimiento sin interrupciones y una disponibilidad de servicio del 99,995% (aproximadamente 25 minutos de interrupción al año).

2.3 Tier 1

A continuación, se muestran las especificaciones necesarias en un CPD para ser considerado de Tier I.

2.3.1 Telecomunicaciones

a) **General**

El cableado, racks, gabinetes y rutas tienen que cumplir con las especificaciones TIA relevantes. Adicionalmente, los paneles de interconexión, las toma de corriente y el cableado deben etiquetarse según la ANSI/TIA-606-B [6]. Gabinetes y racks deben etiquetarse en su parte delantera y trasera.

2.3.2 Eléctrico

a) **General**

Sobre los puntos único de fallo: pueden existir múltiples puntos únicos de fallo a lo largo del sistema de distribución.
En relación a la realización de diferentes análisis de potencia del sistema, se precisa de un estudio de cortocircuitos actualizado, estudios de coordinación, y análisis del arco eléctrico. En cuanto a los cables de alimentación para el equipo computacional y de telecomunicaciones, es suficiente con un único cable de alimentación con 100% de capacidad.

b) **Suministración eléctrica**

Entrada del suministro eléctrico con alimentación única. No se precisan diferentes proveedores ni entradas, por lo que no es necesaria redundancia.

c) **Cuadro de distribución principal**

El servicio del cuadro puede ser compartido, no tiene por qué ser dedicado. El cuadro debe tratarse de un tablero eléctrico con disyuntores.

d) **Sistema de Alimentación Ininterrumpido**

Debe contarse con una redundancia de tipo N y la topología puede ser Única o Módulos-Paralelos.
Sobre la distribución de la potencia de salida, debe ser un tablero con disyuntores térmicos estándar. Las baterías serán una cadena común de baterías para múltiples módulos y su tipo podrá ser Valve Regulated Lead–Acid (VRLA) de 5 años de duración o inercial (Flywheel).
Se precisa al menos un tiempo mínimo de respaldo de la batería al final de su vida útil de 5 minutos.

e) **Unidad de distribución de potencia**

Es necesario un transformador, que puede tratarse de cualquiera estándar de alta eficiencia.

f) **Tomas de tierra**

Se contempla un sistema de protección contra rayos, basado en análisis de riesgo por la normativa NFPA 780 [7] y requerimientos del seguro.
En cuanto a la infraestructura de toma a tierra del CPD en la sala de ordenadores, el estándar establece que se precisa la requerida por la norma ANSI/TIA-607-B [8].

g) **Apagado de emergencia en la sala de ordenadores**

En este nivel Tier, la instalación es necesaria solo si es requerido por AHJ, y debe tratarse de un pulsador con protección y etiqueta de aviso.

h) **Sistema de generación de reserva**

El generador tiene que estar disponible al menos para albergar carga de la unidad SAI sin redundancia y puede tratarse de un generador con un único Bus.

i) **Mantenimiento del equipo**

Disponibilidad de personal de operación y mantenimiento, pueden estar fuera del CPD y de guardia.

2.3.3 Arquitectura

a) **Requisitos de resistencia al fuego**

Los siguientes partes del CPD deben cumplir los requisitos mínimos establecidos en la construcción del CPD: paredes de carga interiores y exteriores, marco estructural, tabiques interiores de salas no informáticas, tabiques interiores de salas informáticas, suelos y techos.

b) **Tejado**

Sobre la resistencia al levantamiento del viento e inclinación del techo se deben cumplir los mínimos exigidos.

c) **Puertas y ventanas**

Se cumplen los requisitos mínimos exigidos de resistencia al fuego. En relación a los tamaños de las puertas, se exigen los requisitos mínimos y no pueden menores que 1 m (3 ft) de ancho y 2.13 m (7 ft) de alto.
En cuanto a las ventanas en el perímetro de la sala de computación, están permitidas con el mínimo requerido de resistencia al fuego.

d) **Requisitos para las distintas salas del CPD (Vestíbulo, oficina, etc.)**

Solo se exigen los mínimos de separación con la sala de computación en caso de incendios.

e) **Seguridad de control de acceso y monitorización**

Se requieren candados industriales en zonas de generadores, SAI, telefonía, salidas de emergencia y acceso a la sala de computación.

f) **Estructura**

El diseño de la estructura debe ser respecto a los requisitos de International Building Code (IBC) y Seismic Design Category (SDC), concretamente tienen que seguirse los requisitos de

localización de la SDC.
Factor de importancia de I=1.
Se precisa reforzamiento de cables y circuitos eléctricos según el código pertinente.
En cuanto a las capacidades de carga del piso, carga viva superpuesta de $7.2kPa(150lbf/ft^2)$.
Capacidad del techo para soportar cargas colgantes (iluminación, refrigeración, etc.) mínima de $1.2kPa(25lbf/ft^2)$.
El espesor de la losa de hormigón del suelo debe ser de 127 mm (5 in).
Acabado mínimo de hormigón sobre canales para anclaje de equipos cuando se emplea estructura cubierta de metal rellena de hormigón para suelos técnicos, de 102 mm (4 in).
Construcción de suelo técnico con cemento PT.

2.3.4 Infraestructura mecánica

a) **General**

Respecto al enrutamiento de tuberías de agua o drenaje no asociado con el equipo en los espacios del CPD, se permite pero no se recomienda. Son necesarios desagües en la sala de computación para el drenaje de agua que se pueda condensar, de los humidificadores y de los aspersores del techo.

b) **Sistema refrigerado por agua.**

En cuanto a la alimentación del sistema (servicio eléctrico a los equipos mecánicos), basta con un solo camino eléctrico a los equipos.
Sobre el sistema de tuberías, sistema de tuberías de agua fría y de agua condensada, también puede ser de vía única, sin redundancia.

c) **Sistema refrigerado por aire.**

Al igual que en el apartado anterior, en el servicio eléctrico a los equipos mecánicos basta con un solo camino eléctrico a los equipos, no se contempla redundancia.

d) **Sistema de control Heating Ventilating Air Conditioned (HVAC)**

Se permite que fallos en el sistema de control suponen interrupción de enfriamiento en zonas críticas. En el estándar se permite una única vía de alimentación eléctrica en este Tier.

e) **Cañerías para el rechazo de calor con agua fría**

En relación al suministro de agua de reposición, puede tratarse de un suministro único de agua, sin respaldo, con un único punto de conexión.

f) **Sistema de combustible**

Un único tanque de almacenamiento, de bomba y tubería única.

g) **Supresión de incendios**

El estándar requiere un sistema de detección de incendios, con un sistema de aspersores incluido. Además, sistemas de supresión de gases, detectores de humo temprano y de filtraciones de agua no se requieren por encima de AHJ.

2.4 Tier 2

A continuación, se muestran las especificaciones necesarias en un CPD para ser considerado de Tier 2.

2.4.1 Telecomunicaciones

a) **General**

El cableado, racks, gabinetes y rutas tienen que cumplir con las especificaciones TIA relevantes. Además, deben existir varias entradas enrutadas de proveedores de acceso y agujeros de mantenimiento con una separación mínima de 20 m.
Los paneles de interconexión, las toma de corriente y el cableado deben etiquetarse según la ANSI/TIA-606-B. Adicionalmente, gabinetes y racks deben etiquetarse en su parte delantera y trasera.
En cuanto a routers y switches, estos deben tener fuentes de alimentación redundantes.
Los cables de conexión y jumpers han de estar etiquetados en ambos extremos con el nombre de la conexión a ambos extremos del cable.

2.4.2 Eléctrico

a) **General**

Se establece que el sistema permite mantenimiento concurrente al menos en el suministro externo, generador y unidad SAI. En cuanto a los puntos únicos de fallo, pueden existir múltiples puntos únicos de fallo a lo largo del sistema de distribución, tal y como pasaba en el Tier 1.
Sobre el análisis de potencia del sistema, ha de tenerse un estudio de cortocircuitos actualizado, estudio de coordinación, y análisis del arco eléctrico.
En cuanto a la alimentación para el equipo computacional y de telecomunicaciones, puede tratarse de un único cable de alimentación con 100% de capacidad.

b) **Suministración eléctrica**

Entrada del suministro eléctrico con alimentación única. No se precisan diferentes proveedores ni entradas, por lo que no es necesaria redundancia.

c) **Cuadro de distribución principal**

El servicio del cuadro puede ser compartido, no tiene por qué ser dedicado. El cuadro debe tratarse de un tablero eléctrico con disyuntores automáticos estacionarios.

d) **Sistema de Alimentación Ininterrumpido**

En relación al SAI, este ya debe contar con redundancia de tipo N. Su topología puede ser Única o Módulos-Paralelos, al igual que en el nivel anterior. Debe contar con un bypass automático con un alimentador que no tiene por qué ser dedicado dedicado. A su vez, dispondrá también de un bypass de mantenimiento con un alimentador no dedicado a la salida del SAI en el cuadro de distribución.
Sobre la distribución de la potencia de salida, se contará con un tablero con disyuntores térmicos estándar.
Las baterías del SAI estarán dedicadas para cada módulo y su tipo podrá ser Valve Regulated Lead–Acid (VRLA) de 10 años de duración, inercial (Flywheel) o inundada.
El tiempo mínimo de respaldo de la batería al final de su vida útil será de 7 minutos.

e) **Unidad de distribución de potencia**

Es necesario un transformador, que puede tratarse de cualquiera estándar de alta eficiencia.

f) **Tomas de tierra**

Se contempla un sistema de protección contra rayos, basado en análisis de riesgo por la normativa NFPA 780 y requerimientos del seguro.
En cuanto a la infraestructura de toma a tierra del CPD en la sala de ordenadores, el estándar establece que se precisa la requerida por la norma ANSI/TIA-607-B.

g) **Apagado de emergencia en la sala de ordenadores**

En este nivel Tier, la instalación es necesaria solo si es requerido por AHJ, y debe tratarse de un pulsador con protección y etiqueta de aviso.

h) **Monitorización de energía central**

Se realizará monitorización de las siguientes zonas: suministro eléctrico externo, SAI y generador. Para notificar incidencias, se realizará mediante la consola de la sala de control.

i) **Sistema de generación de reserva**

El generador debe contar con la capacidad para albergar carga de la unidad SAI y los sistemas mecánicos sin redundancia. De la misma forma que en el Tier 1, los generadores podrán contar con un único Bus.

j) **Banco de carga**

La instalación podrá ser portátil, sin necesidad de estar situado en el CPD y el equipo testeado será al menos el generador.

k) **Testing**

A diferencia del nivel anterior, se realizará comisionamiento a nivel de componentes.

l) **Mantenimiento del equipo**

En relación a la disponibilidad de personal de operación y mantenimiento, solo durante el turno de día tendrán que estar presentes en el CPD. De guardia en otros horarios.
Se realizará mantenimiento preventivo mínimo en el generador.
Tendrán que llevarse a cabo programas de capacitación de la instalación para el personal, sin

embargo no serán extensos y correrán de la cuenta del fabricante de los equipos.

2.4.3 Arquitectura

a) **Elección del sitio de construcción del CPD**

Para la elección del sitio de construcción, sin inundaciones en los últimos 50 años. El edificio puede estar ocupado por otros inquilinos, pero solo en el caso de que las ocupaciones no sean peligrosas, es decir , instalaciones que puedan suponer riesgos al encontrarse el CPD en sus cercanías, tales como laboratorios.

b) **Requisitos de resistencia al fuego**

Los siguientes partes del CPD deben cumplir los requisitos mínimos establecidos en la construcción del CPD: paredes de carga interiores y exteriores, marco estructural, tabiques interiores de salas no informáticas, tabiques interiores de salas informáticas, suelos y techos.
Adicionalmente, tendrán que cumplir con los requerimientos de la NFPA 75 [9], la normativa para la protección contra incendios para los equipos TI.

c) **Varios componentes de construcción**

En cuanto a barreras de vapor para las paredes y techo de la sala de computación, sí son requeridas para las paredes, pero no son necesarias para el techo.

d) **Tejado**

El tejado del CPD debe ser de Clase A, altamente resistente a incendios.Además, debe contar con un factor de resistencia al levantamiento del viento de FM I-90. La inclinación del techo debe seguir los mínimos requeridos por la norma vigente.

e) **Puertas y ventanas**

Se cumplen los requisitos mínimos exigidos de resistencia al fuego. En relación a los tamaños de las puertas, se exigen los requisitos mínimos y no pueden menores que 1 m (3 ft) de ancho y 2.13 m (7 ft) de alto.
En cuanto a las ventanas en el perímetro de la sala de computación, están permitidas con el mínimo requerido de resistencia al fuego.

f) **Requisitos para las distintas salas del CPD**

El vestíbulo debe contar con los requisitos mínimos de separación con la sala de computación en caso de incendios y estar físicamente separado de otras áreas del CPD.
Sobre las oficinas administrativas, también deben contar con los requisitos mínimos de separación con la sala de computación en caso de incendios y estar físicamente separado de otras áreas del CPD.
La oficina de seguridad debe contar con los mismos requisitos que las salas anteriores y adicionalmente con mirillas de 180 grados en salas de vigilancia, equipos de seguridad dedicados y reforzados y salas de monitorización.

g) **Zona de carga y descarga**

A este nivel de Tier no se requiere como tal. En caso de tenerla, el número de muelles de carga debe ser 1 cada $2500m^2(25.000ft^2)$ de sala de computación.

h) **Seguridad**

Hablando de la capacidad del SAI para la CPU del sistema, este debe contar con la capacidad suficiente para soportar la carga de trabajo del edificio entero.
Sobre la capacidad del SAI para los paneles de recopilación de datos, debe poder soportar la carga de trabajo del edificio entero y las baterías adicionales (durante 4 horas mínimo). Se seguirá el mismo criterio para la capacidad del SAI para los dispositivos de campo.
Adicionalmente, en este Tier se contempla la presencia de personal de seguridad físico, durante el funcionamiento programado del CPD (típicamente 5 días a la semana durante horas laborales normales).

i) **Seguridad de control de acceso y monitorización**

Los generadores, SAI, telefonía y salas Mechanical, Electrical and Pumbling (MEP) deben contar con sistemas de detección de intrusiones. Adicionalmente, las salidas de emergencia deben estar monitorizadas.
En cuanto a ventanas o aperturas accesibles desde el exterior y puertas de acceso al perímetro, se contará también con un sistema de detección de intrusiones (con vigilancia ”offsite” durante los turnos en los que el personal de seguridad no está presente).
Todas aquellas habitaciones con equipo de seguridad y salas de ordenadores deberán contar

también con este tipo de sistemas.
Por último, la entrada principal a la sala de computación estará protegida mediante un acceso con tarjeta.

j) **Monitorización Circuito Cerrado de Televisión (CCTV)**

En el Tier 2, solo será necesario en puertas con control de acceso.

k) **Estructura**

El diseño de la estructura debe ser respecto a los requisitos de International Building Code (IBC) y Seismic Design Category (SDC), concretamente tienen que seguirse los requisitos de localización de la SDC.
Factor de importancia de I=1.5.
Se precisa reforzamiento de cables y circuitos eléctricos según el código pertinente. Adicionalmente, los equipos de comunicaciones (tales como racks), deben estar anclados al suelo.
En cuanto a las capacidades de carga del piso, carga viva superpuesta de $8.4kPa(175lbf/ft^2)$.
Capacidad del techo para soportar cargas colgantes (iluminación, refrigeración, etc.) mínima de $1.2kPa(25lbf/ft^2)$.
El espesor de la losa de hormigón del suelo debe ser de 127 mm (5 in).
Acabado mínimo de hormigón sobre canales para anclaje de equipos cuando se emplea estructura cubierta de metal rellena de hormigón para suelos técnicos, de 102 mm (4 in).
Construcción de suelo técnico con cemento CIP Mild.

2.4.4 Infraestructura mecánica

a) **General**

Es necesaria la presencia de redundancia de equipo mecánico (unidades de aire acondicionado, refrigeración , bombas, condensadores, torres de refrigeración) de tipo N+1, la pérdida de electricidad puede generar pérdida de refrigeración. Sobre el enrutamiento de tuberías de agua o drenaje no asociado con el equipo en los espacios del CPD, este se permite pero no se recomienda, ya que puede suponer problemas.
La presión en la sala de computación y espacios asociados con el exterior debe ser positiva.
El estándar exige la existencia de desagües en la sala de computación para el drenaje de agua que se pueda condensar, de los humidificadores y de los aspersores del techo. Por último, los sistemas mecánicos (refrigeración, supresión de incendios...) deben estar respaldados por un

generador de emergencia.

b) **Sistema refrigerado por agua.**

Sobre el sistema refrigerado por agua, en el caso de unidades de aire acondicionado para interiores, deben existir al menos una unidad redundante por cada área crítica. Además, debe tenerse un control de humedad en la sala de computación.
En cuanto a la alimentación eléctrica (servicio eléctrico a los equipos mecánicos), basta con un solo camino eléctrico a los equipos, sin redundancia.
Los sistemas de tuberías, sistemas de tuberías de agua fría y de agua condensada pueden ser de vía única igualmente, no se precisa redundancia para la distribución.

c) **Sistema refrigerado por aire.**

En cuanto a la alimentación eléctrica (servicio eléctrico a los equipos mecánicos), basta con un solo camino eléctrico a los equipos, sin redundancia. De la misma forma que en el apartado anterior, debe tenerse un control de humedad en la sala de computación.

d) **Sistema de control Heating Ventilating Air Conditioned (HVAC)**

Los fallos en el sistema de control NO suponen interrupción de enfriamiento en zonas críticas. Sin embargo, aquí si que son necesarias vías de alimentación eléctrica redundantes.

e) **Cañerías para el rechazo de calor con agua fría**

En este ámbito, en relación al agua de reposición, debe contarse con un suministro doble de agua, o suministro único pero con almacenamiento de respaldo en el CPD, pero se permite un único punto de conexión.

f) **Sistema de combustible**

La normativa indica que se puede contar con un único tanque de almacenamiento, pero este ha de tener varias bombas y tuberías de suministro.

g) **Supresión de incendios**

El estándar requiere para este nivel Tier un sistema de detección de incendios, con un sistema

de aspersores incluido (de preacción). Además, es necesario un sistema de supresión de gases, así como de detección temprana de humo y de filtraciones de agua.

2.5 Tier 3

Comparando los niveles anteriores, vemos como no hay una diferencia excesiva entre los requisitos de un CPD con certificación Tier 1 y Tier 2, el gran salto se produce a partir del Tier 3. A continuación, se muestran las especificaciones necesarias en un CPD para ser considerado de Tier 3.

2.5.1 Telecomunicaciones

a) **General**

En primer lugar, el cableado, racks, gabinetes y rutas tienen que cumplir con las especificaciones TIA relevantes.
Es obligatorio contar con varias entradas enrutadas de proveedores de acceso y con varios proveedores (existencia de redundancia) y agujeros de mantenimiento con una separación mínima de 20 m, así como la entrada de acceso también debe ser redundante.
Las rutas y el cableado vertical deben estar redundados. A su vez, se cuenta con routers redundantes y switches con puertos Uplink redundantes. En cuanto a los paneles de interconexión, las tomas de corriente y el cableado deben etiquetarse según la ANSI/TIA-606-B. Gabinetes y racks deben etiquetarse en su parte delantera y trasera.
Es necesario adicionalmente que los routers y switches tengan fuentes de alimentación redundantes. Los cables de conexión y jumpers deben ser etiquetados en ambos extremos con el nombre de la conexión a ambos extremos del cable. Por último, los paneles de conexión y sus cables estarán documentados de acuerdo a la ANSI/TIA-606-B.

2.5.2 Eléctrico

a) **General**

En cuanto al subsistema eléctrico, el sistema debe permitir mantenimiento concurrente en todo salvo la unidad de distribución de energía. Solo se permite un único punto de fallo desde el último panel de distribución hasta solamente la carga crítica y esencial.
En cuanto a la realización de análisis de potencia del sistema, se contará con un estudio de cortocircuitos actualizado, estudios de coordinación, análisis del arco eléctrico y del flujo de carga.

Sobre los cables de alimentación para el equipo computacional y de telecomunicaciones, deben ser redundantes con 100% de capacidad.

b) **Suministración eléctrica**

Sobre la suministración eléctrica, la entrada del suministro eléctrico debe contar con alimentación con redundancia N+1, a diferencia de lo que se pedía para los Tier anteriores.

c) **Cuadro de distribución principal**

El servicio del cuadro de distribución principal debe ser dedicado, y este debe contar con disyuntores extraíbles. Además, a diferencia de los niveles anteriores debe contar con un supresor de sobretensiones.

d) **Sistema de Alimentación Ininterrumpido**

En cuanto a las indicaciones sobre el SAI, la redundancia debe ser de tipo N+1 y su topología de módulos redundantes distribuidos. Además contará con un sistema de bloqueo redundante. El SAI dispondrá de bypass automático, con un alimentador dedicado y también con un bypass de mantenimiento, igualmente con un alimentador dedicado a la salida del SAI en el cuadro de distribución.
Sobre la distribución de la potencia de salida, constará de un cuadro de conexiones con disyuntores extraíbles y función de disparo instantáneo.
Las baterías estarán dedicadas para cada módulo del SAI y su tipo podrá ser Valve Regulated Lead–Acid (VRLA) de 15 años de duración, inercial (Flywheel) o inundada.
El tiempo mínimo de respaldo de la batería al final de su vida útil será 10 minutos y se llevará a cabo monitorización de las mismas.

e) **Unidad de distribución de potencia**

El transformador empleado deberá ser k-rated o de cancelación de armonías y será de alta eficiencia.

f) **Interruptor de transferencia estática automática**

Contará con un disyuntor en caso de corrientes excesivas y el procedimiento del bypass para mantenimiento será manual con enclavamiento mecánico. El output contará con disyuntores

duales.

g) **Tomas de tierra**

Al igual que en los niveles anteriores, será necesario un sistema de protección contra rayos. Además, los aparatos de iluminación estarán conectados a un circuito neutral aislado del punto de entrada del servicio eléctrico, derivado de un transformador de iluminación con el propósito de aislar y proteger contra fallas a tierra.
En relación a la infraestructura de toma a tierra del CPD en la sala de ordenadores será la requerida por la norma ANSI/TIA-607-B.

h) **Apagado de emergencia en la sala de ordenadores**

El apagado de emergencia estará instalado solo si es requerido por AHJ, siendo un pulsador con protección y etiqueta de aviso. Contará con modo test disponible, alarma y con un interruptor para abortar (según permitan los códigos locales).

i) **Monitorización de energía central**

En relación a la monitorización, estarán monitorizadas las siguientes salas: suministro externo, SAI, generador, transformador principal, circuitos de alimentación, Power Distribution Unit (PDU), switches de transferencia automáticos.El método de notificación se realizará mediante la consola de la sala de control, email o mensaje de texto.

j) **Sala de baterías**

Esta sala debe estar separada de la sala del SAI y se tratará de cadenas de baterías individuales separadas unas de otras.

k) **Sistema de generación de reserva**

El generador debe poder albergar la carga total del edificio y con redundancia distribuida N+1. A diferencia de lo que ocurría en los niveles anteriores, no se permiten generadores con un único Bus.

l) **Banco de carga**

La instalación sigue siendo portátil, sin necesidad de estar fija en el CPD, el equipo testeado serán generadores y SAI. Se contará con un apagado automático al fallo.

m) **Testing**

En cuanto al testing, las pruebas de aceptación de fábrica son obligatorias para el SAI y generador. También se realizarán pruebas de los disyuntores, que serán pruebas de resistencia a todos los disyuntores en zonas críticas y vías esenciales, las pruebas serán de 225 A o superiores. Adicionalmente se realizará comisionamiento a nivel de componentes.

n) **Mantenimiento del equipo**

Se contará con personal de operación y mantenimiento disponible 24 horas de lunes a viernes y de guardia en fines de semana. Adicionalmente se realizará mantenimiento preventivo en el generador y el SAI.
Es necesario llevar a cabo programas de capacitación de la instalación, que se tratarán de programas de formación integral para el funcionamiento normal de los equipos.

2.5.3 Arquitectura

a) **Elección del sitio de construcción del CPD**

El CPD debe estar en un zona sin inundaciones en los últimos 100 años y a más de 91 m (300 ft) de distancia de zonas con alguna inundación en los últimos 50 años.
Su proximidad a vías navegables interiores o costeras tiene que ser mayor a 91 m (300 ft). En relación a su proximidad a autopistas o vías de tren también será mayor a 91 m (300 ft). En el caso de aeropuertos cercanos, deben estar a más de 1.6 km (1 mile), y menos de 48 km (30 miles) del CPD. En cuanto a la ocupación del edificio por otros inquilinos, se permitirá solo si las ocupaciones son de otros CPD o compañías de telecomunicación.

b) **Aparcamiento**

El aparcamiento estará físicamente separado para empleados y visitantes, con entradas separadas.Adicionalmente, tendrá que estar también separado físicamente de muelles de carga y con entradas separadas.
La proximidad entre el aparcamiento de visitantes y las paredes del perímetro del CPD debe contar con al menos 9.1 m (30 ft) de separación, con barreras físicas para prevenir a vehículos conducir cerca.

c) **Construcción del edificio**

Tipo de construcción en relación a sus características de resistencia al fuego: Tipo IIA, IIIA o VA.

d) **Requisitos de resistencia al fuego**

Los siguientes partes del CPD deben cumplir con al menos 1 hora de resistencia a fuegos: paredes de carga interiores y exteriores, marco estructural, tabiques interiores de salas no informáticas, tabiques interiores de salas informáticas, suelos y techos.
Adicionalmente, tendrán que cumplir con los requerimientos de la NFPA 75, la normativa para la protección contra incendios para los equipos TI.

e) **Varios componentes de construcción**

Deben existir barreras de vapor para las paredes y techo de la sala de computación. Todas las entradas del edificio contarán con controles de seguridad (la entrada principal del edificio con personal incluido).
Los paneles de suelo técnico serán de acero y su subestructura de larguero atornillado.

f) **Tejado**

El tejado debe ser de clase A. No tiene por qué ser redundante, con plataforma no combustible. Sobre la resistencia al levantamiento del viento será FM I-90 mínimo. La inclinación del techo será de 1:48 (1/4 por pie) mínimo.

g) **Puertas y ventanas**

Se cumplen los requisitos mínimos exigidos de resistencia al fuego, pero no pueden ser menos de 3/4 horas de resistencia en las puertas de la sala de computación. En relación a los tamaños de las puertas, se exigen los requisitos mínimos y no pueden menores que 1 m (3 ft) de ancho y 2.13 m (7 ft) de alto.
En cuanto a las ventanas en el perímetro de la sala de computación, están permitidas con al menos 1 hora de resistencia al fuego.

h) **Requisitos para las distintas salas del CPD**

- Vestíbulo: seguirán los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de una hora). El vestíbulo tendrá que estar físicamente separado de otras áreas del CPD, con un control de seguridad y hardware para evitar Piggybacking o Pass back

- Oficinas administrativas: cumplen los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de una hora). Estará físicamente separado de otras áreas del CPD.

- Oficina de seguridad: seguirán los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de una hora). Mirillas de 180 grados en equipos de seguridad y salas de vigilancia. Equipos de seguridad dedicados y reforzados y salas de monitorización, paredes revestidas de madera contrachapada y puertas de núcleo sólido. Físicamente separado de otras áreas del CPD.

- Centro de operaciones: tiene que estar físicamente separado de otras áreas del CPD. Separación mínima de una hora en caso de incendio con otras áreas no computacionales del CPD. No tiene por qué tener acceso directo a la sala de computación (máximo 1 sala adjunta).

- Salas y zonas de descanso: si son adyacentes a la sala de computación, deben estar dotadas con barreras de prevención de fugas. Separación mínima de una hora en caso de incendio con otras áreas no computacionales del CPD.

- Salas de Baterías y de SAI: adyacentes a la sala de computación. Separación mínima de una hora en caso de incendio con otras áreas del CPD. Anchos de pasillo para mantenimiento, reparación o eliminación de equipo de no menos de 1 m (3 ft) libre.

- Pasillos de emergencia: tendrán una separación mínima de una hora en caso de incendio con otras áreas del CPD. Ancho libre de no menos de 1,2 m (4 ft).

- Salas de generadores o de almacenamiento de combustible: si se encuentran dentro del CPD, provistas mínimo de 2 horas de separación en caso de incendio con otras áreas. Su proximidad a otras áreas de acceso público no puede ser menor a 9 m (30 ft).

i) **Zona de carga y descarga**

Estas zonas deben estar separadas físicamente de otras zonas del CPD, con una separación mínima de una hora en caso de incendio con otras áreas. En cuanto a la protección física de paredes expuestas a zonas donde se emplea maquinaria de levantamiento de carga, será mínimo 19 mm (3/4 in) de madera contrachapada.
Existirá un muelle de carga cada $2500m^2 (25.000ft^2)$ de sala de computación (2 mínimo).

j) **Seguridad**

Hablando de la capacidad del SAI para la CPU del sistema, este debe contar con la capacidad suficiente para soportar la carga de trabajo del edificio entero.
Sobre la capacidad del SAI para los paneles de recopilación de datos, debe poder soportar la carga de trabajo del edificio entero y las baterías adicionales (durante 8 horas mínimo). Se seguirá el mismo criterio para la capacidad del SAI para los dispositivos de campo.
Adicionalmente, en este Tier se contempla la presencia de personal de seguridad físico 7 días a la semana durante las 24 horas del día. También se contará con paredes, puertas y ventanas antibalas de nivel 3 mínimo.

k) **Seguridad de control de acceso y monitorización**

Los generadores, SAI, telefonía y salas Mechanical, Electrical and Pumbling (MEP) deben contar con sistemas de acceso mediante tarjeta, las salidas de emergencia tendrán un código de acceso. En cuanto a ventanas o aperturas accesibles desde el exterior y puertas de acceso al perímetro, se contará con un sistema de detección de intrusiones.
Todas aquellas habitaciones con equipo de seguridad y salas de ordenadores deberán contar con accesos mediante tarjeta. Las puertas en la sala de computación estarán protegidas mediante un acceso con tarjeta o biométrico, y la entrada principal contará con un control de seguridad y hardware para evitar Piggybacking o Pass back

l) **Monitorización Circuito Cerrado de Televisión (CCTV)**

Este tipo de monitorización se llevará a cabo en puertas con control de acceso, en el perímetro del edificio y aparcamiento, generadores, salas de computación, en el SAI, telefonía y salas Mechanical, Electrical and Pumbling (MEP).

m) **Circuito Cerrado de Televisión (CCTV)**

Se realizará grabación digital CCTV de toda la actividad en todas las cámaras, con una tasa

de grabación de 20 frames/sec mínima.

n) **Estructura**

El diseño de la estructura debe ser respecto a los requisitos de International Building Code (IBC) y Seismic Design Category (SDC), concretamente tienen que seguirse los requisitos de localización de la SDC. Adicionalmente respecto al nivel anterior, se tendrá en cuenta el grado de aceleración sísmica local, con un estado de operación de un 10% en 50 años.
Factor de importancia de I=1.5.
Se precisa reforzamiento de cables y circuitos eléctricos según la importancia de los mismos. Adicionalmente, los equipos de comunicaciones (tales como racks), deben estar anclados al suelo o reforzados completamente y la limitación de la desviación en el equipo de telecomunicaciones debe estar dentro de los límites aceptables.
En cuanto a las capacidades de carga del piso, carga viva superpuesta de $12kPa(250lbf/ft^2)$. Capacidad del techo para soportar cargas colgantes (iluminación, refrigeración, etc.) mínima de $2.4kPa(50lbf/ft^2)$.
El espesor de la losa de hormigón del suelo debe ser de 127 mm (5 in).
Acabado mínimo de hormigón sobre canales para anclaje de equipos cuando se emplea estructura cubierta de metal rellena de hormigón para suelos técnicos, de 102 mm (4 in). A diferencia del nivel anterior, en el Tier 3 el edificio debe estar diseñado para disipar energía en caso de seísmos.
La construcción de suelo técnico se realizará con Steel deck & Fill.

2.5.4 Infraestructura mecánica

a) **General**

En cuanto a este tipo de infraestructura, existirá redundancia de equipo mecánico (unidades de aire acondicionado, refrigeración , bombas, condensadores, torres de refrigeración) al menos N+1, la pérdida de electricidad no genera pérdida de refrigeración, pero puede significar el aumento de la temperatura en equipo crítico.
En cuanto al enrutamiento de tuberías de agua o drenaje no asociado con el equipo en los espacios del CPD, este no estará permitido. Además, se requiere presión positiva en la sala de computación y espacios asociados con el exterior.
Es obligatoria la presencia de desagües en la sala de computación para el drenaje de agua que se pueda condensar, de los humidificadores y de los aspersores del techo. Por último, los sistemas mecánicos (refrigeración, supresión de incendios...) estarán respaldados por un ge-

nerador de emergencia.

b) **Sistema refrigerado por agua.**

Sobre las unidades de aire acondicionado para interiores, se deben contar con la cantidad suficiente de unidades de aire para mantener áreas críticas durante la pérdida de una unidad o de la electricidad, existiendo redundancia clara. También se contempla el control de humedad en la sala de computación.
Sobre el servicio eléctrico a los equipos mecánicos, se precisan múltiples caminos eléctricos a los equipos de aire acondicionado, conectados de forma que exista redundancia. Adicionalmente existirá un sistema de tuberías y de agua condensada, de tuberías paralelas en ambos sistemas. El sistema de tuberías para agua fría contará con un bucle de doble camino para el agua fría con válvulas de aislamiento.

c) **Sistema refrigerado por aire.**

Al igual que en el apartado anterior, el servicio eléctrico a los equipos mecánicos constará de múltiples caminos eléctricos a los equipos y también se realizará un control de humedad en la sala de computación.

d) **Sistema de control Heating Ventilating Air Conditioned (HVAC)**

Los fallos en el sistema de control NO suponen interrupción de enfriamiento en zonas críticas y existen vías de alimentación eléctrica redundantes.

e) **Cañerías para el rechazo de calor con agua fría**

Sobre el agua de reposición, el CPD necesita contar con un suministro doble de agua, o suministro único pero con almacenamiento de respaldo en el CPD y al menos dos puntos de conexión.

f) **Sistema de combustible**

A diferencia de los Tiers anteriores, existirán múltiples tanques de almacenamiento, con varias bombas y tuberías de suministro.

g) **Supresión de incendios**

El estándar requiere para este nivel Tier un sistema de detección de incendios, con un sistema de aspersores incluido (de preacción). Además, es necesario un sistema de supresión de gases (contemplando los agentes limpios listados en la NFPA 200 [10]), así como de detección temprana de humo y de filtraciones de agua.

2.6 Tier 4

El Tier 4 es el máximo nivel contemplado, por lo que contará con los requisitos más específicos y severos. A continuación, se muestran las especificaciones necesarias en un CPD para ser considerado de Tier 4.

2.6.1 Telecomunicaciones

a) **General**

El cableado, racks, gabinetes y rutas deben cumplir con especificaciones TIA relevantes. El CPD contará con Varias entradas enrutadas de proveedores de acceso y agujeros de mantenimiento con una separación mínima de 20 m. Adicionalmente, se dispondrá de múltiples proveedores de acceso.
El área de distribución principal y las áreas de distribución intermedias deben ser redundantes (en el caso de las intermedias, solo si existen). En el caso del cableado, las rutas y cableado tanto vertical como horizontal deben estar redundados.
En cuanto a equipamiento de red, routers redundantes y switches con puertos Uplink redundantes. Los paneles de interconexión, las tomas de corriente y el cableado deben etiquetarse según la ANSI/TIA-606-B. Gabinetes y racks deben etiquetarse en su parte delantera y trasera y los routers y switches tendrán fuentes de alimentación redundantes.
Los cables de conexión y jumpers estarán etiquetados en ambos extremos con el nombre de la conexión a ambos extremos del cable y los paneles de conexión y sus cables documentados de acuerdo a la ANSI/TIA-606-B.

2.6.2 Eléctrico

a) **General**

En cuanto al subsistema eléctrico, el sistema debe permitir mantenimiento concurrente en todo el sistema de distribución de energía. No se permiten puntos únicos de fallo en los sistemas

de distribución que dan servicio a equipo eléctrico o carga esencial.
En cuanto a la realización de análisis de potencia del sistema, se contará con un estudio de cortocircuitos actualizado, estudios de coordinación, análisis del arco eléctrico y del flujo de carga.
Sobre los cables de alimentación para el equipo computacional y de telecomunicaciones, deben ser redundantes con 100% de capacidad.

b) **Suministración eléctrica**

En relación a la entrada del suministro eléctrico, la alimentación tendrá redundancia 2N, proveniente de diferentes subestaciones, para asegurar la continuidad del suministro. Se contempla aquí una gran diferencia con el Tier 3, ya que la redundancia 2N implica dos sistemas actuando simultáneamente, lo cual se traduce en mejor servicio pero con mayor complejidad y gasto.

c) **Cuadro de distribución principal**

El servicio del cuadro de distribución principal debe ser dedicado, y este debe tratarse de una subestación de control con disyuntores extraíbles. Al igual que en el Tier 3 se debe contar con un supresor de sobretensiones.

d) **Sistema de Alimentación Ininterrumpido**

En cuanto a las indicaciones sobre el SAI, la redundancia debe ser de tipo 2N y su topología de módulos redundantes distribuidos. Además contará con un sistema de bloqueo redundante. El SAI dispondrá de bypass automático, con un alimentador dedicado y también con un bypass de mantenimiento, igualmente con un alimentador dedicado a la salida del SAI en el cuadro de distribución.
Sobre la distribución de la potencia de salida, constará de un cuadro de conexiones con disyuntores extraíbles, con funciones ajustables de tiempo largo, corto e instantáneas, además de la posibilidad de desactivar la función instantánea.
Las baterías estarán dedicadas para cada módulo del SAI y su tipo podrá ser Valve Regulated Lead–Acid (VRLA) de 20 años de duración, inercial (Flywheel) o inundada.
El tiempo mínimo de respaldo de la batería al final de su vida útil será 15 minutos y se llevará a cabo monitorización de las mismas, mediante un sistema centralizado para comprobar voltaje y resistencia de cada célula.

e) **Unidad de distribución de potencia**

El transformador empleado deberá ser k-rated o de cancelación de armonías y será de alta eficiencia.

f) **Interruptor de transferencia estática automática**

Contará con un disyuntor en caso de corrientes excesivas y el procedimiento del bypass para mantenimiento será de operación automática para este nivel Tier. El output contará con disyuntores duales.

g) **Tomas de tierra**

Al igual que en los niveles anteriores, será necesario un sistema de protección contra rayos. Además, los aparatos de iluminación estarán conectados a un circuito neutral aislado del punto de entrada del servicio eléctrico, derivado de un transformador de iluminación con el propósito de aislar y proteger contra fallas a tierra.
En relación a la infraestructura de toma a tierra del CPD en la sala de ordenadores será la requerida por la norma ANSI/TIA-607-B.

h) **Apagado de emergencia en la sala de ordenadores**

El apagado de emergencia estará instalado solo si es requerido por AHJ, siendo un pulsador con protección y etiqueta de aviso. Contará con modo test disponible, alarma y con un interruptor para abortar (según permitan los códigos locales).

i) **Monitorización de energía central**

En relación a la monitorización, estarán monitorizadas las siguientes salas: suministro externo, SAI, generador, transformador principal, circuitos de alimentación, Power Distribution Unit (PDU), switches de transferencia automáticos, dispositivos de protección contra sobretensiones y los circuitos de carga crítica. El método de notificación se realizará mediante la consola de la sala de control, email o mensaje de texto a diferente personal de la instalación.

j) **Sala de baterías**

Esta sala debe estar separada de la sala del SAI y se tratará de cadenas de baterías individuales

separadas unas de otras. La sala contará con cristal a prueba de roturas en la puerta de la sala de baterías.

k) **Sistema de generación de reserva**

El generador debe poder albergar la carga total del edificio y con redundancia distribuida N2. Al igual que en el nivel Tier anterior, no se permiten generadores con un único Bus.

l) **Banco de carga**

Por primera vez en los diferentes niveles, se exige que el banco de carga sea permanente para los equipos más grandes, el equipo testeado serán generadores y SAI. Se contará con un apagado automático al fallo.

m) **Testing**

En cuanto al testing, las pruebas de aceptación de fábrica son obligatorias para el SAI y generador, así como de los controles de los generadores y sistemas de pruebas automáticas de software. También se realizarán pruebas de los disyuntores, que serán pruebas de inyección primaria y de resistencia a todos los disyuntores en zonas críticas y vías esenciales, las pruebas serán de 225 A o superiores. Adicionalmente se realizará comisionamiento a nivel de componentes.

n) **Mantenimiento del equipo**

Se contará con personal de operación y mantenimiento disponible 24 horas los siete días a la semana. Adicionalmente se realizarán programas de mantenimiento preventivo integral.
Es necesario llevar a cabo programas de capacitación de la instalación, que se tratarán de programas de formación integral para el funcionamiento de los equipos tanto en situaciones normales como en casos de emergencia.

2.6.3 Arquitectura

a) **Elección del sitio de construcción del CPD**

Al igual que en Tier 3, el CPD debe estar en un zona sin inundaciones en los últimos 100 años y a más de 91 m (300 ft) de distancia de zonas con alguna inundación en los últimos 50 años.

Su proximidad a vías navegables interiores o costeras tiene que ser mayor que 0.8 km (1/2 mile). En relación a su proximidad a autopistas o vías de tren también será mayor a 0.8 km m (1/2 mile). En el caso de aeropuertos cercanos, deben estar a más de 8 km (5 mile), y menos de 48 km (30 miles) del CPD. En cuanto a la ocupación del edificio por otros inquilinos, se permitirá solo si las ocupaciones son de otros CPD o compañías de telecomunicación.

b) **Aparcamiento**

El aparcamiento estará físicamente separado para empleados y visitantes, con entradas separadas. Adicionalmente, tendrá que estar separado físicamente de muelles de carga y con entradas separadas.
La proximidad entre el aparcamiento de visitantes y las paredes del perímetro del CPD debe contar con al menos 18.3 m (60 ft) de separación, con barreras físicas para prevenir a vehículos conducir cerca.

c) **Construcción del edificio**

Tipo de construcción en relación a sus características de resistencia al fuego: Tipo IA o 1B.

d) **Requisitos de resistencia al fuego**

Los siguientes partes del CPD deben cumplir con al menos 4 horas de resistencia a fuegos: paredes exteriores tanto de carga como normales. El marco estructural, las paredes de carga interiores, los tabiques interiores de salas informáticas, suelos y techos deberán contar con al menos 2 horas mínimo de resistencia a fuegos. Por último, los tabiques interiores de salas no informáticas deberán contar con 1 hora de resistencia.
Adicionalmente, tendrán que cumplir con los requerimientos de la NFPA 75, la normativa para la protección contra incendios para los equipos TI.

e) **Varios componentes de construcción**

Deben existir barreras de vapor para las paredes y techo de la sala de computación. Todas las entradas del edificio contarán con controles de seguridad (la entrada principal del edificio con personal incluido).
Los paneles de suelo técnico serán de acero o de acero con relleno de cemento y su subestructura de larguero atornillado (de 1.2m x 1.2m o 4ft x 4ft siguiendo del patrón de ”tejido de cesta”).

f) **Tejado**

El tejado debe ser de clase A, de tipo redundancia doble y con plataforma de cemento. Sobre la resistencia al levantamiento del viento será FM I-120 mínimo. La inclinación del techo será de 1:24 (1/2 por pie) mínimo.

g) **Puertas y ventanas**

Se cumplen los requisitos mínimos exigidos de resistencia al fuego, pero no pueden ser menos de 1/2 horas de resistencia en las puertas de la sala de computación. En relación a los tamaños de las puertas, se exigen los requisitos mínimos y no pueden ser menores que 1.2 m (4 ft) de ancho y 2.49 m (8 ft) de alto en salas de computación, eléctricas y mecánicas.
En cuanto a las ventanas en el perímetro de la sala de computación, están permitidas con al menos 2 horas de resistencia al fuego.

h) **Requisitos para las distintas salas del CPD**

- Vestíbulo: seguirán los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de dos horas). El vestíbulo tendrá que estar físicamente separado de otras áreas del CPD, con un control de seguridad y hardware para evitar Piggybacking o Pass back

- Oficinas administrativas: cumplen los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de dos horas). Estará físicamente separado de otras áreas del CPD.

- Oficina de seguridad: seguirán los requisitos mínimos de separación con la sala de computación en caso de incendios (no menos de dos horas). Mirillas de 180 grados en equipos de seguridad y salas de vigilancia. Equipos de seguridad dedicados y reforzados y salas de monitorización, paredes revestidas de madera contrachapada y puertas de núcleo sólido. Físicamente separado de otras áreas del CPD.

- Centro de operaciones: tiene que estar físicamente separado de otras áreas del CPD. Contará con una separación mínima de dos horas en caso de incendio con otras áreas no computacionales del CPD. En el caso del Tier 4, el centro de operaciones debe ser directamente accesible desde la sala de computación.

- Salas y zonas de descanso: estas salas no podrán ser adyacentes a la sala de computación, deben estar dotadas con barreras de prevención de fugas. Contarán con una separación mínima de dos horas en caso de incendio con otras áreas no computacionales del CPD.

- Salas de Baterías y de SAI: adyacentes a la sala de computación. Separación mínima de dos horas en caso de incendio con otras áreas del CPD. Anchos de pasillo para mantenimiento, reparación o eliminación de equipo de no menos de 1.2 m (4 ft) libre.

- Pasillos de emergencia: tendrán una separación mínima dos horas en caso de incendio con otras áreas del CPD. Ancho libre de no menos de 1.5 m (5 ft).

- Salas de generadores o de almacenamiento de combustible: este tipo de salas no podrán encontrarse dentro del edificio del CPD y deben ser a prueba de diferentes condiciones meteorológicas. Su proximidad a otras áreas de acceso público no puede ser menor a 18 m (60 ft).

i) **Zona de carga y descarga**

Estas zonas deben estar separadas físicamente de otras zonas del CPD, con una separación mínima de dos horas en caso de incendio con otras áreas. En cuanto a la protección física de paredes expuestas a zonas donde se emplea maquinaria de levantamiento de carga, se emplearán bolardos de acero o similares.
Existirá un muelle de carga cada $2500m^2 (25.000ft^2)$ de sala de computación (2 mínimo).

j) **Seguridad**

Hablando de la capacidad del SAI para la CPU del sistema, este debe contar con la capacidad suficiente para soportar la carga de trabajo del edificio entero y las baterías adicionales (durante 8 horas mínimo).
Sobre la capacidad del SAI para los paneles de recopilación de datos, debe poder soportar la carga de trabajo del edificio entero y las baterías adicionales (durante 24 horas mínimo). Se seguirá el mismo criterio para la capacidad del SAI para los dispositivos de campo.
Adicionalmente, en este Tier se contempla la presencia de personal de seguridad físico 7 días a la semana durante las 24 horas del día, se tratará de suficiente personal como para permitir la realización de inspecciones, supervisiones, etc. También se contará con paredes, puertas y ventanas antibalas de nivel 3 mínimo.

k) **Seguridad de control de acceso y monitorización**

Los generadores, SAI, telefonía, salas Mechanical, Electrical and Pumbling (MEP) y bóvedas de fibra deben contar con sistemas de acceso mediante tarjeta, las salidas de emergencia tendrán un código de acceso. En cuanto a ventanas o aperturas accesibles desde el exterior y puertas de acceso al perímetro, se contará con un sistema de detección de intrusiones.
Todas aquellas habitaciones con equipo de seguridad y salas de ordenadores deberán contar con accesos mediante tarjeta. Las puertas en la sala de computación estarán protegidas mediante un acceso con tarjeta o biométrico (cualquier salida sin autorización debe hacer saltar la alarma y ser monitorizada), y la entrada principal contará con un control de seguridad y hardware para evitar Piggybacking o Pass back, preferiblemente con tecnología biométrica.

l) **Monitorización Circuito Cerrado de Televisión (CCTV)**

Este tipo de monitorización se llevará a cabo en puertas con control de acceso, en el perímetro del edificio y aparcamiento, generadores, salas de computación, en el SAI, telefonía y salas Mechanical, Electrical and Pumbling (MEP).

m) **Circuito Cerrado de Televisión (CCTV)**

Se realizará grabación digital CCTV de toda la actividad en todas las cámaras, con una tasa de grabación de 20 frames/sec mínima.

n) **Estructura**

El diseño de la estructura debe ser respecto a los requisitos de International Building Code (IBC) y Seismic Design Category (SDC), concretamente tienen que seguirse los requisitos de localización de la SDC, con un mínimo de SDC-C. Adicionalmente respecto al nivel anterior, se tendrá en cuenta el grado de aceleración sísmica local, con un estado de operación de un 5% en 100 años.
Factor de importancia de I=1.5.
Se precisa reforzamiento de cables, circuitos eléctricos y conductos de los equipos mecánicos según la importancia de los mismos. Adicionalmente, los equipos de comunicaciones (tales como racks), deben estar anclados al suelo o reforzados completamente y la limitación de la desviación en el equipo de telecomunicaciones debe estar dentro de los límites aceptables.
En cuanto a las capacidades de carga del piso, carga viva superpuesta de $12kPa(250lbf/ft^2)$.
Capacidad del techo para soportar cargas colgantes (iluminación, refrigeración, etc.) mínima

de $2.4kPa(50lbf/ft^2)$.
El espesor de la losa de hormigón del suelo debe ser de 127 mm (5 in).
Acabado mínimo de hormigón sobre canales para anclaje de equipos cuando se emplea estructura cubierta de metal rellena de hormigón para suelos técnicos, de 102 mm (4 in). A diferencia del nivel anterior, en el Tier 3 el edificio debe estar diseñado para disipar energía en caso de seísmos.
La construcción de suelo técnico se realizará con Steel deck & Fill.

2.6.4 Infraestructura mecánica

a) **General**

En cuanto a este tipo de infraestructura, existirá redundancia de equipo mecánico (unidades de aire acondicionado, refrigeración , bombas, condensadores, torres de refrigeración) al menos N+1, la pérdida de electricidad no genera pérdida de refrigeración.
En cuanto al enrutamiento de tuberías de agua o drenaje no asociado con el equipo en los espacios del CPD, al igual que en el nivel anterior este no estará permitido. Además, se requiere presión positiva en la sala de computación y espacios asociados con el exterior.
Es obligatoria la presencia de desagües en la sala de computación para el drenaje de agua que se pueda condensar, de los humidificadores y de los aspersores del techo. Por último, los sistemas mecánicos (refrigeración, supresión de incendios...) estarán respaldados por un generador de emergencia.

b) **Sistema refrigerado por agua.**

Sobre las unidades de aire acondicionado para interiores, se deben contar con la cantidad suficiente de unidades de aire para mantener áreas críticas durante la pérdida de una unidad o de la electricidad, existiendo redundancia clara. También se contempla el control de humedad en la sala de computación.
Sobre el servicio eléctrico a los equipos mecánicos, se precisan múltiples caminos eléctricos a los equipos de aire acondicionado, conectados de forma que exista redundancia. Adicionalmente, los sistemas de tuberías de agua fría y de agua condensada serán duales, estando completamente redundados.

c) **Sistema refrigerado por aire.**

Al igual que en el apartado anterior, el servicio eléctrico a los equipos mecánicos constará de

múltiples caminos eléctricos a los equipos y también se realizará un control de humedad en la sala de computación.

d) **Sistema de control Heating Ventilating Air Conditioned (HVAC)**

Los fallos en el sistema de control NO suponen interrupción de enfriamiento en zonas críticas y existen vías de alimentación eléctrica redundantes.

e) **Cañerías para el rechazo de calor con agua fría**

Sobre el agua de reposición, el CPD necesita contar con un suministro doble de agua, o suministro único pero con almacenamiento de respaldo en el CPD y al menos dos puntos de conexión.

f) **Sistema de combustible**

Al igual que ocurría en el Tier 3, existirán múltiples tanques de almacenamiento, con varias bombas y tuberías de suministro.

g) **Supresión de incendios**

El estándar requiere para este nivel Tier un sistema de detección de incendios, con un sistema de aspersores incluido (de preacción). Además, es necesario un sistema de supresión de gases (contemplando los agentes limpios listados en la NFPA 200), así como de detección temprana de humo y de filtraciones de agua.

Capítulo 3

Metodología

En este capítulo se presentará y desarrollará la metodología diseñada, a lo largo del mismo, describiremos paso a paso nuestra metodología, destacando las etapas clave y las consideraciones importantes para lograr una implementación exitosa. Analizaremos las actividades necesarias, como la evaluación de la infraestructura existente, la identificación de áreas a mejorar, la planificación de la implementación, etc.

Se ha buscado que la metodología sea de naturaleza iterativa, permitiendo su empleo de forma continua para el mantenimiento del nivel Tier que sea preciso en el CPD, o bien en el caso de querer adquirir una certificación mayor con el paso del tiempo.

Las fases principales de la metodología son las siguientes:

-Inicio del proyecto.
-Análisis del entorno.
-Diseño del plan de cambio.
-Implementación del plan de cambio.
-Validación de los cambios.
-Mejora y mantenimiento.

La fase de inicio de proyecto será la primera de la metodología, y se seguirán por orden hasta la "última" fase de mejora y mantenimiento, la palabra "última", va entre comillas porque como se mencionó anteriormente, la naturaleza de la metodología es iterativa. Para tener una mejor visualización de como se distribuyen estas fases, se presenta a continuación un diagrama del flujo de la metodología:

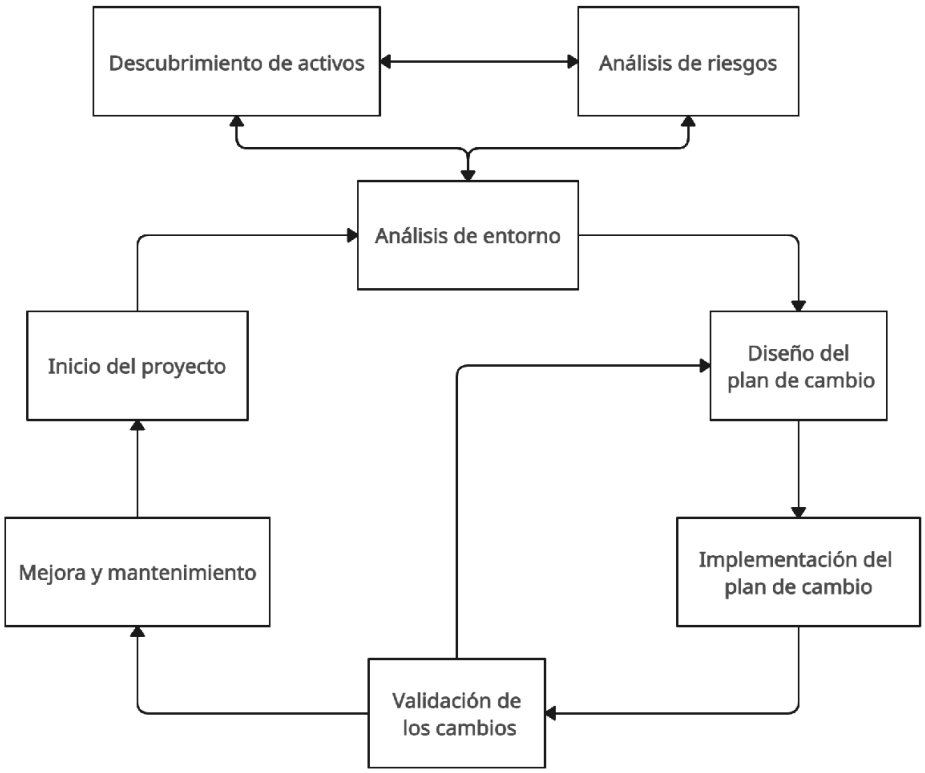

Figura 3.1: Diagrama de flujo

3.1 Generalidades

Esta metodología se centrará en el sistema de niveles, conocidos como Tiers, que emplea la normativa para realizar la clasificación de la disponibilidad y redundancia de un centro de datos. Como ya explicamos anteriormente, la ANSI/TIA-942 recoge hasta 4 niveles de Tier dependiendo de las características del CPD.

Los requisitos establecidos en esta metodología son aplicables a cualquier CPD, en base a las necesidades de la organización y al objetivo que se quiera alcanzar.

3.1.1 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, se aplica la edición citada.

ANSI/TIA-942-A:2012 *Estándar de infraestructura de telecomunicaciones para centros de datos.*
ANSI/TIA-606-B *Estándar de administración para infraestructura de telecomunicaciones [6].*
ANSI/TIA-607-B *Vinculación genérica de telecomunicaciones y tomas de tierra para instalaciones cliente [8].*
NFPA 75 *Estándar para la protección contra incendios relativa a los equipos TI [9].*
NFPA 200 *Estándar para colgar y reforzar sistemas de extinción de incendios [10].*
NFPA 780 *Estándar para la instalación de sistemas de protección contra rayos [7].*

3.1.2 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en la norma ANSI/TIA-942:2012.

3.2 Inicio del proyecto

En la etapa inicial, se realizan una serie de actividades clave para establecer las bases del proyecto. Se determinarán diferentes aspectos del proyecto que son necesarios para garantizar la correcta evolución del mismo a lo largo de las diferentes fases. Es de vital importancia que todas las cuestiones a tratar en esta etapa queden resueltas, ya que esto permitirá una fluidez a lo largo del proceso. El objetivo principal de esta fase es el de evitar posibles problemas posteriores al inicio del proyecto.

Esta fase permite establecer las bases sólidas necesarias para el proyecto. Al definir el alcance, formar el equipo del proyecto, obtener el compromiso de la dirección y realizar una evaluación de riesgos inicial, se crea una estructura y un marco de trabajo que guiarán el proceso de cambio del CPD.

3.2.1 Contexto de la organización

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos.

Es importante obtener una comprensión clara del entorno de la organización y sus necesidades, analizar la importancia de las operaciones que se desarrollan en el CPD en el contexto de la organización y establecer la importancia de las mismas. Hay que estudiar como puede afectar el cambio del CPD a la actividad diaria de la empresa y el impacto que supone la transformación del centro.

3.2.2 Determinación del alcance del proyecto y el objetivo a cumplir

La organización debe determinar el objetivo a cumplir en el contexto del proyecto, en concreto establecer la certificación Tier que se desea adquirir. Esto es vital para visualizar el tamaño de la reforma que se va a llevar a cabo, ya que dependiendo del Tier serán necesarios más cambios en el propio centro, y por consecuencia mayor presupuesto, tiempo, personal, etc.

Una vez acordado el Tier objetivo, deben establecerse fechas límite para completar el proceso, así como marcos presupuestarios en los que se moverá el proyecto.

3.2.3 Responsabilidades y compromiso

La dirección de la organización debe mostrar compromiso con respecto al cambio a producir en el CPD, esta parte es fundamental para la realización del proyecto, evitando problemas de gestión entre la dirección y los responsables del desarrollo del mismo. Se busca lograr una organización y comunicación claras, generando un ambiente idílico para trabajar, con la idea principal de que no se generen retrasos en el proyecto por cuestiones administrativas. Esto se logrará tomando las siguientes medidas:

-Asegurando la disponibilidad de los recursos para realizar el proceso de cambio. El personal de desarrollo del plan de cambio deberá contar con todo lo necesario para realizar las reformas

antes de comenzar, con el objetivo de evitar parones debido a la ausencia de recursos.

-Asegurando que se cumplen los resultados previstos, es decir, la dirección fomenta el cumplimiento al pie de la letra del proceso de reforma, para obtener el resultado que se desea inicialmente y no acabar con un producto incompleto.

-Designando la carga de trabajo en el personal encargado y estableciendo diferentes roles y responsabilidades para lograr una organización clara y precisa. El personal de la organización debe tener en todo momento conocimiento total de sus funciones y limitaciones, algo clave para el desarrollo natural de la reforma del CPD.

-Asegurando que los cambios en el CPD se realicen de forma adecuada y cumpliendo con las normas de la seguridad de la información. El tratamiento de los datos que se encuentran en el CPD debe ser un aspecto primordial en cuanto a la reforma, ya que se trata de información sensible.

3.2.4 Impacto en la operación del CPD

Al realizar las reformas en el CPD, es necesario tener en cuenta diferentes aspectos para asegurar la continuidad operativa y mantener la seguridad de la información. Determinar como va a afectar la reforma tanto en el ámbito interno de la organización como en la actividad de posibles clientes externos que realicen uso del CPD.

Antes de iniciar las reformas, es esencial realizar una planificación adecuada y definir claramente los objetivos y requisitos de la reforma. Esto implica evaluar el impacto de las reformas propuestas en la infraestructura existente, los sistemas y servicios, y considerar aspectos como la capacidad, la seguridad física y lógica, la disponibilidad, etc.

Durante el proceso de reformas, es importante minimizar el impacto en los servicios que se prestan desde el CPD. Se deben identificar las áreas o servicios críticos que podrían verse afectados y desarrollar planes de contingencia o de migración para garantizar la continuidad de los servicios durante las reformas. En cuanto al cumplimiento normativo, siempre es importante asegurarse de que las reformas realizadas en el CPD cumplan con los requisitos normativos y legales vigentes. Esto incluye considerar regulaciones relacionadas con la privacidad, protección de datos y seguridad de la información, según sea aplicable a la industria y al país en el que opera el CPD.

Al abordar estos aspectos, se puede asegurar que las reformas se realicen de manera se-

gura y eficiente, minimizando el impacto en los servicios y manteniendo la seguridad de la información del CPD.

3.3 Análisis del entorno

En esta etapa se llevarán a cabo dos procesos para conocer el estado en el que se encuentra el CPD. Antes de elaborar un plan de cambio, necesitamos saber los recursos de los que dispone el centro y en qué punto se encontraría respecto a las especificaciones del estándar ANSI/TIA-942. Los procesos a realizar son los siguientes:

- Descubrimiento de activos.
- Análisis de riesgos.

Esta se trata de una fase importante, ya que podremos analizar los recursos de los que disponemos y cuan grande será el cambio necesario en el CPD para adquirir el nivel Tier deseado. Esta etapa constará un hito en el proceso, pues se trata del ecuador de la metodología.

3.3.1 Descubrimiento de activos

El descubrimiento de activos es un proceso clave para identificar y comprender los activos relevantes en el entorno del CPD. Se refiere a la recopilación de información sobre los activos de TI, la infraestructura, los sistemas y los recursos que se utilizan en el CPD. Esto ayuda a tener una visión clara de los activos y a evaluar su capacidad para cumplir con los requisitos de una certificación específica.

Dividiremos el proceso en varias fases, durante las cuales haremos uso de diferentes herramientas para lograr nuestros objetivos, de las que se hablará en el siguiente capítulo.

Inventario de activos

Se realiza un inventario exhaustivo de todos los activos físicos y lógicos que se utilizan en el CPD. Esto puede incluir servidores, dispositivos de red, sistemas de almacenamiento, sistemas de seguridad, equipos de respaldo, software y cualquier otro componente relevante. Se recomienda apoyarse en herramientas específicas de inventariado de activos, ya que están dotadas de todo lo necesario para facilitar el proceso.

Análisis de la infraestructura

Se evalúa la infraestructura física del CPD, incluyendo la capacidad de almacenamiento, la refrigeración, ventilación, el suministro eléctrico y la redundancia. Este proceso se realizará viendo las propias instalaciones y hablando con el personal responsable del centro. Se comprobará el cableado, paneles de distribución, cuadros eléctricos... Así como las diferentes salas del CPD y su relación con la sala principal de computación. Otros aspectos a tener en cuenta son los estándares empleados para construir el edificio, salidas de emergencia, diseño del techo, paredes y puertas, etc.

Evaluación de la seguridad física y lógica

Se revisan las medidas de seguridad física implementadas en el CPD, como sistemas de acceso, cámaras de vigilancia, sistemas de detección de intrusiones y sistemas contra incendios. Es necesario evaluar también las medidas de seguridad lógica implementadas en el CPD, como firewalls, sistemas de prevención de intrusiones y políticas de seguridad. Se tendrán en cuenta el personal de seguridad físico presente en el CPD, así como su disponibilidad durante todos los días de la semana.

3.3.2 Análisis de riesgos

Esta etapa implica identificar, evaluar y mitigar los riesgos que podrían afectar la seguridad, disponibilidad e integridad de la infraestructura y los activos de información en el entorno del CPD. Esta fase está directamente ligada con el descubrimiento de activos, ya que ambos procesos se complementan mutuamente y son de vital importancia para tener un enfoque sólido sobre la seguridad en el centro.

El descubrimiento de activos proporciona la base de información necesaria para realizar un análisis de riesgos efectivo, esto se debe a que al conocer los activos presentes en el CPD y su ubicación, se puede evaluar de manera más precisa las amenazas y las vulnerabilidades asociadas con cada activo. Además, el descubrimiento de activos ayuda a garantizar que no se pasen por alto activos críticos en el análisis de riesgos.
A su vez, el análisis de riesgos influye en el descubrimiento de activos, ya que puede revelar nuevos riesgos o áreas que requieren una mayor atención en términos de identificación y documentación de activos.

Análisis de vulnerabilidades

Se identifican las posibles vulnerabilidades o debilidades en los activos y en los controles de seguridad existentes en el CPD. Para ello se realizan evaluaciones técnicas como escaneos

de seguridad, pruebas de penetración y revisiones de configuración para identificar posibles puntos débiles en el sistema.

Impacto de las vulnerabilidades

Hay que determinar el impacto que pueden tener estas vulnerabilidades en la operación del CPD, como pueden afectar a la seguridad e integridad de los datos que se almacenan, el impacto en cuanto a tiempo que podrían suponer, etc. Es clave tener certeza sobre el potencial daño que tendría cada amenaza sobre los activos del CPD.

Probabilidad de ocurrencia

Se evaluará la probabilidad o la frecuencia con la que es probable que ocurran las amenazas identificadas. Para esto pueden tenerse en cuenta estadísticas sobre los riesgos estudiados o datos históricos del propio CPD. La probabilidad de que un riesgo desencadene en un problema es un factor importante a tener en cuenta a la hora de tratar con el mismo.

Clasificación de los riesgos

Una vez se tiene en cuenta el impacto y la probabilidad de ocurrencia de los riesgos, es necesario clasificarlos para decidir que riesgos tienen más prioridad y poder destinar más cantidad de recursos para la mitigación de los mismos.

Para realizar esta tarea, se empleará una matriz de riesgos 5x5, esta matriz organiza los riesgos en función de su probabilidad y su impacto, lo que permite visualizar y analizar de manera más clara la importancia relativa de cada riesgo [11].

Según la probabilidad de ocurrencia e impacto se asignan unos valores más altos, para lograr así un sistema de puntuación y poder clasificar nuestros riesgos. El resultado de multiplicar estas dos variables será la clasificación global del riesgo, los que obtengan una puntuación más alta tendrán que ser tratados con mayor prioridad.

Impacto de la vulnerabilidad

Probabilidad de ocurrencia	1-Mínimo	2-Menores	3-Moderadas	4-Mayores	5-Severas
5-Frecuente	Medio 5	Alto 10	Muy alto 15	Extremo 20	Extremo 25
4-Probable	Medio 4	Medio 8	Alto 12	Muy alto 16	Extremo 20
3-Ocasional	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
2-Poco probable	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
1-Raro	Muy bajo1	Muy bajo 2	Bajo 3	Medio 4	Medio 5

Figura 3.2: Matriz de riesgos

Mitigación de los riesgos

Una vez clasificados los riesgos por importancia, es necesario tomar acciones para mitigarlos. Para ello, se identificarán y seleccionarán los controles y medidas de mitigación apropiados para cada riesgo. Estos controles pueden incluir medidas técnicas como firewalls, sistemas de detección de intrusiones, sistemas de respaldo y recuperación ante desastres, así como controles administrativos como políticas de seguridad, procedimientos operativos y capacitación del personal. Muchos riesgos pueden reducirse mediante una formación dedicada para el personal, ya que gran cantidad de los problemas que pueden surgir se deben al factor humano.

Cuando se hayan decidido las acciones a tomar, se implementarán los controles de mitigación seleccionados de manera efectiva en el CPD. Esto implica asegurarse de que los controles estén configurados correctamente, que se realicen pruebas y verificaciones periódicas, y que se mantengan actualizados.

Por último, es necesario realizar monitorización continua de los riesgos y los controles implementados en el CPD, por lo que se realizarán revisiones periódicas y actualizaciones de los riesgos a medida que cambien los activos o el entorno operativo. Los riesgos no tienen una naturaleza estática, ya que pueden tener tendencias a evolucionar con el tiempo, por lo que realizar seguimientos de los mismos es una actividad importante para evitar un descontrol de los riesgos.

3.4 Diseño del plan de cambio

Una de las fases más importantes de la metodología consistirá en llevar a cabo el diseño del plan de cambio del CPD. Una vez realizadas las etapas anteriores, se debe tener una imagen clara de todos los activos, recursos y estado general en el que se encuentra el CPD. Es el momento de identificar la brecha entre el estado actual del centro y las especificaciones requeridas en el Tier que se desea obtener.

3.4.1 Creación del plan

Una vez comprobados los requisitos que tenemos que cumplir y los determinados cambios que tenemos que llevar a cabo, se pasa a la creación del plan que se seguirá durante el proceso de cambio del CPD. Se debe realizar una planificación detallada del proyecto, considerando los objetivos, el alcance, los plazos, los recursos y el presupuesto disponibles. Esto incluye definir las metas y requisitos del proyecto, así como identificar los posibles desafíos y riesgos.

Se definirán claramente quiénes serán los responsables de cada actividad y se asignarán roles y tareas específicas. Hay que asegurarse de que cada miembro del equipo comprenda sus responsabilidades y tenga los recursos necesarios para llevar a cabo su trabajo.

Es importante tener en cuenta que si se realizan reformas en las salas, estas sigan contando con los requisitos en cuanto a espacio marcados por el estándar. Los cambios han de realizarse en el orden correcto y siguiendo una planificación lógica, ya que no se pueden interrumpir de forma significativa las actividades del CPD.

3.5 Implementación del plan de cambio

Durante el proceso de reformas en el CPD, se debe llevar a cabo una supervisión constante del progreso de la reforma. La organización debe asegurarse de que las actividades se estén llevando a cabo según lo planeado y de que se cumplan los plazos establecidos. Es necesario realizar reuniones de seguimiento regularmente para evaluar el avance y abordar cualquier problema o desviación que surja.

En la medida necesaria la organización debe mantener información documentada, para tener la confianza de que los procesos se han llevado a cabo según lo planificado.

Se deben controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario. Adicionalmente, la organización debe garantizar que los procesos contratados externamente estén controlados.

En cuanto al personal, deben ser provistos con la capacitación necesaria para que puedan utilizar y mantener adecuadamente los nuevos equipos y sistemas implementados durante la reforma. Es importante documentar todas las configuraciones, procedimientos y cambios realizados durante el proceso de reforma para facilitar la gestión y el mantenimiento futuro.

3.6 Validación de los cambios

Una vez acabada la reforma del CPD, se deben evaluar y validar los cambios realizados, para asegurar la eficacia de los mismos y comprobar que el centro recoge todas las características necesarias para adquirir la certificación Tier deseada. Es fundamental llevar a cabo una validación exhaustiva de todos los cambios realizados para asegurarse de que el CPD funcione de acuerdo con los requisitos y expectativas establecidos.

3.6.1 Auditoría interna

La organización debe llevar a cabo auditorías internas en intervalos planificados para comprobar que se siguen los requisitos del estándar ANSI/TIA-942 y los cambios se han implementado de manera eficaz. Para realizar las auditorías, la organización debe definir los criterios y alcance de la misma, seleccionar los auditores para asegurarse de la objetividad y la imparcialidad del proceso de auditoría y asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías. Se debe:

- Realizar una inspección física detallada del CPD para asegurar que todos los componentes y equipos instalados estén en su lugar y funcionando correctamente. Verificar la correcta conexión de cables, la ubicación de los dispositivos y el cumplimiento de las normas de seguridad.

- Realizar pruebas rigurosas de funcionamiento en todos los sistemas y equipos del CPD. Esto incluye pruebas de encendido y apagado, pruebas de rendimiento, pruebas de conectividad de red, pruebas de respaldo de energía, etc. Todos los sistemas deben estar operativos y cumplir con los estándares y requisitos establecidos.

- Se deben llevar a cabo pruebas de seguridad para evaluar la resistencia y efectividad de las medidas de seguridad implementadas. Esto puede incluir pruebas de acceso físico, pruebas de detección de intrusos, pruebas de redundancia de sistemas, entre otras.

- Realizar pruebas de conectividad de red para asegurar que los equipos estén comunicándose correctamente y que los sistemas estén accesibles desde las ubicaciones requeridas. Probar también la conectividad externa, como el acceso a Internet y las conexiones con proveedores externos si corresponde.

- Se deben mantener registros detallados de todas las pruebas realizadas, los resultados obtenidos y los cambios implementados durante la reforma. La documentación adecuada de los procedimientos, las configuraciones y las políticas es vital para facilitar la gestión y el mantenimiento continuo del CPD.

Una vez acabadas las pruebas se deberá realizar una evaluación final de los resultados de las pruebas y la validación. Estudiar si se han cumplido los objetivos y requisitos establecidos, y si los cambios implementados cumplen con lo establecido en el estándar. En caso de encontrar problemas, se volverá a la fase anterior de la metodología de diseño del plan de cambio, para volver a realizar un estudio sobre los requisitos necesarios del nivel Tier y suprimir los inconvenientes.

3.7 Mejora y mantenimiento

A medida que pase el tiempo, es posible que se realicen algunos cambios en el CPD, se compre nuevo equipo o se realicen cambios en el personal. Esto puede provocar que se pierdan las características necesarias para mantener el nivel Tier del que dispone el CPD, por ejemplo, si se adquiere más infraestructura para una sala en concreto, podríamos incumplir requisitos como el ancho necesario en un pasillo, O en caso de construir una nueva sala en el centro, que está cuente con los niveles requeridos de separación en caso de incendios con la sala de computación.

Por estos motivos es importante la naturaleza iterativa de la metodología, ya que no está diseñada para un único uso, si no para aplicarse de forma periódica para asegurar que se siguen manteniendo los niveles necesarios para la cumplir con la certificación obtenida. En este último paso de la metodología, podríamos volver a la fase principal de ”Inicio de proyec-

to" para volver a analizar nuestros objetivos actuales y mantener el nivel de calidad de forma continua en el CPD.

Lo mismo pasaría en caso de querer adquirir un certificado Tier mayor, pudiendo volver a la casilla inicial para establecer unas metas nuevas. Además, en las sucesivas iteraciones que se realicen, se podrán emplear la documentación creada durante procesos anteriores, facilitando el proceso y permitiendo corregir errores pasados.

3.8 Planificación y presupuesto del proyecto

En este apartado hablaremos de la planificación y esfuerzo planteados inicialmente en el proyecto, para compararlos posteriormente con los esfuerzos y horas reales, así como desvíos en la propia planificación debido a cambios o problemas inesperados. La planificación adecuada de un proyecto es un proceso clave para lograr los resultados esperados, por eso se ha intentado seguir de forma fiel la planificación a lo largo del proyecto

La planificación inicial daba comienzo al proyecto el 28 de febrero y pretendía tener todo terminado para el 18 de junio. En este lapso de tiempo se llevarían a cabo dos procesos separados, que podríamos definir como la parte teórica y la parte práctica del proyecto. Para tener todo más claro, numeraremos las tareas con el formato T1.-/T2.- etc.

T1.-"Inicio del proyecto": esta es la primera tarea real de la parte teórica, en la cual nos dedicamos a realizar reuniones con el responsable del CPD, para aclarar distintos asuntos relacionados con el trabajo y ver las opciones disponibles para valorar la forma en la que íbamos a proceder. Este proceso se divide en varias subtareas, **T1.1 "Contexto de la organización", T1.2 "Alcance del proyecto y objetivo a cumplir", T1.3 "Responsabilidades y compromiso" y T1.4 "Impacto de la operación en el CPD".** Estas 4 subtareas comprenden el núcleo del inicio del proyecto, y se realizaron mediante reuniones y correos con el responsable del CPD, debido a la naturaleza de estas tareas, no se les estimó en la planificación un número elevado de horas.

T2.-"Estudio del ANSI/TIA-942": como tarea principal de la parte teórica tenemos el estudio del estándar ANSI/TIA-942, esto comprende en la memoria el capítulo del "Estado del arte", en el cual se plasma toda la información filtrada que se extrajo del estándar y que nos era necesaria para realizar el caso práctico. Es por este motivo que no podíamos empezar la parte práctica del trabajo hasta no tener información clara y ordenada sobre los distintos tipos de

Tier y sus especificaciones. Para esta parte se estimó poco más de un mes, sobre unos 33 días, ya que había que se trata de un estándar relativamente extenso y con mucha información. Al final de esta fase marcamos un hito, pues se trata del final de la parte teórica del trabajo y podemos dar comienzo a la parte práctica.

Para la parte práctica, se estimaron dos meses, ya que esta parte contiene distintas fases que podían extenderse con facilidad, al tener que tratar con herramientas desconocidas y terceros, tal y como sería el CPD del CITIC, puesto que dependíamos de la disponibilidad de los responsables para poder llevar a cabo las pruebas.

T3.- ”Análisis de entorno”: esta es la fase de la metodología que se estimó inicialmente con mayor duración, ya que se trata de la fase con mayor carga de trabajo debido a sus subtareas **T3.1 ”Descubrimiento de activos” y T3.2 ”Análisis de riesgos”.** La subtarea que se estimó con mayor duración fue la del descubrimiento de activos, esto se debe a que en relación al análisis de riesgos, se acordó que no se realizaría muy afondo, debido al impacto que las pruebas podrían producir en el CPD por su invasividad.

T4.- ”Diseño del plan de cambio”: una vez tuvimos todo lo necesario para determinar en que certificación Tier cuadraba el CPD, se elaboró el plan de cambio ayudándonos de la herramienta GLPI, esta tarea no se estimó tampoco con una duración alta. Al final de esta tarea se establece también un hito, marcando el final de la parte práctica del trabajo.

Hay que recordar que como al fin y al cabo este no es un trabajo ”real”, no se han tenido en cuenta para la planificación las fases de la metodología de ”Implementación del plan de cambio”, ”Validación de los cambios” y ”Mejora y mantenimiento”, debido a la imposibilidad de realizar las propias reformas en el CPD.

T5.- ”Estudio de los resultados”: tras acabar ambas partes del trabajo, se estudiaron los resultados obtenidos y el tiempo empleado, para ver como se había comportado la metodología y contemplar posibles cambios y aplicaciones en el futuro.

T6.- ”Elaboración de la memoria” esta tarea se llevará a cabo a lo largo de todo el proyecto, ya que se trata de una tarea influenciada por las demás así como la más larga de todas. Por estos motivos, inicialmente se contemplo una duración equivalente a la suma de las partes teórica y práctica, es decir, un total de unos tres meses.

A continuación, se muestra un diagrama de Gantt de la planificación inicial estimada,

puntualizo que en este diagrama no aparecen las subtareas de la T1 ”Inicio de proyecto”, puesto que se trata de subtareas que no iban a suponer un impacto lo suficientemente significativo como para separarlas en el diagrama de su tarea padre:

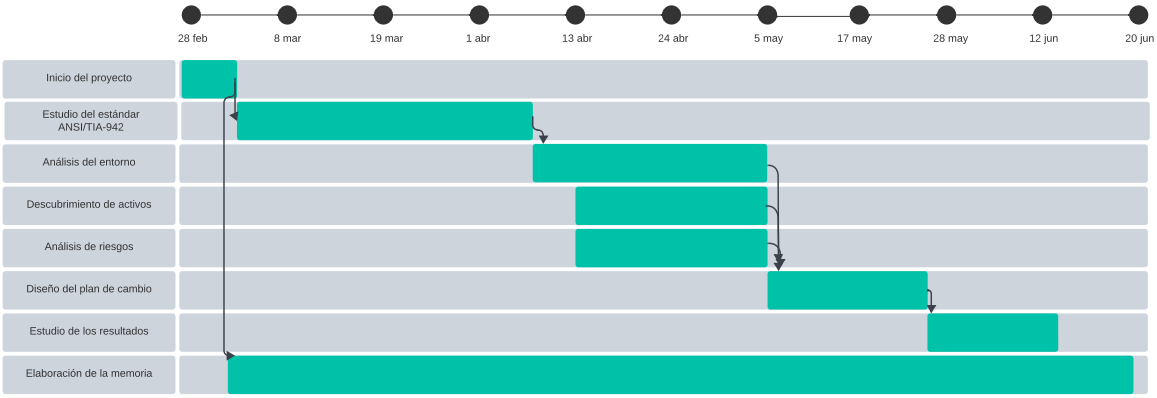

Figura 3.3: Planificación inicial.

Sin embargo, al avanzar en el proyecto nos hemos encontrado con diversas adversidades que han provocado retrasos en algunas de las tareas. En un inicio, rápidamente se comprobó que la duración respecto a la tarea del estudio del estándar fue bastante optimista, ya que se produjo un retraso considerable en el proceso de extraer la información, siendo un proceso mucho más lento de lo esperado debido a los tecnicismos del estándar y a la comprensión de la información que se extraía del mismo. Esto provocó un retraso en el inicio del caso práctico, pues se trataban de tareas dependientes.

En cuanto al caso práctico en sí, la fase de análisis del entorno también supuso una carga de trabajo superior, así como un aumento en el número de horas previstas. Esto se debió a dos motivos principales, el primero se trataría del empleo de las herramientas, ya que tanto GLPI como OpenVAS eran herramientas desconocidas para mí, por lo que tuve que documentarme y aprender a utilizarlas, además de experimentar problemas de instalación o probar otras herramientas que finalmente fueron descartadas. Por otra parte, los días que podía acceder al CPD eran contados, ya que lo más importante era que la operación del centro no se viese alterada por nuestro trabajo. Esto provocó que en ocasiones hubiese que esperar varios días para poder fijar una fecha adecuada para proseguir con las pruebas en el CPD.

Es importante destacar que no todo fueron demoras, ya que las tareas de ”Diseño del plan de cambio” y ”Estudio de los resultados” se realizaron en un período menor de tiempo del estimado. Toda esta información y experiencia será de gran utilidad para la elaboración de

planificaciones en futuros proyectos, sobretodo cuando hay implicadas herramientas de las que no se tiene conocimiento o se depende de organizaciones externas.

Las alteraciones se aprecian mejor en el diagrama de Gantt de la planificación real, que se muestra a continuación:

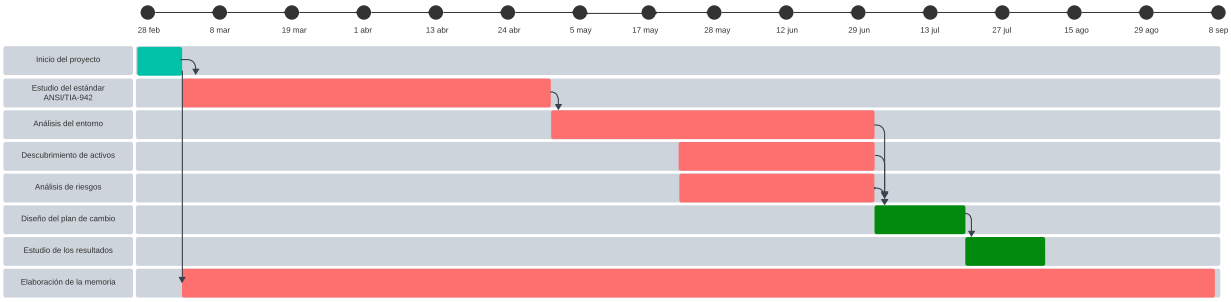

Figura 3.4: Planificación real, tareas atrasadas (en rojo), tareas reducidas (en verde oscuro).

Con respecto a la memoria, fue un trabajo que se realizó paralelamente a todo el proyecto y que también supuso un esfuerzo mayor del estimado. En la memoria se refleja todo lo que se ha ido haciendo a lo largo del proyecto, por lo que será la última tarea en terminarse y la que contará con el mayor cómputo de horas. En relación a las horas, en la siguiente tabla se mostrarán las diferentes tareas y su duración aproximada en horas, para entender un poco mejor la cantidad de esfuerzo en horas hombre que ha tenido el proyecto.

Tarea del proyecto	Duración aproximada en horas
Inicio del proyecto	20
Estudio de la ANSI/TIA-942	85
Análisis del entorno	60
Diseño del plan de cambio	15
Estudio de los resultados	12
Elaboración de la memoria	115
Total	**307**

Tabla 3.1: Duración de las tareas en horas.

Viendo el número de horas invertido, si tenemos en cuenta que el salario promedio de un auditor de TI es de 14,08€ la hora, si quitamos las tareas relacionadas con la elaboración de

la memoria y el estudio de la normativa ANSI/TIA-942 (ya que son tareas propias del trabajo y no se llevarían a cabo en un caso real), el proyecto alcanza un coste de unos 1.506,56€. Como en general podemos decir que el proyecto se ha alargado debido a diversos factores, esto ha supuesto en un aumento del costo del mismo, al incrementar el número de horas. He de mencionar que al tratarse de la primera vez que me veo envuelto en un proyecto de estas dimensiones, la planificación del mismo fue bastante complicada debido a la falta de experiencia o historial en el que apoyarme, pero todo el proceso ha servido de experiencia que buenamente será aplicable en casos futuros.

Capítulo 4

Herramientas empleadas

En este capítulo de la memoria se hablará de las herramientas que se han empleado al aplicar la metodología en un caso práctico real, se han escogido en base a diferentes factores como son su utilidad, facilidad de uso, si son de código abierto o no, precio, etc.

Estas herramientas están destinadas al descubrimiento y gestión de activos, así como al análisis de riesgos. Profundizaremos más en unas herramientas que en otras dependiendo de la importancia que tengan en la aplicación de la metodología, haciendo hincapié en la herramienta de gestión de activos sobre la cual se realizará el plan de cambio del CPD mencionado en la misma. Por este motivo, esta será la herramienta de la cual empezaremos hablando, seguido de las empleadas para el descubrimiento de activos y análisis de riesgos.

Las capturas que se muestran de las diferentes herramientas son propias, tomadas del ordenador particular que se empleará durante todo el trabajo.

4.1 GLPI

Para realizar la gestión de los activos del CPD, emplearemos la herramienta Gestion Libre de Parc Informatique (GLPI), una herramienta de gestión de servicios informáticos de software libre que nos ofrece una amplia gama de funcionalidades para ayudar a gestionar los recursos de TI de una organización.

El principal propósito de GLPI es permitir la gestión centralizada de los activos de TI, ya sean hardware, software u otros elementos relacionados. Permite mantener un inventario actualizado de los activos de TI, incluyendo detalles como número de serie, ubicación, estado, usuarios activos, personal del centro, entre otros. Esto facilita el seguimiento y control de los

activos, lo que a su vez ayuda a optimizar la gestión de inventario y la toma de decisiones relacionadas con la infraestructura de TI. La herramienta también nos permite registrar y gestionar los incidentes, solicitudes y problemas reportados por los usuarios, asignar tareas a los equipos de mantenimiento, realizar un seguimiento de las soluciones implementadas y generar informes sobre el rendimiento del servicio.

Para este trabajo, la usaremos para llevar a cabo un control preciso de los activos del CPD y poder disponer de un inventario ordenado de todos nuestros recursos. Emplearemos la herramienta a lo largo de todo el proceso de prueba de la metodología, ganando importancia en las fases de ”Análisis de entorno” y de ”Mejora y mantenimiento”.

Sin embargo, su aplicación principal vendrá en la fase de ”Implementación del plan de cambio” ya que la usaremos para la creación del proyecto de cambio del CPD, en el que se definirán todas las tareas a cumplir, se asignarán recursos, presupuestos, fechas límite, etc. Esto nos permitirá seguir el desarrollo del cambio y llevar un control del progreso de todos los cambios a realizar, de forma ordenada y con posibilidad de corregir errores en caso de ocurrencia.

Otra de las razones por las que se ha empleado esta herramienta es porque ofrece una interfaz amigable para el gestor, así como una amplia documentación disponible y sencillez en su instalación [3]. Para trabajar con GLPI será necesaria también una base de datos de tipo MariaDB/MySQL.

En la interfaz de inicio que nos ofrece la herramienta, disponemos de un resumen inicial de nuestros activos disponibles, así como de peticiones de cambios, problemas, tickets y demás. También tenemos accesos directos a las diferentes secciones navegables que nos ofrece la herramienta. A continuación se muestra una captura de la página de inicio:

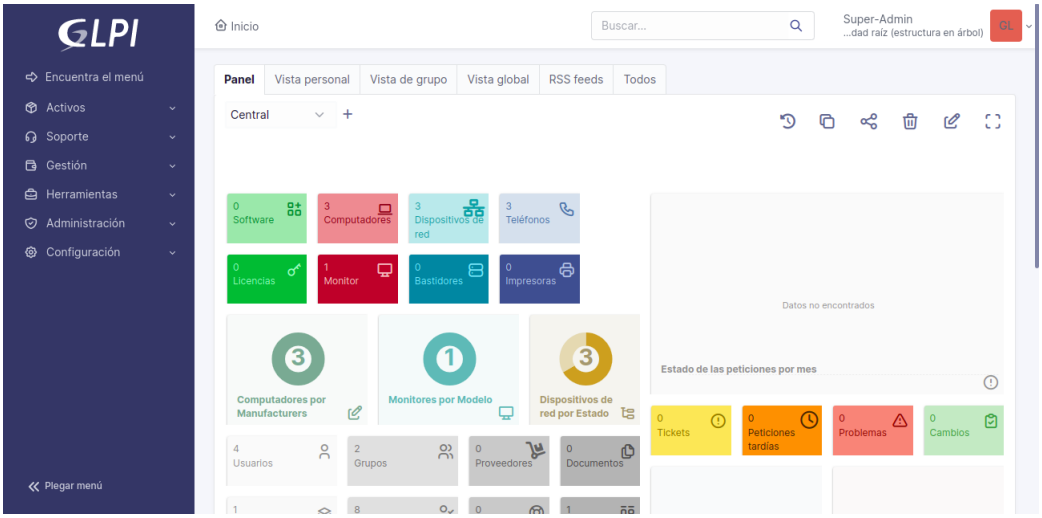

Figura 4.1: Página de inicio de GLPI.

Como mencionamos anteriormente, el uso principal que le daremos a la herramienta será el de definir un proyecto para realizar y seguir el proceso de cambio en el CPD. En la captura que tendremos a continuación, se muestran las tareas de un proyecto que está siendo llevado a cabo. Vemos como se marca el progreso de las tareas, fechas de inicio y fin, prioridad y otras características. También podemos crear tareas que sean hijo de otras, lo que nos permite crear diferentes grupos de tareas, cada una con tareas hijo a su vez.

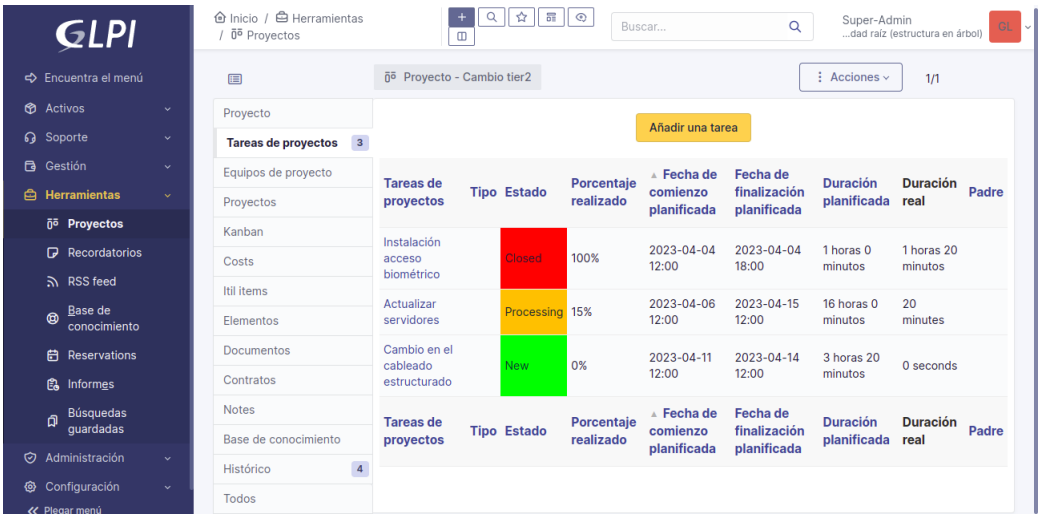

Figura 4.2: Tareas del proyecto.

GLPI guarda además un histórico de todos los cambios y actualizaciones que se vayan realizando tanto en el proyecto en general como en cada una de sus tareas. Otra opción de

la que disponemos es la de generar informes de los activos de gestión, pudiendo generarlos en función de los activos disponibles, de si tienen algún contrato con terceros, información financiera, entre otros.

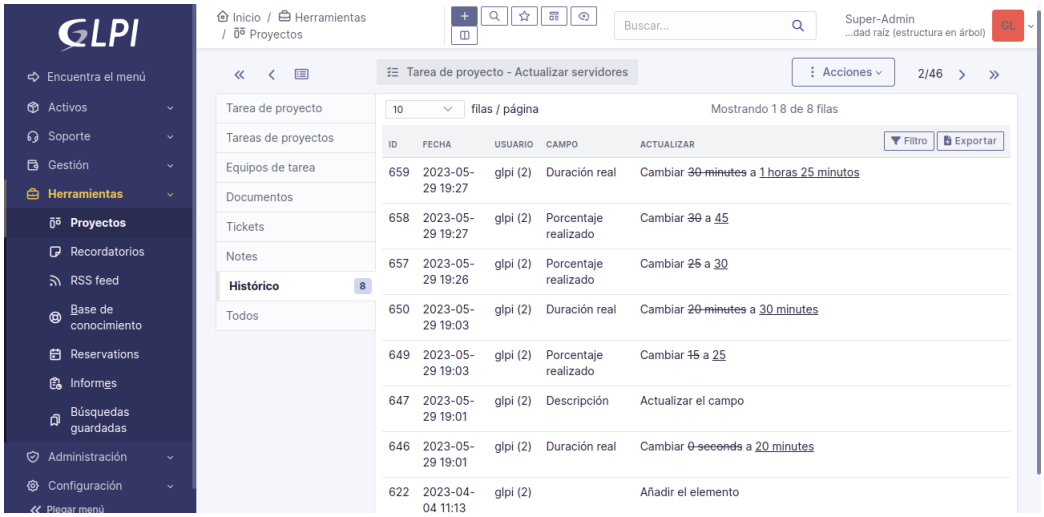

Figura 4.3: Histórico de tarea.

Dentro de GLPI, es posible asociar documentos a los activos o a otros elementos registrados. Estos documentos pueden ser manuales de usuario, contratos, licencias, certificados, diagramas de red u otro tipo de archivos relevantes para la gestión de los activos de TI.

Esto lo que nos permite es que cuando asociamos documentos a un activo o a otro elemento en GLPI, se crea un vínculo que permite acceder rápidamente a la documentación relacionada cuando sea necesario. Esto nos ayuda a mantener un registro centralizado de la documentación y facilita su consulta y actualización.

Otra de las funcionalidades que emplearemos durante el caso práctico es la posibilidad de crear plantillas. Las plantillas nos permiten añadir activos, tareas, grupos de trabajo, etc, de forma rápida y cómoda, facilitando el proceso de crear un inventario completo y eficiente.

4.2 OpenVAS

Como herramienta para la fase de ”descubrimiento de activos” y ”análisis de riesgos”, emplearemos Open Vulnerability Assessment System (OpenVAS), una herramienta de escaneo de seguridad utilizada para identificar y evaluar vulnerabilidades en sistemas informáticos. Su objetivo principal es detectar debilidades en redes, sistemas operativos y aplicaciones, pro-

porcionando información detallada sobre las mismas. OpenVAS nace como una bifurcación del código abierto de Nessus (otra conocida herramienta de análisis de riesgos), por lo que comparte características similares con ella.

OpenVAS hace uso de una extensa base de datos que recoge miles de vulnerabilidades conocidas, para realizar escaneos completos y detallados en sistemas y redes. Examina puertos abiertos, servicios y aplicaciones en busca de configuraciones inseguras o fallos que podrían ser explotados por atacantes. La base de datos que emplea OpenVAS está en actualización constante, añadiendo más vulnerabilidades cada vez, adicionalmente, cuenta con una documentación extensa que proporciona toda la información necesaria para entender y manejar la herramienta [4].

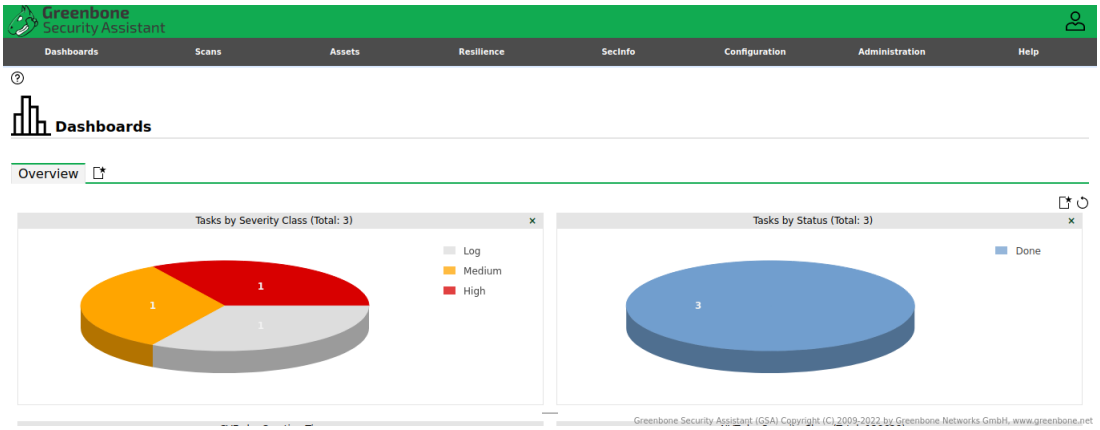

Figura 4.4: Pantalla de inicio de la interfaz web.

Como vemos en la captura, en la pantalla de inicio se mostrarán los paneles que tengamos configurados, por defecto viene un resumen de las tareas, mostrándonos las tareas realizadas (3 análisis, separadas por colores dependiendo de su gravedad) así como las tareas en ejecución. Esta pantalla se puede configurar sin problema para que muestre diferente información, pudiendo crear diversos paneles sobre los recursos que más interesen tener a la vista de forma rápida.

Nos centramos ahora en los análisis, que es el uso principal que le daremos a esta herramienta.

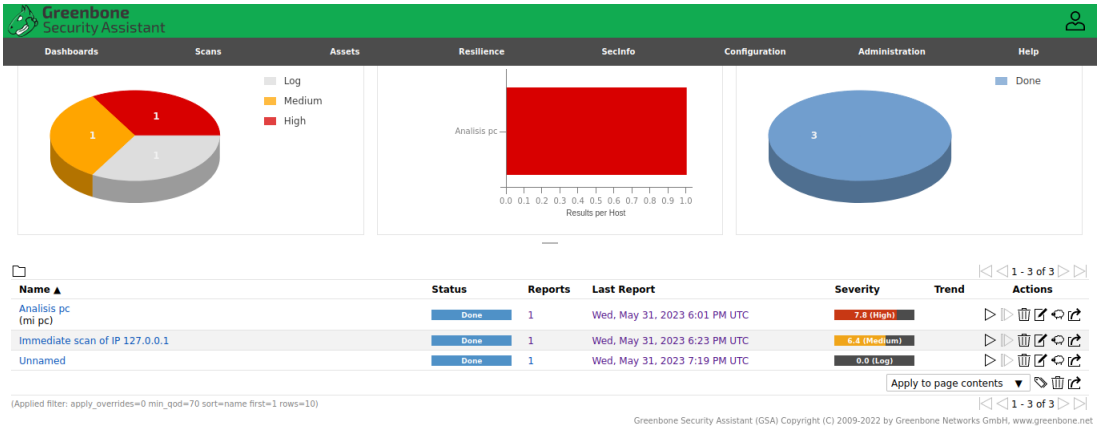

Figura 4.5: Pantalla de tareas.

OpenVAS nos muestra los últimos análisis realizados, con un resumen inicial de sus detalles y características, podemos filtrar por fecha, severidad, nombre, estado... Desde esta pestaña podremos crear una nueva tarea, esto podemos hacerlo de forma manual o a través de un asistente de creación. El programa nos permite ajustar los escaneos de acuerdo con las necesidades y requisitos específicos de cada sistema o red. Los usuarios pueden configurar escaneos específicos, seleccionar los puertos a analizar y adaptar las pruebas de seguridad según sus necesidades. Como vemos en la siguiente captura, contamos con diferentes opciones de configuración de la tarea:

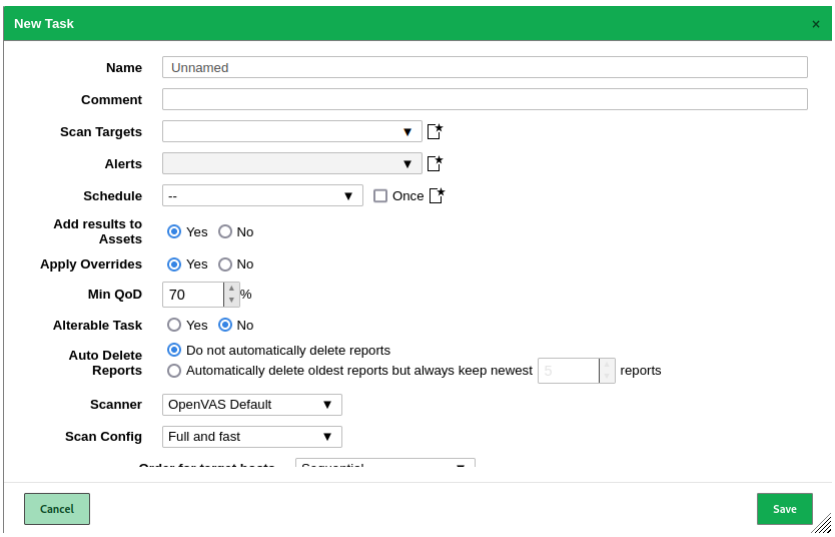

Figura 4.6: Menú de configuración de la tarea.

Podemos seleccionar los objetivos sobre los que realizar el análisis, alertas a emitir o programar la ejecución del análisis según nos convenga. Un valor importante a tener en cuenta es

el Quality of Detection (QoD), que nos indica la fiabilidad de las vulnerabilidades detectadas en el escaneo, esto implica que si ponemos por ejemplo un valor del 100%, las vulnerabilidades que aparezcan se habrán detectado directamente por un exploit. Por defecto, este valor viene en un 70%, que implica comprobaciones remotas que realizan algún análisis pero que no siempre son totalmente fiables.

En cuanto a los diferentes tipos de escaneos, se nos ofrecen diferentes opciones, desde escaneos dirigidos a recopilar información del sistema hasta profundos y lentos de todo el sistema. La opción más empleada y recomendada es la ”full and fast” que realizará el escaneo de vulnerabilidades sin demorarse demasiado y sin provocar problemas en el equipo. En nuestro caso práctico, emplearemos también la opción de ”system discovery”, destinada a realizar un análisis de la red estudiada. Este análisis nos servirá para saber los diferentes sistemas operativos que operan en las máquinas de la red, así como los servicios que están corriendo y puertos abiertos en cada host, lo cual nos será de gran utilidad para el descubrimiento de activos.

Una vez definida la tarea, la podremos ejecutar para llevar a cabo el análisis, podremos ir siguiendo el proceso y analizando los resultados que va obteniendo. Cuando el análisis haya terminado, se nos mostrarán directamente las amenazas detectadas, clasificadas según su severidad.

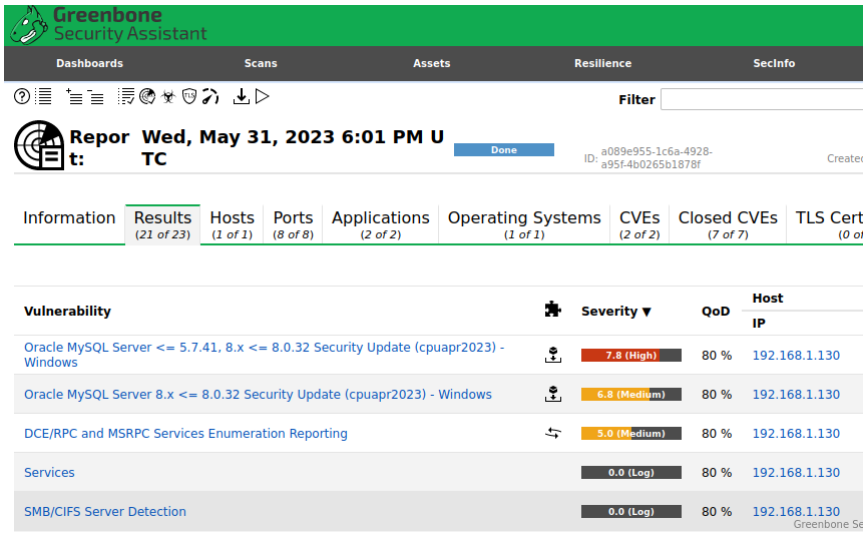

Figura 4.7: Resultado del análisis.

Como vemos en los resultados, tenemos diferentes vulnerabilidades con un factor de severidad distinto, OpenVAS nos indicará entre otras cosas, el problema, el método de detección y la solución al mismo. En este caso de estudio, tenemos un par de vulnerabilidades derivadas

de la versión que estamos empleando de MySQL Server, por lo que nos indicará la versión a la que debemos actualizar para mitigar este problema.

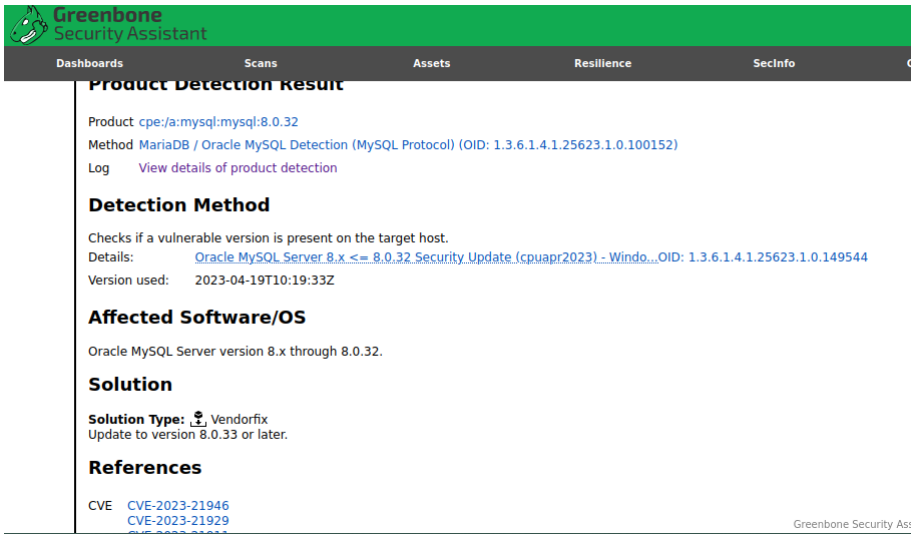

Figura 4.8: Solución a la vulnerabilidad.

4.3 Nmap

Network Mapper (NMap) es una herramienta de exploración de redes y escaneo de puertos que se utiliza ampliamente en el descubrimiento de activos. Será la herramienta que emplearemos en la fase de ”descubrimiento de activos” presente en la metodología, la usaremos para descubrir los dispositivos presentes en la red, como ordenadores, servidores, routers, impresoras, etc.

También puede escanear los puertos abiertos en los dispositivos para identificar los servicios que están en funcionamiento. Esto nos ayuda a determinar qué servicios están disponibles en cada host y qué puertos están siendo utilizados. Además permite realizar un análisis de la topología de red, ya que puede trazar la topología de la red, mostrando cómo los dispositivos están interconectados, lo que nos ayudará a comprender la estructura de la red, identificar enlaces críticos y puntos de acceso [5].

Nmap es empleado por OpenVAS en algunos de sus escaneos de red o vulnerabilidades, por lo que también se estará usando de en segundo plano mediante esa herramienta.

Capítulo 5

Caso práctico

En este capítulo expondremos el empleo de la metodología en un caso real, empleándola en un CPD primero para comprobar el nivel Tier que podría alcanzar en su estado actual, analizando los 4 subsistemas que se contemplan en la ANSI/TIA-942, para luego hacer una recopilación de todos los requisitos que no se cumplen en relación al nivel Tier determinado que se quiere alcanzar.

Es importante destacar que ciertos aspectos en cuanto al descubrimiento de activos, inventario y características técnicas del CPD han sido cambiadas para evitar una representación completamente fiel a la realidad, por motivos de seguridad del propio CPD, ya que se trata de información sensible.

5.1 Inicio del proyecto

Como indica la metodología, el primer paso es conocer los intereses de la organización y sentar las bases del proyecto que queremos realizar. En nuestro caso, tras realizar entrevistas con personas responsables en el centro, estableceremos el siguiente objetivo de nuestro proyecto: realizar un estudio del CPD para determinar en que certificación Tier se encontraría actualmente, para luego cubrir todos los requisitos que falten y obtener un nivel de certificación mayor, mediante el desarrollo de un proyecto de reforma del centro.

5.1.1 El CPD a estudiar

El CPD empleado para realizar la parte práctica se trata del que se encuentra en el Centro de Investigación en Tecnologías de la Información y las Comunicaciones (CITIC), que cuenta con dos edificios modulares con una superficie de 3200 m^2 repartidos en diferentes plantas. Como se trata de edificios que son considerados independientes, se realizará un estudio en

profundidad solo del edificio que contiene el CPD, aunque se tendrá en cuenta el hecho de que comparten la infraestructura, ya que esto influye directamente en la certificación Tier que se puede obtener.

Es importante destacar en cuanto al contexto de la organización y el impacto del proyecto en la operación del CPD, que tanto el propio edificio como los servicios que presta el CPD son compartidos entre diferentes organizaciones, por lo que las pruebas se han realizado con cuidado, excluyendo algunos activos intencionadamente para evitar que el trabajo de descubrimiento supusiese un impacto notable en servicios ajenos.

5.2 Análisis del entorno

Para realizar esta parte, se llevaron a cabos pruebas presenciales en el CPD, empleando tanto las herramientas descritas anteriormente como recolección de información mediante entrevistas con responsables del centro, realizando visitas guiadas para comprobar el estado del CPD y sus características.

5.2.1 Descubrimiento de activos

El descubrimiento de activos se realizó en la propia sala de computación, accediendo vía Ethernet a una de las subredes disponibles, y con la debida autorización de las personas responsables. Una vez dentro de la red se realizaron varias pruebas: un escaneo general de la red empleando OpenVAS y algunas pruebas contra dispositivos concretos con Nmap, en caso de querer saber más información que la recogida inicialmente por OpenVAS.

Como se ha mencionando anteriormente, los resultados expuestos en el trabajo no son completamente fieles a lo obtenido por motivos de privacidad y seguridad del CPD y los datos que se manejan en el mismo.

Uso de OpenVAS y Nmap

Una vez conectado a la red, se realizó un escaneo empleando el método ”system discovery”, para encontrar sistemas operativos, servicios disponibles, puertos y hosts en la red. También se realizaron pruebas con Nmap sobre algunos de los hosts para obtener más información. El escaneo general de la red tuvo una duración aproximada de una hora y media, debido a que OpenVas lleva a cabo numerosas pruebas contra los hosts para ir extrayendo información, estas pruebas pueden ser más o menos intrusivas en los equipos, por este motivo añadimos algunas excepciones en el escaneo, ya que podrían suponer un problema en los servicios del CPD.

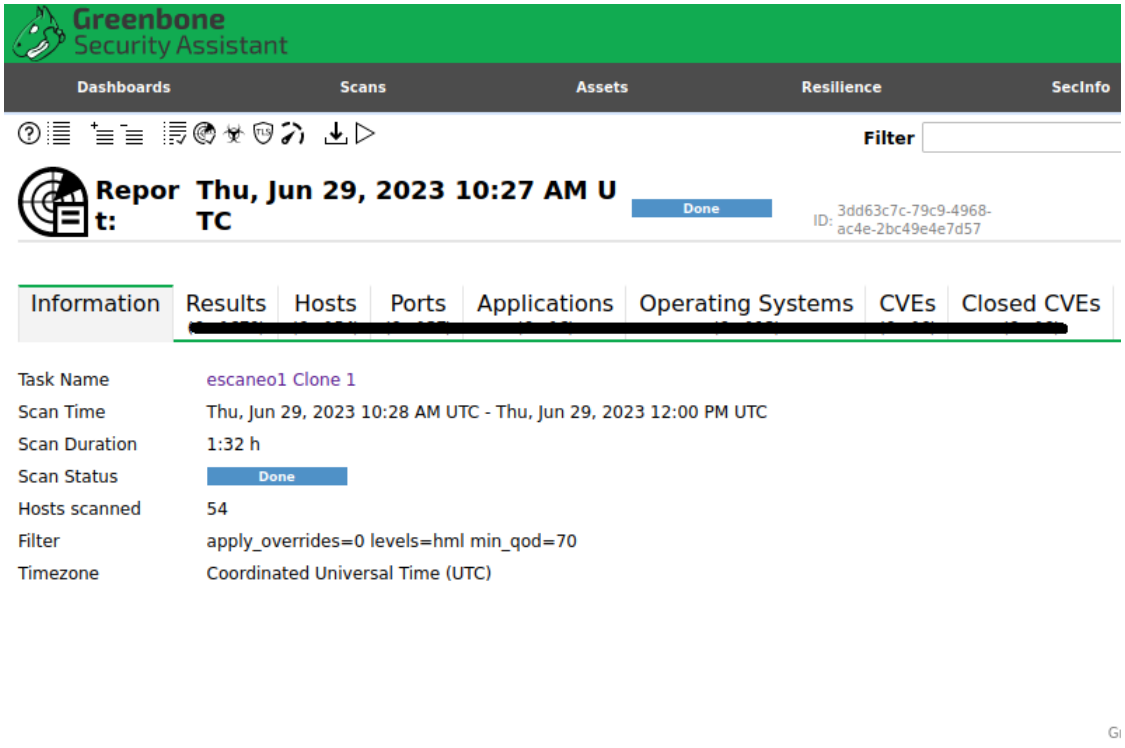

Figura 5.1: Escaneo realizado.

Vemos como la duración del escaneo ha sido bastante larga, debido al número de pruebas que se realizan contra los hosts para conseguir información. Los resultados se exponen a continuación:

Sistemas operativos: se encontraron un total de 12 sistemas operativos diferentes activos en los hosts analizados, entre ellos tenemos Windows, hipervisores de VMware así como diferentes distribuciones de Linux (Ubuntu en varias versiones, CentOS...)

Aplicaciones: existen varias aplicaciones en los diferentes hosts estudiados, podemos encontrar servidores mysql, postgress, samba, zabbix...

Puertos abiertos: hay un total de 37 puertos diferentes disponibles que alojan varios servicios, entre los que podemos encontrar los comunes 22, 80, 443... Así como otros más particulares presentes en un número mucho menor de hosts.

Hosts: Se encontraron cerca de unos 50 hosts activos en la red, en su mayoría se tratan de los servidores del CPD, además de los hipervisores de VMware, IPs de gestión de servidores, así como ordenadores conectados a la red o impresoras.

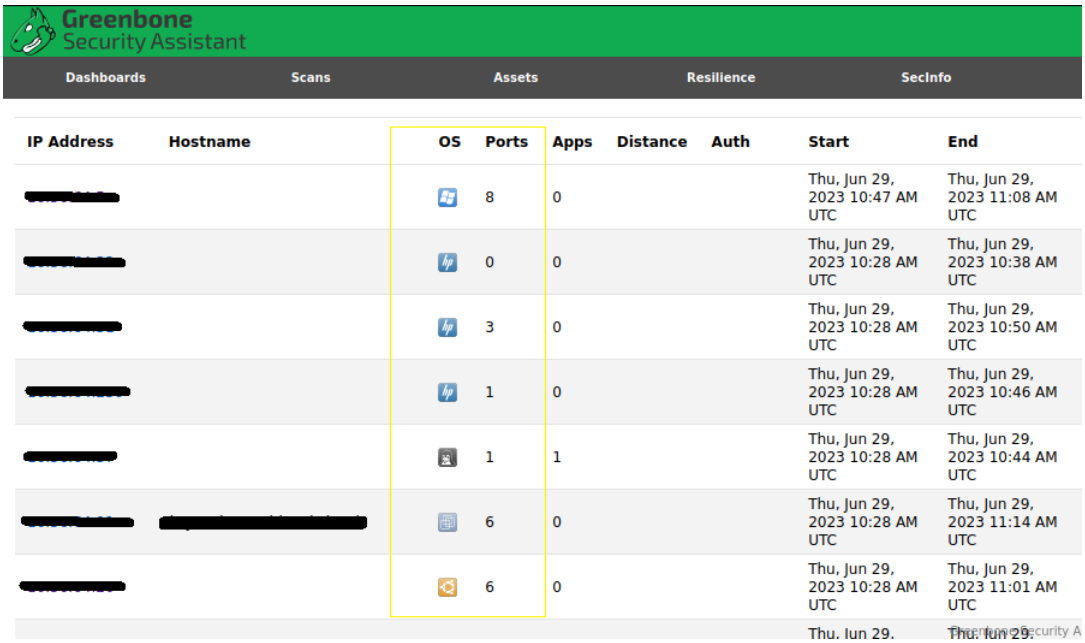

Figura 5.2: Algunos de los hosts encontrados.

Gestión de los activos con GLPI

Una vez realizado el descubrimiento de activos mediante el escaneo de la red, realizamos un inventario de los equipos que tenemos en la sala de computación del CPD. Esto lo haremos para ver el tipo de servidores de los que disponemos, así como otros dispositivos tales como routers, switches o firewalls. De esta forma iremos comprobando los diferentes hosts encontrados en el escaneo de la red y su localización física en la sala de computación (en qué racks se encuentran).

Este inventario se realizó abriendo y mirando uno por uno los diferentes racks, anotando el número de servidores que contienen, el modelo de dichos servidores o si contienen switches u otros dispositivos. Tras realizar el estudio, tenemos un inventario claro de todos los elementos presentes en la sala de computación. A continuación, se exponen algunos de los contenidos de ciertos racks (manteniendo siempre algunas diferencias con la realidad, como se explicó anteriormente).

Rack 1:
Este rack cuenta con 6 unidades de servidores DELL PowerEdge R200, y 3 y 1 unidades de servidores DELL PowerEdge R210 y R410 respectivamente. También encontramos un servi-

dor HP Proliant DL360 Gen 10 y un interruptor de transferencia automática APC.
Finalmente, contiene un firewall Cisco (modelo omitido) y un servidor NAS EMC IOMEGA StorCenter px12.

Rack 2:
En cuanto a equipamiento de red, aquí encontraremos 2 unidades de switch Ethernet APC y un switch Cisco SG300 28 puertos, así como un router Tp-link TL-ER6120.
En relación a los servidores, tendremos una unidad de servidores DELL PowerEdge R720xd y R220, 2 unidades de servidores HP Proliant DL120 Gen 5 y servidores HP Proliant DL360e, DL360 Gen 9, DL380e, DL380p, también uno de cada.

Rack 3:
En este rack encontramos un switch Alcatel-Lucent OS6860E 48 puertos y un switch Linksys LGS124 24 puertos como equipamiento de red.
Sobre los distintos servidores, tenemos una unidad de cada uno de los siguientes: servidores DELL PowerEdge R300 y R415, servidores NAS Synology RS2414+ y RS2212+, un servidor HP Proliant DL360 Gen 5 y servidores IBM eServer xSeries 345 y 346 (1 y 2 unidades respectivamente). Por último, contamos con una unidad de almacenamiento HP StorageWorks MSA20.

Estos son algunos de los racks inventariados, cabe destacar que el inventario completo consta de 14 racks. Aunque solo se ha mostrado una pequeña parte del inventario real, emplearemos el inventario completo en GLPI, para ser lo más fiel posible a una aplicación real de la metodología.

Con el inventario hecho y los activos identificados, es hora de introducir todos nuestros datos en GLPI, para poder llevar una gestión clara y sencilla durante la reforma del CPD. Ya que tenemos que introducir bastantes datos y equipos en la herramienta, el uso de plantillas nos facilitará el proceso en gran medida.

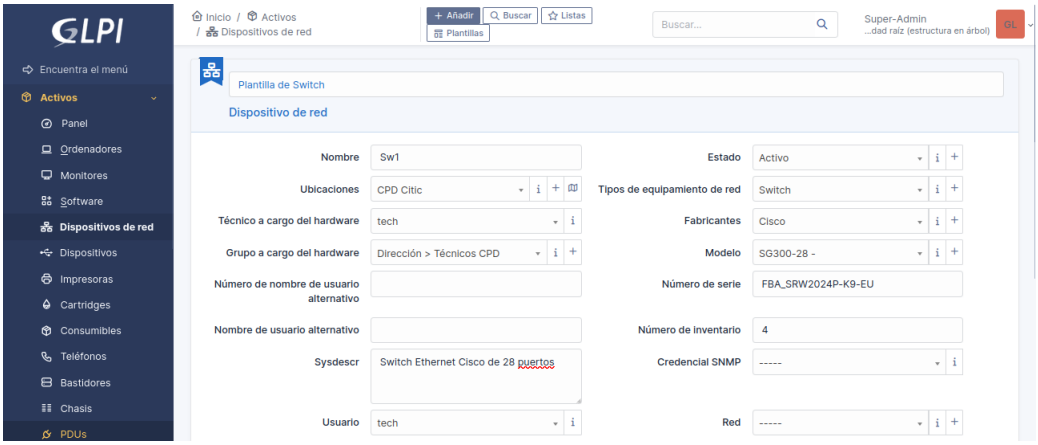

Figura 5.3: Plantilla correspondiente a un Switch.

Añadimos todos los servidores, ordenadores, dispositivos de red, aplicaciones, racks, monitores... También dejamos plasmada la distribución de los diferentes dispositivos en los racks, lo cual nos es de gran ayuda sobretodo si vamos a realizar reformas, para tener claro la situación de cada uno de los dispositivos y su localización. GLPI nos permite hacer esto con una interfaz gráfica muy visual y sencilla de utilizar. En la captura que se muestra a continuación, aparece la distribución del rack 1, inventariado anteriormente:

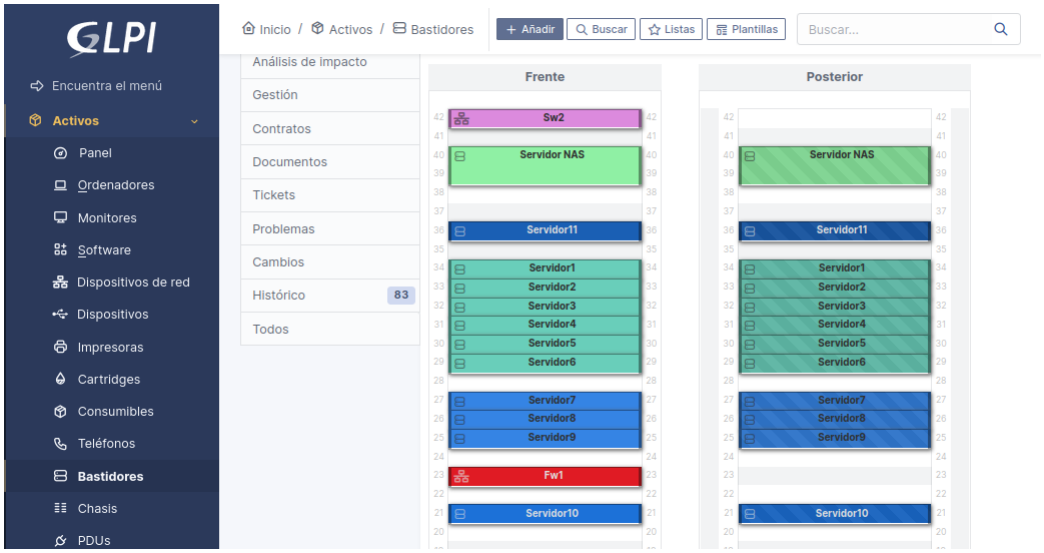

Figura 5.4: Distribución de los elementos del rack 1.

Vemos como tenemos organizados los diferentes dispositivos en el rack, la mayoría de ellos ocupan 1U (1 unidad de espacio del rack) salvo el Servidor NAS que ocupa 2U y que la profundidad en el rack de la mayoría es de 1, lo que quiere decir que lo ocupan desde el frente

hasta la parte posterior, en este caso son los servidores los que ocupan la mayor parte del espacio.

Tras añadir todos los activos y demás elementos disponibles, nos queda la siguiente visión del panel general:

Figura 5.5: Panel de los activos disponibles.

La gran mayoría de los activos se clasifican en el campo de ”ordenadores”, en esta sección es donde se encuentran los servidores, de ahí su gran número, pero también podemos encontrar ordenadores del CPD o portátiles. En los ”dispositivos de red” tenemos switches, firewalls y routers y en ”software” se encuentran diferentes aplicaciones encontradas mediante el escaneo de la red con OpenVAS, como pueden ser bases de datos o software de monitorización. También introducimos en GLPI los documentos relacionados con el proyecto, tales como nuestra propia metodología desarrollada o diferentes estándares que se emplean, entre ellos la ANSI/TIA-942, NFPA 75, etc.

Con el inventario hecho, podemos pasar ya a comprobar el nivel Tier en el que se podría encontrar el CPD actualmente.

Comprobando el nivel Tier actual del CPD

Para poder realizar la fase del diseño del plan de cambio, necesitamos determinar antes la certificación Tier que podría alcanzar el CPD en su estado actual. En un primer análisis, se establece que la certificación general del CPD sería de Tier 1, esto se debe a que como se men-

cionó en capítulos anteriores, el nivel general de un CPD se rige por el nivel **menor** de todos sus subsistemas. Analizando los subsistemas de forma individual, nos encontramos conque su certificación estaría en $T_2E_1A_2M_1$.

En general, el CPD cuenta con la mayoría de características importantes que le permitirían adquirir una certificación Tier 2, pero la ausencia de diversos requisitos en los subsistemas Eléctrico e Infraestructura Mecánica impiden que se pueda garantizar esa certificación. Por ello, esos serán los subsistemas principales en los que se basará el plan de cambio, en el que nos dedicaremos a realizar las modificaciones pertinentes para poder cumplir con los requisitos de un CPD Tier 2. A lo largo del análisis también se han encontrado algunas características que cumplen con requisitos de un CPD de Tier 3, como podrían ser la disponibilidad de personal de mantenimiento o de personal de seguridad físico.

A continuación, se muestran una parte de los resultados del análisis realizado en el CPD, en cuanto a requisitos cumplidos para un nivel Tier 2:

Telecomunicaciones

- El cableado, racks y rutas cumplen con las especificaciones TIA.
- Los racks están debidamente etiquetados.
- Se cuenta con alimentación redundante para routers y switches.
- Los cables de conexión están etiquetados en ambos extremos.

Eléctrico

- Cable único de alimentación para los equipos, sin redundancia.
- Cuadro de distribución principal dedicado y con disyuntores automáticos.
- SAI con redundancia N+1, con una topología de módulos paralelos, bypass automático, disyuntores térmicos y baterías dedicadas para cada módulo, con duración de 10 años.
- PDUs de alta eficiencia.
- Entrada única con el proveedor de telecomunicaciones, tomas de tierra según la normativa vigente.
- Monitorización del SAI y del suministro externo.
- Generador con capacidad para alberga la carga total del edificio.
- Disponibilidad de personal de mantenimiento 24/7.
- Se realiza mantenimiento preventivo en el generador.

Arquitectura

- Provisto de requisitos mínimos de resistencia contra incendios en todo el edificio.
- Provisto los requisitos estructurales exigidos en cuanto a techo (inclinación, protección contra el viento).
- Se cumplen los tamaños de puertas ajustados a la normativa.
- Las diferentes salas circundantes a la sala de computación están separadas cumpliendo los requisitos mínimos de protección contra incendios.
- Existe detección de intrusiones en las salidas del edificio del CPD, y la salida de emergencia está monitorizada.
- El acceso principal a la sala de computación se realiza mediante el uso de tarjeta.
- Existe monitorización Circuito Cerrado de Televisión (CCTV) en las puertas de control de acceso.
- En la sala de computación, se cumple con los requisitos establecidos para la capacidad del suelo frente a cargas vivas superpuestas, así como la capacidad del techo para soportar cargas colgantes.

Infraestructura mecánica

- Hay redundancia N+1 en el sistema de refrigeración, tanto respecto a las torres de refrigeración, como a los componentes in-row pero la red de distribución es única.
- Hay presión positiva en la sala de computación.
- Existe un único suministro de agua, así como un único tanque de combustible.
- Se cuenta con sistema de detección de incendios, aspersores de preacción, así como detección de filtraciones de agua (instalado bajo el suelo técnico).

5.3 Diseño del plan de cambio

Ahora que ya disponemos de un inventario y una idea general sobre los requisitos que se cumplen en el CPD, centraremos nuestro proyecto en realizar los cambios y reformas necesarios en el centro para adquirir un certificado Tier 2, modificando los diferentes subsistemas que no alcanzan las condiciones necesarias. En nuestro caso, como se ha mencionado anteriormente se trata de los subsistemas eléctrico e infraestructura mecánica.

Para mantener un control de nuestro proyecto, diseñamos el plan de cambio empleando GLPI. En la pestaña de proyectos, seleccionamos un nuevo proyecto a crear y especificamos las diferentes opciones para la creación del proyecto, tales como fechas, estados, responsables...

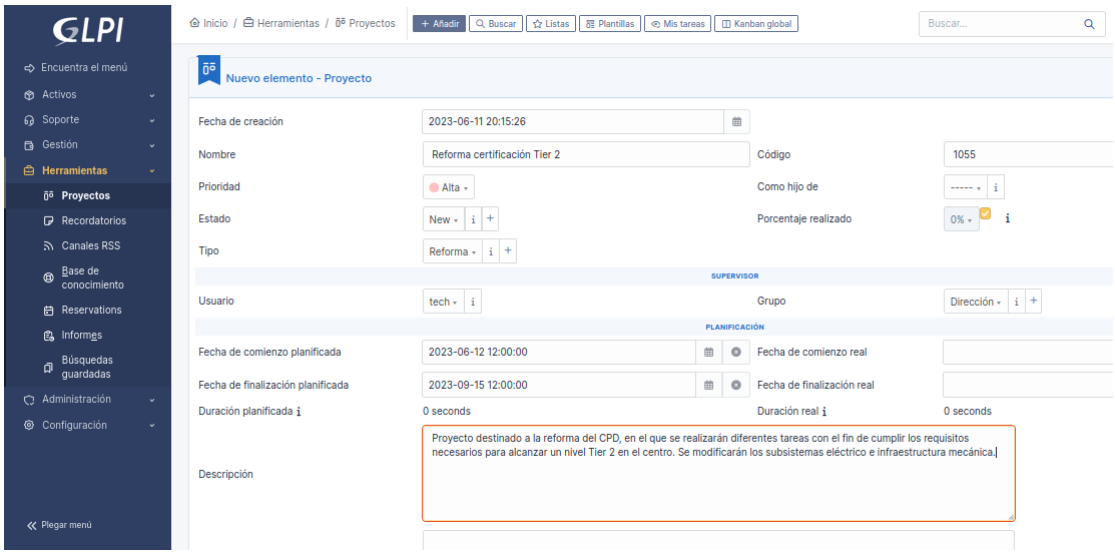

Figura 5.6: Menú de creación de proyecto.

Una de las opciones que nos permite GLPI es anidar proyectos, pudiendo crear proyectos hijo de otros. De esta forma, podemos dividir el proyecto general en dos subproyectos, uno para cada subsistema, para tratar los subsistemas de forma independiente. La idea con esto es destinar los proyectos hijo para agrupar las tareas de reforma, y dejar el proyecto inicial para las labores de supervisión y revisiones. Además, al estar sincronizados, a medida que se vayan completando los objetivos de los subproyectos, se irá avanzando también el proyecto principal.

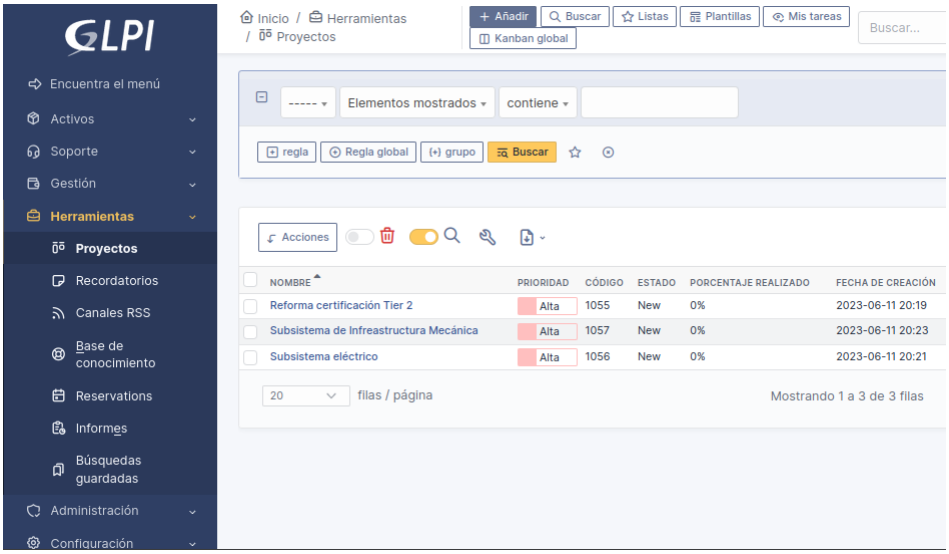

Figura 5.7: Lista de los proyectos actuales.

Con los proyectos creados, comenzaremos con las asignación de las tareas, aplicando prioridades y asignando recursos a cada una de ellas en función de su importancia. Para esto, dentro del proyecto tenemos la opción de añadir las tareas, por lo que iremos añadiendo distintas tareas relacionadas con los requisitos que nos faltan por cumplir en el CPD para obtener el Tier 2. En este paso emplearemos la información recopilada anteriormente, resultado de llevar a cabo el análisis del entorno del CPD.

Figura 5.8: Tareas del proyecto de Infraestructura mecánica.

Hemos añadido cuatro tareas a realizar en cuanto a la infraestructura mecánica, para completar así los requisitos exigidos por el Tier 2. A medida que se vayan avanzando en los proyectos hijo, el progreso del principal también se irá incrementando. Para la siguiente captura, hemos avanzado en los desarrollos de ambos proyectos referidos a los subsistemas, para observar como evoluciona su progreso.

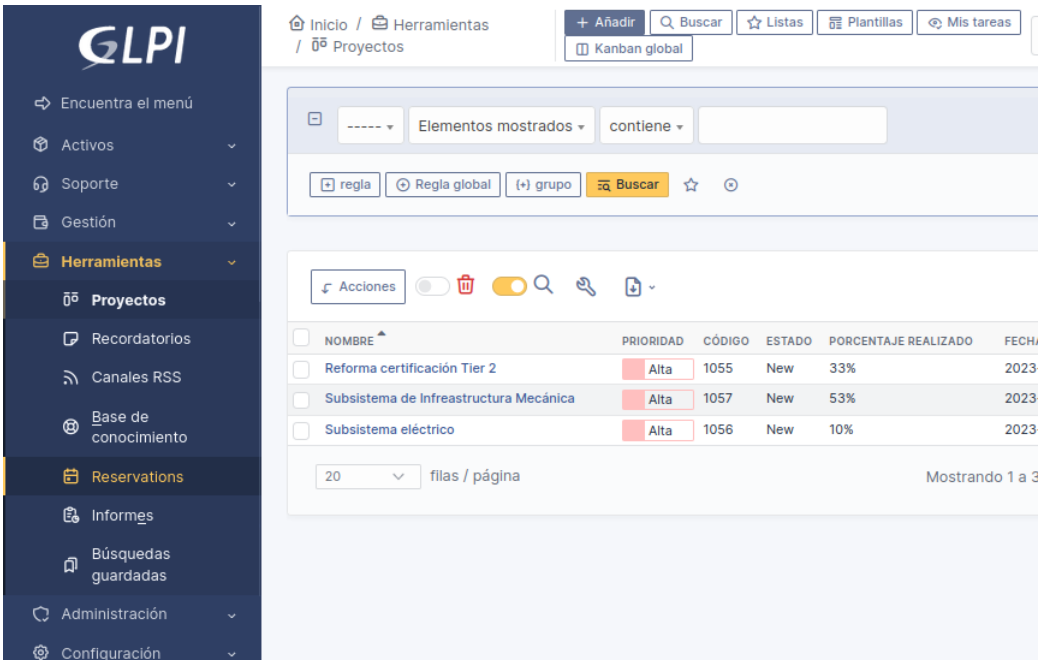

Figura 5.9: Progreso de los proyectos.

Por motivos obvios, no se puede continuar el caso práctico en las siguientes etapas de la metodología, ya que este es un caso hipotético y no contamos con la autorización para realizar reformas en el CPD, por lo que el caso práctico se quedará en los tres primeros pasos de la metodología.

Capítulo 6
Conclusiones

El objetivo principal del trabajo era simplificar la obtención de un nivel Tier para los responsables del CPD, ya que el estándar ANSI/TIA-942 se centra principalmente en los aspectos de construcción del CPD desde cero, siendo algo más secundario la clasificación en Tiers, ya que esta parte viene en un anexo al final del estándar. Nuestra metodología se centra directamente en estos niveles, por lo que está dedicada exclusivamente a ellos, esto fue de gran ayuda al realizar el caso práctico, sobretodo en la parte del diseño del plan de cambio, ya que se seleccionó un determinado nivel Tier a conseguir y se procedió apartado por apartado comprobando si el CPD del CITIC cumplía con las características reflejadas en la metodología. El proceso fue considerablemente rápido, y **en una mañana de entrevistas y estudio ya teníamos una idea general de la situación del CPD y su clasificación Tier tanto general como en cada uno de sus subsistemas**.

Cuando iniciamos el proyecto en el CITIC, los primeros pasos siguiendo la metodología fueron los de hablar con los responsables a cabo del centro. Esto estableció las bases sobres las que podíamos trabajar y los límites entre los que teníamos que llevar a cabo las pruebas, ya que en el contexto del CPD del CITIC, había determinadas subredes a las que no podíamos acceder ya que tenían un carácter más privado ajeno a los permisos que nos podía conceder el responsable del centro. También se eligieron los días para realizar las pruebas teniendo en cuenta si el CPD iba a estar muy concurrido, para evitar causar problemas a los responsables o en la operación normal del CPD. En nuestro caso, al realizar el descubrimiento de activos en una red en la que se encuentran servicios de los que hacen uso una parte considerable de la universidad, había que tener cuidado de no provocar saturaciones en los servidores que pudiesen causar problemas en los servicios, ya que las pruebas con Nmap o OpenVAS pueden generar bastante carga en los dispositivos analizados.

Con respecto a identificar posibles problemas que pudiesen surgir, un caso particular que

tuvimos en cuenta fue que Nmap puede provocar problemas en las impresoras que se encuentran dentro de la red escaneada, haciendo que funcionen de forma errónea imprimiendo sin control. Por este motivo, se excluyeron las direcciones IP que pertenecían a impresoras y se identificaron de otra forma.

En cuanto a las responsabilidades y compromiso, se brindaron todos los recursos necesarios para realizar las pruebas y fueron llevadas a cabo de forma adecuada, cumpliendo con las normas de la seguridad de la información. En los días en los que estuvimos haciendo las pruebas, se dejó registro de nuestra presencia en el centro, con las identificaciones necesarias y las horas en las que se realizaron las pruebas.

Siguiendo con el descubrimiento de activos, el uso de OpenVAS y Nmap cumplió con las expectativas para ello. El análisis de la red se realizó de 20 en 20 hosts, y fue de una duración considerable debido a la información que brinda y las pruebas que realiza. Además, OpenVAS permite generar un informe de los análisis que se realicen, por lo que en al acabar de realizar el mismo, ya contábamos con un documento de más de 400 páginas, en donde se hablaba de cada host activo en la red, dando sus características (puertos abiertos, servicios, sistemas operativos...). Este informe fue enviado al responsable del centro, para compartir con el los resultados y comprender mejor la red estudiada.

En cuanto al uso de GLPI, la herramienta proporciona un soporte ideal para nuestro caso, puede explotarse en profundidad y los servicios que brinda son muy adecuados para el tipo de proyecto que queríamos llevar a cabo. La interfaz gráfica es amigable y sencilla de comprender, y cuenta con una documentación extensa en la que se detallan y explican con ejemplos cada una de sus características y funciones disponibles. En cuanto a su instalación, la herramienta es de código abierto y no necesita nada más que un servidor y una base de datos para funcionar, por lo que su instalación fue relativamente sencilla. Además ofrece gran flexibilidad a la hora de crear los proyectos y gestionar cambios en el CPD, esta parte era especialmente importante a la hora de elegir una herramienta en la que apoyarse para el desarrollo de la metodología, ya que GLPI no se centra exclusivamente en la gestión de los activos.

Tras una reunión inicial para presentar la idea que teníamos pensado realizar en el CITIC, **bastaron con 3 días de pruebas**, con un total de no más de 13 horas para llevar a cabo la parte práctica del trabajo, un tiempo muy asequible. Cabe destacar que no se pudo acceder a todas las subredes existentes, tal y como se mencionó anteriormente, por lo que en un caso completamente real, realizar un estudio a fondo de la red nos llevaría mucho más tiempo del plasmado en este trabajo.

Debido a las limitaciones en cuanto a autorización al no tratarse de un proyecto real, no se puede tampoco explorar a fondo las posibilidades de la metodología, ya que no se han realizado reformas en el CPD al fin y al cabo. Particularmente, me hubiese gustado poder realizar un análisis más profundo del CPD, e incluso llevar a cabo alguna pequeña modificación para obtener unos resultados más fieles del estudio, todo esto hubiese traído un informe más rico en cuanto a información. Aún así, los resultados obtenidos son favorables en cuanto a la aplicación de la metodología, y los pasos a seguir marcados por la misma parecen aplicarse bien en el entorno del CPD.

6.1 Vistas al futuro

En un futuro, creo que la aplicación a un proyecto completamente real de esta metodología podría traer buenos resultados, además de proporcionar esa retroalimentación tan necesaria para la misma. Viendo los resultados, no hay razón para pensar que sería contraproducente emplear esta metodología en un caso real, en mi opinión, creo que se adaptaría bien en particular a empresas que contasen con un CPD de tamaño medio y estén interesadas en los niveles Tier 1 y 2, similar a como vimos en el caso práctico.

Por supuesto, no habría ningún problema en aplicar la metodología en algún CPD más grande, pero como los CPD de Tier 3 y 4 requieren tanto mantenimiento y tantos recursos económicos, las empresas que cuentan con ellos posiblemente puedan destinar grandes cantidades de dinero en decenas de expertos o a solicitar directamente auditorías para la concesión de los certificados al Uptime Institute. Sin embargo, ese puede no ser el caso de empresas más pequeñas, por lo que en un futuro es ahí donde veo mayor potencial.

6.2 Mi experiencia con el trabajo

Por último, quiero hablar de mi experiencia en la aplicación de la metodología, ya que durante el caso práctico he puesto a prueba aptitudes adquiridas en diversas materias de la carrera, tales como ”Legislación y Seguridad Informática” en el uso de programas de escaneo de red o ”Gestión de proyectos” en cuanto a la organización del trabajo. Además, he adquirido experiencia y conocimiento en el proceso de la auditoría en CPD. Pero destacar sobretodo los conocimientos adquiridos en las asignaturas de ”Gestión de infraestructuras”, ”Ingeniería de Infraestructuras Informáticas” y ”Administración de Infraestructuras y Sistemas Informáticos” que me han servido para tener una base sólida sobre los CPD, sus componentes, su

funcionamiento y la importancia de los mismos y han conseguido que me interesase en este campo para proponer este trabajo. Concretamente desde la visita guiada al CPD del CITIC en el tercer curso del grado he sentido interés por el mundo de estos centros y ya tuve claro que quería orientar mi trabajo de fin de grado a ello. Quiero dejar también mi gratitud a los responsables del CPD del CITIC, que me han brindado todas las facilidades posibles para realizar el trabajo cómodamente, y a los profesores de las asignaturas mencionadas anteriormente, puesto que los conocimientos adquiridos han facilitado la realización de este trabajo y no me cabe duda de que serán de gran ayuda de cara al futuro profesional, ya que con este trabajo se cierran los cuatro años de la que fue una gran etapa en la universidad.

Lista de acrónimos

ANSI American National Standards Institute. 1

CCTV Circuito Cerrado de Televisión. 17, 25, 35, 71

CITIC Centro de Investigación en Tecnologías de la Información y las Comunicaciones. 63

CPD Centro de Procesamiento de Datos. 1

GLPI Gestion Libre de Parc Informatique. 55

HVAC Heating Ventilating Air Conditioned. 11, 18, 27, 37

IBC International Building Code. 10, 17, 26, 35

MEP Mechanical, Electrical and Pumbling. 16, 25, 35

NMap Network Mapper. 62

OpenVAS Open Vulnerability Assessment System. 58

PDU Power Distribution Unit. 21, 30

QoD Quality of Detection. 61

SAI Sistema de Alimentación Ininterrumpida. 7

SDC Seismic Design Category. 10, 17, 26, 35

TI Tecnologías de la Información. 1

TIA Telecommunications Industry Association. 1

VRLA Valve Regulated Lead–Acid. 9, 13, 20, 29

Glosario

AHJ En el campo de la construcción y la protección contra incendios, el término AHJ se refiere a la Autoridad con Jurisdicción (Authority Having Jurisdiction, en inglés), que tiene el poder de hacer cumplir los códigos y regulaciones relacionadas con la seguridad de un área específica. 9

Banco de carga Consiste en un conjunto de resistencias eléctricas que se conectan al sistema que se está probando para simular la carga eléctrica que normalmente se encontraría en funcionamiento. Se emplea para comprobar que equipos como generadores de reserva pueden soportar la carga de trabajo. 14, 21, 31

Bus Un bus de datos es un sistema que se encarga de transferir datos entre componentes de un computador o red de computadores. 9, 14, 21, 31

exploit Un exploit es un software, un fragmento de datos o una secuencia de comandos que aprovecha un error o una vulnerabilidad de una aplicación o sistema para provocar un comportamiento involuntario o imprevisto. 61

Factor de importancia El factor de importancia se utiliza para asignar niveles de carga de diseño más altos a estructuras consideradas de mayor importancia. 11, 17, 26, 35

Flywheel Tipo de batería por inercia, que almacena energía cinética, que se emplea en SAI. 9, 13, 20, 29

FM El estándar FM I-90 establece los requisitos y especificaciones para la resistencia al viento de los sistemas de techado, con el objetivo de minimizar el riesgo de daños por viento y proteger los edificios y sus contenidos. 15, 23, 33

in-row El término ”in-row” se utiliza para describir diversos componentes o sistemas que se colocan en filas. En el contexto de un CPD, se refiere a cuando se colocan en las mismas filas que los propios servidores. 71

k-rated El factor K es un indicador que permite estimar la capacidad que tiene un transformador de soportar los efectos térmicos producidos por las corrientes armónicas. 20, 30

Pass back cuando una persona autorizada ingresa a una instalación o área restringida y luego pasa su credencial de acceso, como una tarjeta o llave, a otra persona no autorizada para que la use y obtenga acceso sin tener su propia autorización. 24, 25, 33, 35

Piggybacking Cuando una persona no autorizada se aprovecha de la entrada legítima de otra persona para ingresar a un área restringida sin someterse a los procedimientos de control de acceso. 24, 25, 33, 35

Tier Nivel que se emplea en el estándar ANSI/TIA-942 para clasificar los CPD según sus carácterísticas. 2

Uplink Este tipo de puerto se utiliza para interconectar switches o para conectar un switch a una red de nivel superior, como una red de área amplia (WAN) o un backbone de red. 19, 28

Bibliografía

[1] *Telecommunications Infraestructure Standar for Data Centers*, American National Standards Institute and Telecommunications Industry Association, 2012.

[2] C. W. Astudillo-García and A. E. Cabrera-Duffaut, "Políticas de gestión de seguridad de la información, fundamentadas en la norma iso/iec 27001, centro de datos diseñado con el estándar ansi/tia 942," *Dominio de las ciencias*, 2019.

[3] "Glpi documentation utilisateur," 2023. [En línea]. Disponible en: https://glpi-user-documentation.readthedocs.io/fr/latest/index.html

[4] "Greenbone security manager with greenbone os 20.08 – user manual," 2023. [En línea]. Disponible en: https://docs.greenbone.net/GSM-Manual/gos-20.08/en/index.html

[5] "Guía de referencia de nmap." [En línea]. Disponible en: https://nmap.org/man/es/index.html

[6] *Administration Standard for Telecommunications Infrastructure*, American National Standards Institute and Telecommunications Industry Association, 2012.

[7] *Standard for the Installation of Lightning Protection Systems*, National Fire Protection Association, 2020.

[8] *Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises*, American National Standards Institute and Telecommunications Industry Association, 2012.

[9] *Standard for the Fire Protection of Information Technology Equipment*, National Fire Protection Association, 2020.

[10] *Standard for Hanging and Bracing of Fire Suppression Systems*, National Fire Protection Association, 2020.

[11] C. P. Rodríguez, "¿cómo construir una matri de riesgo operativo?" *Revista de ciencias económicas Vol-29*, 2011.