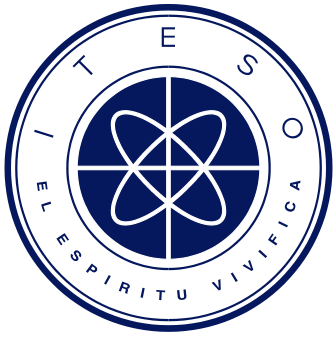
INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación el 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

MAESTRÍA EN INFORMÁTICA APLICADA



GESTIÓN DE LOS PROYECTOS DE DISEÑO E IMPLEMENTACIÓN DE LA PLATAFORMA INFORMÁTICO-TECNOLÓGICA PARA UNA COMPAÑÍA DE LA INDUSTRIA ELECTRÓNICA

Trabajo recepcional que para obtener el grado de

MAESTRO EN INFORMÁTICA APLICADA

Presenta: Francisco Jaime Vázquez

Asesor: Mtro. Ricardo Salas Mejía

Tlaquepaque, Jalisco. Noviembre de 2016.

ÍNDICES

Resumen

El presente trabajo de obtención de grado pretende detallar la gestión realizada durante los procesos de diseño, planeación e implementación de la plataforma informático-tecnológica dentro de una compañía de manufactura de la industria electrónica durante sus inicios de operación en la ciudad de Guadalajara.

Para facilitar la comprensión de los requerimientos del proyecto reportado, su naturaleza y la criticidad de que fuesen cubiertos, se incluye inicialmente una descripción de la organización y de sus actividades.

Dentro del marco de referencia, se encontrará la teoría aplicable reunida en dos grupos; la relacionada con las Tecnologías de la Información, y aquella tocante a los marcos de trabajo, investigación y gestión de proyectos, de manera que conforme se avance en la lectura del reporte, resulte sencillo mapear en cuáles etapas de desarrollo del proyecto se han utilizado unos u otros conceptos.

Posteriormente, se detalla la propuesta obtenida a lo largo del desarrollo del proyecto, éste es el grueso del documento, e incluye detalles que la sustentan, tanto desde el punto de vista técnico-tecnológico, como del de la administración de proyectos, así como la explicación del uso de otras herramientas de gestión, como las de planeación estratégica, también utilizadas para su concepción. Asimismo, se describen los resultados obtenidos tras la realización del proyecto. La propuesta final del mismo, contiene la descripción detallada –en la medida de lo que consideré sería necesario- de los diferentes elementos individuales que la componen, así como las interacciones existentes entre ellos, y su integración final como una solución individual.

Se continúa con un listado de lecciones aprendidas durante el desarrollo del proyecto reportado, así como con una reflexión personal sobre la influencia que los conocimientos adquiridos en la maestría ejercieron en mi desarrollo profesional y cómo contribuyeron en la realización del proyecto. Posterior a este punto, el trabajo cierra con una serie de anexos referentes a conceptos teóricos y a detalles específicos de la solución propuesta.

Objetivo del documento

Sustentar que la utilización de algunos marcos de trabajo propios de la gestión de proyectos, así como de herramientas de planeación estratégica, contribuyen de manera real a la realización exitosa de prácticamente cualquier proyecto, para lo cual, se ejemplifica con el desarrollo del proyecto reportado.

Justificación del documento

Durante la realización de proyectos, existe la tendencia de pasar por alto el proceso de planeación y comenzar a trabajar de inmediato, este fenómeno se presenta con mayor frecuencia cuando los proyectos incluyen tareas similares a trabajos anteriores. Al pasar por alto el proceso de planeación, se corre el riesgo de omitir pasos básicos, a realizarlos sin orden o a destiempo, causando errores costosos, ya que los riesgos pueden no ser evaluados adecuadamente cuando nos vemos presionados a comenzar a trabajar de manera inmediata. Un proyecto que no ha sido planeado lo suficiente, puede también estar ignorando puntos de vista de los demás interesados, con lo que se puede incurrir en la reelaboración de actividades.

Dado lo anterior, se explica la utilización de los marcos de trabajo basados en la Guía PMBOK y de algunas herramientas de planeación estratégica, todos ellos explicados más delante, en el apartado Marcos de trabajo, investigación y gestión de proyectos. Al tratarse de un proyecto de relativa complejidad, la documentación de todo su proceso de gestión puede agruparse de manera que pueda utilizarse como guía de buenas prácticas para la aplicación de esas metodologías en proyectos similares.

Alcance del documento

Este documento ha sido elaborado a partir de la información obtenida a lo largo de las diferentes etapas de realización del proyecto reportado. Dicha recopilación, pretende documentar los siguientes puntos referentes al diseño y la implementación de algunas plataformas informático-tecnológicas, tales como:

- El entorno operativo y una breve historia de la organización donde se realizó el proyecto reportado, esto con la finalidad de comprender la importancia de sus requerimientos.
- Los requerimientos específicos por área o grupo de trabajo.
- Los análisis de alternativas y sus correspondientes tomas de decisión.
- La asignación de usuarios a los diferentes grupos de trabajo de acuerdo con sus funciones y/o responsabilidades.
- Los diagramas conceptuales y físicos de las conexiones entre los diferentes nodos y equipos activos de red.
- La relación de las diferentes conexiones (nodo vs. Panel de conexión).
- Las mediciones de los aspectos más críticos de la conectividad.
- El resumen de la solución propuesta, así como su justificación, tanto técnica como financieramente hablando (esta última en la medida de lo permitido por la compañía en la que se realizó el proyecto reportado).
- Los diagramas conceptuales de la integración de los diferentes elementos de la plataforma.
- El esquema de seguridad informática

De igual forma, el documento incluye explicaciones de los marcos teóricos correspondientes a cada tópico de análisis y estudio observados a lo largo de la realización del proyecto reportado.

Al tratarse de una propuesta técnico-tecnológica integral, no existe un enfoque hacia un área específica, sino que la atención oscila entre los diferentes componentes de la misma, conforme estos van surgiendo a lo largo de la realización del proyecto reportado.

CAPÍTULO 1. MARCO DE REFERENCIA

1.1 Conceptos teóricos aplicables al proyecto

Básicamente existen dos grandes campos del conocimiento que han sido considerados dentro del marco de referencia para el desarrollo del presente documento; el primero de ellos abarca aquellos tópicos inherentes a la naturaleza del proyecto, y el segundo comprende la teoría necesaria para analizar la información con que se cuenta.

Teoría relacionada con las Tecnologías de la Información

Diseño de redes de datos

- Diseño topológico
- Teoría de grafos
- Características físicas y funcionales de equipos activos de red
- Tecnologías de cableado
- Sistemas operativos de red
- Protocolos de comunicación
- Modelo OSI de ISO

Mejores prácticas en Tecnologías de la Información (TI) y normativa aplicables

- Guía de trabajo COBIT[1] para el control y supervisión de las TI.
- Conjunto ITIL[2] de mejores prácticas para la gestión de servicios de TI *Information Technology Infrastructure Library* (ITIL).
- Normas o estándares ANSI/TIA/EIA/IEEE/CENELEC/ISO aplicables.

[1] *Control Objectives for Information and Related Technology* (COBIT) es un marco de trabajo de gobernanza de las TI y un conjunto de herramientas de apoyo que le permiten a los profesionales de las TI disminuir la brecha existente entre los requerimientos de control, cuestiones técnicas y los riesgos de los negocios.

[2] *Information Technology Infrastructure Library* (ITIL) es un conjunto de prácticas para la gestión del servicio de las TI enfocado en la alineación de los servicios de TI con las necesidades de las organizaciones. Se compone de cinco volúmenes correspondientes a las diferentes etapas del ciclo de vida de los servicios de TI: Estrategia de servicio, diseño del servicio, transición del servicio, operación del servicio, y mejora continua del servicio.

Marcos de trabajo, investigación y gestión de proyectos

- Método de solución de problemas *Problem Solving and Decision Making* (PS&DM) – Kepner-Tregoe
- Método de mejora continua *Plan-Do-Check-Act/Adjust* (PDCA), también llamado Ciclo de Deming o de Shewhart
- Conjunto de terminología y directrices para la administración de proyectos *Project Management Body of Knowledge* (PMBOK).

Diseño de redes de datos

Este apartado trata en general de todos los elementos físicos y lógicos que forman una red de datos. El diseño topológico permitió definir la ubicación de los diferentes elementos y su interconexión con otros dentro de esta red. La teoría de grafos fue específicamente útil en el momento de definir un esquema de redundancia de dicha red. Las características físicas y operativas de los equipos y las tecnologías disponibles para cableado permitieron elegir la combinación de alternativas que representarán la mejor relación costo/beneficio. Los sistemas operativos de red y los protocolos de comunicación fueron definidos una vez que se evaluaron aspectos tales como: seguridad, soporte, políticas internas de la compañía (directrices), costo total (*Total Cost of Ownership*, TCO), disponibilidad, recursos, plataforma y utilización.

El modelo OSI de ISO[3] merece mención aparte, ya que es sobre este modelo conceptual que se definen las funciones internas de los sistemas de comunicación. El modelo se divide en 7 capas (ver Figura 1), de manera que cada capa sirve a la capa inmediata superior, y a su vez es alimentada por la capa inmediata inferior, definiendo la forma en la que la información será manipulada durante las diferentes fases de su transmisión.

[3] Este modelo es un producto del proyecto *Open Systems Interconnection* (OSI) dentro del *International Organization for Standarization* (ISO), y se mantiene bajo la identificación ISO/IEC 7498-1

A pesar de ser un modelo básico para los profesionales de las TI, es conveniente enfatizar su importancia, dado que su utilidad es notoria durante los procesos de análisis de problemas de conectividad, facilitando la solución de los mismos.

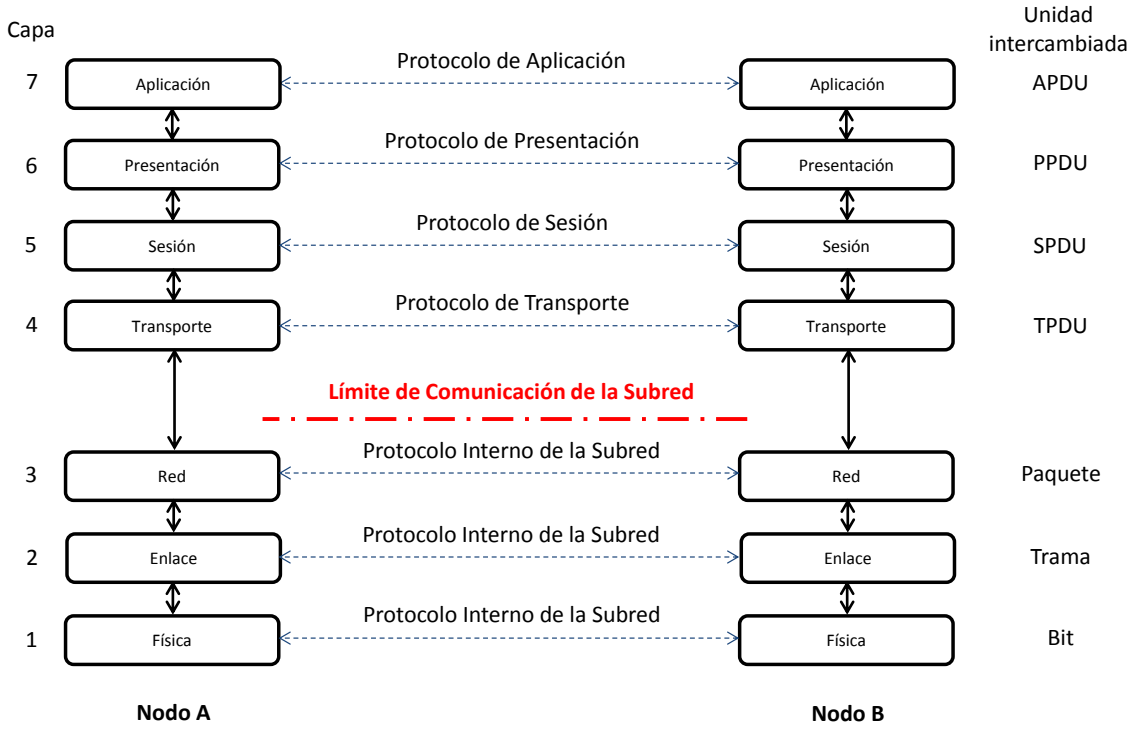


Figura 1. Modelo OSI de ISO. Imagen adaptada de Torlak, M. (s.f.) [Imagen]. Obtenida de https://www.utdallas.edu/~torlak/courses/ee4367/lectures/packet.pdf

Mejores prácticas en TI y normativas aplicables

En las TI como en cualquier disciplina, existen conjuntos de mejores prácticas, ya sea para el diseño de una solución como para la gestión de sus productos y servicios. Para este proyecto se utilizaron conceptos, consejos y orientaciones de versiones –hoy ya prescritas y reemplazadas por nuevas ediciones- de COBIT e ITIL, las cuales han cambiado con el paso de los años hasta evolucionar a las versiones que actualmente rigen la gestión de los recursos y servicios de TI.

Desde el punto de vista del proyecto, las mejores prácticas sirvieron como punto de referencia en el momento de diseñar la solución o alguna de sus partes, de manera que el producto final tuviese el balance adecuado entre lo "recomendado" por estos conjuntos y la viabilidad de su aplicación dentro de la empresa, de manera que su cumplimiento o seguimiento no se volviese más un obstáculo que una solución.

La utilización de la normativa aplicable es necesaria básicamente para garantizar que la solución y los servicios proveídos sean seguros, confiables y de buena calidad. El uso de normas y estándares ayuda a reducir costos al disminuir los desperdicios y reducir los errores, de manera que los materiales, productos, procesos y servicios propuestos cumplan con su propósito. Por otro lado, al seguir estándares, la administración de la plataforma se facilita y permite que un tercero comprenda su lógica de forma más sencilla cuando se requiere su intervención. Adicionalmente, una plataforma de TI basada en el seguimiento de normas, aumenta la percepción de confiabilidad en el usuario, facilitando la introducción de cambios, ya sea en la plataforma en sí como en alguno de sus servicios o aplicaciones.

Marcos de trabajo, investigación y gestión de proyectos

El método PS&DM es conformado por una serie de técnicas sistemáticas que guían el pensamiento crítico de forma que se maximice la experiencia y se utilice la información de manera efectiva; esta metodología es de uso común para situaciones en las que la elección entre dos o más alternativas resulte crítico. Su marco de trabajo aborda el análisis de problemas partiendo de una evaluación de la situación para, posteriormente realizar el análisis del problema, el análisis de decisiones y, finalmente, la identificación de problemas potenciales y el análisis de oportunidades (Kepner-Tregoe, s.f.). Durante el desarrollo del proyecto se utilizó esta metodología de manera continua, algunas ocasiones de manera superficial y en otras de manera detallada, dependiendo de la criticidad del escenario a analizar.

El método de mejora continua basado en el Ciclo de Deming/Shewhart (ver figura 2) permite el análisis de los procesos, de manera que se pueda identificar el origen de alguna variación que cause la desviación en las especificaciones de los servicios o de la plataforma que se hayan planeado y propuesto. Por tal motivo, una buena parte de las actividades del desarrollo del proyecto fueron sometidas a un ciclo de retroalimentación continuo para fin de poder identificar estas posibles desviaciones y corregirlas proactivamente.

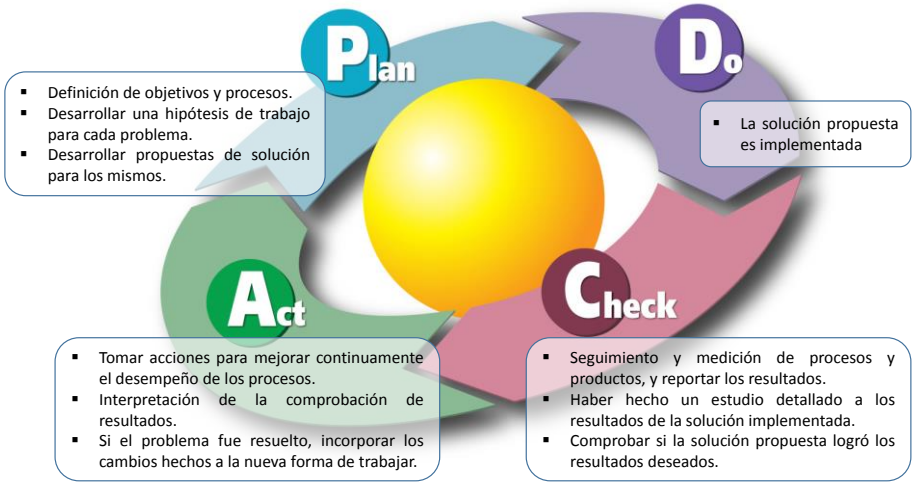


Figura 2. Ciclo de Deming/Shewhart o P-D-C-A. Imagen adaptada de Bulsuk, K. (2009) [Imagen]. Obtenida de http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html

Además de proveer y promover un vocabulario común para la administración de proyectos que facilite el uso y aplicación de sus conceptos, el propósito del PMBOK es delinear una serie de conocimientos y prácticas que pueden aplicarse la mayoría de las veces a la mayoría de los proyectos, de manera que existe consenso sobre su valor y utilidad, todo esto organizado en nueve áreas de conocimiento (ver figura 3 en la siguiente página). De igual forma, define a una buena práctica como el acuerdo en general de que la aplicación de determinados conocimiento, habilidades, herramientas y técnicas pueden aumentar las oportunidades de éxito en muchos proyectos (PMBOK Guide, Fifth Edition, 2013).

De acuerdo con el PMBOK, una buena práctica no significa que el conocimiento descrito deba siempre ser aplicado uniformemente a todos los proyectos; la organización y/o el equipo de administración de proyectos será responsable de determinar qué es apropiado para cada proyecto en cuestión, razón por la cual este marco de trabajo fue aplicado de manera no estricta al desarrollo del presente proyecto.

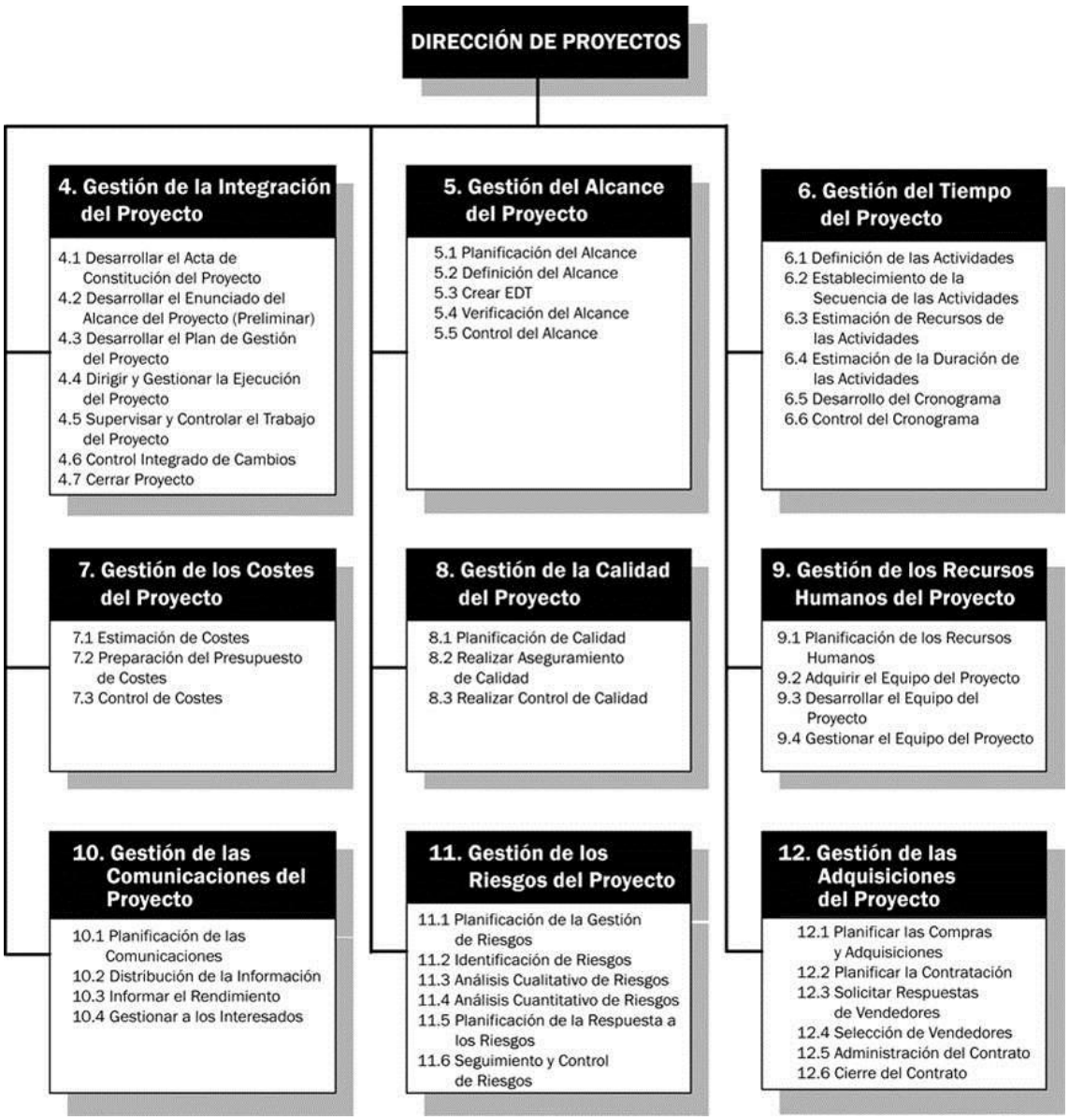


Figura 3. Resumen de las áreas del conocimiento y procesos de la gestión de proyectos. Imagen adaptada de la Guía PMBOK, *Third Edition*, 2004, p.11 [Imagen].

Durante la realización del proyecto reportado, se utilizó como referencia la tercera edición de la Guía PMBOK, la cual solamente incluye 9 áreas de conocimiento, posteriormente, en su quinta edición, la guía añadió un área más, la de Gestión de las partes interesadas. A continuación, son explicadas someramente las 9 áreas originales de la guía.

Gestión de la integración del proyecto. Esta área incluye los procesos y las actividades necesarias para identificar, definir, combinar, unificar y coordinar los diferentes procesos y actividades dentro de los grupos de procesos de la gestión del proyecto.

Gestión del alcance del proyecto. Esta área incluye los procesos requeridos para asegurar que el proyecto incluye todo el trabajo requerido –y solamente el requerido- para concluir el proyecto de manera exitosa.

Gestión del tiempo del proyecto. Esta área incluye los procesos requeridos para el cumplimiento oportuno – a tiempo- del proyecto.

Gestión de los costes del proyecto. En esta área se realizan estimados, presupuestos y control de costos, de manera que el proyecto pueda ser concluido dentro del presupuesto aprobado.

Gestión de la calidad del proyecto. Esta área incluye los procesos y actividades -de la organización que realiza el proyecto- que determinan las políticas de calidad, objetivos, y responsabilidades, de manera que el proyecto satisfaga las necesidades por las cuales es llevado a cabo.

Gestión de los recursos humanos del proyecto. Esta área incluye los procesos que organizan, gestionan, y dirigen al equipo que realiza el proyecto.

Gestión de las comunicaciones del proyecto. Esta área incluye los procesos requeridos para generar, recabar, distribuir, almacenar, recuperar, y dar destino final de manera oportuna y apropiada a la información concerniente al proyecto.

Gestión de los riesgos del proyecto. Esta área incluye los procesos de realización de gestión de riesgos, ya sea en su planeación, identificación, análisis, plan de respuesta, monitoreo y control durante la realización de un proyecto. Los objetivos de la gestión de los riesgos de un proyecto son el aumentar la probabilidad y el impacto de eventos positivos, y –en contraparte- reducir la probabilidad e impacto de eventos negativos en el proyecto.

Gestión de las adquisiciones del proyecto. Esta área incluye los procesos necesarios para comprar o adquirir productos, servicios, o resultados requeridos de manera externa al equipo del proyecto. La organización puede ser ya sea el comprador o el vendedor de los productos, servicios o resultados de un proyecto.

Cabe señalar, que el marco de trabajo PMBOK –como muchos otros marcos de trabajo para la gestión de proyectos- sigue el mismo enfoque que el ciclo P-D-C-A de Deming/Shewhart; sin embargo, el valor agregado del marco PMBOK es que la herramienta permite, a través de sus nueve áreas de conocimiento, una gestión más controlada de un proyecto en particular, ya que cada una de ellas incluye conjuntos de procesos que pueden ser agrupados en una de las cinco clasificaciones posibles: Inicio, Planeación (o Planificación en algunas referencias bibliográficas), Ejecución, Monitoreo y Control, y Cierre.

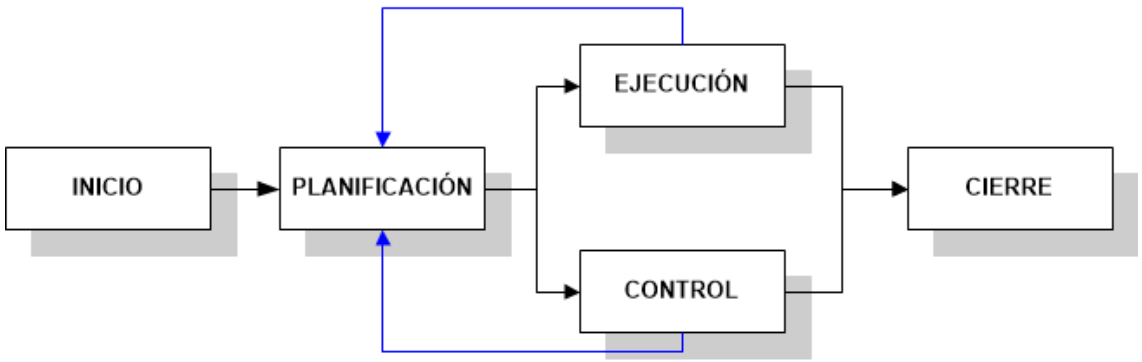


Figura 4. Grupos de procesos para la gestión de proyectos según la Guía PMBOK. Imagen adaptada de Iglesias, M. (2013) [Imagen]. Cambios introducidos en el PMBOK 5ª Edición. Obtenida de http://www.bpmsat.com/cambios-introducidos-en-el-pmbok-5a-edicion/

La figura 4 muestra la forma como esos grupos de procesos interactúan a lo largo de la realización de un proyecto. Estos grupos de procesos corresponden a las tres etapas de desarrollo del proyecto, Inicio, Intermedio y Final. De esta manera, cada grupo de procesos dentro de un área en particular, se aglutina en una de esas clasificaciones.

Para ejemplificar lo anterior, desglosaremos el Área de Conocimiento 4 (Gestión de la Integración del Proyecto) del marco PMBOK. Siguiendo la agrupación de procesos de acuerdo a la fase de realización del proyecto a la que corresponden, tendríamos como resultado la tabla mostrada a continuación.

4. Gestión de la Integración del Proyecto					
Fases del Proyecto	**Fase de Inicio**	**Fase Intermedia**			**Fase Final**
Grupos de Procesos	**Grupo de procesos de Inicio**	**Grupo de procesos de Planeación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y Control**	**Grupo de procesos de Cierre**
	4.1 Desarrollar el acta de constitución del proyecto. 4.2 Desarrollar el enunciado preliminar del alcance del proyecto.	4.3 Desarrollar el plan de gestión del proyecto.	4.4 Dirigir y gestionar la ejecución del proyecto.	4.5 Supervisar y controlar el trabajo del proyecto. 4.6 Control integrado de cambios.	4.7 Cerrar el proyecto.

Tabla 1. Mapeo de los procesos de gestión de proyectos con los grupos de procesos y áreas del conocimiento de la gestión de proyectos. Imagen adaptada y resumida de la Guía PMBOK, *Third Edition*, 2004, p.70 [Imagen].

Gracias a este desglose, es posible identificar, para cada una de las áreas de conocimiento, a cuál etapa del proyecto pertenece cada uno de los procesos (o grupos de procesos) que estemos trabajando. Esto nos permite visualizar la transición de una etapa a otra, ya que esto sucede generalmente cuando se cumplen ciertas actividades o cuando se completan “entregables”, y es comúnmente secuencial, aunque esto –como veremos más delante- no siempre ocurre en la práctica. El mapeo de grupos de procesos para el total de las áreas del conocimiento de la Guía PMBOK se muestra en el apartado de Anexos.

En el caso del proyecto reportado, la aplicación de este marco de trabajo no fue rigurosa, sino que se aprovechó su estructura para definir actividades y monitorear su cumplimiento durante las etapas de desarrollo del mismo, principalmente aquellas relacionadas con la planeación. Todo esto ayudó en buena medida a evitar fallas en la realización del proyecto y contribuyó, definitivamente, a su entrega exitosa.

Esto último cobra importancia dado que el éxito de un proyecto comúnmente se mide en su cumplimiento dentro de las restricciones de alcance, tiempo, costo, calidad, recursos y riesgos aprobadas por el administrador del proyecto y la dirección general. No obstante, en el caso del proyecto reportado, se trataba de un proyecto para el cual no existía referencia respecto a esos criterios, ya que, al tratarse de una nueva empresa, se partió del establecimiento de las necesidades y conforme se fueron proponiendo alternativas para cubrirlas, se fueron definiendo actividades, costos, responsables y tiempos asociados. Siendo así, se puede decir que se trabajó de manera anticipada en los factores de riesgo para cada etapa, de manera que cuando alguna actividad (proceso) quedaba definida, ésta ya había sido diseñada o planeada a “prueba de fallas”, garantizando en cierta medida su acierto.

Habiendo explicado brevemente el marco de trabajo para la administración de proyectos, ahora procedo a detallar la manera en la que fueron abordadas las diferentes áreas del conocimiento de dicho modelo.

Con la finalidad de poder reducir el tiempo de ejecución del proyecto, y con la intención adicional de poder reducir su costo de realización, se procedió a trabajar en las diferentes áreas del conocimiento de manera paralela o sobrepuesta, el llamado *Fast Tracking*. Se tomó el área correspondiente a la Gestión del Tiempo del Proyecto (PMBOK 6) como núcleo, y el resto de las áreas como auxiliares para el cumplimiento de las actividades que fuesen siendo definidas en dicho núcleo, de ahí que una buena cantidad de actividades de diferentes áreas fuesen realizadas simultáneamente.

En el inicio del proyecto se abordaron de manera conjunta, varios grupos de procesos de las áreas de Gestión de la integración del proyecto (PMBOK 4), de Gestión del alcance del proyecto (PMBOK 5), y de Gestión de las comunicaciones del proyecto (PMBOK 10).

La primera actividad realizada fue la definición de roles y responsabilidades (PMBOK 10.4) de acuerdo a la siguiente relación:

- **Gerente del proyecto**. Este rol fue cubierto por mi persona, ya que, debido a la naturaleza del proyecto, éste resultaba ser competencia del área de las Tecnologías de la Información, área de la cual yo era gerente para la planta local de manufactura.
- **Patrocinador (Padrino) del proyecto**. En este caso, el director general de la compañía a nivel local representaba el nivel más alto de responsabilidad en la correcta realización del proyecto.
- **Gerentes funcionales**. Dado que la compañía iniciaba operaciones localmente, el grupo de gerentes funcionales se reducía a tres; uno para las áreas de producción e ingeniería, otro para las áreas de gestión de materiales (tanto de insumos como de producto terminado) y control de la calidad, y un tercero para las áreas de recursos humanos y contabilidad.

Una vez definidos estos roles, se procedió a integrar el proyecto en sí. Al tratarse de una organización con un número reducido de empleados, el arranque del proyecto se dio de manera informal, partimos de una reunión inicial (*kickoff*), en la cual se comenzó con el desarrollo del enunciado del alcance del proyecto (PMBOK 4.2), así como con la planificación tentativa del alcance del proyecto (PMBOK5.1).

Aun cuando no se realizó formalmente una carta del proyecto, se contó con el respaldo irrestricto por parte del patrocinador del proyecto para el cumplimiento en tiempo y forma de las actividades que se llegasen a definir de manera conjunta entre el gerente del proyecto y los gerentes funcionales.

El patrocinador empoderó adecuadamente al gerente del proyecto, para que éste tuviese el nivel de autoridad suficiente como para requerir a los otros involucrados el acatamiento de acuerdos y para poder hacerse de los recursos necesarios para la realización oportuna de las actividades definidas.

A diferencia de otras empresas, en las cuales existen cotos de poder, en BDT no fue necesario evaluar a las demás partes involucradas para determinar su nivel de influencia y cómo éste pudiese afectar negativamente el desarrollo del proyecto. Esto se debió principalmente a que se trataba de una empresa de reciente apertura, cuyo número de personal era bajo, y a que el peso de cada uno de los gerentes dentro de la organización era relativamente similar, por lo que no se corría el riesgo de tomar decisiones y que éstas fuesen revocadas por influencia de alguno de los involucrados.

A lo anteriormente señalado, es necesario añadir que el apoyo al desarrollo del proyecto por parte de las esferas más altas de la estructura organizacional, orillaba a una alineación incondicional por parte de todos los involucrados. En lo personal, identifico este aspecto como un factor determinante de éxito, debido principalmente a que el padrino del proyecto asumió su rol en toda la extensión de la palabra, creando las condiciones necesarias para que el proyecto avanzase en tiempo y en forma.

Como parte de esas condiciones favorables, puedo resaltar la dedicación de su tiempo para revisar los detalles del proyecto, entre ellos, el control y ajuste presupuestal, la obtención de fondos y autorizaciones de niveles organizacionales más elevados que el suyo, la utilización de su nivel de autoridad para alinear al resto del equipo en las pocas situaciones donde fue requerido y apoyarme en las decisiones técnico-tecnológicas que hubiese tomado y que se prestasen a discusión o duda por parte del resto de los involucrados. Estimo que esto pudo deberse a que él compró la idea del proyecto desde su conceptualización y jugó de manera honesta el papel que le correspondía.

Ahora bien, el primer reto en el desarrollo del proyecto es la definición de requerimientos. Aunque ya se contaba con una idea somera sobre lo que se esperaba como producto final, y que sirvió de base para establecer el enunciado del alcance del proyecto, ahora era momento de detallar las características de ese producto final basándose en las necesidades operativas de cada área funcional. Para tal efecto, hicimos uso de dos métodos para la obtención y definición de los requerimientos: **entrevistas** y **talleres dirigidos**.

Las **entrevistas** consistieron en sesiones individuales con las diferentes partes interesadas, comenzando con los gerentes funcionales y continuando con el personal a su cargo que fuese responsable de procesos que pudiesen ser afectados por el desarrollo del proyecto.

Los **talleres dirigidos** consistían en reuniones con las diferentes partes interesadas, o sus representantes, con la finalidad de contar con una visión general de la manera como se verían afectadas las diferentes áreas durante el desarrollo del proyecto. De esta manera se logran dos objetivos: contar con las necesidades de cada área, y una comprensión homogénea del proyecto.

Ambas técnicas de obtención de requerimientos se aplicaron tanto con personal local, como con personal ubicado en el corporativo; este último, por su experiencia en la empresa aportaba una buena cantidad de información pertinente para la captación de necesidades a cubrir con el proyecto en curso y que posteriormente fue de mucha utilidad en la etapa de Gestión de los Riesgos del Proyecto.

El proyecto reportado formaba parte de un proyecto aún mayor, el de transferir de manera exitosa la producción de determinados productos de la planta de manufactura ubicada en Alemania a la naciente planta en Guadalajara. Como tal, la mayor parte del seguimiento al cumplimiento del proyecto se llevaba a cabo por medio de un documento llamado *Issue Tracker*, en el que se reflejaban actividades, fechas compromiso, responsables y resultados entre otros aspectos.

De manera paralela, también se abordó la gestión de los riesgos del proyecto (PMBOK 11); en el caso del proyecto reportado, básicamente recurrimos a los análisis cuantitativo y cualitativo. Existen varias opiniones respecto a cuál es el mejor momento en el que se debe hacer un análisis de riesgos, cuando hay metas específicas que deban cumplirse, cuando sobreviene un nuevo desarrollo no esperado dentro de un proyecto, o en los puntos de cambio en el ciclo de vida de un proyecto; sin embargo, el mejor momento de hacer un análisis de riesgos es justo cuando existe incertidumbre para la realización de alguna actividad o la toma de decisiones durante el desarrollo del proyecto, de manera que dé lugar a un riesgo significativo. Pudiera ser que no se cuente con información relevante suficiente como para realizar un análisis cuantitativo; no obstante, este tipo de escenario no es razón como para que un análisis cualitativo no sea realizado.

En el caso del proyecto reportado, la gestión de los riesgos se fue trabajando conforme se establecían actividades, ya que de inmediato valorábamos la viabilidad de las mismas, es por esto que no era de extrañarse que terminásemos reuniones de definición de actividades en las cuales también hubiésemos identificado los riesgos, planeado nuestra respuesta a los mismos, y definido nuestra estrategia para su seguimiento y control. Dado que el número de personal involucrado era reducido y apremiaba el tiempo límite de implementación del proyecto, el análisis de riesgos se realizó mayormente sobre grupos afines de actividades y no sobre actividades individuales.

Cabe señalar que para algunos grupos de actividades se realizaron los análisis, tanto cuantitativo como cualitativo; el primer paso para realizarlos fue la identificación de los riesgos, lo cual es considerado por algunos como el elemento más importante del proceso, ya que una vez que un riesgo ha sido identificado, es posible hacer algo al respecto.

La figura 5 muestra los pasos a seguir bajo un planteamiento sistemático de gestión de riesgos, en el cual partimos precisamente de haber definido la actividad o grupo de actividades (PMBOK 6.1 y 6.2) para posteriormente poder identificar las amenazas.

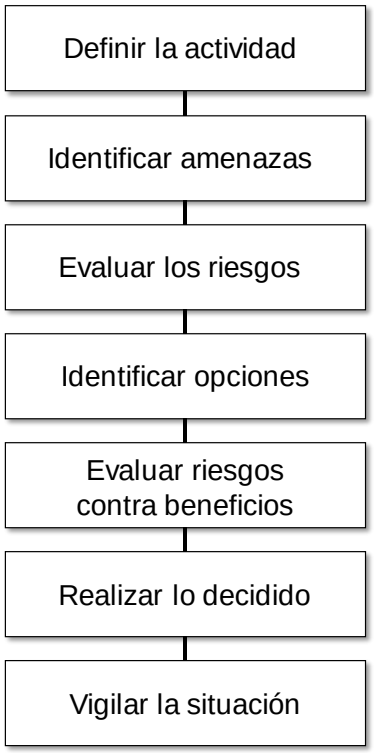


Figura 5. Pasos de la gestión de riesgos. Imagen adaptada de United States Coast Guard (2004) [Imagen]. Team Coordination Training Guide 8/98. Obtenida de https://www.uscg.mil/auxiliary/training/tct/chap3.pdf

Por medio de entrevistas, talleres dirigidos y reuniones de lluvia de ideas, fue posible identificar las amenazas y evaluar los riesgos para poder categorizarlos, tanto por su probabilidad de ocurrencia como por su nivel de impacto al proyecto en caso de que algún riesgo se llegase a materializar.

Ahora bien, para cubrir los análisis cualitativo y cuantitativo de los riesgos, nos guiamos por la norma British Standard EN 61508-5:2010[4]. Esta, introduce el concepto de ALARP, acrónimo de *As Low As Reasonably Practicable*; es decir, "tan bajo como sea razonablemente viable". En su sección dedicada al modelo ALARP, se indica que, al regular riesgos propios de alguna actividad, se debe determinar:

A. Que el riesgo sea tan grande que deba ser rechazado completamente.
B. Que el riesgo es, o se ha hecho, tan pequeño que se considera insignificante; o
C. Que el riesgo cae dentro de los dos puntos anteriores y ha sido reducido al nivel más bajo posible, teniendo en mente los beneficios resultantes de su aceptación y teniendo en cuenta los costos de cualquier reducción futura.

La misma norma define tres zonas en las cuales puede catalogarse un riesgo específico, estas zonas son explicadas en la figura 6. Arriba de cierto nivel, un riesgo es considerado como no tolerable y no puede ser justificado bajo cualquier circunstancia normal.

Debajo de ese nivel, existe la región de tolerabilidad, donde se permite que una actividad tenga lugar provista de sus riesgos asociados y éstos hayan sido reducidos tanto como sea razonablemente factible. En este punto, tolerable no significa lo mismo que aceptable; aquí indica un deseo por vivir con un riesgo de manera que nos garantice ciertos beneficios y, al mismo tiempo, esperar que dicho riesgo se mantenga bajo revisión y sea reducido, a sabiendas de cuándo ocurrirá eso. Aquí se requiere una valoración costo-beneficio, ya sea explícita o implícitamente, para sopesar el costo y la necesidad de medidas adicionales de seguridad.

[4] *British Standard* (BS) norma 6158. Es la implementación del Reino Unido de la norma IEC del mismo número, la cual delinea la seguridad funcional básica aplicable a todo tipo de industria. En su parte 5, se define la seguridad como parte de la seguridad total relacionada con equipamiento bajo control que dependan del funcionamiento correcto de sistemas Eléctricos/Electrónicos/Electrónicos Programables, de otros sistemas relacionados con la tecnología, así como la reducción de riesgos externos en los centros de operación.

Mientras más alto sea el riesgo, el gasto ejercido para reducirlo será proporcionalmente más alto. En el límite de la tolerabilidad, los gastos desproporcionados en búsqueda del beneficio, serán justificados. El riesgo será, por definición, substancial, y un esfuerzo considerable será justificado aun cuando se obtenga una reducción marginal.

Cuando los riesgos son menos significativos, se necesita proporcionalmente menos gasto para reducirlos, y se encontrarán en la parte más baja de la región de tolerabilidad, y bastará hacer un balance entre costos y beneficios.

Debajo de la región de tolerabilidad se encuentra la región ampliamente aceptable, donde los riesgos son pequeños en comparación con los riesgos que todos experimentamos diariamente. Aun cuando en la región ampliamente aceptable no hay necesidad de hacer un trabajo detallado para demostrar ALARP, es necesario, de cualquier forma, permanecer atento de que el riesgo se mantenga en ese nivel.

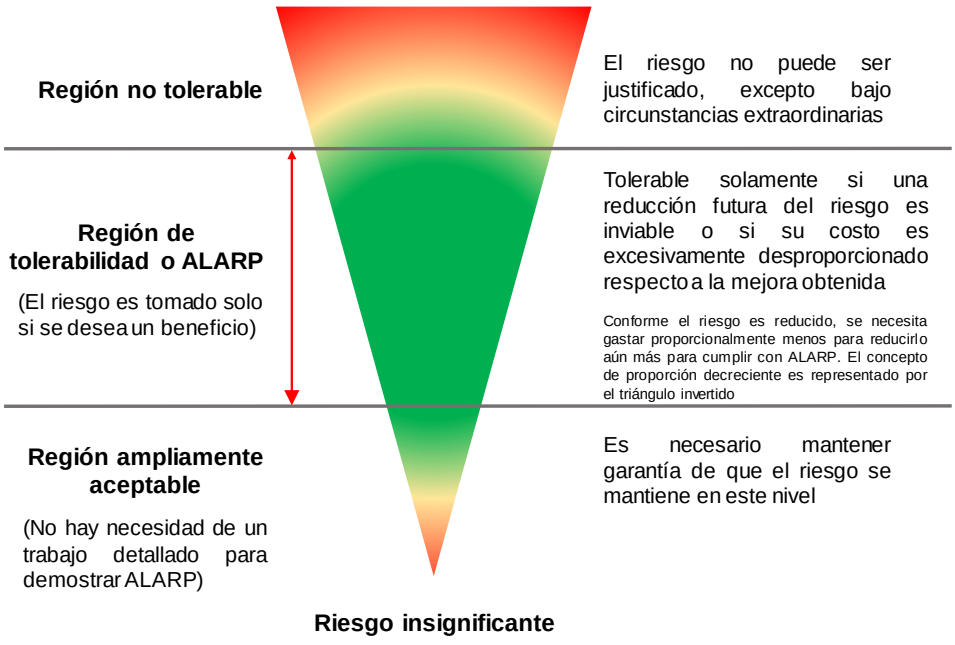


Figura 6. Riesgos tolerables en el modelo ALARP. Imagen adaptada de la norma BS EN 61508-5:2010 (2010) [Imagen]. Functional safety of electrical/electronic/programmable electronic safety related systems. Part 5: Examples of methods for determination of safety integrity levels.

El modelo ALARP considera que un riesgo tolerable puede ser obtenido a partir de un número de consecuencias a determinar y de las frecuencias de ocurrencia asociadas a él. Esta correspondencia entre consecuencias y frecuencias de ocurrencia tolerables puede obtenerse a partir de discusiones y acuerdos entre las partes interesadas. Este modelo propone que para realizar esta correspondencia se utilicen cuatro clases: I, II, III, y IV (descritas en la tabla 3) para seis tipos de frecuencia de ocurrencia, lo cual se muestra en la tabla 2.

Frecuencia	**Consecuencias**			
	Catastróficas	**Críticas**	**Marginales**	**Despreciables**
Frecuente	I	I	I	II
Probable	I	I	II	III
Ocasional	I	II	III	III
Remota	II	III	III	IV
Improbable	III	III	IV	IV
Increíble	IV	IV	IV	IV
Nota: la información vertida en la tabla es para fines de ejemplificación, y no implica que forzosamente las clases de riesgos se distribuyan de esa manera.				

Tabla 2. Ejemplo de clasificación de riesgos. Tabla adaptada de: BS EN 61508-5:2010 (2010). Functional safety of electrical/electronic/programmable electronic safety related systems. Part 5: Examples of methods for determination of safety integrity levels.

Ahora bien, para el ejemplo de la tabla 2, el modelo ALARP nos propone la siguiente interpretación de clases de riesgos.

Clase de riesgo	Interpretación
Clase I	Riesgo no tolerable
Clase II	Riesgo no deseado, y tolerable solo si la reducción del riesgo es irrealizable o si los costos de reducción son excesivamente desproporcionados en comparación con la mejora obtenida
Clase III	Riesgo tolerable si el costo de la reducción del riesgo rebasa la mejora obtenida
Clase IV	Riesgo despreciable o insignificante

Tabla 3. Interpretación de las clases de riesgos. Tabla adaptada de: BS EN 61508-5:2010 (2010). Functional safety of electrical/electronic/programmable electronic safety related systems. Part 5: Examples of methods for determination of safety integrity levels.

Según la tabla 2, los riesgos dentro de esas definiciones de clases de riesgo son los riesgos que están presentes cuando se han tomado medidas de reducción de riesgos. Con respecto a la tabla 3, las clases de riesgo definidas son:

- Riesgos Clase I se encuentran en la región no tolerable
- Riesgos Clase II y III están en la región ALARP, estando los de clase II apenas dentro de esta región
- Riesgos Clase IV están en la región ampliamente aceptable

La norma enfatiza que estas tablas y clasificación son meramente ejemplos y que para situación específica o tipo de industrias se deben de llenar tablas similares con valores que dependerán de un amplio rango de factores inherentes al sector al que pertenezca la empresa que realiza el análisis de riesgos.

Para la realización del proyecto reportado, se identificaron los siguientes riesgos y se estableció la relación entre sus posibles frecuencias de ocurrencia y las consecuencias de presentarse esos riesgos.

Frecuencia	Consecuencias			
	Catastróficas	**Críticas**	**Marginales**	**Despreciables**
Frecuente	I	I	Indisponibilidad del BDC	Pérdida de información no almacenada en la red
Probable	Falla de energía eléctrica por largo tiempo	Falla de algún equipo activo de red (switch)	Pérdida de información almacenada en la red	Indisponibilidad de varios equipos dentro del área local
Ocasional	Indisponibilidad del PDC	Pérdida de conectividad entre manufactura/almacén y el sistema MES	Pérdida de conectividad entre el almacén y el sistema ERP	Indisponibilidad del servicio WiFi
Remota	No realización de los respaldos de información	Pérdida de conectividad entre LAN y WAN	Pérdida de la conectividad dentro del área local	Represalia por parte de exempleados inconformes
Improbable	Pérdida de información del sistema ERP	Infección de virus informático o algún tipo de malware	Indisponibilidad del acceso a Internet	Ausencia o falta del administrador de los servicios
Increíble	Indisponibilidad de la totalidad de los servicios de la plataforma	Pérdida de información del sistema MES	Pérdida de información del correo electrónico	IV

Tabla 4. Clasificación de riesgos para el proyecto reportado. Tabla adaptada de: BS EN 61508-5:2010 (2010). Functional safety of electrical/electronic/programmable electronic safety related systems. Part 5: Examples of methods for determination of safety integrity levels.

De acuerdo con esta tabla, se puede observar que detectamos un total de 21 riesgos divididos entre las diferentes categorías. No fue posible detectar riesgos que tuviesen una posible ocurrencia catalogada como frecuente o probable y que a la vez sus consecuencias fuesen catastróficas o críticas; de igual manera, tampoco fue posible detectar riesgos insignificantes cuya ocurrencia pudiese ser clasificada como increíble.

Los riesgos identificados para el proyecto, han sido remarcados en la tabla 4 para facilitar su ubicación. Estos riesgos fueron identificados, abordados y reducidos a la par de la realización de las actividades a las cuales podrían haber afectado; razón por la cual, al presentar la propuesta, se estaban presentando también las medidas de contingencia para aminorar o eliminar la posibilidad de ocurrencia de sus riesgos asociados.

Teoría relacionada con la investigación documental

Áreas de conocimiento relevantes para el desarrollo del estudio de caso

- Investigación documental
- Métodos de investigación
- Administración de proyectos

Conceptos y términos clave

- Investigación cualitativa
- Fuentes de información
- Documentación
- Análisis de la información
- Estudio de caso

Técnicas y métodos de investigación y documentación aplicables al caso

Dada la naturaleza de la información que será utilizada para el desarrollo del estudio del caso, se consideró que el método de investigación cualitativa es el que podía ofrecer el enfoque más adecuado, ya que dicha técnica es comúnmente utilizada con el propósito de describir y comprender algún evento desde el punto de vista del participante, lo que precisamente es el objetivo principal de este estudio de caso.

Algunos puntos muy importantes a considerar para haber seleccionado esta técnica son: primero; la forma de razonamiento utilizada en el análisis tendría que ser de tipo inductivo, segundo; las conclusiones serán comunicadas por medio de narrativa, haciendo uso de citas personales, y tercero; el propósito de la investigación será el de describir, explicar e interpretar un evento y sus escenarios y relativamente construir una teoría, no para probar una ya existente.

1.2 Discusión sobre el sustento

Por lo general en este tipo de reportes, se realiza un apartado específico para la discusión sobre el sustento teórico del proyecto reportado. Sin embargo, en este reporte en particular, he optado por integrar el sustento teórico a lo largo de la redacción del documento; esto se debe principalmente a que se aborda la temática bajo múltiples enfoques teóricos, con lo que resulta mucho más sencilla la lectura del texto al redactarse el sustento teórico a la par de su ejecución real dentro del proyecto reportado, y no de manera separada.

De cualquier forma, no sobra mencionar que el proyecto fue abordado haciendo uso de diferentes herramientas de gestión, tales como la guía PMBOK para la administración de proyectos, las matrices QSPM de la planeación estratégica y el método PS&DM de Kepner-Tregoe, utilizados en la toma de decisiones, así como el cotejo contra normas internacionales en los diferentes aspectos del proyecto reportado, con lo cual se evidenció que un proyecto gestionado bajo métodos formales, tiene una mayor probabilidad de éxito que aquellos realizados sin el soporte de un marco teórico o de trabajo.

CAPÍTULO 2. DESCRIPCIÓN DEL PROYECTO REPORTADO

2.1 Antecedentes del proyecto reportado

A mediados de 1999 fui contratado por la compañía BDT de México para desempeñar las funciones de la gerencia de las Tecnologías de la Información, teniendo como primer proyecto de gran alcance, el diseño y la implementación de la plataforma tecnológica que permitiera la adecuada gestión de la compañía a nivel local.

2.1.1 Descripción de la organización y de sus actividades

BDT de México pertenece al grupo de BDT AG, cuyo corporativo se ubica en el poblado de Rottweil, en el suroeste de Alemania. En la época de la realización del proyector reportado, la compañía empleaba a más de 500 personas y contaba –además de la recién creada planta de manufactura en México- con puntos de manufactura en Alemania y oficinas comerciales y de reparación en Irvine, California en los Estados Unidos.

Posteriormente la compañía amplió sus operaciones a nivel mundial, estableciendo una planta de manufactura para sub-ensambles en la región de libre comercio (FTZ: *Free Trade Zone* por sus siglas en inglés, más usual en la literatura de negocios) de Zhuhai en la República Popular China, cuya operación también requirió de ser integrada a la plataforma tecnológica existente en el grupo.

BDT (*Büro und Datentechnik*) fue fundada en Rottweil, Alemania a inicios de la década de los sesenta. Esta empresa se ha hecho acreedora de una buena reputación al desarrollar y manufacturar innovadores dispositivos manejadores de papel para compañías líderes en la impresión y el copiado con tecnología láser, así como soluciones de automatización de almacenamiento de datos para organizaciones de tecnología de información en todo el mundo. Desde sus inicios, la compañía ha mantenido la tradición de desarrollar productos novedosos o primicias de mercado, tal como lo muestra la Figura 7 en la página siguiente.

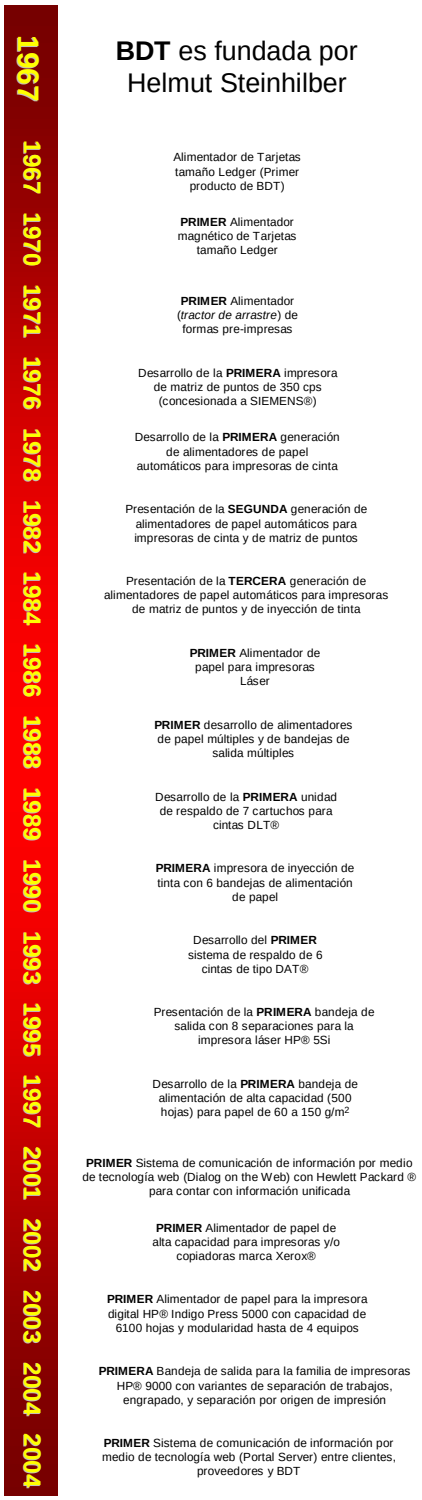


Figura 7. Cronograma de desarrollo o lanzamiento de primicias de productos de BDT.

Las ideas, la creatividad y la sensibilidad caracterizan el enfoque de BDT en el desarrollo de productos, la compañía combina las habilidades de su personal con las más modernas tecnologías para manufacturar productos eficientes que sean amigables con el ambiente a un costo efectivo.

BDT es una compañía comprometida con la calidad y con la mejora continua, razones por las cuales cumple con estándares internacionales tales como ISO 9000[5], y normas técnicas y/o tecnológicas, tales como TÜV[6] y UL[7]. Durante el año 2004, la compañía logró una doble certificación en ISO 14000 y OHSAS[8] 18000 y una re-certificación en ISO 9000:2002, convirtiéndose en una de las pocas compañías a nivel mundial que en esa época ostentaba certificación en las tres normas.

Dado que la mayoría de los productos fabricados por BDT AG tenían como destino final a clientes ubicados en los Estados Unidos o en Asia, la creación de un sitio de manufactura en México resultaba por demás necesaria. Los costos de transporte, tanto de suministros como de producto final se verían reducidos de forma considerable, y el tiempo de respuesta ante requerimientos de parte de los clientes se vería –también- acortado, ya que la mayoría de los clientes cuentan con corporativos u oficinas en los Estados Unidos, con lo que el tiempo disponible para la atención de los mismos sería mayor que de continuar siendo atendidos desde Alemania, ya que por la diferencia de zonas horarias, las horas de atención eran a lo sumo cuatro.

[5] *International Organization for Standarization* (ISO) es una organización no gubernamental conformada por una red de institutos de estandarización ubicados en 146 países con un secretariado central en Ginebra, Suiza que coordina el sistema. Sus normas se han vuelto referencia internacional de requerimientos de calidad en los negocios (ISO 9000) y del manejo ambiental de los mismos (ISO 14000). http://www.iso.org

[6] *Technischer Überwachungs Verein* (TÜV Rheinland) es una compañía de servicio internacional dedicada a la documentación y certificación de la seguridad y calidad de productos, servicios y sistemas existentes, nuevos o en desarrollo. http://www.de.tuv.com/de/index.php

[7] *Underwriters Laboratories* (UL) es una organización independiente, no lucrativa dedicada a probar y certificar la seguridad de los productos nuevos (principalmente eléctricos). http://www.ul.com

[8] *Occupational Health and Safety Assessment Series* (OHSAS) es un conjunto de especificaciones de origen británico, para ser utilizadas en un sistema de administración de seguridad y salud ocupacional.

BDT se encuentra constantemente desarrollando nuevas tecnologías para cumplir con los cambios en los requerimientos y con los calendarios de lanzamientos críticos de parte de sus clientes; de igual forma, hace uso de herramientas de gestión y marcos de trabajo vanguardistas que le permiten mantener una adecuada competitividad en un mercado siempre cambiante. Siendo consistente con ese compromiso, a inicios del 2009, la compañía utilizó la herramienta de medición de desempeño estratégico *Balanced Scorecard*[9] (BSC) para revisar y discutir la vigencia de su visión y misión; tras esta evaluación, surgieron los nuevos objetivos estratégicos y operativos de la organización, lanzando posteriormente una campaña interna para crear esta conciencia de los mismos entre sus empleados por medio de la publicación periódica interna *Das BEDETE Journal*, bajo la declaración mostrada en la figura 8.

Figura 8. Visión de la compañía, actualizada al año 2009. Imagen adaptada de: Glunk M. (Número 13, agosto 2009) [Imagen]. Visionen realisierbar machen. Das BEDETE Journal, p.1.

[9] *Balanced Scorecard* (BSC) es una herramienta de la planeación estratégica desarrollada por Robert S. Kaplan y David Norton en 1992, la cual permite cuantificar las actividades de una compañía en términos de su visión y estrategias.

Debido a que diseña lo que produce, BDT se enorgullece en ofrecer uno de los tiempos más cortos dentro de la industria entre el inicio del proyecto, desarrollo del producto y el primer embarque del mismo. Lo anterior es crítico si se considera que la unidad de negocios de almacenamiento en cinta de BDT cuenta con una gran cantidad de clientes de renombre, tales como HP, IBM, Quantum, Iomega, ADIC, Tandberg, Certance, SUN (actualmente ORACLE), entre otros, a quienes les desarrolla o fabrica equipos robotizados de manejo de cintas con un amplio rango de tecnologías, desde la antigua DLT y su posterior reemplazo, la SDLT, hasta las LTO1/2/3/4 (actuales en la época de realización del proyecto reportado); así como las DDS3/4 y DAT7210, todas ellas manufacturadas en altos volúmenes. Una descripción sobre las tecnologías de almacenamiento de datos en cinta se incluye en el apartado de Anexos al final del presente documento.

Uno de los objetivos de la compañía es el de mantener y promover la innovación, para BDT la innovación no está limitada a la investigación y al diseño, la innovación también incluye el uso de las más modernas tecnologías, materiales y métodos. En el trabajo diario, BDT fomenta entre sus empleados el ideal de contribuir de forma activa con mejoras que agreguen valor a los productos o servicios de la compañía. Para tal efecto, los empleados suelen presentar propuestas, ideas o mejoras durante las reuniones departamentales, por medio de la intranet o de la publicación periódica interna *Das BEDETE Journal*. Este es un proceso que se vive a lo largo de toda la compañía y que resulta evidente con el cambio informal del significado de BDT a ***B****est in* ***D****evelopment and* ***T****echnology*.

Con ingresos de € 78 millones ($ 94 millones de dólares) en el 2003 y con un crecimiento promedio anual del 8 por ciento, BDT había emergido, a inicios de la década del 2000, como un líder en esta industria especializada. Aunado a este crecimiento, la compañía había encontrado algunos retos tecnológicos clave que en definitiva podrían afectar su posición competitiva en el mercado.

[10] Un resumen de las características y funcionamiento de las diferentes tecnologías de almacenamiento de datos en cinta puede ser consultado en el glosario de términos ubicado al final del presente documento.

A pesar de que una de las actividades preponderantes del grupo es el diseño de los productos, la actividad primordial de BDT en México sería la de manufactura de tipo maquiladora; es decir, se importarían suministros y sub-ensambles libres de impuestos, bajo la condición de que los productos fabricados, ensamblados o procesados a partir de ellos, fuesen exportados. Para el cumplimiento de dicha actividad, la operación de BDT de México fue dividida en tres grupos principales de trabajo: Manufactura, Almacén, y Administración, mencionadas en orden de criticidad.

Manufactura

El proceso de manufactura dentro de BDT se basa en el uso de una aplicación MES[11] que permite el control de la mayoría de los procesos de sub-ensamble generando información que brinda la posibilidad de rastrear unidades terminadas en caso de ser necesario. La aplicación también permite el control, tanto del estadístico de procesos, como de la calidad de los materiales y componentes utilizados en la fabricación de los diferentes productos.

Dado que el personal operario ingresa en dicha aplicación el cumplimiento de sus actividades por cada estación de trabajo, una caída de esa aplicación o la interrupción en la comunicación entre los equipos del área de manufactura y el servidor de la aplicación MES representa forzosamente un “paro de línea” que implica –invariablemente- pérdidas monetarias.

Almacén

Esta área hace uso mayormente de la aplicación ERP[12] para responder de forma eficiente a los requerimientos de suministros por parte del área de manufactura, de manera que el ya mencionado “paro de línea” no se llegue a presentar debido –precisamente- a una gestión inadecuada del inventario de materiales.

[11] *Manufacturing Enterprise System* (Sistema Empresarial de Manufactura): Sistema de cómputo que permite el control de los diferentes procesos de manufactura.

[12] *Enterprise Resource Planning* (Planeación de Recursos Empresariales): Sistema de cómputo que permite la planeación de los diferentes recursos dentro de una empresa.

Administración

Dentro de esta categoría se incluye a todo aquel personal que no labora directamente en las dos áreas previamente mencionadas, a pesar de que sus actividades estén directamente relacionadas con las primeras. Dependiendo de sus funciones, las aplicaciones utilizadas por este personal serán, además del MES y el ERP, el correo electrónico, aplicaciones de nóminas y de tipo financiero, así como algunos requerimientos de almacenamiento masivo de información para ser compartida con otras áreas dentro de la compañía.

Una buena cantidad de la información generada por las diferentes áreas, así como toda aquella documentación referente a los variados sistemas de calidad, tendría que ser compartida por medio del portal web de la compañía, el cual se basaba en una implementación de la plataforma SharePoint Portal Server/Services de Microsoft. La mencionada información debería de poder ser compartida por medio de la red de área amplia (WAN por sus siglas en inglés) entre las diferentes ubicaciones de la compañía, pero para compartirla con proveedores y clientes, se utilizaría el portal web mencionado.

Problemática a resolver

Tratándose de un fabricante de diseño original (ODM: *Original Design Manufacturer*), BDT de México necesitaba de una plataforma tecnológica que permitiera el flujo de información entre sus proveedores y clientes para asegurar calidad en los productos y su entrega a tiempo; así como todo proceso de comunicación electrónica entre el personal de las diferentes localidades de la compañía y su capacidad para compartir información relevante para cada área de trabajo. El personal del área de Investigación y Desarrollo, por ejemplo, necesitaba poder colaborar de forma eficiente y precisa con los clientes en el diseño de procesos y cambios de ingeniería. Por otra parte, los proveedores necesitaban contar con visibilidad de los inventarios de partes para evitar paros de producción.

A su vez, los responsables de los nuevos proyectos en suelo mexicano requerían de una creciente comunicación con sus contrapartes en Alemania con la finalidad de poder realizar un proceso de transición de manera controlada que permitiera la liberación de la producción en México en el menor tiempo posible, representando –con esto- ahorros en el costo de transferencia de productos.

Adicionalmente, una vez que la producción de los diferentes productos era designada a la planta mexicana, se presentaba la necesidad de contar con la infraestructura de tecnología que permitiera la debida implementación de las líneas de producción para tal efecto. La planta de manufactura de BDT en México comenzó sus operaciones a mediados del año 2000 pero el edificio que alberga a la compañía estaba disponible desde finales de 1999, por lo que la infraestructura de red de comunicaciones pudo ser diseñada con buena anticipación considerando que la superficie a cubrir sería de 5,000 metros cuadrados, subdivididos físicamente de acuerdo a las funciones de las tres áreas principales de trabajo mencionadas anteriormente.

2.2 Objetivo del proyecto reportado

El objetivo principal del proyecto reportado consistía en proveer a la organización (BDT de México) de una plataforma informático-tecnológica que fuese lo suficientemente robusta y confiable, de manera que fungiese como núcleo o base sobre la cual se pudiese desarrollar o proveer todas las demás aplicaciones y servicios informático-tecnológicos que la compañía llegase a requerir en el mediano y largo plazo. Todo esto en estrecha coordinación con las oficinas corporativas y con aquellos centros que requiriesen acceso a la información o aplicaciones utilizadas localmente, ya fuese para consulta o para modificación de las mismas.

2.2.1 Justificación

Al tratarse de una compañía de clase mundial, perteneciente al ramo tecnológico, el corporativo de BDT había reconocido ya anteriormente el valor de la disponibilidad de la información “en línea” para sus empleados, clientes y socios de negocios. Los empleados necesitaban acceso a información de ventas, mercadotecnia, ingeniería y financiera, entre otras; a su vez, los proveedores y clientes requerían acceso a inventarios, órdenes y planes de producción, de embarque y de entrega.

Dado lo anterior, la integración de la naciente instancia en México, debía alinearse en ese mismo sentido. Quedaba claro, por otra parte, que se enfrentarían condiciones diferentes, tales como una cantidad menor de proveedores locales con acceso a Internet y a herramientas informáticas del mismo nivel que aquellos ubicados en Europa o en los Estados Unidos, por lo que la estrategia informática estaba enfocada a lograr que la empresa localmente tuviese –por un lado- una infraestructura informático-tecnológica de tipo similar a la existente en el corporativo, y por otro, acercar a aquellos proveedores al uso de tecnologías de la información a su mismo nivel con la finalidad de incrementar la productividad de ambos.

BDT, al igual que muchas compañías en esa época, se estaba dirigiendo a un modelo de negocio globalizado, en el cual las redes de datos son utilizadas –entre muchas otras razones- para contactar a socios, proveedores, distribuidores, y clientes, tanto existentes como potenciales; por ende, la necesidad de contar con una infraestructura informático-tecnológica que fuese confiable se volvió un factor crítico para el éxito de la compañía localmente.

Considerando que para finales de los 90, las redes de voz y datos aún eran tratadas de forma separada, al grado de que algunas empresas contaban con personal independiente para cada área, la compañía requería que la totalidad de los servicios relacionados a la informática y a las comunicaciones electrónicas quedasen integradas bajo una misma unidad organizacional, es decir, bajo el enfoque de las tecnologías de la información.

2.2.2 Alcance

Proveer localmente de la plataforma informático-tecnológica a la compañía BDT de México, considerando las tres áreas operativas descritas en el apartado 2.1.1, *Descripción de la organización y sus actividades*, las cuales en total sumaban una cantidad cercana a los 200 usuarios, cubriendo los puntos de captación de necesidades, diseño e implementación que serán detallados posteriormente en los apartados 2.4, *Planeación o cronología del proyecto llevado a cabo*, y 2.5, *Resumen de la documentación e información recabada*, de este mismo documento.

2.3 Descripción de la metodología empleada

El proyecto fue abordado haciendo uso de las nueve áreas del conocimiento de la gestión de proyectos propuesta por la guía del PMBOK; cabe señalar que no todas las áreas fueron desarrolladas al mismo detalle y que algunas de ellas, de hecho, fueron tratadas superficialmente. Entre los procesos más desarrollados, podemos numerar a aquellos pertenecientes a la gestión del tiempo (procesos relativos a las actividades), la gestión de riesgos, la gestión de costos, y la gestión de adquisiciones.

Adicionalmente, al revisar algunos aspectos de la planeación del proyecto reportado, se recurrió de manera informal a herramientas de formulación de estrategias, principalmente de aquellas correspondientes a la etapa de adecuación (también mencionada como de cotejo o pareo en algunas referencias bibliográficas), por lo que se realizaron ejercicios con matrices de tipo TOWS[13] y QSPM[14], siempre en busca de un análisis objetivo que pudiese apoyarnos en la toma de decisiones, pero sin permitir que la obtención de valores numéricos nos diese un falso sentido de certidumbre, sino que ayudara a balancear los sesgos derivados de mi propia experiencia al momento de definir estrategias de trabajo.

---

[13] *Threats-Opportunities-Weaknesses-Strengths* (TOWS), es un marco de trabajo conceptual introducido por Heinz Weihrich al percatarse de que a muchos usuarios se les dificultaba traducir los resultados del análisis SWOT (de origen desconocido, pero atribuido a Albert Humphrey) en acciones que pudiesen ser adoptadas como estrategias corporativas. Esta herramienta analiza las fortalezas y debilidades internas de una organización, así como las oportunidades y amenazas externas a la misma.

[14] *Quantitative Strategic Planning Matrix* (QSPM), es un método analítico diseñado para determinar el atractivo relativo de alternativas de acción viables.

Ahora bien, así como se utilizaron herramientas de gestión de proyectos y de planeación estratégica, también se hizo uso se instrumentos propios del diseño de redes. De hecho, el diseño de la red propuesta se basó en el uso de la metodología *top-down*[15]; esta metodología, ampliamente conocida, divide el diseño de redes en cuatro etapas principales que son llevadas a cabo de forma cíclica (Oppenheimer, P., 2004); dichas etapas son mencionadas a continuación.

Etapas del diseño

- Analizar los requerimientos
- Desarrollar el diseño lógico
- Desarrollar el diseño físico
- Probar, optimizar y documentar el diseño.

A esta estrategia, llevada de manera cíclica, se le conoce como Ciclo de diseño e implementación de redes, y es representada gráficamente en la figura 9.

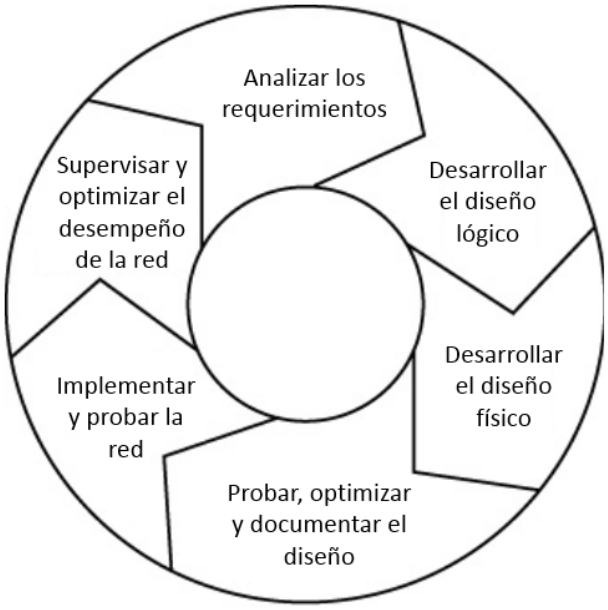


Figura 9. Ciclo de diseño e implementación de redes. Imagen adaptada de: Oppenheimer, P. (2004) [Imagen]. Analyzing Business Goals and Constraints of Network Design. Obtenida de http://www.ciscopress.com/articles/article.asp?p=328773

[15] Diseño de redes *top-down*: es una metodología para el diseño de redes que comienza en las capas superiores del modelo de referencia OSI antes de trabajar con las capas inferiores. Se enfoca en las aplicaciones, sesiones y transporte de información antes que en la selección de *routers*, *switches* y medios de comunicación que operan en las capas inferiores.

Para el desarrollo del proyecto, algunas partes del ciclo fueron consolidadas en una sola etapa; tal es el caso de la etapa de Análisis de los requerimientos, que fue integrada a la de Desarrollo del diseño lógico, descrito en la sección que a continuación comienza. De igual forma, las etapas de Prueba, optimización y documentación del diseño, Implementación y prueba de la red, y Supervisión y optimización del desempeño de la red, fueron integradas parcialmente en la etapa del diseño físico, que será descrito también posteriormente en dicha sección.

Al hacer esta "personalización" de la metodología, se definieron las siguientes etapas específicas de trabajo:

- Planeación del diseño lógico
- Planeación y diseño de componentes
- Diseño físico
- Planeación de recursos

El seguimiento de estas etapas sería de manera secuencial, comenzando con la primera de la lista, y avanzando sucesivamente; de esta manera, iniciaríamos especificando la arquitectura de la plataforma y terminaríamos con su diseño físico.

2.4 Planeación o cronología del proyecto llevado a cabo

En la siguiente página se presenta una estructura de descomposición del trabajo (WBS[16]) simplificada, en la cual se señalan los tres objetivos particulares del proyecto como componentes principales del mismo, y se brinda una idea somera, pero clara de la cronología de actividades y tareas realizadas en cada uno de esos componentes.

[16] *Work Breakdown Structure* (WBS), dentro de la administración de proyectos e ingeniería de sistemas es la descomposición –orientada a entregables- de un proyecto en componentes más pequeños, de manera que permite organizar el trabajo de los diferentes equipos en secciones administrables y manejables.

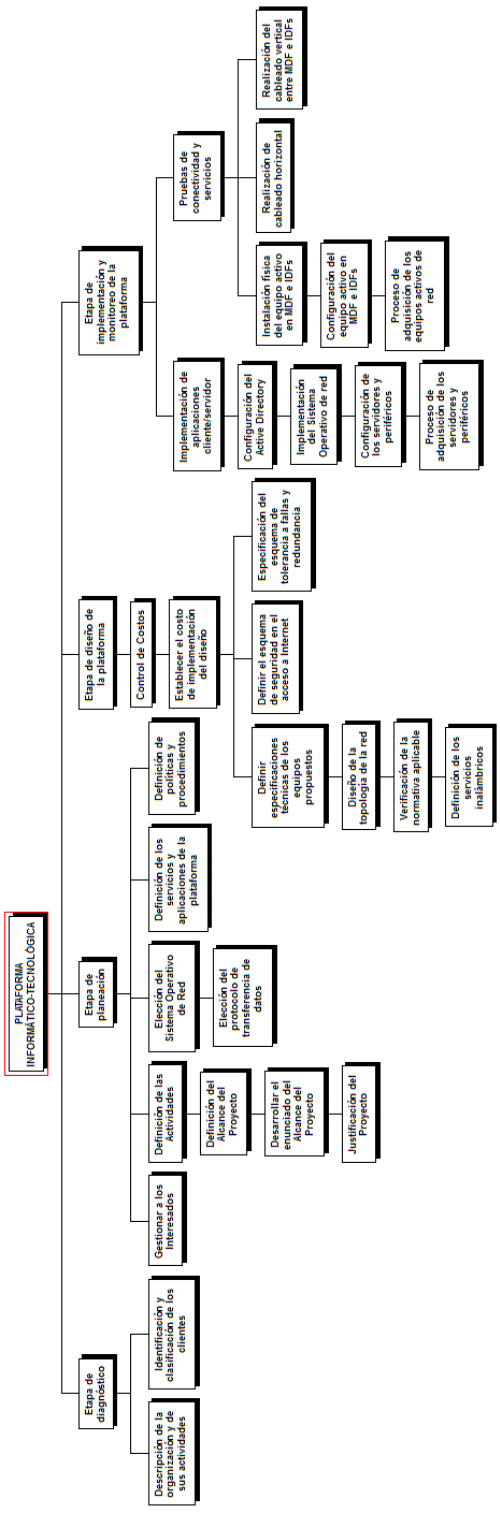


Figura 10. Estructura de descomposición del trabajo correspondiente al proyecto reportado.

Como se menciona en el apartado 2.1.1, *Descripción de la organización y de sus actividades*, existen cuatro aplicaciones básicas que deben estar disponibles el 100% del tiempo destinado a la manufactura; estas son el MES, el ERP y, en menor importancia, el correo electrónico y el portal web.

Considerando que se preveía una red de datos de cerca de 250 nodos, y que sus dos aplicaciones más críticas serían de tipo cliente-servidor, era necesario que los dispositivos de red empleados entre un equipo activo dado y cualquier nodo cumpliese con la velocidad de transmisión establecida para una red 100BaseT (100Mbps), la cual resultaba adecuada para los estándares de conectividad existentes en la década iniciada en el año 2000, teniendo una topología de estrella. De igual manera, se debería de considerar una velocidad de transmisión más elevada para las conexiones existentes entre los diferentes equipos activos de red y se procuraría algo similar para las conexiones existentes entre los equipos activos de red y los servidores de aplicaciones o archivos, es decir siguiendo un diseño jerárquico.

Debido a que el área destinada a la manufactura debería de poder ser modificada de forma casi inmediata, se requería que el cableado de red fuese sumamente flexible y permitiese la realización de cambios de ubicación desde una estación de trabajo hasta una línea de producción completa sin impactar de manera considerable la operación diaria.

Por seguridad de todos los equipos activos de red, éstos deberían quedar fuera del alcance de personal ajeno al del área de las Tecnologías de la Información (TI). En los espacios de manufactura y almacén, además deberían estar fuera del alcance de aquellos equipos y vehículos propios para la operación, tales como montacargas, patines hidráulicos, etcétera, que pudieran llegar a dañarlos en caso de algún accidente o mala operación.

Desde el punto de vista lógico o de gestión de la información de la compañía, la plataforma propuesta debería de:

- Contar con una estructura y perfiles de usuarios acorde a los grupos de trabajo y sus responsabilidades
- Brindar capacidades de conectividad para el acceso a las herramientas de trabajo ejecutables desde algún servidor, así como a los diferentes recursos compartidos de acuerdo con un tipo de usuario específico y su correspondiente nivel de acceso
- Proporcionar y administrar el acceso inalámbrico a la totalidad de equipos portátiles propios de la compañía
- Proporcionar y administrar direcciones IP[17] por medio de mecanismos DHCP[18] para las computadoras en general, y de IP estática para el resto de los dispositivos de red (servidores, *switches*, impresoras, teléfonos, cámaras, etcétera)
- Contar con los elementos de seguridad informática necesarios a nivel de estación de trabajo, de red local y de red de área amplia y/o acceso a Internet, de forma que se evitasen –en la medida de lo posible- situaciones que comprometiesen la integridad de la información y/o de los componentes que conformarían la plataforma (*e.g*., ataques de virus, accesos no autorizados, *hacking*, *spamming*, etcétera)
- Poseer un equipo de acceso a Internet que permitiese el control de los accesos realizados por parte de los usuarios, así como de la aplicación de políticas de acceso a Internet y de la ejecución de los diferentes tipos de contenido de sus páginas web

[17] Dirección de tipo *Internet Protocol* (IP): Etiqueta numérica asignada a cada dispositivo que participa en una red de datos que utiliza el *Internet Protocol* como protocolo de comunicación, corresponde a un número conformado por 4 octetos separados por un punto (para IPv4), y a uno de 16 octetos para IPv6.

[18] *Dynamic Host Configuration Protocol* (DHCP): Protocolo utilizado para la asignación y distribución de direcciones IP dinámicas e información de la configuración a dispositivos dentro de una red de datos. Comúnmente un servidor DHCP proporciona a los clientes al menos la siguiente información básica: dirección IP, máscara de sub-red y *gateway* predefinido. El protocolo está definido por la RFC 1541 (reemplazada por la RFC 2131).

- Proveer mecanismos de redundancia que permitiesen la continuidad de la operación en caso de falla de algún elemento de la plataforma tecnológico-informática
- Tener implementados sistemas de respaldo de la información que permitiesen la recuperación de la operación de la compañía en caso de llegar a perder –por cualquier motivo- la información en uso

2.4.1 Etapa de diagnóstico

La etapa de diagnóstico es un mecanismo para que todos los involucrados en el desarrollo del proyecto reportado puedan reflexionar sobre sus necesidades y requerimientos, tanto en el corto como en el mediano plazo, y para que analicen los problemas potenciales a los que se pueden enfrentar. De esta manera, se pueden definir estrategias de implementación y de operación. Adicionalmente, la etapa de diagnóstico, sirve para analizar los recursos con los que cuenta el equipo a cargo de la realización del proyecto para lograr los objetivos que se establezcan, o bien para gestionar los recursos necesarios y/o faltantes para el cumplimiento las expectativas.

Es en esta etapa en la que se revisa la naturaleza y dinámica de la organización en la que se desarrollará el proyecto, así como la operación de sus diferentes áreas, con la finalidad de comprender su funcionamiento y determinar qué aspectos deberán ser cubiertos durante el desarrollo de la etapa de diseño de la plataforma. Esta etapa, adicionalmente permite identificar los problemas existentes y/o potenciales, así como algunas de sus posibles causas, con lo que se facilita la orientación y dirección adecuadas para evitarlos antes de que se presenten durante la operación normal de la organización.

En el presente documento, la etapa de diagnóstico ha sido abordada ampliamente en el apartado 2.1.1, *Descripción de la organización y de sus actividades*. A pesar de que la Guía PMBOK nos indica que la etapa de planeación debe ser abordada en primer lugar; no obstante, en el caso del proyecto reportado se presentó la situación de primero afrontar la etapa de diagnóstico, ya que era

necesario conocer la naturaleza de la empresa, su operación y dinámica antes de poder planear una solución a requerimientos que hasta ese momento aún eran desconocidos. Se acordó con el asesor del trabajo de obtención de grado, mantener esta secuencia, con la finalidad de describir de manera fidedigna la realización del proyecto documentado en el presente trabajo de obtención de grado.

2.4.2 Etapa de planeación

2.4.2.1 Elección del sistema operativo de red

Para la elección del sistema operativo de red, se tomaron en cuenta los siguientes criterios de selección: madurez, compatibilidad (tanto con las implementaciones existentes en el mercado en general como con las existentes en las oficinas corporativas de la compañía), así como las ventajas competitivas derivadas de las características individuales de cada producto evaluado.

Durante la época de realización del proyecto reportado, existían en el mercado cuatro productos principales: Unix (en una gran variedad de versiones), Novell NetWare, MacOS y Windows. No debemos olvidar que justo en esas fechas comenzaba el auge de las implementaciones de Linux, pero que en los entornos empresariales era aún visto con desconfianza.

De elegirse la utilización de alternativas del tipo Unix y MacOS, prácticamente se obligaba a los usuarios a adquirir equipos de cómputo basados en procesadores RISC, los cuales explotaban enormemente las capacidades de procesamiento basado en arquitectura *hardwired* (también mencionada como *cableada* en algunas referencias bibliográficas), pero que resultaban considerablemente más costosos que los procesadores CISC utilizados por las llamadas computadoras personales, cuyo mercado ya era dominado por los modelos PC de IBM y su infinidad de clones “compatibles”, todos ellos basados en procesadores 8080, y que por su facilidad de reproducibilidad, se obtenían a precios muy por debajo de los primeros.

Esta primera exclusión, nos dejó ante la disyuntiva de elegir entre Novell NetWare y Windows para ser utilizado como sistema operativo de red, y por extensión, como sistema operativo de escritorio. En lo personal, yo contaba con experiencia en la implementación y utilización de entornos totalmente Windows (que incluían productos Windows tanto en los servidores como en las estaciones de trabajo), como en entornos híbridos (servidores NetWare con estaciones de trabajo Windows en su versión 95), por lo que se evaluaron ambas alternativas a detalle.

Novell NetWare representaba sobradamente la alternativa más madura, ya que se encontraba en el mercado desde inicios de la década de los ochenta, y las versiones de Windows que podrían competirle, habían incursionado en el mercado apenas a finales de esa misma década. Características como los servicios globales de directorio (NetWare Directory Services, NDS), que Novell había incluido desde 1993, y que serían posteriormente imitadas por las versiones de Windows casi una década después, le hacían una excelente alternativa.

No obstante, es necesario ubicar la época de realización del proyecto y la volatilidad de los desarrollos tecnológicos; las empresas se enfrentaban a entornos cambiantes de manera constante y se tendía de manera deliberada a imitar los llamados casos de éxito de las grandes corporaciones, como si esas soluciones fuesen infalibles, irrefutables y reproducibles en cualquier entorno, independientemente de su naturaleza y tamaño. De esta manera, las oficinas corporativas de la compañía, habían optado desde tiempo atrás por la utilización de la llamada suite Backoffice, la cual incluía Windows NT, Exchange y Proxy Server, entre otros, para operar las funciones básicas de una red de cómputo: recursos compartidos, correo electrónico y acceso a Internet. Novell no contaba con un producto similar con el cual competir con Microsoft, por lo que, paulatinamente, esta alternativa fue perdiendo peso en el proceso de toma de decisiones.

Con la finalidad de evitar que la fase de toma de decisiones se volviese un proceso meramente intuitivo y subjetivo, procedí a hacer uso de la planeación estratégica por medio de una matriz QSPM, de manera que pudiésemos contar con un método analítico que respaldase la decisión tomada en esta fase.

El primer paso para utilizar esta herramienta es la identificación de los factores estratégicos clave, lo cual, se logra a partir de la elaboración de matrices EFE e IFE, la primera surge a partir de dos grupos de factores, oportunidades y amenazas, y la segunda, nace a partir de la identificación de fortalezas y debilidades. Estas dos primeras matrices corresponden a la primera etapa del marco de trabajo de la planeación estratégica, la etapa de insumos o aportaciones. Estas matrices contemplan un peso para cada factor y una calificación correspondiente a cada uno de ellos, la cual indica que tan efectivamente las estrategias de la compañía responden a ese factor; en el caso del proyecto reportado, al tratarse de una estrategia totalmente nueva, no existían antecedentes sobre esta correlación, por lo tanto, en este punto solamente estarán enlistados tanto los Factores Clave Externos como los Factores Clave Internos, pero carecerán de ponderación.

Factores Clave Externos
Oportunidades
Madurez del Sistema Operativo
Utilización de servidores primarios
Utilización de servidores secundarios
Disponibilidad de interfaz gráfica (GUI)
Base de datos de objetos distribuída
Auditoría de transacciones
Multiprotocolo (cubre TCP/IP)
Multiprocesamiento
Asignación y limitación de espacio de almacenamiento
Utilización de Listas de Control de Acceso
Amenazas
Acceso único a la red
Memoria RAM máxima
Tamaño máximo de volúmen
Tamaño máximo de archivo
Número máximo de usuarios conectados a un servidor
Número máximo de cuentas de usuarios

Factores Clave Internos
Fortalezas Internas
Utilización y dominio del Sistema Operativo
Disponibilidad de soporte local del S. O.
Facilidad de mapeo lógico de la empresa
Compatibilidad de S. O. con clientes, proveedores e internamente
Debilidades Internas
Soporte interno con diferencia de horario
Utilización de suite Back Office a nivel corporativo

Tabla 5. Listado de Factores Clave Externos y Factores Clave Internos.

Una vez que se han identificado y analizado los factores estratégicos clave, éstos son utilizados como datos de entrada para la generación de la matriz QSPM, la cual se muestra a continuación, cuyos resultados nos dan una clara idea sobre cuál estrategia era recomendable seguir.

Factores Clave Externos	Peso	Alternativas de estrategia			
		Novell NetWare		Windows NT	
		CA	CAT	CA	CAT
Oportunidades					
Madurez del Sistema Operativo	0.080	4	0.32	2	0.16
Utilización de servidores primarios	0.035	4	0.14	2	0.07
Utilización de servidores secundarios	0.050	4	0.20	4	0.20
Disponibilidad de interfaz gráfica (GUI)	0.025	3	0.08	3	0.08
Base de datos de objetos distribuída	0.060	4	0.24	2	0.12
Auditoría de transacciones	0.065	3	0.20	3	0.20
Multiprotocolo (cubre TCP/IP)	0.100	4	0.40	4	0.40
Multiprocesamiento	0.060	2	0.12	4	0.24
Asignación y limitación de espacio de almacenamiento	0.013	4	0.05	3	0.04
Utilización de Listas de Control de Acceso	0.045	4	0.18	4	0.18
Amenazas					
Acceso único a la red	0.010	3	0.03	3	0.03
Memoria RAM máxima	0.025	3	0.08	3	0.08
Tamaño máximo de volúmen	0.065	1	0.07	4	0.26
Tamaño máximo de archivo	0.050	1	0.05	4	0.20
Número máximo de usuarios conectados a un servidor	0.045	2	0.09	2	0.09
Número máximo de cuentas de usuarios	0.035	1	0.04	4	0.14
Fortalezas Internas					
Utilización y dominio del Sistema Operativo	0.070	2	0.14	4	0.28
Disponibilidad de soporte local del S. O.	0.010	2	0.02	2	0.02
Facilidad de mapeo lógico de la empresa	0.010	3	0.03	3	0.03
Compatibilidad de S. O. con clientes, proveedores e internamente	0.060	1	0.06	3	0.18
Debilidades Internas					
Soporte interno con diferencia de horario	0.013	1	0.01	3	0.04
Utilización de suite Back Office a nivel corporativo	0.075	1	0.08	4	0.30
Suma de la Calificación de Atractivo Total	**1.000**		**2.60**		**3.32**

CA = Calificación del Atractivo
CAT = Calificación del Atractivo Total
1 = No Aceptable
3 = Probablemente Aceptable
2 = Posiblemente Aceptable
4 = Muy Aceptable

Figura 11. Matriz QSPM para la elección del Sistema Operativo de Red.

Resulta oportuno hacer una advertencia respecto a la utilización de la matriz QSPM, ya que a pesar de que la herramienta cae en la categoría de modelos compensatorios para la toma de decisiones (es decir valora y pondera tanto los criterios positivos como los negativos), siempre se requerirán opiniones intuitivas y suposiciones fundamentadas de parte de quien aplica la herramienta. Las calificaciones de valoración y del atractivo requerirán de decisiones intuitivas, aun cuando para obtenerlas se base en información objetiva.

Por las razones previamente señaladas y considerando la amplitud de mercado cubierta por los dos sistemas operativos de red sobre los que se tomó la decisión final, se optó por la utilización de un ambiente de trabajo basado en Microsoft Windows, inicialmente la versión NT –la primera versión de 32 bits de Windows-, y posteriormente la versión 2000. La elección de dichas versiones de este sistema operativo se basó en la madurez que el producto tenía a la fecha (Windows NT estaba en el mercado desde 1993 y Windows 2000 desde finales de 1999), y se contemplaron –de cualquier forma- posibles actualizaciones a versiones más nuevas y/o poderosas conforme éstas dejasen de ser una mera novedad, se corrigiesen sus *bugs* iniciales y se volviesen más confiables.

La versión inicial elegida fue la 4.0 de Windows NT; este sistema operativo estaba disponible tanto para servidor como para las estaciones de trabajo. En el caso de la versión para servidor, podía utilizarse tanto en equipos dotados de un solo procesador, como en aquellos diseñados para trabajar con multiprocesamiento simétrico. Como todo sistema operativo de 32 bits, Windows NT tenía un límite de utilización de memoria RAM de 4GB, valor muy por encima de lo típicamente instalado en la época de realización del proyecto; de estos 4GB, 3GB estaban disponibles para las aplicaciones y 1GB se asignaba al *kernel*[19] y a los componentes "ejecutivos" o propios del sistema operativo.

[19] *Kernel*. Es un programa dentro del sistema operativo que gestiona las solicitudes de entrada y salida -E/S- generadas por el software y que las traduce a instrucciones de procesamiento de información para el procesador (CPU) y para otros componentes electrónicos de una computadora. Las solicitudes de una aplicación al *kernel,* se denominan llamadas al sistema (*system call*).

Esta versión del sistema operativo mostraba mejoras, con respecto a sus antecesores, en la interfaz gráfica del usuario (GUI por sus siglas en inglés) correspondiente a herramientas administrativas, tales como el administrador de usuarios para dominios, el administrador del servidor y el administrador de DNS, entre otras. Adicionalmente, esta versión incluía los servicios de información de Internet (IIS por sus siglas en inglés), e introducía el administrador de tareas de Windows por vez primera.

Algunas de las características de esta versión del sistema operativo, detalladas en Managing Windows NT Server Domains, obtenida de https://www.microsoft.com/resources/documentation/windowsnt/4/server/proddocs/en-us/concept/xcp01.mspx?mfr=true, son:

- *Encrypting File System* (EFS). Esto permite que los archivos puedan ser encriptados, a nivel archivo, directorio o disco, con la finalidad de evitar accesos no deseados a la información.
- *New Technology File System* (NTFS). Este sistema de archivos permite la aplicación del esquema de encriptación (EFS) y cuenta con muchas ventajas sobre sus antecesores, tales como FAT y HPFS (*File Allocation Table* y *High Performance File System* respectivamente por sus siglas en inglés)-. Incluye, entre otras funcionalidades: Escalabilidad, es decir definición de los tamaños de volúmenes; la compresión, así como la asignación de espacio de almacenamiento a utilizar por el usuario.
- Servicios de *Active Directory* (AD)[20]. Estos servicios comprenden un marco de trabajo jerárquico, utilizado principalmente para administrar usuarios, grupos, contactos, computadoras y unidades organizacionales entre muchos otros objetos.
- *Distributed File System* (DFS). Este sistema de archivos permite compartir los recursos con elementos pertenecientes al Active Directory.

[20] Un resumen de las características del *Active Directory* puede ser consultado en el glosario de términos ubicado en la sección de Anexos al final del presente documento.

- *Multilingual User Interface* (MUI). Permite la utilización de múltiples lenguajes en la interfaz de usuario.
- *Multiprocesamiento.* Capaz de operar hasta con 8 procesadores.
- *Tamaño máximo de volumen.* En teoría el tamaño máximo de volumen y de archivo es de 16 EB, aunque el aprovechamiento de ese tamaño no es realizable debido a las limitantes de las interfaces de los discos duros existentes (aún los actuales).
- *Número máximo de cuentas de usuarios*. En teoría es ilimitado; sin embargo, la cantidad efectiva máxima de cuentas de usuarios probada, es de 40,000, manteniendo una base de datos SAM[21] máxima de 40MB, con lo que se evita la lentitud en el tiempo de arranque, en el uso del ancho de banda y en la creación y/o modificación de los objetos dentro del *Active Directory*.

Elección del protocolo de transferencia de datos

Uno de los puntos más importantes del diseño lógico de una red es la elección del protocolo de red. Esta elección deberá basarse en términos del tipo de aplicaciones que pretendemos ejecutar en nuestra red y a las comunicaciones que se establecerán entre nuestra red y las redes externas, aun cuando estas últimas pertenezcan a la compañía, pero que se encuentran en distintas ubicaciones geográficas.

Considerando lo anterior, la red propuesta utilizaría el *Transmission Control Protocol / Internet Protocol* (TCP/IP) como protocolo de red debido a que:

- Se ha convertido en el protocolo estándar de red desde finales de la década de los ochenta. Para cualquier propósito práctico, TCP/IP permite un mayor margen de compatibilidad de la red propuesta con otras redes con las que se pudiera llegar a interconectar ya que no es un protocolo de red de tipo propietario.

[21] SAM (*Security Account Manager*): es la base de datos de Windows en donde son definidas todas las cuentas de usuarios, cuentas de grupos, así como definiciones de recursos tales como impresoras y espacios de almacenamiento compartidos. Se encuentra almacenada en el controlador de dominio.

- Ya que la versión 4 de TCP/IP es el protocolo más ampliamente utilizado, la migración hacia una nueva versión (IPv6) vendrá del núcleo de Internet hacia los bordes, donde reside la red propuesta, por lo que la plataforma informático-tecnológica estaría preparada para hacer frente a ese cambio.

- Aun si no se tuviera una conexión a Internet (lo cual es inimaginable para una empresa en la actualidad), el TCP/IP sería la opción más práctica debido a que una gran cantidad de aplicaciones trabajan con dicho protocolo y existe un amplio mercado de profesionistas capacitados en él que pueden ser contratados para administrar una red basada en TCP/IP.

- Otros sistemas operativos existentes, tales como NetWare han modificado sus productos para utilizar TCP/IP como su protocolo interior, tal como sucede en sus versiones 5.X y 6.X, dejando atrás la utilización exclusiva de los protocolos IPX/SPX[22].

- A pesar de que protocolos como IPX/SPX proveen servicios de conexión similares a los proveídos por TCP/IP, su desempeño no es el mejor para las redes de área amplia (WAN por sus siglas en inglés) y en Internet, donde TCP/IP tiene un desempeño superior. Esto se debe, principalmente, a que IPX/SPX fue diseñado mayormente para las redes de área local (LAN por sus siglas en inglés), en donde su desempeño es incluso mejor que el de TCP/IP.

[22] IPX/SPX (*Internetwork Packet Exchange/Sequenced Packet Exchange*): una descripción más detallada de estos protocolos puede ser consultada en el glosario de términos ubicado en la sección de Anexos al final del presente documento.

- TCP/IP es un protocolo desarrollado originalmente por el Departamento de Defensa de los Estados Unidos en tiempos de la guerra fría, por lo que su diseño tuvo que cumplir con:

  a) Permitir la continuidad de la operación durante una guerra nuclear. Se requirió que la red continuara funcionando aun cuando 7/8 de la red no fueran operacionales.

  b) Ser completamente descentralizado, sin ninguna instalación central que pudiera ser destruida y diera de baja la red.

  c) Ser completamente redundante y ser capaz de continuar las comunicaciones entre los puntos A y B, incluso cuando enlaces o sitios intermedios dejaran de funcionar durante la conversación.

  d) La arquitectura debería ser lo suficientemente flexible en función del creciente rango de aplicaciones (desde transferencia de archivos hasta información sensible al tiempo, tal como la voz y el vídeo)

- El punto anterior indica que TCP/IP es un protocolo muy robusto que puede recuperarse automáticamente de cualquier falla en los enlaces de comunicación. *Re-enruta* paquetes de información si las líneas de transmisión son dañadas o si una computadora no responde por medio de cualquier camino de red disponible. De igual forma, se deduce que es un protocolo muy maduro que fue desarrollado específicamente para cubrir necesidades muy particulares de comunicación.

- TCP/IP es proveído por casi todos los sistemas operativos y, por lo tanto, permite la conectividad entre sistemas distintos (v.g., entre un equipo UNIX y una computadora con Windows XP).

Los protocolos están en un dominio público disponibles de forma gratuita, lo cual los convierte en una opción popular para las compañías de software ya que no hay restricciones en su uso y no se pagan regalías por su utilización. Adicionalmente, debido a que es un estándar abierto y ninguna compañía controla el protocolo, cualquiera puede utilizarlo y desarrollar aplicaciones basadas en él fácilmente.

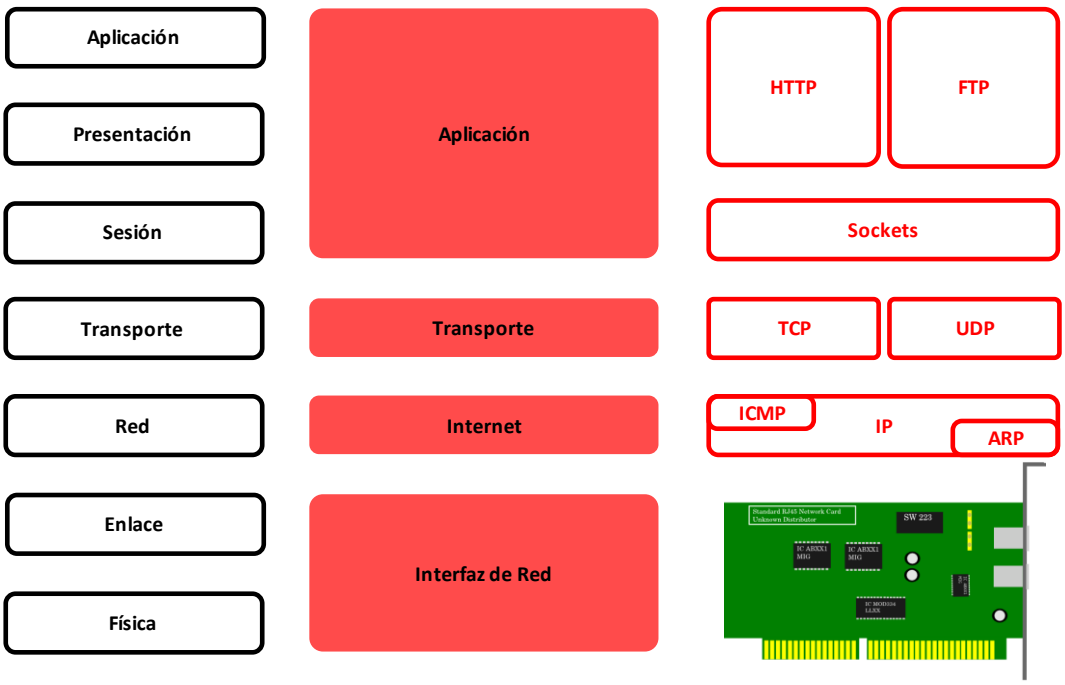


Figura 12. Comparación del modelo OSI y el conjunto de protocolos TCP/IP. Adicionalmente, se muestra su correspondencia con un modelo conceptual de cuatro capas conocido como modelo ARPA, mostrado al centro. Imagen adaptada de: Blanchard, E. (2005) [Imagen]. Introduction to Data Communications. Obtenida de http://www.techbooksforfree.com/intro_to_data_com/page235.html

2.4.2.2 Definición de los servicios y aplicaciones de la plataforma

La plataforma propuesta debería de:

- Contar con una estructura y perfiles de usuarios acorde a los grupos de trabajo y sus responsabilidades
- Brindar capacidades de conectividad para el acceso a las herramientas de trabajo ejecutables desde algún servidor, así como a los diferentes recursos compartidos de acuerdo con un tipo de usuario específico y su correspondiente nivel de acceso
- Proporcionar y administrar el acceso inalámbrico a la totalidad de equipos portátiles propios de la compañía
- Proporcionar y administrar direcciones IP[23] por medio de mecanismos DHCP[24] para las computadoras en general, y de IP estática para el resto de los dispositivos de red (servidores, *switches*, impresoras, teléfonos, cámaras, etcétera)
- Contar con los elementos de seguridad informática necesarios a nivel de estación de trabajo, de red local y de red de área amplia y/o acceso a Internet, de forma que se evitasen –en la medida de lo posible- situaciones que comprometiesen la integridad de la información y/o de los componentes que conformarían la plataforma (*e.g*., ataques de virus, accesos no autorizados, *hacking*, *spamming*, etcétera)
- Poseer un equipo de acceso a Internet que permitiese el control de los accesos realizados por parte de los usuarios, así como de la aplicación de políticas de acceso a Internet y de la ejecución de los diferentes tipos de contenido de sus páginas web

[23] Dirección de tipo *Internet Protocol* (IP): Etiqueta numérica asignada a cada dispositivo que participa en una red de datos que utiliza el *Internet Protocol* como protocolo de comunicación, corresponde a un número conformado por 4 octetos separados por un punto (para IPv4), y a uno de 16 octetos para IPv6.

[24] *Dynamic Host Configuration Protocol* (DHCP): Protocolo utilizado para la asignación y distribución de direcciones IP dinámicas e información de la configuración a dispositivos dentro de una red de datos. Comúnmente un servidor DHCP proporciona a los clientes al menos la siguiente información básica: dirección IP, máscara de sub-red y *gateway* predefinido. El protocolo está definido por la RFC 1541 (reemplazada por la RFC 2131).

- Proveer mecanismos de redundancia que permitiesen la continuidad de la operación en caso de falla de algún elemento de la plataforma tecnológico-informática
- Tener implementados sistemas de respaldo de la información que permitiesen la recuperación de la operación de la compañía en caso de llegar a perder –por cualquier motivo- la información en uso

2.4.2.3 Definición de políticas y procedimientos

No hay que olvidar que resultaba necesario la creación y administración de una serie de políticas, en términos de gobernabilidad -no de reglas de control de permisos del sistema operativo-, para regular el uso de la plataforma informático-tecnológica que comprendiera puntos tales como:

- Manejo y confidencialidad de las cuentas de usuarios y contraseñas
- Manejo y confidencialidad del contenido de la información a la que se tiene acceso
- Penalización por intentar –exitosa o infructuosamente- el acceso a información por medio de una cuenta de usuario y contraseña ajenas
- Penalización por intentar –exitosa o infructuosamente- deshabilitar las medidas de protección (*firewall*, *proxy*, anti-virus, etcétera) implementadas por la compañía para garantizar la seguridad informática
- Cuidado en el manejo del equipo de TI que le sea asignado
- Manejo, comportamiento y reglas en el envío de mensajes de correo electrónico y de mensajería instantánea
- Restricción en el uso de la cuenta de correo electrónico para otros fines que no sean aquellos directamente relacionados con la operación de la compañía o para fines personales
- Discreción en la navegación en Internet y al tipo de contenido al que se tiene acceso

De igual manera, se preveía la existencia de procedimientos para realizar las diferentes actividades que involucrasen el uso de la plataforma de manera adecuada. Aun cuando en el momento de la realización del proyecto, la compañía no contaba localmente con una certificación de tipo ISO, era claro que se requería la existencia de procedimientos que permitiesen eliminar o disminuir los malos entendidos al identificar las responsabilidades individuales y establecer los límites entre los colaboradores; de manera similar, los procedimientos ayudarían a controlar anticipadamente eventos que podrían resultar costosos para la empresa. Básicamente, con los procedimientos, se les daría a los usuarios de la plataforma un plan a seguir para su adecuado aprovechamiento. Los procedimientos iniciales que acompañaron el lanzamiento de la plataforma técnico-tecnológica fueron:

- Generación y manejo de archivos dentro de las ubicaciones de red
- Almacenamiento de información crítica en ubicaciones de red que fuesen respaldadas regularmente
- Solicitud de alta de nuevos usuarios (a los diferentes servicios de la plataforma) que hayan sido integrados a las actividades de la compañía
- Solicitud de modificación de los tipos y niveles de acceso a los usuarios, conforme sea requerido por un cambio de puesto o responsabilidades dentro de la compañía
- Solicitud de baja de cuentas de usuarios (a los diferentes servicios de la plataforma) que hayan dejado de prestar sus servicios a la compañía
- Generación de trabajos de respaldos de información crítica, así como su adecuada gestión
- Documentación de cambios, anexiones, crecimientos y modificaciones de las instalaciones de la plataforma técnico-tecnológica

Estos puntos fueron establecidos como indicativos, pero de ninguna manera se consideraron como limitativos, razón por la cual posteriormente se anexaron más, conforme fue siendo necesario, y conforme las nuevas herramientas informático-tecnológicas demandaron sus propios puntos a administrar y controlar.

2.4.3 Etapa de diseño de la plataforma

2.4.3.1 Definición de las especificaciones técnicas de los equipos propuestos

Equipos activos de red (*switches*)

La definición de los equipos activos a utilizar se dio a partir de una revisión exhaustiva de sus características y el cumplimiento –en mayor o menor medida- de requerimientos propios de la plataforma técnico-tecnológica. De esta manera, y tras varias revisiones en conjunto con proveedores y personal técnico del corporativo, se llegó a las siguientes tablas de modelos y características de los equipos que comprenderían mi propuesta formal para cubrir los requerimientos de la compañía en el ámbito de las TI.

Para los equipos de *switcheo*, se propuso la utilización de equipos llamados capa 3 para las áreas del núcleo y de distribución, tal como será detallado en la sección siguiente, 2.4.3.2, *Diseño de la topología de la red*. Lo anterior se debió a que este tipo de equipos realizan funciones tanto de los *switches* de capa de enlace como de los enrutadores de capa de red; con esto, se logra que cada puerto sea un dominio de colisión y las interfaces pueden ser agrupadas en dominios de trasmisión o difusión (*broadcast*). Además, se puede seleccionar un protocolo de enrutamiento para proveer información de la red a otros *switches* de capa 3, o a algún enrutador en caso de ser necesario.

Para el segmento inalámbrico se propuso el uso de un *Access Point* certificado como WiFi, contaba con una velocidad de transmisión de 54Mbps, y -utilizando el estándar IEEE 802.11g- con una cobertura cercana a los 100 metros tanto para recibir como para transmitir. Su nivel de seguridad, permitía la autenticación por medio de direcciones MAC o claves WPA TKIP; de igual forma utiliza encriptación por medio de WPA avanzado de 256 bits, WEP de 40/64, 128 y 154 bits, así como el protocolo propietario del fabricante de encriptación dinámica de la seguridad del enlace (*Dynamic Security Link*, no confundir con *Digital Subscriber Line*, ambos términos con el acrónimo DSL por sus siglas en inglés).

El equipo propuesto contaba con amplias posibilidades de crecimiento, desde ampliaciones o actualizaciones por medio de tarjetas mini-PCI hasta diversas antenas externas que podrían cubrir las diferentes necesidades de ampliación de la cobertura originalmente brindada por el dispositivo.

Un resumen de las especificaciones de los equipos activos de red, tanto *switches* como de acceso inalámbrico, se incluye en la sección de Anexos al final de este reporte.

Dispositivo Firewall

Inicialmente tomamos la decisión de utilizar la misma marca de *firewall* y configuración existentes en la red de Alemania. Esta decisión, que aparentemente resultaba la más adecuada en su momento, terminó siendo errónea, ya que el fabricante (BorderWare) proporcionaba un servicio de soporte y consultoría demasiado pobre, limitado y considerablemente costoso respecto a los beneficios obtenidos. Esto ocasionó que en muy corto tiempo volviésemos a revisar otras alternativas con la finalidad de corregir la mala decisión originalmente tomada y optar por una que hubiese sido evaluada exhaustivamente en conjunto con el corporativo.

Al no tratarse de un dispositivo de hardware (*appliance*), la inversión realizada había sido exclusivamente en licenciamiento del software, por lo que, una vez terminada la vigencia del mismo, podríamos optar por un producto diferente. Trabajando en conjunto con el corporativo, se evaluaron diferentes productos para, finalmente, optar por uno que pudiese darnos consultoría de manera más eficiente que su antecesor en ambos países; el resultado de esta discusión fue la decisión de utilizar el *firewall* Astaro Security Linux V5 instalado en un hardware Nexcom NSA1080L; esta combinación se conocía como TimeNET SecuRACK P-8/100.

Dado que la opción inicial fue errónea, decidí reportar la opción que sirvió de corrección, ya que de esta última alternativa es de la que realmente se explotarían sus funcionalidades, y cuya elección más demandaría de nuestras habilidades en el proceso de toma de decisiones.

Resulta obvio que el haber tomado inicialmente una decisión de tal envergadura de manera ligera, redundó en un resultado fallido que pudo haberse evitado de haber realizado una evaluación más profunda de las diferentes opciones que nos hubiese permitido percatarnos -anticipadamente- de las debilidades que el fabricante tenía localmente.

En la sección Anexos, se incluye una descripción detallada de algunos aspectos clave que nos condujeron a la elección final del firewall Astaro.

Servidores

El procesamiento de cómputo primario se realizaría en cuatro servidores, los cuales tendrían un rol específico con la finalidad de responder a los requerimientos de procesamiento centralizado de la plataforma técnico-tecnológica. Un quinto servidor estaría en modo de espera. Estos roles serían:

- Servidor 1 – PDC y servidor de archivos
- Servidor 2 – Correo Electrónico
- Servidor 3 – Sistema ERP
- Servidor 4 – Sistema MES
- Servidor 5 – Modo de espera

Para los cinco roles se analizaron alrededor de 3 marcas de equipos, y se optó por el modelo ProLiant ML370 G3 de Hewlett Packard, ya que este modelo representaba la mejor relación entre prestaciones y precio.

El procesamiento de cómputo secundario se realizaría en dos servidores. Sus roles serían:

- Servidor 1 – Aplicaciones financieras y de Recursos Humanos.
- Servidor 2 – Sistema de respaldo de información en cintas.

Para ambos roles se optó por el modelo ProLiant ML330 G3 de Hewlett Packard, ya que, para los requerimientos de ambos roles, este modelo representaba la mejor relación entre prestaciones y precio al compararlo con marcas como Dell e IBM.

Las características principales o relevantes para el diseño de la plataforma, de ambos modelos de servidores, se detallan en el apartado de Anexos, *Características y configuración de los servidores*, al final de este documento.

Red de Área de Almacenamiento

Un aspecto relevante al momento de definir el diseño propuesto fue la consideración del almacenamiento masivo de la gran cantidad de información que se generaría durante la operación de la compañía. Pensando en que la plataforma estaría compuesta por aplicaciones tales como ERP y MES, ambas con extensas bases de datos de tipo Oracle, correo electrónico con alrededor de doscientos buzones y sus correspondientes archivos de almacenamiento personal (archivos tipo .pst[25]), así como el gran número de documentos que serían generados conforme la compañía creciese, tuvimos que decidirnos entre dos posibles estrategias de implementación: 1) almacenar toda esta información en un servidor de archivos, o 2) utilizar una red de área de almacenamiento (*Storage Area Network* o SAN[26]).

[25] Personal Storage Table (PST). También conocido como *Personal Folder*, es un tipo de archivo de propietario abierto utilizado para almacenar copias de mensajes, eventos en calendario, y otros objetos utilizados por software de Microsoft, tal como Microsoft Exchange o Microsoft Outlook.

[26] Storage Area Network (SAN). Es una red dedicada al almacenamiento de manera centralizada que se encuentra conectada a la red de datos y se tiene acceso a ella por medio de servidores. En una SAN los controladores de conectan a los discos duros comúnmente por medio de Fibra Canal y a la red de datos de la organización por medio de servidores o equipos de cómputo de alto desempeño.

La primera alternativa tenía la ventaja de un costo de inversión más bajo que la segunda, debido principalmente al número reducido de hardware requerido para su implementación; sin embargo, se consideró el aspecto del crecimiento y la escalabilidad, de manera que se tuviese en mente una solución a largo plazo. Debido a lo anterior, se tomó la decisión de implementar una SAN.

Tras una revisión de las alternativas de los diferentes tipos de hardware para esa tecnología, llegamos a la decisión de implementar un equipo de la marca Hewlett Packard que nos brindaba la mejor relación costo-beneficio, el modelo MSA (Modular Smart Array) 1000.

El equipo MSA1000 es un sistema de almacenamiento de tecnología Fibra Canal de 2Gb, diseñado para implementaciones de redes de área de almacenamiento de nivel inicial a rango medio. El diseño de este equipo permitía reducir la complejidad, el costo y el riesgo de la implementación de una SAN; el MSA1000 es un sistema de almacenamiento escalable de alto desempeño, fabricado teniendo en mente la protección de la inversión. El diseño modular de este equipo nos permitiría incrementar las capacidades de almacenamiento conforme fuese necesario. Con la incorporación de dos cajas de discos del tipo MSA30 con espacio para un total de cuarenta y dos discos de tipo empresarial, se podría obtener una capacidad máxima de almacenamiento de 12 TB; una capacidad de almacenamiento que aún en la actualidad resultaría sobrada para muchas compañías de tamaño medio.

Un resumen de las características relevantes para habernos decidido por este equipo, se incluyen en el apartado de Anexos, *Características y configuraciones, física y lógica de la SAN*.

2.4.3.2 Diseño de la topología de la red

La topología de la red es básicamente una representación gráfica del acomodo de una red, incluyendo sus nodos y líneas de conexión. Sin embargo, hay que tener cuidado al hablar sobre la topología de una red, ya que existen dos formas de definir su geometría; la física y la lógica.

En el caso del proyecto reportado, ocurre que la topología lógica es la misma que la física, pero se hace la aclaración de que esto podría no siempre ser el caso. La topología propuesta contempla la utilización de un diseño de *switcheo* jerárquico; es decir, se parte de una instancia central –núcleo- en donde se realiza el mayor tráfico de paquetes de datos, el cual envía esos paquetes a los demás equipos (que son la capa de distribución), y éstos entregan los paquetes a su destino final por medio de equipos que componen la capa de acceso.

Cada una de las capas del diseño mencionado se detalla a continuación:

Núcleo

El núcleo está definido como el *backbone* de la red, y por lo tanto debe cumplir con requerimientos tales como:

- Confiabilidad
- Redundancia y/o tolerancia a fallas
- Rápida adaptabilidad a cambios
- Bajos niveles de retraso
- Eliminación o disminución de la lentitud del manejo de paquetes debido a filtros u otros procesos

Para la red propuesta, se pretendía mantener el núcleo lo más descargado posible de todas aquellas tareas diferentes a las que debía enfocarse. Por lo anterior el núcleo propuesto constaba de un equipo de *switcheo* principal con características de trabajo en capa 3, un total de 24 puertos 10/100/1000, 56Gbps de capacidad de *switcheo* y que permitía priorizar el tráfico. Todos los dispositivos de *switcheo* de la capa de distribución serían conectados a este elemento.

Con la finalidad de cubrir posibles crecimientos futuros y aprovechando la mínima diferencia en el costo de los elementos físicos, entre cableado categoría 5 y categoría 5e, la totalidad del cableado –es decir, el utilizado en las capas de distribución y de acceso- sería precisamente de categoría 5e de manera que fuese posible el cumplimiento de la norma IEEE 802.3ab que especifica la operación de Ethernet Gigabit sobre par trenzado de cobre, con distancias máximas entre segmentos de 100 metros para el tipo 1000BaseT.

Capa de distribución

La capa de distribución permite la implementación de las siguientes funciones:

- Aplicación de políticas
- Seguridad
- Acceso de grupos de trabajo o departamentos
- Definición de los dominios de *broadcast/multicast*
- Enrutamiento entre redes virtuales (VLAN)
- Traducción de los diferentes medios
- Punto de demarcación entre protocolos de enrutamiento estático y dinámicos

La solución propuesta contemplaba la inclusión de dispositivos de *switcheo* con capacidades similares a los utilizados en el núcleo, pero con un menor número de puertos 10/100/1000 (12 puertos en total), de manera que permitiesen una interconexión acorde al estándar IEEE 802.3ab Ethernet Gigabit. Todos los dispositivos de *switcheo* de la capa de acceso estarán conectados a estos elementos. Adicionalmente, existirían conexiones directamente entre los *switches* del núcleo y los *switches* de la capa de acceso utilizando configuraciones del tipo *resilient links* o *spanning tree* que son manejados –de forma nativa- por dichos equipos.

En esta capa asociamos los diferentes dispositivos de *switcheo* a los grupos definidos en la Tabla 6, dando un total de cuatro grupos de distribución.

Grupo	Sub-grupo
MDF	Granja de servidores
	Oficina de TI
Planta Alta	Administración – Área 1
	Administración – Área 2
Planta Baja	Almacén
	Administración – Área 3
Manufactura	*Storage* – Área 1
	Storage – Área 2
	Paper Handling

Tabla 6. Distribución de usuarios en diferentes grupos de acuerdo con su funciones operativas.

Este acomodo permite una sencilla definición de dominios de *broadcast/multicast*, y –muy importante- la implementación futura de redes virtuales (VLAN) de una manera sencilla, mejorando las capacidades de seguridad y permitiendo la aplicación de mecanismos de Calidad de Servicio (QoS). Ya que la totalidad de la red está planeada en un mismo tipo de medio, no se llevarían a cabo labores de traducción entre diferentes medios.

Capa de acceso

La función primordial de esta capa es la de proporcionarle al usuario el acceso adecuado a la red de datos. Se puede tomar ventaja de la segmentación por medio de *switches* de manera que se aproveche el ancho de banda proporcionado por tales equipos.

La solución propuesta contempla la utilización de dispositivos de *switcheo* de capa 2 con capacidades de *switcheo* entre los 12.8 y los 13.6 Gbps y con configuraciones de 24 o 48 puertos 10/100 y al menos dos puertos 10/100/1000 en cada equipo. Éstos últimos servirán para conectar los equipos con aquellos especificados en la capa de distribución y poder mantener una velocidad de transmisión entre ellos acorde a la norma IEEE 802.3ab

Los dispositivos ubicados en el área de trabajo (computadoras, impresoras, etcétera) estarán conectados a los elementos de *switcheo* de la capa de acceso a una velocidad de 100 Mbps; esta velocidad permite un desempeño adecuado de los 24 o 48 usuarios conectados a ellos. La geometría resultante de este diseño es mostrada en la figura 13.

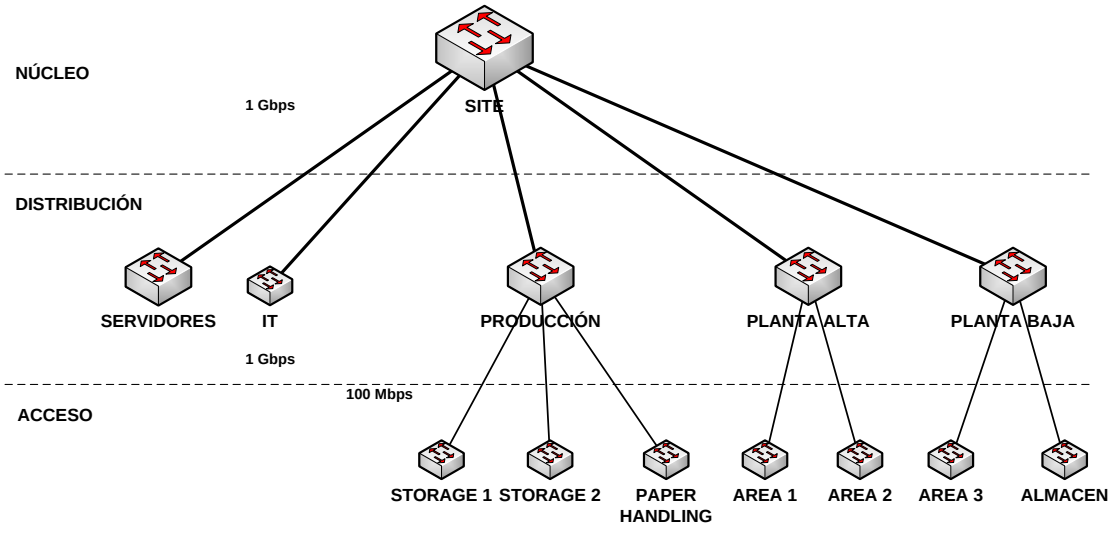


Figura 13. Diseño de *switcheo* jerárquico propuesto para la red de datos.

2.4.3.3 Verificación de la normativa aplicable

Para la plataforma técnico-tecnológica, existía un solo aspecto que requería del cumplimiento específico de alguna normativa, se trataba del cableado estructurado. Este es un aspecto muy amplio, ya que múltiples organizaciones se han involucrado en el desarrollo de estándares asociados con el cableado de redes. Algunas de esas organizaciones se han enfocado en desarrollar especificaciones para la fabricación y prueba de componentes, mientras que otras han trabajado los lineamientos para el diseño, instalación o administración de las infraestructuras de cableado. Para la realización de este proyecto se recurrió al segundo enfoque con la finalidad de cumplir, en la medida de lo posible, con la normatividad existente.

Los seis subsistemas de un sistema de cableado estructurado según la norma ANSI/TIA/EIA-569-A

Acometida al edificio

La acometida al edificio proporciona el punto en el cual los cables exteriores y el cableado dorsal son interconectados. Los requerimientos físicos de la interconexión de la red son definidos en el estándar ANSI/TIA/EIA-569-A (s.f.). Commercial Building Standards for Telecommunications Pathways and Spaces. Obtenido de https://www.belden.com/docs/upload/2030.pdf

En el caso de BDT, existen dos puntos de acometida; uno anterior, y uno posterior.

Anterior: Es el punto de acometida más antiguo y proviene de la parte frontal del edificio de manera subterránea por medio de cuatro tubos de PVC de 1½" de diámetro cada uno. Este acceso cuenta con un registro (40 CMS *a* x 109 CMS *l* x 50 CMS *h*) a una distancia aproximada de 20 metros de su destino final en donde es terminado en un registro empotrado en uno de los muros del MDF[27]. Esta acometida proporciona el ingreso de 6 líneas telefónicas analógicas.

[27] Main Distribution Frame (MDF): Punto de distribución principal que recibe, por un lado, los servicios vitales y, por otro lado, entrega las líneas de conexión hacia el usuario final por medio de los IDF.

Posterior: El segundo punto de acometida proviene de la parte posterior del edificio, lugar donde se ubica la antena de microondas, la cual provee los servicios tanto de telefonía como de acceso a Internet; el cable proveniente de la antena es conducido hasta su destino final por medio de una escalerilla de aluminio de 6” que “corre” por encima del plafón de la planta baja y termina en el piso intermedio del MDF.

Ambas acometidas tienen como destino final el MDF de la red de la compañía, ubicado en la segunda planta del edificio.

Cuarto de equipamiento

Un cuarto de equipamiento es esencialmente un closet de telecomunicaciones grande que puede contener el MDF, conmutador, protección eléctrica secundaria, etcétera. El cuarto de equipamiento comúnmente se ubica contiguo a la acometida al edificio o a un centro de cómputo para compartir el aire acondicionado, seguridad, control de incendios, iluminación y acceso controlado.

El cuarto de equipamiento en BDT alberga –de hecho- todos los elementos arriba señalados en una sola habitación. Sus especificaciones son las siguientes:

- Ubicado en la segunda planta del edificio se encuentra alejado de transformadores y motores eléctricos o de cualquier fuente generadora de interferencia electromagnética considerable. Al encontrarse en un segundo nivel, el lugar resulta difícil de inundarse.
- El cuarto cuenta con piso y techo falso registrables en color blanco, de igual forma las paredes del cuarto están pintadas en el mismo color.
- Debajo del piso falso y encima del plafón, se ubican escalerillas de aluminio de 6” de ancho que contienen los cables que parten hacia los diferentes IDF.
- El acceso al cuarto está limitado por una puerta doble sin cerradura, pero el cuarto se encuentra dentro de una habitación a la que solo tiene acceso el personal autorizado por medio de una puerta con cerradura.

- El control de la temperatura es proveído por dos sistemas de aire acondicionado; uno de ellos se encuentra operando las 24 horas del día durante los 365 días del año, y el segundo opera durante las horas hábiles de la compañía. La temperatura promedio dentro del cuarto es de 22° C
- La iluminación del lugar es proveída por dos módulos que contienen tres tubos fluorescentes ubicados a 3.0 metros de altura.
- La alimentación eléctrica es proveída por dos líneas separadas de 120 VAC a 10A, a las cuales se conectan cuatro equipos de alimentación eléctrica ininterrumpida (UPS por sus siglas en inglés) con capacidad de 3kVA cada uno.
- Existen conectores eléctricos tipo NEMA L5-15R y NEMA 5-15R ubicados por debajo del piso falso registrable. Las líneas eléctricas están –adicionalmente- conectadas en paralelo a una planta generadora de electricidad de emergencia que entra en operación a los 10 segundos de que se detecta una falla en el suministro eléctrico.

Cableado dorsal

El cableado dorsal proporciona interconexión entre los closets de telecomunicaciones, los cuartos de equipamiento y las diferentes acometidas. Consiste de cables dorsales, puntos –principales e intermedios- de conexión cruzada, terminaciones mecánicas y cables de parcheo.

En BDT el cable dorsal estaría implementado por medio de cable UTP categoría 6 del tipo no pleno. Este tipo de cableado, adicionalmente cumple con las normas TIA/EIA-568-B e ISO/IEC-11801. Debido a la distribución arquitectónica de la nave industrial, no es posible ubicar los closets de telecomunicaciones uno sobre otro por lo que el cable dorsal “sufre” de más de dos dobleces de 90 grados en algunas de sus trayectorias.

Closet de telecomunicaciones

El closet de telecomunicaciones en cada piso es el punto de unión entre el cableado dorsal y las trayectorias horizontales. Contiene equipamiento activo para voz y datos, puntos de terminación y cableado de conexiones cruzadas.

En BDT solamente existen dos puntos que –por cumplir con el área mínima de $9m^2$ para un closet- pueden ser considerados como closet de telecomunicaciones, sin embargo –para fines prácticos- se considera a los diferentes IDF como si fuesen closet de telecomunicaciones debido a que cumplen con esa función.

Ya que el único equipo alimentado por electricidad en los closets o IDF son los *switches*, y que éstos no generan demasiado calor, los closets no cuentan con aire acondicionado exclusivo, sino que utilizan el existente dedicado a uso general. De cualquier forma, el acceso a estos closets está limitado, ya sea por puertas con cerradura, o por encontrarse localizados fuera del alcance inmediato de personas ajenas (ubicado a 6 metros del piso) o ambas.

Cableado horizontal

El sistema de cableado horizontal se extiende desde el conector de telecomunicaciones en el área de trabajo hasta el closet de telecomunicaciones y consiste de:

- Cableado horizontal
- Conector de telecomunicaciones
- Terminación de cableado
- Conexiones cruzadas

El cableado horizontal en BDT estaría basado en tramos de cable UTP categoría 5e (4 pares, 100 Ω, conductores sólidos calibre 24 AWG) que no excedieran los 90 metros que deben existir –de acuerdo a la norma- entre puntos de interconexión.

La mayor parte de este cableado es distribuido por medio de escalerillas de aluminio de 6” y de éstas por tubos de PVC o *conduit* con diámetros desde ¾” hasta 1½” que conducen los cables hasta terminar en las cajas donde se ubican los conectores de telecomunicaciones. Éstos se presentan en dos tipos, categoría Giga Ethernet y categoría 5e.

Los puntos de terminación son implementados por paneles de parcheo tipo 1100GS3 GigaSPEED XL ya sea de 24 o 48 puertos según sea requerido, su desempeño eléctrico está garantizado para cumplir o exceder las especificaciones TIA/EIA-568-B.2-1 Categoría 6, e ISO/IEC Categoría 6/Clase E.

Los medios de conexión cruzada son cables de parcheo modulares del modelo GS8E con distancias que oscilan entre los 6 y los 20 metros, dependiendo del lugar en el que se utilicen, siguiendo un código de colores de acuerdo a su uso (azul para voz, rojo para datos).

Los conectores de telecomunicaciones son del tipo MGS400 GigaSPEED XL cuyo desempeño eléctrico está garantizado para cumplir o exceder las especificaciones TIA/EIA-568-B.2-1 Categoría 6, e ISO/IEC Categoría 6/Clase E. Además, puede manejar cables de categoría inferiores, tales como 5e, 5, y 3.

Debido a la configuración del mobiliario y la distribución arquitectónica, desafortunadamente no se puede cubrir la norma en cuanto a la longitud máxima permitida para los cables de conexión en el área de trabajo, siendo en muchos de los casos mayores a los 3 metros especificados en el estándar; de cualquier forma, **sí** se respeta que la longitud final entre equipo activo y equipo activo no sea mayor a los 100 metros indicados en la norma.

Área de trabajo

Los componentes del área de trabajo se extienden desde el conector de telecomunicaciones hasta la estación de trabajo. El cableado de esta área está diseñado para permitir cambios rápidos y sencillos a las conexiones, de forma que los cambios y crecimientos puedan ser administrados fácilmente.

Los elementos básicamente son los cables de conexión con las características ya mencionadas en el subsistema anterior.

Un resumen de las especificaciones de desempeño de los diferentes componentes del cableado de red, se incluye en la sección de Anexos, *Características de los componentes del cableado de red* al final de este documento.

2.4.3.4 Definición de los servicios inalámbricos

Con la intención de que los usuarios de equipos portátiles de cómputo (*notebooks*, *laptops*, *PDA*, etcétera) explotasen las capacidades de portabilidad de sus equipos, se observó la necesidad de contar con un punto de acceso inalámbrico de manera que su operación no estuviera sujeta o limitada a una sola ubicación dentro de la nave industrial, sino que pudiera ser llevada a cabo desde prácticamente cualquier lugar dentro de las instalaciones de la compañía.

Considerando que la totalidad de los equipos portátiles no excedía –en ese entonces- las 20 unidades y que la mayoría de ellos demandaban una movilidad bastante limitada, se propuso la utilización de un solo punto de acceso (*Access Point o AP*) para satisfacer esta necesidad, y dado que el área que dicho punto debía de cubrir era –por lo tanto- limitada, se propuso un equipo que cumpliese con la norma IEEE 802.11g con velocidad de operación máxima de 54 Mbps.

Haciendo caso de las anteriores consideraciones, y al revisar los planos arquitectónicos y de servicios, también se estableció que la ubicación más idónea del AP era en el área del Almacén, conectándolo al equipo activo que se encontraría en el IDF[28]-06, ubicación desde la cual se establecería un "círculo" de cobertura con un radio aproximado de 100 metros, suficiente para cubrir la totalidad del área del edificio.

[28] *Intermediate Distribution Frame* (IDF): dentro de los elementos físicos de un cableado estructurado, el IDF es un punto de distribución de los servicios de red; por un lado, recibe dichos servicios y, posteriormente, los entrega al usuario final, comúnmente por medio de equipos activos y paneles de conexión.

De cualquier manera, se previó que conforme la configuración del área fuese cambiando (anaqueles o mobiliario que pudiesen crear interferencias al AP), sería necesario reconsiderar su ubicación, agregar antenas externas o integrar unidades adicionales que permitiesen incrementar la potencia de la señal y/o el área de cobertura.

Debido a que las conexiones inalámbricas son demasiado susceptibles de ataques a su seguridad; se recomendó la utilización del siguiente esquema de operación de las mismas:

- Cambiar el SSID[29] de fábrica por uno propio y no mostrarlo ni hacerlo público
- Cambiar la contraseña de administrador de fábrica por una propia
- Utilización de WEP[30] como forma de encriptación
- Habilitación de las listas de direcciones MAC[31] como forma de autenticación

Este esquema de operación podría ser modificado conforme algunas formas de seguridad fuesen implementadas tanto en el AP como en los equipos que tuviesen acceso a él.

[29] *Service Set Identifier* (SSID): en las redes WiFi, el SSID es un código integrado a todos los paquetes para identificar cada paquete como parte de esa red. El código consiste de un máximo de 32 caracteres alfanuméricos. Además de identificar cada paquete, el SSID también sirve para identificar de manera única a cada grupo de dispositivos de red inalámbricos.

[30] *Wireless Equivalent Privacy* (WEP): protocolo de privacidad especificado en la norma IEEE 802.11 que proporciona a los usuarios de acceso inalámbrico a una red, la protección contra "escuchas secretas" realizadas por personas ajenas a la red.

[31] Dirección tipo *Media Access Control* (MAC): es un identificador único asignado a interfaces de red para comunicaciones en el segmento de la red física (subcapa del protocolo de control de acceso al medio del modelo OSI). Se representa por seis grupos de dos dígitos hexadecimales, separados por guiones (-) o dos puntos (:) de acuerdo con la norma IEEE 802.

2.4.3.5 Definición del esquema de seguridad en el acceso a Internet

El esquema de seguridad propuesto para el acceso a Internet, ya sea para navegación o para uso del medio como canal de comunicación, se compone de tres elementos básicos:

- **Hardware y software de contención**. Los componentes de hardware propios para el acceso a Internet, navegación y seguridad, serían un dispositivo físico (*appliance*) para los servicios de firewall, y un servidor autónomo para los servicios de proxy; ambos harían uso de sus respectivas aplicaciones de software. Adicionalmente se contaría con un antivirus dedicado a monitorear las descargas y envíos de paquetes desde/a Internet.
- **Perfiles de usuario**. Se definirían los niveles y tipos de acceso para cada perfil de usuario de acuerdo con sus niveles de responsabilidad, actividades, y puesto dentro de la organización.
- **Políticas de acceso**. Se establecerían las políticas –en términos de gobernanza- aplicables para la utilización adecuada del acceso a Internet por parte de los usuarios finales.

Hardware y software de contención - Firewall

La operación del firewall se basa en el software que el dispositivo tiene instalado. El software de Astaro está compuesto de seis elementos; *Firewall*, *gateway* para VPN[32], Protección anti-*spam*, Protección de navegación, Protección anti-virus, y Protección contra intrusiones; la plataforma propuesta contemplaba la utilización de cuatro de estos elementos, dejando fuera las protecciones anti-spam y anti-virus, ya que ambos aspectos serían cubiertos por otras herramientas.

[32] Virtual Private Network (VPN): Una red virtual privada es una configuración que permite extender una red privada –de área local- haciendo uso de redes públicas o el Internet para conectarse con otra red privada. Este concepto permite que los usuarios envíen y reciban información –de otras redes- en sus equipos como si estuviesen conectados directamente a esa otra red diferente a la suya.

La funcionalidad de esos cuatro elementos, se menciona a continuación:

- *Firewall*: Elemento basado en Linux maneja el tráfico de comunicaciones de entrada y de salida; los administradores pueden bloquear o permitir el acceso, por protocolo, a cada red interna, servidor, servicio, y grupo de usuarios. El *firewall* inspecciona tanto a la información de la red (encabezados de los paquetes) como información de las aplicaciones con la finalidad de detectar y bloquear tráfico sospechoso.
- *Gateway para VPN*: Permite conectividad de redes virtuales privadas (VPN por sus siglas en inglés; para intercomunicar, tanto a la oficina local con el corporativo, como a los usuarios móviles (*road warriors*) con la red empresarial.
- *Protección de navegación:* Esta protección se compone básicamente de dos técnicas: el filtrado de contenido o de URL, y la protección anti-*spyware*.
- *Protección de intrusiones*: El *firewall* cuenta con un conjunto de criterios de detección extensiva que utiliza una base de datos de cerca de 2,000 reglas para detectar patrones específicos de vulnerabilidades.

Una descripción detallada de estos cuatro aspectos se incluye en el apartado de Anexos, Especificaciones detalladas del dispositivo firewall y sus componentes.

Hardware y software de contención - Proxy

Un servidor proxy es una computadora que funciona como un intermediario entre un navegador de Internet (Internet Explorer, Google Chrome, Mozilla Firefox, etcétera) y el Internet mismo. Los servidores proxy ayudan a mejorar el desempeño de acceso a la web ya que almacena una copia de las páginas web que más frecuentemente se usan; de esta manera, cuando un navegador solicita alguna página web almacenada en la colección del servidor proxy (su cache), ésta es proveída por el servidor proxy, lo cual es mucho más rápido que ir hasta el sitio en Internet. Los servidores proxy, además ayudan a mejorar la seguridad de acceso a Internet al filtrar algo del contenido web y de software malicioso.

Tal como se mencionó en el apartado 2.4.2.1, *Elección del Sistema Operativo de red*; la suite elegida incluiría inicialmente el software Microsoft Proxy Server, el cual se actualizaría posteriormente a Microsoft Internet Security and Acceleration (ISA Server). Este software permitía una integración total con las cuentas de usuario (establecidas en el *Active Directory*), lo cual permitiría un acceso correcto al tipo de contenido para el cual el usuario estaba autorizado.

A diferencia del firewall, que se trataba de un dispositivo específico, el software Microsoft Proxy sería instalado en un servidor autónomo, pero que podría tomar otros roles propios de un servidor, tales como servicios DNS, IIS, etcétera.

Para poder realizar sus funciones, el servidor proxy contaría con dos tarjetas de red; una para conectar el equipo a la red de área local, y otra para conectarlo a Internet, tal como se muestra en la figura 14. El servidor proxy no solo hace cache del contenido al que se ha tenido acceso, también realiza filtrado de contenido y permite que las conexiones provenientes de la red local de datos permanezcan anónimas, ya que el servidor destino solo tendrá referencia de la dirección IP pública del servidor proxy.

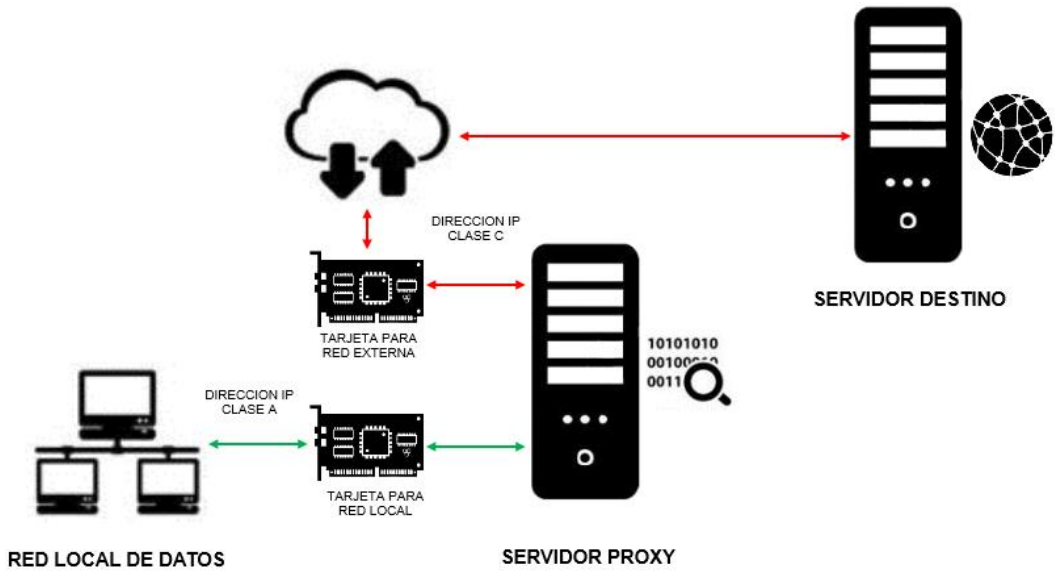


Figura 14. Conectividad del servidor proxy, mostrando el flujo entre la red local de datos y el acceso a sitios en Internet.

Hardware y software de contención – Antivirus

Las aplicaciones antivirus son la protección mínima indispensable que cualquier organización debe tener en mente en términos de seguridad informática. Los virus, gusanos y otro software malicioso ingresan a las redes de datos de las compañías, ya sea por medio de los servidores de correo electrónico como por medio de descargas de archivos realizadas directamente por los usuarios; considerando como descargas, no solo aquellas realizadas desde sitios de Internet, sino todas aquellas copias de archivos realizadas desde cualquier medio de transporte digital, tales como discos CD, DVD, cintas, memorias flash USB o de otros tipos, etcétera. el *firewall* seleccionado cubre ambos puntos.

Para cubrir este aspecto tan importante, también se realizaron evaluaciones de diferentes suites antivirus que existían en el mercado; obviamente quedaron excluidas todos aquellos productos denominados como “gratuitos”, ya que la gratuidad en este tipo de aplicaciones viene a cambio de limitaciones en las capacidades de su operación. Se evaluaron los productos líderes del mercado de esa ápoca y se consideró enormemente la existencia de una buena disponibilidad de oficinas de soporte para las diferentes opciones.

Finalmente, se optó por la suite VirusScan Enterpise versión 8.0i, fabricada en ese tiempo por Network Associates bajo el nombre de McAfee Labs. Esta suite antivirus incluía protección tanto para servidores como para equipos de escritorio. Una descripción detallada del funcionamiento del antivirus, se incluye en el apartado de Anexos, *Especificaciones de operación del antivirus*.

Perfiles de usuario

Todas las cuentas de usuario fueron creadas bajo un perfil acorde con el tipo de actividad que su propietario realizaría; así habría cuentas para operadores, limitadas al acceso a una o dos aplicaciones además de la típica suite de escritorio Office (en diferentes versiones e idiomas), hasta cuentas del área gerencial con acceso a la mayoría de las aplicaciones y fuentes de información de las denominadas “confidenciales”, tales como volúmenes de producción y ventas,

órdenes de compra y manufactura, así como los precios de los productos entre otras.

La separación inicial entre usuarios con acceso limitado y aquellos con mayores niveles de acceso se detalla al generar dos grupos primarios, los cuales son representados gráficamente en la figura 15.

Figura 15. Definición primaria de grupos de usuarios y las aplicaciones básicas a las que tendrían acceso.

Los usuarios incluidos dentro del grupo *Operators* fueron aquellos que esencialmente contarían con acceso a las aplicaciones MES y ERP y no tendrían -en su mayoría- acceso al correo electrónico, a la navegación en Internet, ni al contenido de algunas carpetas compartidas ubicadas en algún elemento de almacenamiento de red; a excepción de aquellas carpetas que contuviesen información específica para sus actividades, tales como instrucciones de trabajo. Los operadores de manufactura y del almacén pertenecían a este grupo.

Al grupo *Non Operators* pertenecería todo el personal que debiese contar con acceso más amplio a los recursos compartidos por medio de la red y a las aplicaciones en general. La mayoría del personal de tipo administrativo (incluidas las ingenierías de producto y de procesos) o no directamente involucrado con la manufactura pertenecía a este grupo.

La razón primordial de establecer estos dos grupos era para evitar o reducir el mal uso o abuso de los recursos que brindaría la red de datos, así como la de optimizar el uso de los mismos al asignarlos a quienes realmente los requirieran.

Políticas de acceso

Debido a que Internet es una herramienta poderosa y que su uso se estaba volviendo cada vez más frecuente para fines privados, la segunda división entre usuarios fue realizada con la finalidad de evitar abusos en la utilización de esta herramienta dentro de la compañía. Los usuarios fueron agrupados de acuerdo con el tipo de acceso con el que deberían de contar para utilizar Internet; estos grupos fueron: Internet_A, Internet_B, e Internet_C.

Con la intención de poder establecer los mecanismos de control apropiados, se generaron las políticas de acceso de acuerdo con cada uno de los grupos, así como una política restrictiva general para evitar la ejecución de música, radio, vídeo, *chat*, etcétera desde los navegadores de Internet.

De esta manera, los usuarios pertenecientes a Internet_C solamente contarían con acceso a las páginas propias de la compañía (intranet, *web portal*, etcétera), los usuarios del grupo Internet_B contarían con el acceso anterior y adicionalmente podrían realizar consultas y transacciones en las páginas de servicios, tales como e-gobierno, bancos, teléfono, educativas, etcétera. Además, este grupo tendría acceso a una limitada cantidad de páginas de búsqueda, diccionarios, enciclopedias, etcétera, como apoyo para la realización de sus actividades.

Finalmente, los usuarios incluidos en Internet_A serían aquellos con acceso ilimitado a Internet. Haciendo uso de estos tres grupos, la administración podría volverse relativamente sencilla, ya que, al presentarse cambios de actividades de un usuario, su acceso a Internet podría modificarse rápidamente.

El esquema mostrando las relaciones entre grupos de usuarios y tipos de acceso a Internet se detalla a continuación.

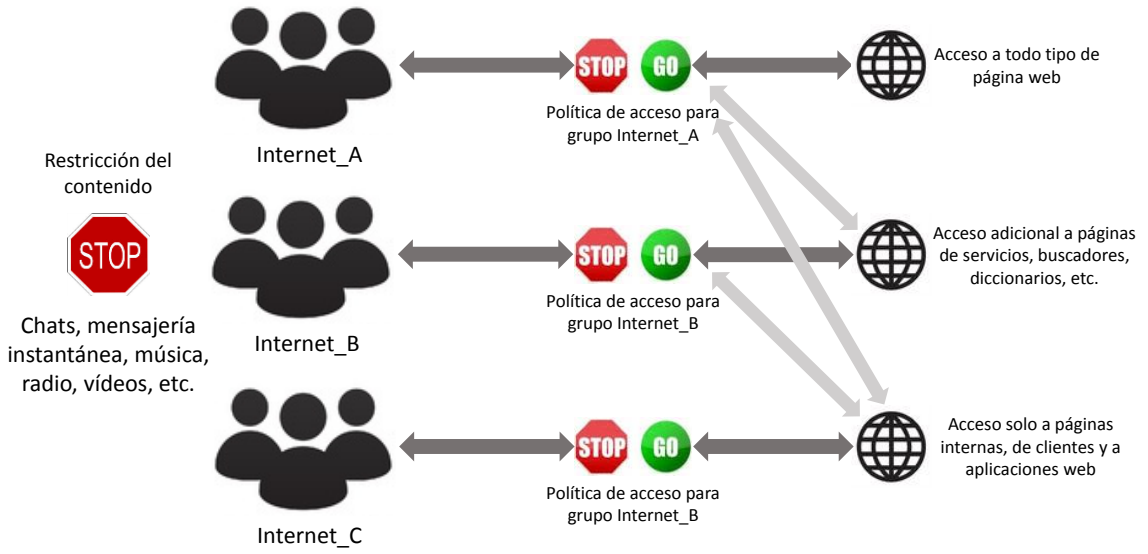


Figura 16. Definición de grupos de usuarios por su nivel de acceso a Internet y las políticas aplicables a éstos.

Obviamente podrían existir más grupos de trabajo que servirían para organizar la manera de trabajar de cada departamento o área funcional, los cuales –de hecho- se fueron creando e integrando a la plataforma conforme fueron siendo requeridos.

2.4.3.6 Especificación del esquema de tolerancia a fallas y redundancia

Los esquemas de redundancia y tolerancia a fallas fueron considerados con la finalidad de poder proporcionar los servicios ofrecidos por la plataforma, aún cuando algún elemento de ésta se encontrase fuera de operación o presentando fallas en su funcionamiento.

Por el tipo de operación de la compañía, los elementos redundantes de tipo *hot-swap*, *hot-plug* o *stand by*, resultaban ser los más adecuados a nivel de servidores, almacenamiento masivo y de *firewall*. El resto de los equipos utilizados, contaban con una menor propensión a fallas, o su reemplazo y configuración podía realizarse de manera rápida, razón por la cual no era necesario contar con unidades en paralelo para cubrir su función, o bien, eran menos críticos para la operación de la compañía.

A nivel de conectividad, se propuso un esquema de cableado que permitiese que cada punto de distribución de la señal de red, tuviese al menos una segunda trayectoria de conectividad, de forma que, en caso de existir un corte en algún punto del cableado dorsal, siempre se mantuviese la conectividad en sus extremos. Este esquema es detallado más delante en el apartado de implementación del esquema general de redundancia.

Debido a que la mayor cantidad de la información ubicada en los servidores de la plataforma se utilizaría para las actividades diarias de la compañía, se evidenció la necesidad de realizar respaldos de esa información en algún medio magnético u óptico que permitiesen la posterior recuperación de los datos en caso de que el servidor o los servidores que contuviesen la información en línea llegasen a dañarse o no se encontrasen disponibles por cualquier motivo.

2.4.3.7 Establecer el costo de implementación del diseño

Este apartado es tratado de manera superficial debido a su naturaleza delicada; solamente se incluye un resumen con un costo aproximado de implementación de la propuesta, con cantidades no son exactas, sino orientativas.

COSTO DE IMPLEMENTACIÓN DE RED LOCAL DE DATOS				
Concepto	**Unitario Dólares**	**Cantidad**	**Unidad de Medida**	**Total Dólares**
3Com SuperStack 3 switch 4924 3C17701-US	$4,358.50	2	Piezas	$8,717.00
3Com SuperStack 3 switch 4900 3C17700	$3,507.50	3	Piezas	$10,522.50
3Com SuperStack 3 switch 4250T 3C17302-US	$1,138.50	8	Piezas	$9,108.00
3Com SuperStack 3 switch 4228G 3C17304-US	$500.25	1	Pieza	$500.25
3Com 1000Base-T GBIC 3CGBIC93A	$345.00	2	Piezas	$690.00
3Com Wireless LAN Access Point 7250 3CRWE725075A	$650.00	1	Pieza	$650.00
SYSTIMAX GigaSPEED XL Cable (305m) 1071-004ESL	$174.00	25	Piezas	$4,350.00
SYSTIMAX GigaSPEED XL Outlet MGS400BH-317	$12.00	159	Piezas	$1,908.00
SYSTIMAX Faceplate 197613	$2.50	49	Piezas	$122.50
SYSTIMAX GigaSPEED XL Modular Patch Panel 24 puertos	$260.00	6	Piezas	$1,560.00
SYSTIMAX GigaSPEED XL Modular Patch Panel 48 puertos	$520.00	7	Piezas	$3,640.00
SYSTIMAX GigaSPEED XL Patch Cord CPC3312-02(7)F006 (Azul o rojo)	$15.00	159	Piezas	$2,385.00
PANDUIT TX-6 Plus Modular Plug RJ-45 SP688-C	$2.00	186	Piezas	$372.00
Chatsworth CPI Aluminum rack 45U, 7'	$250.00	4	Piezas	$1,000.00
Blackbox Elite Wallmount Cabinet 12U, 24" RM339A	$1,000.00	4	Piezas	$4,000.00
Blackbox Wallmount cabinet dual-fan kit RM386	$200.00	4	Piezas	$800.00
Escalerilla de aluminio de 6" de ancho	$9.00	140	Metros	$1,260.00
Tubería estimada (incluída en la construcción inicial)	$2,520.00	1	Evento	$2,520.00
Cancelería para IDF a nivel de piso	$1,500.00	1	Evento	$1,500.00
Mano de obra e instalación	$10,860.00	1	Evento	$10,860.00
Costo total estimado de implementación				**$66,465.25**

Tabla 7. Costo de implementación aproximado de la red local de datos para 250 nodos.

A partir de esta información, podemos determinar un costo estimado de $266.00 dólares por nodo de red instalado.

De igual forma, en la tabla 8, se muestra el costo estimado de la implementación de los servidores y de la red de área de almacenamiento. Debe aclararse que el costo derivado de algunas adecuaciones, tales como instalaciones eléctricas específicas, obras civiles, etcétera, no ha sido incluido en este apartado, debido a que fue absorbido por otras áreas y cargado a sus presupuestos. Tampoco se han incluido los costos por licenciamiento de software, el cual se asoció a la operación del área de TI corporativa; ni el costo de las computadoras personales, el cual se asoció al costo individual del personal. Esto con la finalidad de asociar los costos de manera adecuada.

Mención aparte debe hacerse del costo de operación de la plataforma técnico-tecnológica, ya que incluye gastos recurrentes por acceso a Internet, contratos de servicio y/o garantías extendidas, etcétera, los cuales, tampoco son considerados en este estimado de costo de implementación.

COSTO DE IMPLEMENTACIÓN DE SERVIDORES Y RED DE ÁREA DE ALMACENAMIENTO				
HP Cabinet 42U plus tower to rack conversion kits	$5,344.72	1	Kit	$5,344.72
ATEN KVM Switch plus KVM cables for servers	$1,315.60	1	Kit	$1,315.60
HP MSA1000 SAN plus HDDs and all options configuration	$83,873.61	1	Pieza	$83,873.61
HP MSA30 Second Disk Cage for SAN plus HDDs	$13,037.27	1	Pieza	$13,037.27
HP ProLiant ML330 G3 Server for backups process	$4,172.83	1	Pieza	$4,172.83
HP ProLiant ML330 G3 Server for HR-Finance software	$3,973.25	1	Pieza	$3,973.25
HP ProLiant ML370 Server for E-Mail	$15,452.00	1	Pieza	$15,452.00
HP ProLiant ML370 Server for ERP software	$12,620.10	1	Pieza	$12,620.10
HP ProLiant ML370 Server for MES software	$12,552.25	1	Pieza	$12,552.25
HP ProLiant ML370 Server for E-Mail	$14,734.95	1	Pieza	$14,734.95
HP ProLiant ML370 Server for Redundancy strategy	$10,810.00	1	Pieza	$10,810.00
Tripp Lite SmartPro 3000W 2U UPS	$1,093.95	2	Piezas	$2,187.89
HP TFT7600-US Rackmount Keyboard plus 17" LCD	$2,998.05	1	Pieza	$2,998.05
Costo total estimado de implementación				**$183,072.52**

Tabla 8. Costo aproximado de la implementación de los servidores y red de área de almacenamiento de la plataforma técnico-tecnológica.

La suma de los dos rubros más relevantes, se muestra en la tabla 9, el cual se considera el costo aproximado total –expresado en dólares estadounidenses- para fines orientativos en el presente documento.

COSTO TOTAL APROXIMADO DE IMPLEMENTACIÓN DE LA PLATAFORMA	
Costo aproximado de implementación de la red local de datos	$66,465.25
Costo aproximado de implementación de servidores y red de área de almacenamiento	$183,072.52
Costo total aproximado de implementación de la plataforma	**$249,537.77**

Tabla 9. Costo aproximado de la implementación de la plataforma técnico-tecnológica.

2.4.4 Etapa de implementación y monitoreo de la plataforma

En esta etapa, se realizó la integración de los diferentes elementos o grupos de elementos individuales o específicos de cada área de la plataforma técnico-tecnológica. Es por esta razón, que el reporte se desarrolla desde lo micro a lo macro de dicha plataforma, esto último evidenciando la integración final de la plataforma.

2.4.4.1 Configuración de los servidores y periféricos

Servidores

Tal como ya se mencionó en el apartado 2.4.3, *Etapa de diseño de la plataforma*, se utilizarían cinco servidores de categoría crítica y dos servidores de categoría secundaria. Los servidores de categoría crítica serían utilizados de la siguiente forma: uno para los roles de PDC, servidor de archivos, uno para correo electrónico, uno para almacenar el sistema ERP y su base de datos operativa, uno más para almacenar el sistema MES y su base de datos operativa, y un quinto servidor que estaría en modo de espera a ser utilizado en caso de que alguna contingencia causase la indisponibilidad de alguno de los otros tres servidores.

Los servidores de categoría secundaria, serían utilizados para las aplicaciones de tipo financiero y de recursos humanos, y para la realización de los respaldos de la información en cintas. La tarea fundamental de estos siete servidores sería precisamente la de brindar la capacidad de cómputo centralizado

para esas labores de manera que dichas aplicaciones y servicios estuviesen disponibles para los múltiples clientes o usuarios de la plataforma.

El hardware utilizado sería de características idénticas para los cinco servidores de categoría crítica, lo cual obedecía a un requerimiento del esquema de tolerancia a fallas y redundancia que será detallado más delante. Para los servidores secundarios se eligió un equipo menos robusto que para los de categoría crítica, pero siendo de características idénticas entre sí.

Una descripción detallada de la configuración de estos equipos, así como de sus características más relevantes se incluyen en el apartado de Anexos, *Características y configuración de los servidores*.

Adicionalmente, se configuraron dos periféricos críticos para la plataforma técnico-tecnológica: 1) el equipo destinado a la red de área de almacenamiento (SAN) y 2) el equipo de respaldos en cintas (biblioteca de cintas), este último para realizar los trabajos de respaldo de información crítica.

Red de área de almacenamiento

Tal como lo mencioné en la etapa de diseño de la plataforma, se utilizaría un equipo MSA 1000 que serviría de almacenamiento masivo centralizado; su configuración se realizó en dos pasos: 1) se instalaron todos los componentes de hardware necesarios para su configuración, y 2) se crearon los arreglos de discos y sus volúmenes correspondientes, los cuales fueron también habilitados para su utilización desde los diferentes servidores.

La figura 17 muestra el diagrama conceptual de la conectividad del equipo MSA 1000 y un gabinete MSA 30 adicional, conformando la red de área de almacenamiento. Como puede notarse, existe conectividad entre cada servidor de categoría crítica y el equipo MSA 1000. Los servidores de categoría secundaria también tendrían acceso a la SAN, pero por medio de los servidores de categoría crítica y no directamente, de igual forma los demás equipos conectados a la red local de datos.

De acuerdo con esta propuesta, los servidores fungirían como puentes entre las computadoras de los usuarios finales y la información contenida en la SAN (o su espacio de almacenamiento disponible), por lo que sería necesario que los servidores estuviesen disponibles para que los usuarios y las aplicaciones pudiesen hacer uso de dicha información o espacio de almacenamiento.

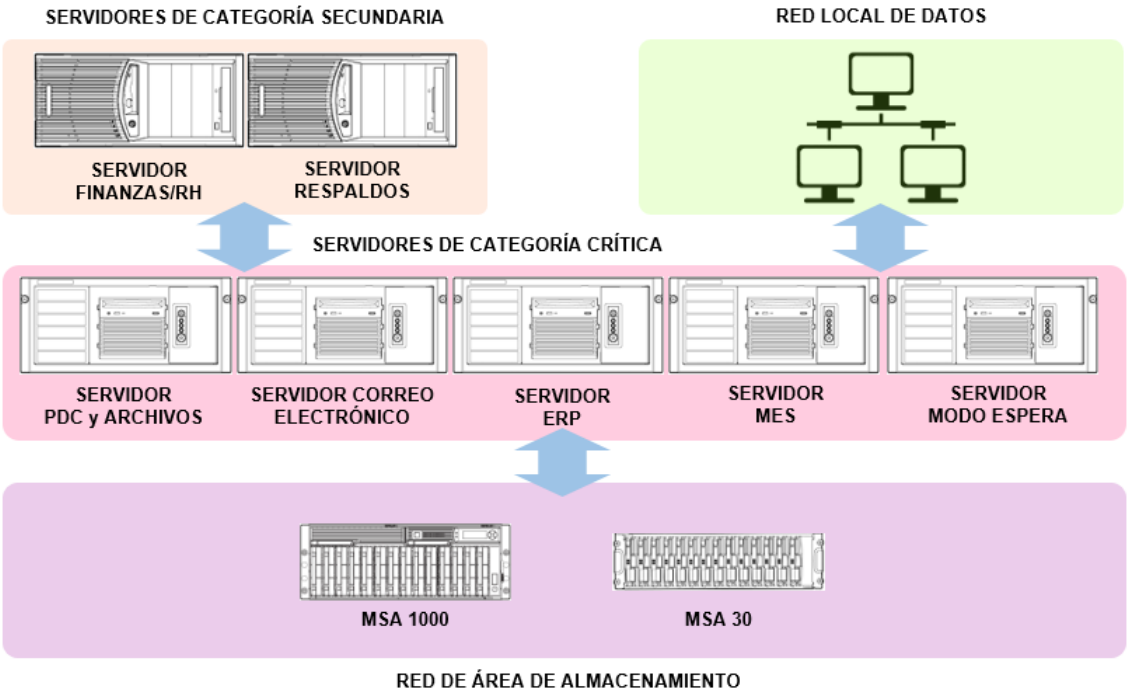


Figura 17. Diagrama conceptual de conectividad entre los módulos de la SAN (MSA 1000 y MSA 30), así como entre la SAN y los diferentes servidores y la red de datos.

Una descripción detallada de las configuraciones física y lógica de la red de área de almacenamiento se incluye en el apartado de Anexos, *Configuración de la SAN*, al final del presente reporte.

Biblioteca de cintas

El segundo periférico de importancia es el equipo destinado a la realización de respaldos en cintas. En el apartado 2.4.3, *Etapa de diseño de la plataforma*, se definió la utilización del equipo HP MSL4048; de hecho, este equipo fue manufacturado internamente ex profeso para cubrir las necesidades de respaldos en cinta que la plataforma pudiese requerir.

Este equipo estaría conectado a uno de los servidores secundarios, anteriormente señalados, y a través de dicho servidor y por medio del software de gestión de respaldos Veritas, se podrían realizar respaldos, tanto en línea como fuera de línea en dos cartuchos de cintas paralelamente. La figura 18 muestra el diagrama conceptual de conectividad de dicha biblioteca de cintas.

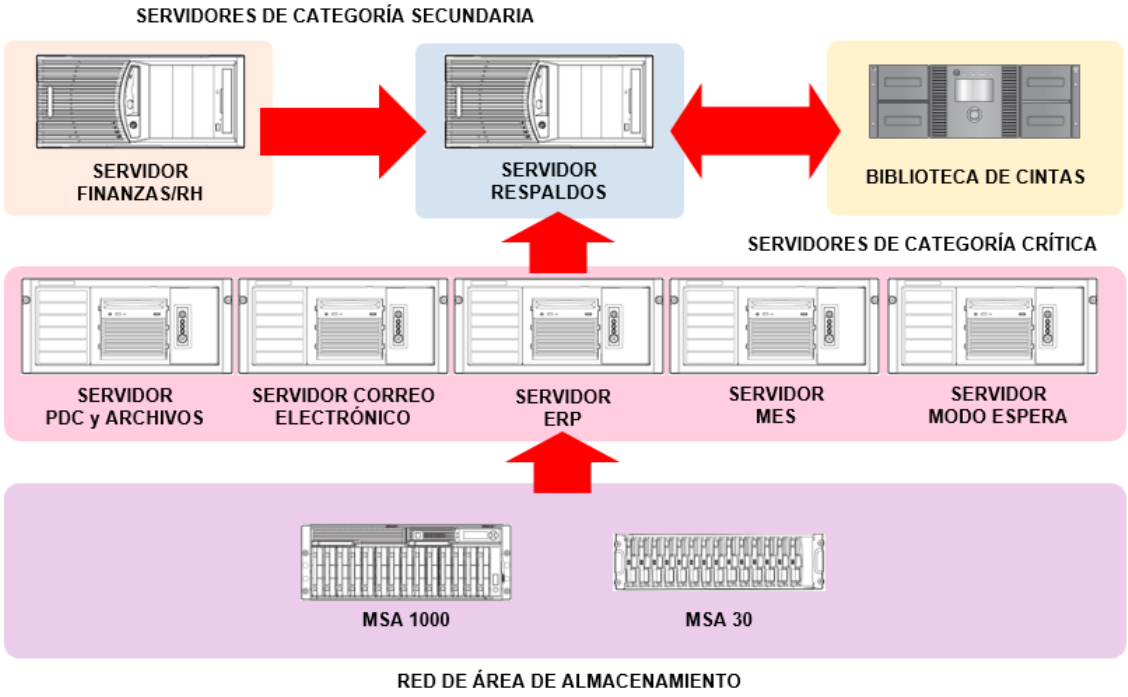


Figura 18. Diagrama conceptual del flujo de información entre las diferentes fuentes de almacenamiento masivo y la biblioteca de cintas para la realización de sus respaldos.

La configuración de dicho equipo, constaba de dos controladores que podrían trabajar paralela o alternadamente, según fuese necesario. Su capacidad de 48 cintas de tipo LTO-3 (400GB nativos/800GB comprimidos), permitiría un ciclo largo de retención de cintas, y una capacidad total de almacenamiento cercana a los 37.5TB, muy por encima de los requerimientos de respaldo de la plataforma, pero previsto para crecimientos futuros.

Las imágenes utilizadas en las figuras 17 y 18 proceden de

HP ProLiant ML370 (G3) Quick Specs (2005) [Guía rápida de especificaciones], obtenida de https://h10057.www1.hp.com/ecomcat/hpcatalog/specs/emeapsg/99/HP_ProLiant_ML370_Generation_3.pdf,

HP ProLiant ML330 (G3) Quick Specs (2005) [Guía rápida de especificaciones], obtenida de https://www.hpe.com/h20195/v2/getpdf.aspx/c04283012.pdf

HP StorageWorks Modular Smart Array 1000 for Small Business SAN G2 Kit, Quick Specs (2007) [Guía rápida de especificaciones], obtenida de https://www.senetic.ro/i/objects/HP_literature_emea_en_DA-12095.pdf

HP StorageWorks Modular Smart Array 30 User Guide (2003) [Guía del usuario], obtenida de http://www.istoragenetworks.com/servermanuals/msa30_manual.pdf

HP StorageWorks MSL4048 Tape Library Getting Started (2007) [Guía de inicio rápido], obtenida de http://h10032.www1.hp.com/ctg/Manual/c00908882.pdf

La figura 19 muestra la configuración del servicio de respaldo propuesto para la implementación del proyecto. De igual forma, se indican las aplicaciones a las que se les brinda dicho servicio; las bases de datos de los sistemas ERP y MES eran del tipo Oracle, y la del correo electrónico era la propia de Microsoft Exchange. Para ambos casos se utiliza un “agente” específico en la aplicación que gestiona los respaldos, asegurando que las bases de datos y sus servicios asociados son detenidos y desmontados de manera adecuada antes de ser respaldadas, e iniciadas apropiadamente una vez terminado este proceso.

Figura 19. Diagrama de configuración del servicio de respaldo de información.

En el caso del Exchange, se respalda la base de datos y adicionalmente se respaldan los *transaction logs*, los cuales son archivos donde se almacenan los cambios realizados precisamente a la base de datos; para los archivos de usuarios, se previó la utilización de un agente que permitiese el respaldo de archivos que estuviesen en uso.

De acuerdo con esta configuración, se realizarían respaldos diarios en línea, y al menos una vez a la semana (tentativamente dos veces), se realizarían respaldos fuera de línea de la misma información.

Implementación del Sistema Operativo de Red

Durante la implementación del sistema operativo de red, se especificaron los roles para los diferentes servidores; Controlador Primario del Dominio (PDC por sus siglas en inglés), para uno de los servidores de categoría crítica y servidores miembro para el resto de los servidores de la plataforma. El rol de Controlador de Respaldo del Dominio (BDC por sus siglas en inglés) se le asignó a un equipo de escritorio con hardware robusto, ya que se supone que la utilización de un BDC como PDC (es decir promover el equipo BDC al rol de PDC) debe ser estrictamente temporal mientras se reestablece el equipo PDC original.

Ahora bien, cómo trabajarían en conjunto el PDC y el BDC. En un dominio de Windows NT, solamente uno de sus servidores puede ser PDC; este servidor almacena las cuentas de dominio y la información de seguridad en la copia maestra de la base de datos del directorio. Cuando se realizan cambios a las cuentas de usuario o a la información de seguridad, el PDC registra los cambios en la copia maestra de la base de datos del directorio; el PDC es el único servidor que recibe directamente esos cambios, es decir, almacena una copia de lectura y escritura de esa copia maestra. A diferencia de la unicidad del PDC, en un dominio de Windows NT, puede haber múltiples BDC; en el caso de BDT, se optó por un solo BDC, el cual mantendría una copia de solo lectura de la base de datos maestra del directorio del PDC.

Al contar con un BDC dentro del dominio, se garantizaba que, en caso de que el PDC fallase, ese BDC pudiese ser promovido a PDC para mantener la continuidad de la operación, ya que aseguraría el acceso a los recursos de red, y mantendría la base de datos del directorio accesible para el dominio. Si esto no sucediese así, las computadoras no podrían identificarse con el dominio y por lo tanto no podrían crear el canal seguro necesario para la comunicación entre las computadoras del dominio. Las cuentas de grupos no tendrían acceso a los recursos dentro del dominio, entre otras muchas dificultades para operar.

La posibilidad de poder utilizar un BDC como PDC de manera temporal, radica en el proceso de sincronización de la base de datos del directorio entre ambos equipos; el sistema regularmente sincronizaría el BDC del dominio con la finalidad de mantener esta seguridad centralizada. Cuando se realizó la implementación del sistema operativo de red y se asignaron los roles de PDC y BDC, estos equipos se sincronizaron totalmente de manera automática. Posteriormente, se realizarían sincronizaciones parciales conforme de realizaran cambios a la base de datos del directorio en el PDC. Considerando la eventualidad de una pérdida en la sincronía entre ambos equipos, ya sea por caída del BDC o cortes en la conectividad de la red, el sistema operativo permite la sincronización manual entre ambos equipos.

En BDT, el PDC ejecutaría los servicios DNS, WINS, IIS, entre otros, y su configuración con respecto a la red de datos del corporativo, sería a la par del dominio Windows del mismo; es decir, que tendrían conectividad y relaciones de confianza entre sus miembros, pero pertenecerían –inicialmente- a dominios diferentes.

Para el resto de los servidores, el sistema operativo se instalaría y configuraría de manera similar a como se realiza en una computadora personal, ya que sus roles serían simplemente de pertenencia al dominio. Nótese, que para la totalidad de los servidores el idioma del sistema operativo sería el inglés, esto para facilitar el acceso tanto al personal local como al personal del corporativo en caso de que fuese necesario.

Configuración del Active Directory

En el caso del Active Directory, se inició con una configuración sumamente sencilla; se partió de la generación de cuentas de usuario, y se continuó con la agrupación de los mismos, tal como se ejemplificó en el apartado de *Políticas de Acceso* dentro de la sección 2.4.3.5 Conforme se establecían las necesidades de acceso a los diferentes recursos compartidos, tales como drives de red, impresoras, aplicaciones, y otros más, cada cuenta de usuario se volvería miembro de uno o varios grupos de seguridad que le permitiesen –o denegasen- el acceso a esos recursos.

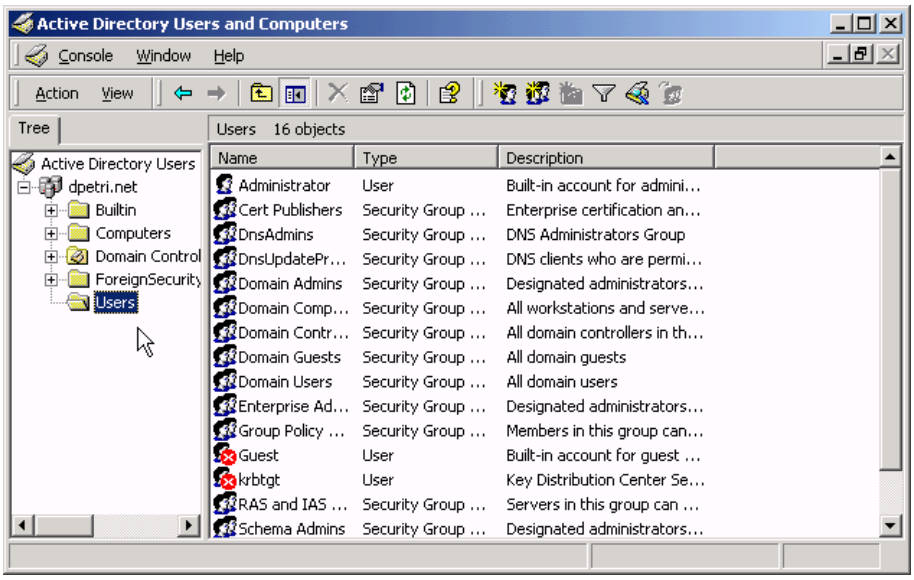


Figura 20. Imagen ilustrativa del complemento Esquema de Active Directory para usuarios y computadoras.

Por medio del Active Directory es que se crearían, modificarían, bloquearían o eliminarían las cuentas para los diferentes elementos del dominio, tales como cuentas de usuario, cuentas de equipos, grupos de seguridad, etcétera.

2.4.4.2 Configuración de los equipos activos y el cableado de red

Los equipos activos fueron configurados de manera que pudiesen cubrir los requerimientos detallados en el apartado 2.4.3.2, *Diseño de la topología de la red*; de igual forma, la disposición física del cableado de la red obedecería a ese mismo diseño topológico.

A continuación, se muestra una de las trayectorias del cableado de red, la ubicación de los gabinetes de distribución intermedia (IDF), así como la ubicación de los nodos de red activos. El resto de las trayectorias se incluye en el apartado de Anexos, *Trayectorias de cableado por área operativa*. Cabe señalar, que, por motivos de confidencialidad, solo se muestran las áreas individuales, y por lo tanto no se muestra un diagrama de conjunto que pueda llegar a poner en evidencia la configuración general de las instalaciones ni de su infraestructura.

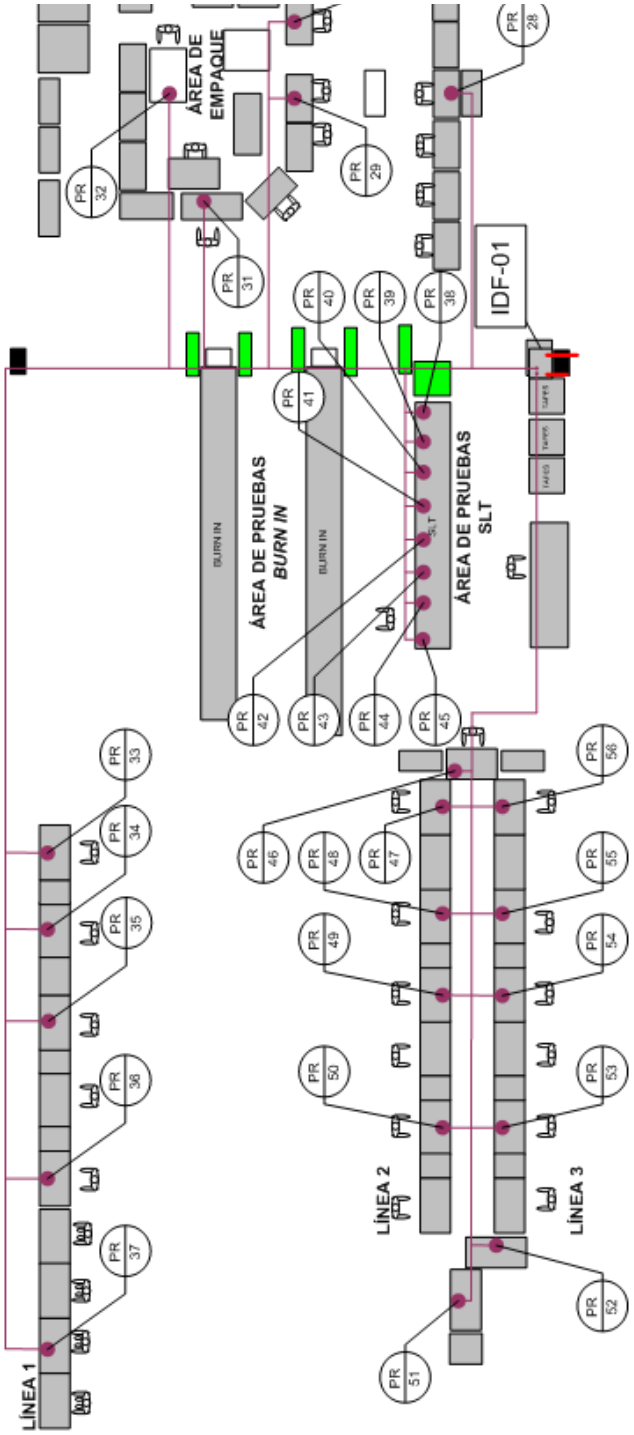


Figura 21. Diagrama de conexión de los servicios de red de datos desde el IDF01 hasta los equipos ubicados en las líneas de producción 1, 2, y 3 del área de manufactura de productos *Storage*, las diferentes pruebas de esos productos y su empaque final.

2.4.4.3 Configuración del esquema de tolerancia a fallas y redundancia

Uno de los puntos clave del proyecto reportado es que al desarrollar cada uno de los componentes que conforman la solución integral propuesta, dicho desarrollo se realizó paralelamente con el proceso de gestión de riesgos, por lo tanto, se pudo entregar una propuesta que ya incluía la previsión de los riesgos y cómo enfrentarlos en caso de alguna eventualidad. En esta sección describo cómo tratamos de protegernos contra esas posibles eventualidades al presentar configuraciones redundantes o con tolerancia a fallas en los diferentes elementos de la plataforma.

Servidores y red de área de almacenamiento

Como ya fue mencionado en las etapas 2.4.3.1 y 2.4.4.1, para los servidores de categoría crítica, se utilizaría un servidor en modo de espera. Esto para lograr un nivel adecuado de redundancia en términos de capacidad de procesamiento.

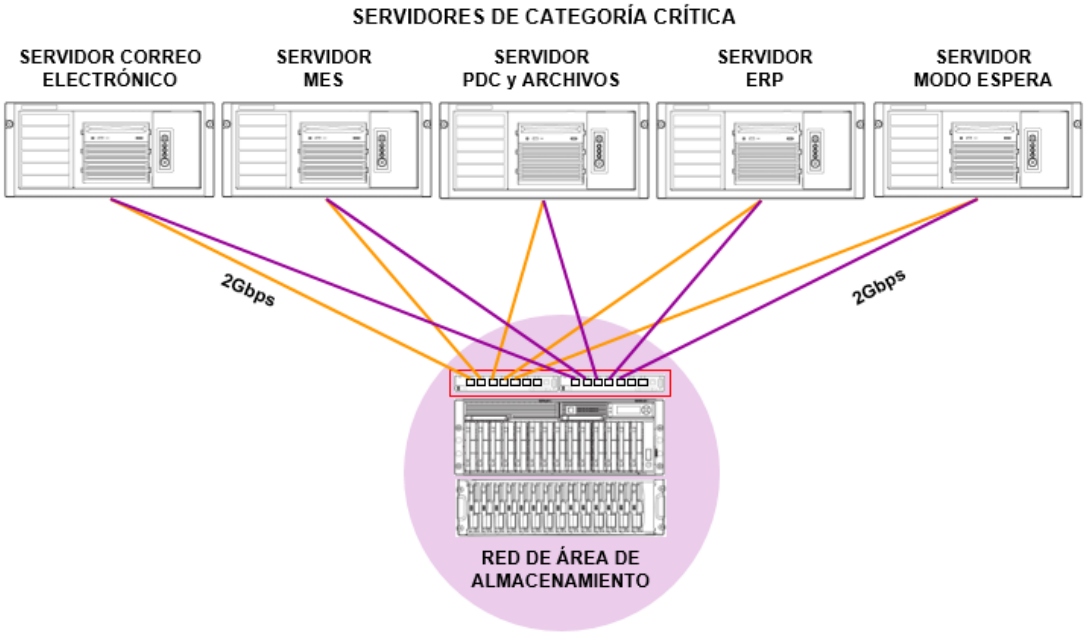


Figura 22. Esquema redundante para los servidores de categoría crítica.

La figura 22 muestra la implementación de dicho esquema de redundancia. Entre cada servidor y la red de área de almacenamiento (SAN) existen dos conexiones de fibra óptica con velocidad de transferencia de datos de 2Gbps cada una. Como las bases de datos y los archivos residen en la SAN, en caso de que algún servidor falle, el servidor en modo de espera tomará su lugar y será el “puerto” de entrada, ya sea a la base de datos de la aplicación o a los archivos del servidor dañado correspondiente.

Todos los servidores de categoría crítica contarían con fuentes de voltaje y ventiladores redundantes, lo cual, aunado a su configuración de doble procesador y arreglos de discos duros, disminuirían notablemente la probabilidad de una pérdida de disponibilidad. Para incrementar el nivel de redundancia aún más, cada fuente de voltaje de los servidores sería alimentada por dos unidades de energía ininterrumpida (UPS por sus siglas en inglés), conectado cada uno a un circuito de alimentación de corriente alterna distinto y con toma a tierra física homologada.

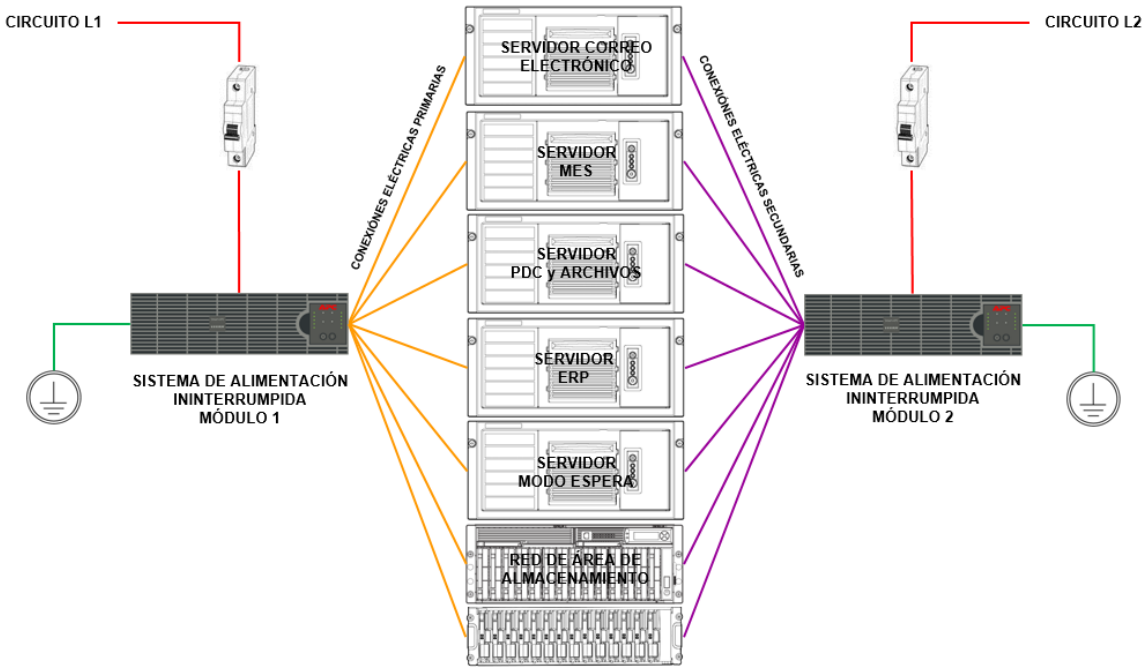


Figura 23. Esquema redundante de conexión eléctrica para los servidores de categoría crítica.

Las imágenes utilizadas en las figuras 22 y 23 proceden de

HP ProLiant ML370 (G3) Quick Specs (2005) [Guía rápida de especificaciones], obtenida de https://h10057.www1.hp.com/ecomcat/hpcatalog/specs/emeapsg/99/HP_ProLiant_ML370_Generation_3.pdf,

HP StorageWorks Modular Smart Array 1000 for Small Business SAN G2 Kit, Quick Specs (2007) [Guía rápida de especificaciones], obtenida de https://www.senetic.ro/i/objects/HP_literature_emea_en_DA-12095.pdf

HP StorageWorks Modular Smart Array 30 User Guide (2003) [Guía del usuario], obtenida de http://www.istoragenetworks.com/servermanuals/msa30_manual.pdf

Conectividad local

Una de las razones de haber propuesto los equipos de *switcheo* indicados en la sección 2.4.3.1 es la de que éstos cuentan con la funcionalidad de poder implementar esquemas de redundancia basados en técnicas de Spanning Tree, Rapid Spanning Tree, así como Resilient Link, además de poder implementar VLAN de forma nativa.

Con el objetivo de cubrir este aspecto, recurrimos a la teoría de grafos de forma que podamos obtener una cantidad de conexiones adyacentes por nodo que nos permitan eliminar puntos únicos de falla y –debido a que cada nodo cuenta con más de un origen- aumentar la probabilidad de que cada nodo tenga capacidad de comunicación en caso de que la topología falle.

Obviamente el caso óptimo sería que cada nodo contara con conexiones a todos y cada uno de los otros nodos de la red, es decir una malla; sin embargo, dicha configuración resultaría demasiado costosa para el tipo de operación de BDT que no es de misión crítica.

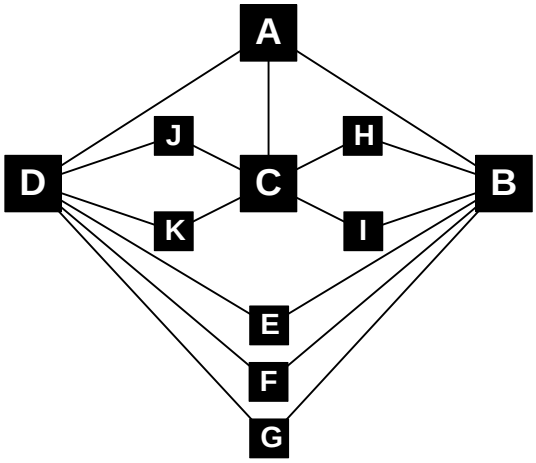


Figura 24. Esquema tolerante a fallas para la conectividad de red de datos.

En la figura 24 los nodos de mayor tamaño representan a los equipos localizados en la capa de distribución del modelo jerárquico, los nodos de menor tamaño representan a los equipos localizados en la capa de acceso del mismo modelo.

Nótese que los nodos de la capa de distribución cuentan con capacidades físicas que les permiten el manejo del tráfico de red generado en otros segmentos durante una falla sin que su desempeño se vea degradado notoriamente.

El número de conexiones adyacentes se obtiene de duplicar el número de conexiones y dividirlo entre el número de nodos, de esta forma tenemos que:

E= 2 x (17/11), **3.09**

Esta configuración se puede obtener a un costo razonable y brinda un nivel de redundancia sustancialmente alto, denominado malla parcial.

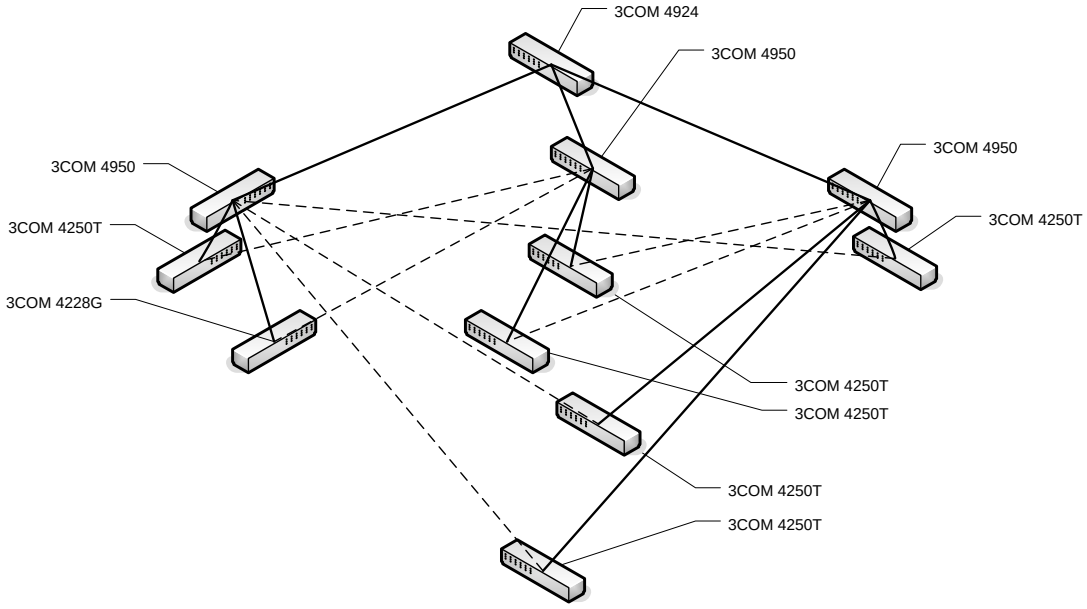


Figura 25. Implementación física del esquema anteriormente señalado. Las líneas continuas representan las conexiones activas, mientras que las punteadas representan las conexiones redundantes.

Conectividad a la red de área amplia e Internet

Para la conectividad a Internet, diseñamos una solución basada en dos equipos firewall, uno estaría operativo y otro como *fail-over*; de esta manera, si el equipo operativo dejaba de funcionar, el equipo en modo *fail-over* tomaría control de la conectividad hacia y desde Internet. La razón por la cual solo el equipo firewall estaría por duplicado, radica en que el resto de los elementos resultaban más fácil de reemplazar que el primero; excepto por el *router*, pero este elemento era propiedad del ISP, y su contrato de nivel de servicio indicaba solución de problemas en el enlace –y sus elementos- en máximo 4 horas.

Una segunda red no protegida, con menor ancho de banda, estaría destinada a visitantes, proveedores o clientes con necesidad de conectividad a Internet. La figura 26 muestra gráficamente este concepto.

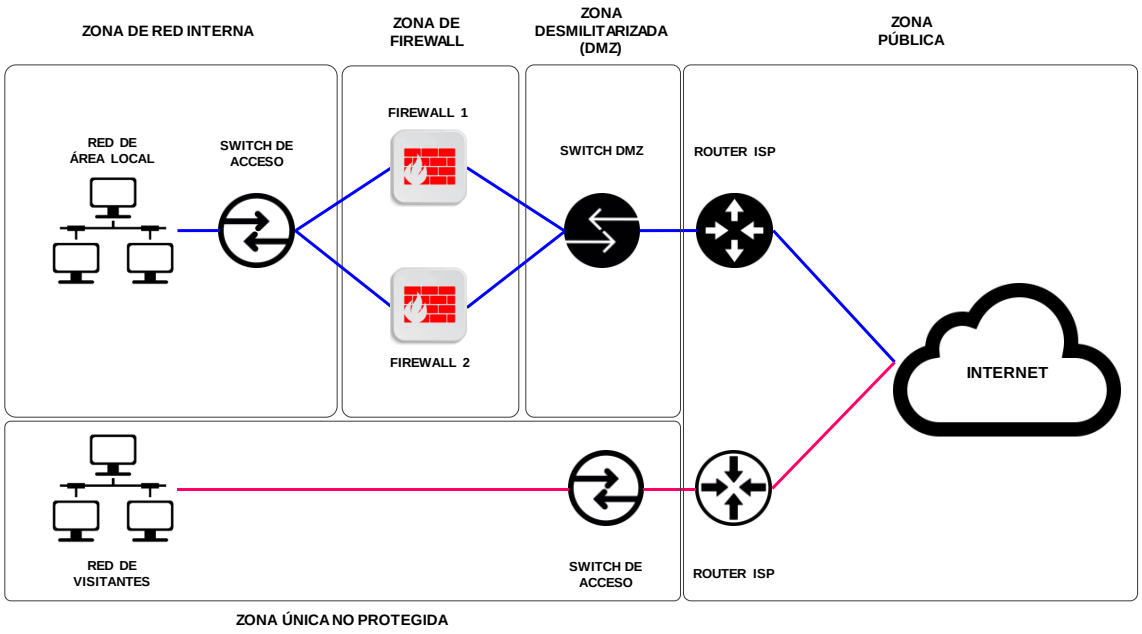


Figura 26. Diagrama conceptual del acceso a Internet desde la red de área local de BDT de México mostrando las diferentes zonas de operación y sus niveles de seguridad correspondientes. Nótese la redundancia existente a nivel del firewall, el cual permite el acceso continuo a Internet. De igual forma, se muestra el acceso a Internet para visitantes o personal externo a la empresa. Este es un acceso totalmente aislado del servicio principal.

Gracias al modelo propuesto para el acceso a Internet, y a las características mencionadas en el apartado de Anexos, *Especificaciones detalladas del dispositivo firewall y sus componentes*, se pudo establecer una propuesta de conectividad explotando precisamente esas características; una de ellas, el manejo de VPN, con lo cual, la red local de datos de BDT de México podría conectarse a la red de datos del corporativo en Alemania, a un costo relativamente bajo, ya que solo se pagaría precisamente el servicio de acceso a Internet, pero no el manejo de los VPN.

Debe señalarse, que al contar con servicios de VPN, estos también podrían aprovecharse por usuarios móviles (*road-warriors*) fuera de las instalaciones de la compañía, que requiriesen acceso a información o recursos compartidos en la red local de datos, ya fuesen en México o en Alemania mientras se encuentran viajando.

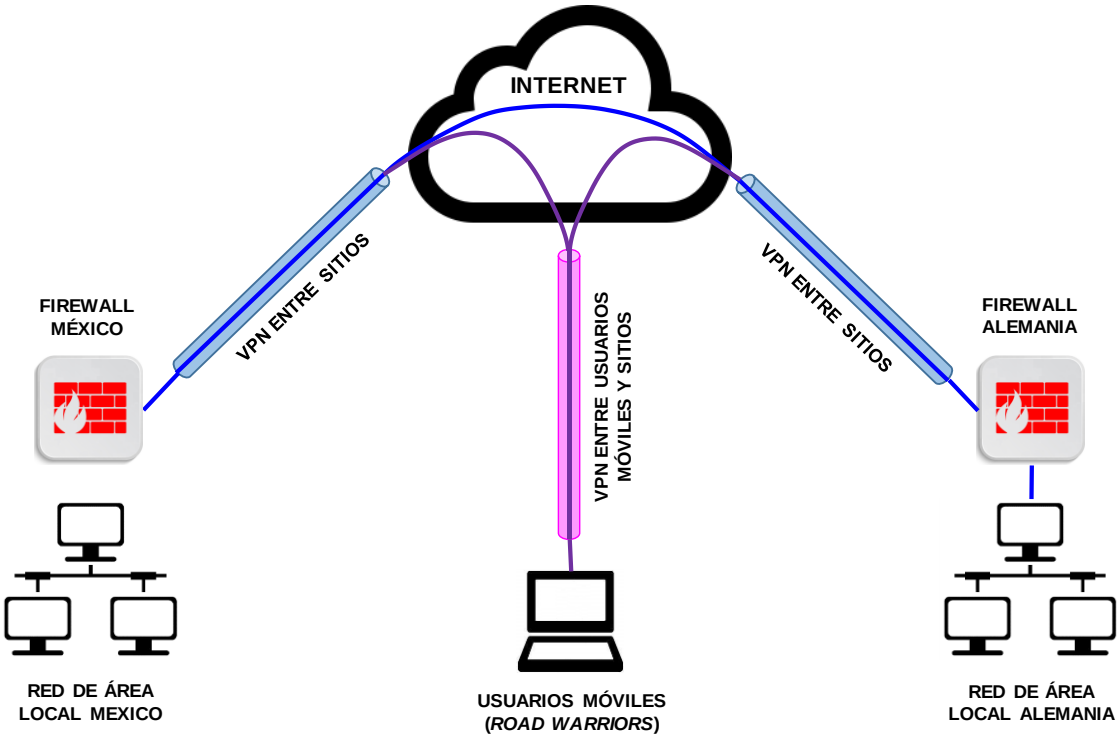


Figura 27. Diagrama conceptual de la conectividad entre sitios por medio de redes privadas virtuales (VPN por sus siglas en inglés), formando –de esta manera- la red de área amplia (WAN por sus siglas en inglés). Mismo concepto para la conectividad entre usuarios móviles en el camino y las diferentes redes locales de datos.

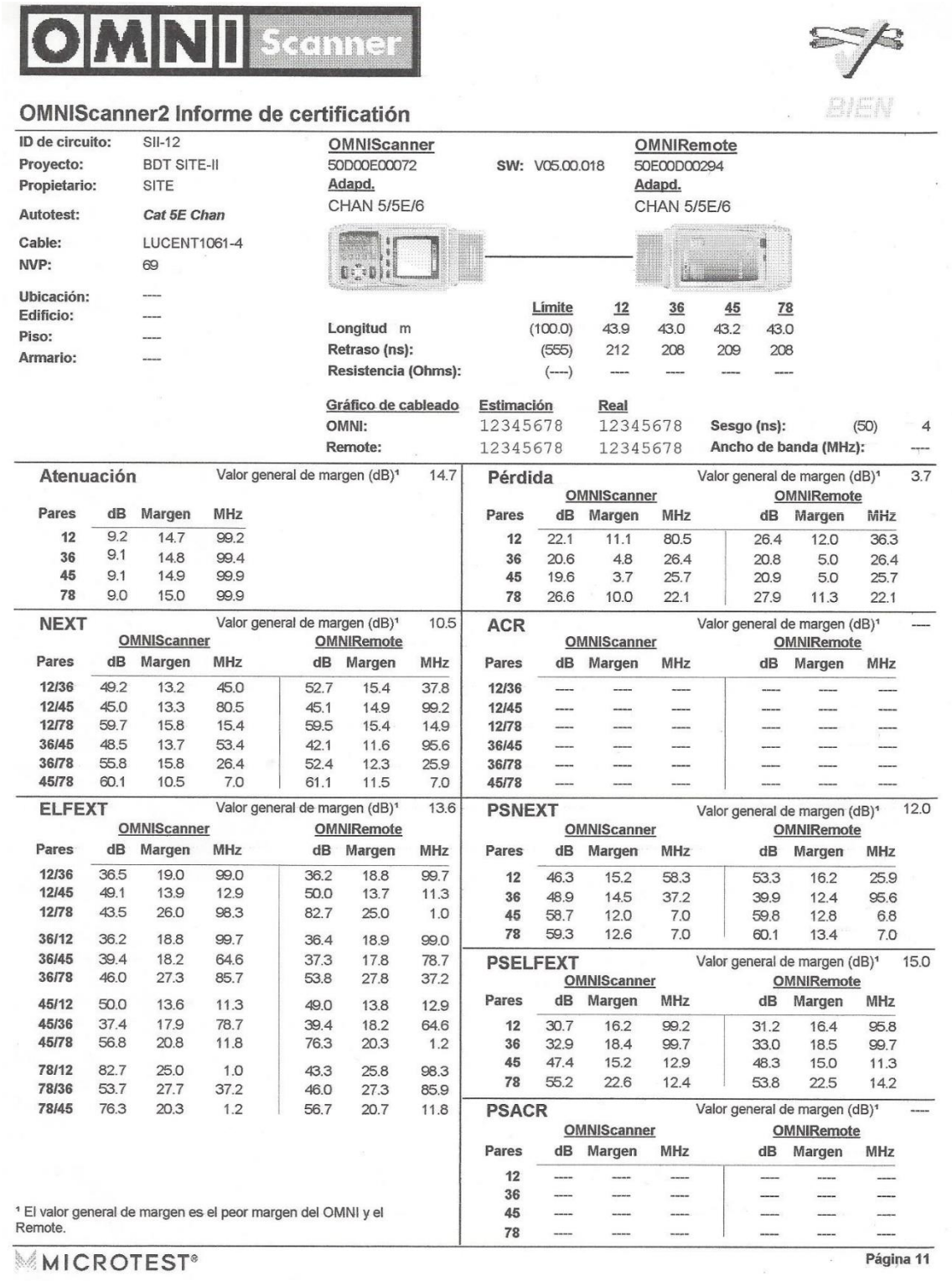
2.4.5 Pruebas de conectividad y servicios

Una vez integrados todos los elementos de la plataforma técnico-tecnológica, se procedió a realizar las pruebas pertinentes para garantizar su correcto funcionamiento. Las pruebas efectuadas a los servidores, SAN y firewall, aunque pudieron ser documentadas, no pueden ser compartidas en este documento, ya que evidencian parámetros de conectividad, configuraciones detalladas, nombres de equipos y sus correspondientes direcciones IP, etcétera. Las pruebas que sí pueden mostrarse, son los resultados de cumplimiento de parámetros de conectividad para las diferentes capas de cableado de red.

Un resumen con las tablas de referencia de terminación de los diferentes nodos de red, en la cual se muestran las distancias entre dichos nodos y el IDF que les alimenta, se encuentra en el apartado de Anexos, *Tablas de conectividad*, al final de este documento. Estas tablas demuestran el cumplimiento de las restricciones de distancia del cableado entre equipos activos.

En las siguientes páginas, se muestran un par de ejemplos de pruebas de conectividad para los diferentes tipos de cableado, tal como lo definen las normas ANSI/TIA/EIA-568-B e ISO/IEC 11801. Entre estas pruebas se incluyen atenuación, pérdida, NEXT[33], PSNEXT[34], ELFEXT[35], PSELFEXT[36], cuyos resultados pueden ser valores de aprobación o falla, y las pruebas ACR[37], PSACR[38], cuyos resultados son meramente informativos para la norma ANSI, pero de aprobación o falla para la norma ISO.

[33] NEXT (Near-End Crosstalk): Es el hecho de que la señal de un cable irradie e interfiera con la señal de otro par de cables.
[34] PSNEXT (Power Sum NEXT): Es la suma de los valores NEXT para la afectación que tres pares de cables inciden en el par de cables restantes.
[35] ELFEXT (Equal-Level Far-End Crosstalk): Mide la interferencia igual que NEXT, pero en el lado receptor de la conexión (alejado del transmisor de prueba).
[36] PSELFEXT (Power Sum ELFEXT): Es la suma de los valores FEXT para la afectación que tres pares de cables inciden en el par de cables restantes, menos la pérdida por inserción del canal.
[37] ACR (Attenuation-to-crosstalk ratio): parámetro que indica la proporción de atenuación respecto a la interferencia en el extremo cercano para cada combinación de pares de cables, se mide en decibeles (dB).
[38] PSACR (Power Sum ACR): Misma prueba que ACR, pero utilizando el valor PSNEXT en lugar del de NEXT.



OMNIScanner

BIEN

OMNIScanner2 Informe de certificatión

ID de circuito:	SII-12	**OMNIScanner**			**OMNIRemote**		
Proyecto:	BDT SITE-II	50D00E00072	**SW:**	V05.00.018	50E00D00294		
Propietario:	SITE	**Adapd.**			**Adapd.**		
Autotest:	***Cat 5E Chan***	CHAN 5/5E/6			CHAN 5/5E/6		
Cable:	LUCENT1061-4						
NVP:	69						
Ubicación:	----						
Edificio:	----						
Piso:	----						
Armario:	----						

	Límite	12	36	45	78
Longitud m	(100.0)	43.9	43.0	43.2	43.0
Retraso (ns):	(555)	212	208	209	208
Resistencia (Ohms):	(----)	----	----	----	----

Gráfico de cableado	**Estimación**	**Real**		
OMNI:	12345678	12345678	**Sesgo (ns):**	(50) 4
Remote:	12345678	12345678	**Ancho de banda (MHz):**	----

Atenuación

Valor general de margen (dB)[1] 14.7

Pares	dB	Margen	MHz
12	9.2	14.7	99.2
36	9.1	14.8	99.4
45	9.1	14.9	99.9
78	9.0	15.0	99.9

Pérdida

Valor general de margen (dB)[1] 3.7

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12	22.1	11.1	80.5	26.4	12.0	36.3
36	20.6	4.8	26.4	20.8	5.0	26.4
45	19.6	3.7	25.7	20.9	5.0	25.7
78	26.6	10.0	22.1	27.9	11.3	22.1

NEXT

Valor general de margen (dB)[1] 10.5

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12/36	49.2	13.2	45.0	52.7	15.4	37.8
12/45	45.0	13.3	80.5	45.1	14.9	99.2
12/78	59.7	15.8	15.4	59.5	15.4	14.9
36/45	48.5	13.7	53.4	42.1	11.6	95.6
36/78	55.8	15.8	26.4	52.4	12.3	25.9
45/78	60.1	10.5	7.0	61.1	11.5	7.0

ACR

Valor general de margen (dB)[1] ----

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12/36	----	----	----	----	----	----
12/45	----	----	----	----	----	----
12/78	----	----	----	----	----	----
36/45	----	----	----	----	----	----
36/78	----	----	----	----	----	----
45/78	----	----	----	----	----	----

ELFEXT

Valor general de margen (dB)[1] 13.6

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12/36	36.5	19.0	99.0	36.2	18.8	99.7
12/45	49.1	13.9	12.9	50.0	13.7	11.3
12/78	43.5	26.0	98.3	82.7	25.0	1.0
36/12	36.2	18.8	99.7	36.4	18.9	99.0
36/45	39.4	18.2	64.6	37.3	17.8	78.7
36/78	46.0	27.3	85.7	53.8	27.8	37.2
45/12	50.0	13.6	11.3	49.0	13.8	12.9
45/36	37.4	17.9	78.7	39.4	18.2	64.6
45/78	56.8	20.8	11.8	76.3	20.3	1.2
78/12	82.7	25.0	1.0	43.3	25.8	98.3
78/36	53.7	27.7	37.2	46.0	27.3	85.9
78/45	76.3	20.3	1.2	56.7	20.7	11.8

PSNEXT

Valor general de margen (dB)[1] 12.0

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12	46.3	15.2	58.3	53.3	16.2	25.9
36	48.9	14.5	37.2	39.9	12.4	95.6
45	58.7	12.0	7.0	59.8	12.8	6.8
78	59.3	12.6	7.0	60.1	13.4	7.0

PSELFEXT

Valor general de margen (dB)[1] 15.0

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12	30.7	16.2	99.2	31.2	16.4	95.8
36	32.9	18.4	99.7	33.0	18.5	99.7
45	47.4	15.2	12.9	48.3	15.0	11.3
78	55.2	22.6	12.4	53.8	22.5	14.2

PSACR

Valor general de margen (dB)[1] ----

	OMNIScanner			OMNIRemote		
Pares	**dB**	**Margen**	**MHz**	**dB**	**Margen**	**MHz**
12	----	----	----	----	----	----
36	----	----	----	----	----	----
45	----	----	----	----	----	----
78	----	----	----	----	----	----

[1] El valor general de margen es el peor margen del OMNI y el Remote.

MICROTEST®

Página 11

Figura 28. Impresión de pruebas de conectividad para cableado Categoría 5e.

LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

ID. Cable: D-FIA 12

Sumario de Pruebas: PASA

Paso Libre: 5.9 dB (NEXT 12-36)
Limite de Prueba: Cat 6 Link
Tipo de Cable: PANDUIT CAT.6 GIGA PUR600

Versión de Software: V06.12
NVP: 74%

Modelo: OMNIScanner2
Principal N/S: 50D00E00072
Remoto N/S: 50E00D00294
Adaptador Principal: CHAN 5/5E/6
Adaptador Remoto: CHAN 5/5E/6

Mapa de Cableado		Esperado	Actual
PASA	Omni:	12345678	12345678
	Remoto:	12345678	12345678

Longitud (m), Lím. 90.0	[Par 78]	23.5
Tiempo de Prop. (ns), Lím. 498	[Par 36]	109
Diferencia Retardo (ns), Lím. 44	[Par 36]	3
Resistencia (ohm.)		N/A
Atenuación (dB)	[Par 78]	22.6
Frecuencia (MHz)	[Par 78]	238.9
Límite (dB)	[Par 78]	30.3

Margen de Peor Caso

PASA	MAIN	SR
Peor Par	12-36	12-36
NEXT (dB)	7.2	5.9
Frec. (MHz)	51.1	73.6
Límite (dB)	46.6	44.0
Peor Par	78	12
PSNEXT (dB)	8.9	8.4
Frec. (MHz)	244.3	73.6
Límite (dB)	32.9	41.5

PASA	MAIN	SR
Peor Par	45-12	12-45
ELFEXT (dB)	11.8	11.8
Frec. (MHz)	1.2	1.2
Límite (dB)	62.8	62.8
Peor Par	12	45
PSELFEXT (dB)	11.9	12.0
Frec. (MHz)	1.2	1.2
Límite (dB)	59.8	59.8

PASA	MAIN	SR
Peor Par	36	78
RL (dB)	4.2	5.0
Frec. (MHz)	73.4	56.1
Límite (dB)	15.4	16.5

Estándares de Red Compatibles:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

FLUKE networks

Figura 29. Impresión de pruebas de conectividad para cableado Categoría 6.

2.5 Resumen de la documentación e información recabada

La documentación e información que han sido utilizados para la realización del presente reporte, se compone de archivos financieros, mensajes de correo electrónico, cotizaciones por parte de proveedores, órdenes de compra, así como reportes de funcionamiento o de cumplimiento con alguna normativa o requerimiento específico. A continuación, se muestran algunos de esos documentos para fines demostrativos. Por razones de privacidad, algunas de las figuras mostradas, podrán contar con filtros ópticos para proteger información delicada.

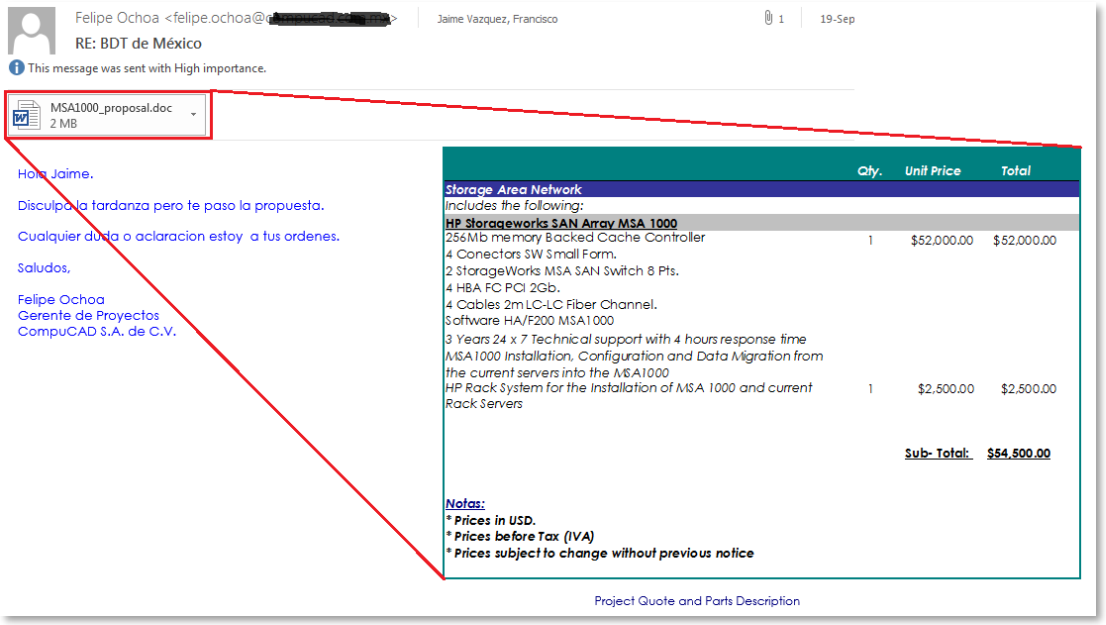
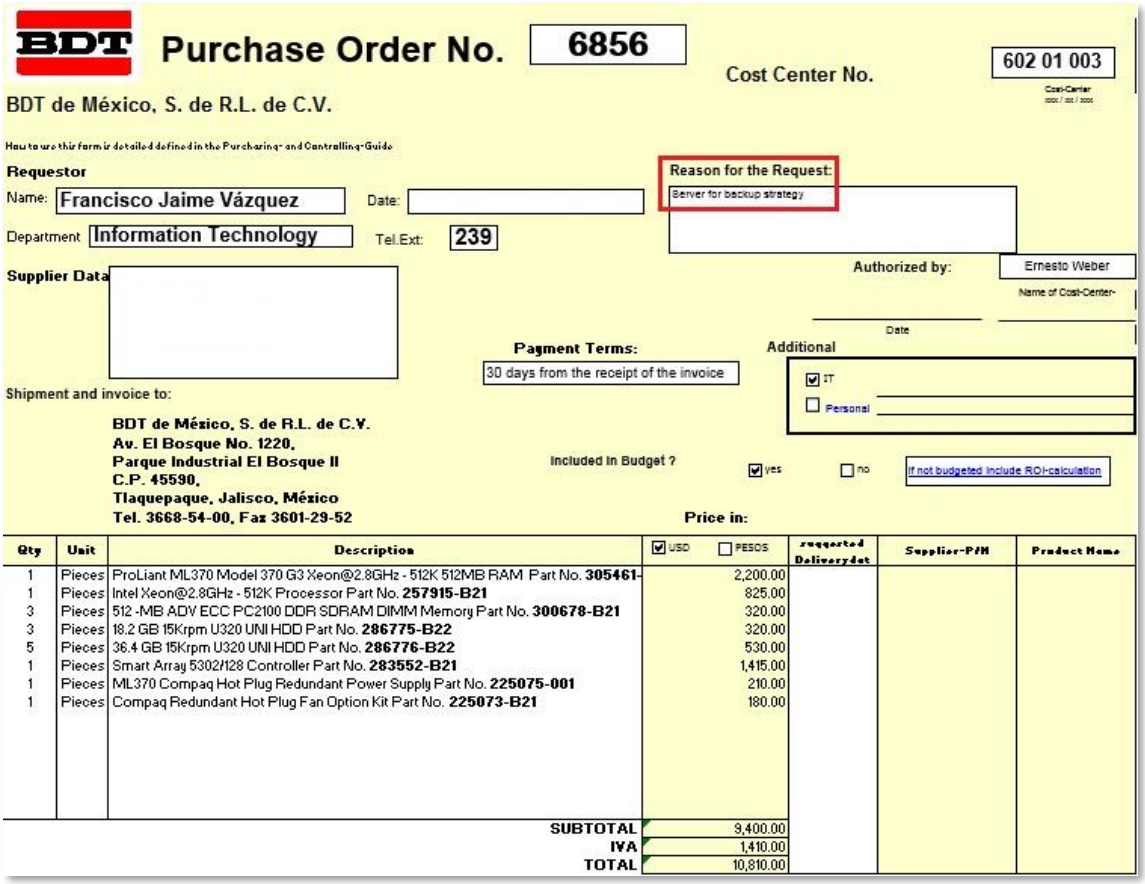


Figura 30. Mensaje de correo electrónico (imagen superior) en donde el proveedor nos hace llegar su cotización para la SAN. La cotización se muestra en la imagen inferior.



BDT

Purchase Order No. 6856

Cost Center No. 602 01 003

BDT de México, S. de R.L. de C.V.

How to use this form is detailed defined in the Purchasing and Controlling Guide

Requestor

Name: Francisco Jaime Vázquez Date:

Department: Information Technology Tel.Ext: 239

Reason for the Request: Server for backup strategy

Authorized by: Ernesto Weber

Name of Cost-Center-

Date

Supplier Data

Payment Terms: 30 days from the receipt of the invoice

Additional

☑ IT

☐ Personal

Shipment and invoice to:

BDT de México, S. de R.L. de C.V.
Av. El Bosque No. 1220,
Parque Industrial El Bosque II
C.P. 45590,
Tlaquepaque, Jalisco, México
Tel. 3668-54-00, Fax 3601-29-52

Included in Budget ? ☑ yes ☐ no If not budgeted include ROI-calculation

Price in: ☑ USD ☐ PESOS

Qty	Unit	Description	suggested Delivery date	Supplier-P/N	Product Name
1	Pieces	ProLiant ML370 Model 370 G3 Xeon@2.8GHz - 512K 512MB RAM Part No. **305461-**	2,200.00		
1	Pieces	Intel Xeon@2.8GHz - 512K Processor Part No. **257915-B21**	825.00		
3	Pieces	512 -MB ADV ECC PC2100 DDR SDRAM DIMM Memory Part No. **300678-B21**	320.00		
3	Pieces	18.2 GB 15Krpm U320 UNI HDD Part No. **286775-B22**	320.00		
5	Pieces	36.4 GB 15Krpm U320 UNI HDD Part No. **286776-B22**	530.00		
1	Pieces	Smart Array 5302/128 Controller Part No. **283552-B21**	1,415.00		
1	Pieces	ML370 Compaq Hot Plug Redundant Power Supply Part No. **225075-001**	210.00		
1	Pieces	Compaq Redundant Hot Plug Fan Option Kit Part No. **225073-B21**	180.00		
		SUBTOTAL	9,400.00		
		IVA	1,410.00		
		TOTAL	10,810.00		

Figura 31. Orden de compra para la adquisición del servidor destinado a la estrategia de redundancia para los servidores de categoría crítica.

2.6 Resultados obtenidos en el proyecto reportado

El principal resultado obtenido tras la realización del proyecto fue la dotación de una plataforma técnico-tecnológica robusta y confiable, cuya característica principal era la escalabilidad. Con el paso del tiempo, esta particularidad le permitió a la compañía renovar equipamiento o incrementar sus alcances con relativa facilidad, al grado que, hasta la fecha de mi desincorporación de la compañía, ocurrida a mediados del 2014, la plataforma aún continuaba operativa y funcional, incluso con una oferta de servicios y una cantidad de usuarios mayor a las establecidas inicialmente.

Gracias a esta plataforma, fue posible que el personal de BDT de México pudiese compartir información y utilizar aplicaciones en los tres niveles de conectividad: local, de área amplia y de Internet. Al hacerlo de esta forma, se obtuvo una enorme ventaja en la realización de procesos de transferencia de productos del corporativo a la naciente planta en Guadalajara, ya que se contaba de manera casi inmediata con información propia de dichos procesos, lo cual generaba que la coordinación de actividades se diera de forma sencilla entre el personal de ambos sitios, reduciendo considerablemente el tiempo estimado para su realización. Así mismo, permitía que la comunicación con los clientes se diera de manera fluida y facilitara la ejecución de actividades y compromisos acordados.

Adicionalmente, se lograba consolidar toda la información necesaria para la operación de la compañía localmente, con lo que se facilitaba su transporte a otra ubicación en caso de presentarse una situación de contingencia que obligara a la empresa a operar desde un lugar diferente. De igual forma, al integrarse la planta de Guadalajara a la red de área amplia de la compañía, se unificaban los esfuerzos de los diferentes departamentos de las Tecnologías de la Información para establecer políticas, cumplir con normativas aplicables, acordar estrategias y planear proyectos conjuntos, lo cual no sería posible si ambas instancias no estuviesen interconectadas entre sí o sí se operasen de manera independiente en cada uno de los sitios.

CAPÍTULO 3. CONCLUSIONES

Diversas fuentes bibliográficas utilizan indistintamente los términos de lecciones aprendidas y mejores prácticas; sin embargo, es oportuno señalar que existen ciertas diferencias importantes. Las lecciones son principios generalizados que se derivan de proyectos o contextos reales, ¿qué se hizo bien y no tan bien, y por qué?, ¿qué hubiera mejorado el trabajo anterior o actual? En contraste, las mejores prácticas tratan de una técnica identificable que es apta para su aplicación en circunstancias específicas. Habiendo señalado lo anterior, tomemos en cuenta que lo que reportaré a continuación, son precisamente las lecciones aprendidas.

3.1 Lecciones aprendidas

En este tenor, puedo enlistar las siguientes lecciones aprendidas que denotan los errores cometidos, los riesgos a los que el proyecto se vio expuesto, las decisiones que mejor funcionaron, así como los procesos y técnicas que mejor eficiencia y efectividad aportaron al proyecto:

El apoyo absoluto del padrino del proyecto es un aspecto imprescindible para que el director del proyecto pueda liderar adecuadamente el proceso de gestión del proyecto, y resulta fundamental para el logro de los objetivos, ya que su posición en el organigrama de la compañía le permite destrabar procesos complejos y alinear a todos los involucrados en el sentido que el director del proyecto desee imprimirle al mismo. Este aspecto es definitivamente un factor determinante para el éxito del proyecto, tal como sucedió en el proyecto reportado.

La utilización de marcos de trabajo o métodos analíticos para abordar las diferentes etapas del proyecto permitieron un manejo detallado de aspectos sobre los cuales hay que observar un mayor cuidado. De igual forma, brindaron un sustento científico a actividades tales como la gestión misma del proyecto, la toma de decisiones, el análisis de riesgos y otras más.

Queda claro que aún con la experiencia profesional con la que yo contaba al momento de realizar el proyecto, éste no hubiese resultado exitoso –al menos no en esa medida-, de no haber tomado la acción estratégica de afrontarlo utilizando las herramientas de gestión arriba señaladas.

Nunca debemos subestimar la importancia o la complejidad de algún proceso de toma de decisiones; categóricamente puedo señalar que no hay decisiones simples, ya que todas deben llevar un proceso de análisis de alternativas, su evaluación y la toma final de decisiones. Durante el proceso de selección del *firewall* a utilizar en la plataforma, mi contraparte en el corporativo y yo caímos en el exceso de confianza y dimos por sentados aspectos que requerían mayor profundidad de análisis, los cuales –a la postre- se tornaron en requerimientos críticos que tuvieron que ser atendidos por segunda ocasión. Afortunadamente este punto no nos afectó enormemente; sin embargo, con nuestra falsa seguridad asumimos un riesgo totalmente innecesario.

Para la elección de algunos elementos o servicios es necesario realizar una evaluación detallada, tanto de sus características como de sus costos según lo indiquen las propuestas que se tengan de los diferentes proveedores. El no hacerlo de esta forma, puede derivar en estimaciones o dimensionamientos erróneos o por debajo de la realidad que, posteriormente, redunden en gastos adicionales a los inicialmente previstos, así como en pérdidas de tiempo y ajustes a la planeación principal y gestión del proyecto.

La gestión de proyectos que involucran a personal local y a personal de corporativos ubicados fuera, no solo de la ciudad, sino del país, sin ninguna duda requieren de un alto nivel de coordinación de juntas, telefónicas en su mayoría y algunas videoconferencias esporádicamente, que permitan garantizar –hasta cierto punto- que la planeación de las diferentes actividades derive en la ejecución de acciones con la mayor precisión posible.

Definitivamente la diferencia de idiomas, alemán y español, incrementaba la posibilidad de malos entendidos (a pesar de que ambas partes tuviésemos una idea del idioma de nuestra contraparte), razón por la cual, la utilización de un lenguaje común, el inglés en este caso, facilitó enormemente la obtención de acuerdos y el establecimiento de estrategias.

Mención aparte merece la consideración de las diferencias culturales en el momento de discutir alternativas, lograr acuerdos y generar la tan codiciada sinergia en el desarrollo del proyecto. De igual forma, hay que hacer conscientes a ambas partes –locales y extranjeros- de las diferencias existentes entre ambas culturas en términos de disponibilidad de equipos y servicios, así como sus formas de compra o contratación y los términos de uso en diferentes países. Aunque esto no es un aspecto crítico, sí es uno que debe tenerse en mente, ya que el resultado exitoso de un proyecto no solo implica que se realice en tiempo y forma, sino que además las relaciones entre los involucrados no se vean desgastadas, sino –por el contrario- resulten fortalecidas.

La gestión de riesgos es un punto muy delicado que debe ser abordado con la debida formalidad; para el proyecto reportado, resultó de gran ayuda hacer el análisis de riesgos en conjunto con la definición de actividades, de esta manera, se establecían los objetivos de cada actividad incluyendo los riesgos que debían de ser evitados o gestionados, según fuese el caso. Esta estrategia fue muy útil y facilitó la comprensión de los involucrados sobre lo que no debía de suceder al realizar las actividades que tuviesen asignadas o de las que fuesen responsables.

Para afrontar un proyecto de la magnitud y de la complejidad que era el proyecto reportado, resultó sumamente útil el contar con proveedores confiables que comprendiesen los objetivos del proyecto y que estuviesen conscientes de lo que se esperaba de ellos. Aun cuando no realizamos una evaluación exhaustiva de los proveedores potenciales, si realizamos labores de benchmarking y solicitamos cotizaciones a por lo menos dos proveedores por tipo de componente a adquirir.

A estos proveedores los evaluamos con criterios sencillos, tales como experiencia de trabajo previo con ellos, solidez de la compañía, presencia en el mercado, nivel de costo cotizado, beneficios adicionales y plazos de crédito entre otros. Conforme pasaba el tiempo de realización del proyecto, BDT lograba un mejor apalancamiento en las negociaciones de precios o beneficios con los diferentes proveedores.

3.2 Propuesta de mejora

A pesar de que estoy reportando un proyecto que puede considerarse abiertamente como exitoso, esto no significa que no se le puedan identificar áreas de oportunidad que puedan ser traducidas en propuestas de mejora. Quizás, la más relevante sea la relativa a la gestión de proyectos en sí. Considero que, de haber contado con una mayor ventana de tiempo para la realización del proyecto, así como una mayor cantidad de recursos en general, podríamos haber seguido el marco de trabajo descrito por la Guía PMBOK a pie juntillas, y no haber omitido abordar algunas de sus áreas del conocimiento, como fue el caso en el proyecto reportado.

De haberse hecho un uso extensivo y exhaustivo de la Guía PMBOK, se podría haber obtenido una cantidad importante de información referente a la operación de la empresa que podría haber sido útil para la realización de otros proyectos, además de que el proyecto reportado hubiese podido resultar más completo en su realización. Afortunadamente, el enfoque PMBOK tiene la suficiente flexibilidad como para que podamos seleccionar los procesos a aplicar y las técnicas concretas a utilizar, lo cual permitió valerse solo de aquello para lo que se contaba con recursos y tiempo suficientes. Sin embargo, considero que hubiese resultado un ejercicio por demás interesante de realizar, de haber sido posible hacerlo.

Recordemos que el proyecto fue dirigido prácticamente por una sola persona, la cual realizó múltiples roles y que, por lo tanto, estaba acotada por una serie de actividades demasiado extensa por un lado y, un tiempo estimado para su realización demasiado corto; por lo que, la forma de desarrollar el proyecto reportado fue la mejor posible en términos de costo-beneficio.

3.3 Conclusiones

Al llegar a este punto, no puedo dejar de traer a mi mente el tríptico informativo sobre el programa de la maestría, en cuyo apartado referente a la vinculación con la industria y otros sectores de la región se leía:

> La Maestría en Informática Aplicada es un vínculo entre la Universidad y su región, da soluciones informáticas a la industria, al gobierno, a otras instituciones de educación y a otras organizaciones de su entorno; es así un agente de cambio para el logro de una mayor calidad y productividad en su región.
>
> **Los trabajos de tesis de maestría de sus alumnos están orientados a la solución de problemas reales de las organizaciones del occidente del país.**

A primera vista, este texto pareciera una mera fórmula mercadológica. De hecho, yo no recuerdo si así lo consideré en su momento, y si así fue, no pude haberme equivocado de mejor manera porque tras haber cubierto el programa de la maestría, mis habilidades gerenciales se potenciaron considerablemente gracias al manejo de nuevas herramientas, tanto administrativas como conceptuales sobre la tecnología, y considero que me volví –efectivamente- un agente de cambio dentro de la organización para la cual laboraba en esa época.

No exagero al comentar que fue grande la ayuda obtenida a partir de los conocimientos adquiridos en la maestría al realizar, no solo en el proyecto reportado, sino en muchos otros proyectos y actividades posteriores. Orgullosamente puedo decir que mi puesto se volvió substancialmente más estratégico dentro de la organización y que mi opinión sirvió en innumerables ocasiones como punto de referencia para el logro de objetivos o el cumplimiento de metas, esto no solo a nivel local, sino extensivo a las sedes internacionales, inicialmente en Alemania, y posteriormente en China y Estados Unidos, denotando que la calidad del conocimiento adquirido en el programa de la maestría es de clase mundial.

No me gustaría dejar de lado, que a la par de la obtención de todo este conocimiento que nos ayuda a ser más competitivos y eficientes, también existe un factor implícito de espiritualidad ignaciana impreso en la totalidad de los programas educativos del sistema de educación jesuita que nos obliga a que sus egresados seamos agentes de cambio, generadores de transformación.

El P. Adolfo Nicolás, S. J. menciona que:

En la concepción ignaciana del servicio, hay siempre un factor muy importante de crecimiento que lleva a la transformación. Si no hay transformación, eso quiere decir que el proceso ha fracasado. El objetivo último es la transformación de la persona, y eventualmente, a través de las personas, de la sociedad. Pero eso se produce a través de un proceso de crecimiento. No hay transformaciones instantáneas…es un proceso largo. (Nicolás, 2013, pp.1-2).

Mi paso por las aulas de la maestría es parte de ese crecimiento, y la aplicación del conocimiento adquirido en ellas dentro de las organizaciones para las cuales he prestado mis servicios, es parte de ese proceso de transformación.

Queda clara la idoneidad de la frase del mismo P. Nicolás, “No formamos a los mejores del mundo, sino a los mejores para el mundo”, mi opinión personal es que el programa de la maestría cumple cabalmente con el significado de esta frase.

BIBLIOGRAFÍA

A guide to the project management body of knowledge (PMBOK ® guide) – Third Edition (2004), Newtown Square, Pennsylvania: Project Management Institute, Inc.

A guide to the project management body of knowledge (PMBOK ® guide) – Fifth Edition (2013), Newtown Square, Pennsylvania: Project Management Institute, Inc.

BICSI, A telecommunications Association (2002). *Network Design Basics [for Cabling Professionals]*. Two Penn Plaza, New York, NY: McGraw-Hill

CISCO PRESS (1999). *Internetworking Design Basics*. Obtenida originalmente en 2005, de

http://www.cisco.com/c/en/us/td/docs/internetworking/design/guide/idg4/

nd2002.html pero movida a

http://docwiki.cisco.com/wiki/Internetwork_Design_Guide, la cual no funciona al momento de la elaboración de este documento

CRESWELL John W. (2013). *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks, California: Sage Publications, Inc.

FINK, Arlene (1998). *Conducting research literature reviews: From paper to the Internet*. Thousand Oaks, California: Sage Publications, Inc.

ITIL (2007). *Service Strategy*. Norwich, UK: The Stationery Office

KENYON, Tony (2002). *High Performance Data Network Design: Design techniques and Tools*. Woburn, Massachusetts: Digital Press (an imprint of Butterworth-Heinemann)

KEPNER-TREGOE (s.f.). *Problem Solving & Decision Making*. Obtenida el 10 de marzo de 2014, de http://www.kepner-tregoe.com/linkservid/B9154B60-5056-A346-5CEC228E33B619AF/showMeta/0/

LEEDY, Paul D. y Ormrod, Jeanne Ellis (2001). *Practical research: planning and design.* Upper Saddle River, New Jersey: Prentice-Hall, Inc.

Manual de publicaciones de la American Psychological Association – Versión abreviada. Segunda edición traducida de la sexta en inglés (2010), México, D.F.: El Manual Moderno, S. A. de C. V.

McCABE, James D. (2007). *Network analysis, architecture, and design*. Burlington, Massachusetts: Morgan Kaufmann Publishers (an imprint of Elsevier)

NICOLÁS, Pachón Adolfo (2013). *Encuentro con superiores y directores de obra de la provincial de Castilla, conferencia sobre liderazgo Ignaciano*. Valladolid, España. Obtenida el 1 de mayo de 2016, de

http://www.sjweb.info/documents/ansj/130506_Valladolid_Liderazgo_ignaciano.pdf

OPPENHEIMER, Priscilla (2004). *Top-Down Network Design*. Indianapolis, Indiana: Cisco Press

RAMPAL, Rohit (2002). *Design and implementation of a Wide Area Network: Technological and managerial issues*. Hershey, Pennsylvania: Idea Group Publishing.

SCHATT, Stan (1993). *Understanding Local Area Networks*. Indianapolis, Indiana: SAMS Publishing

SPOHN, Darren, Brown Tina, Grau Scott (2002). *Data Network Design, Third Edition*. Berkeley, California: McGraw-Hill/Osborne

TABOADA, Cardoso Federico, Nielsen de Allende Mónica (2006). *Archivística y normalización: norma ISO 15489*. Ciudad Autónoma de Buenos Aires: Alfagrama Ediciones S. R. L.

TAYLOR Steven J., Bogdan Robert (1996). *Introducción a los métodos cualitativos de investigación: la búsqueda de significados*. Barcelona: Ediciones Paidós Ibérica, S. A.

TIA/EIA-568-B.1 Standard (2001). *Commercial Building Telecommunications Cabling Standard*.

TOLCHINSKI, Landsman Liliana, Rubio Hurtado María José, Escofet Roig Anna (2002). *Tesis, tesinas y otras tesituras. De la pregunta de investigación a la defensa de la tesis*. Barcelona: Edicions de la Universitat de Barcelona.

YIN, Robert K. (2003). *Case study research: design and methods.* Thousand Oaks, California: Sage Publications, Inc.

ANEXOS

Correspondencia de los procesos de gestión de proyectos

A continuación, se muestra la correspondencia de los 44 procesos de la gestión de proyectos y las nueve áreas de conocimiento según la Guía PMBOK (tercera edición) con los cinco grupos de procesos según la misma guía.

4. Gestión de la Integración del Proyecto				
Fase de Inicio	**Fase Intermedia**			**Fase Final**
Grupo de procesos de Inicio	**Grupo de procesos de Planeación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y Control**	**Grupo de procesos de Cierre**
4.1 Desarrollar el acta de constitución del proyecto. 4.2 Desarrollar el enunciado preliminar del alcance del proyecto.	4.3 Desarrollar el plan de gestión del proyecto.	4.4 Dirigir y gestionar la ejecución del proyecto.	4.5 Supervisar y controlar el trabajo del proyecto. 4.6 Control integrado de cambios.	4.7 Cerrar el proyecto.
5. Gestión del alcance del Proyecto				
	5.1 Planificación del alcance. 5.2 Definición del alcance. 5.3 Crear EDT.		5.4 Verificación del alcance. 5.5 Control del alcance.	
6. Gestión del tiempo del Proyecto				
	6.1 Definición de las actividades. 6.2 Establecimiento de la secuencia de las actividades. 6.3 Estimación de recursos de las actividades. 6.4 Estimación de la duración de las actividades. 6.5 Desarrollo del cronograma.		6.6 Control del cronograma.	
7. Gestión de los costes del Proyecto				
	7.1 Estimación de costes. 7.2 Preparación del presupuesto de costes.		7.3 Control de costes.	

La tabla continúa en la página siguiente.

Continuación de la tabla en la página anterior.

8. Gestión de la calidad del Proyecto				
Fase de Inicio	**Fase Intermedia**			**Fase Final**
Grupo de procesos de Inicio	**Grupo de procesos de Planeación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y Control**	**Grupo de procesos de Cierre**
	8.1 Planificación de calidad.	8.2 Realizar aseguramiento de calidad.	8.3 Realizar control de calidad.	
9. Gestión de los Recursos Humanos del Proyecto				
	9.1 Planificación de los Recursos Humanos.	9.2 Adquirir el equipo del proyecto. 9.3 Desarrollar el equipo del proyecto.	9.4 Gestionar al equipo del proyecto.	
10. Gestión de las comunicaciones del Proyecto				
	10.1 Planificación de las comunicaciones.	10.2 Distribución de la información.	10.3 Informar el rendimiento. 10.4 Gestionar a los interesados.	
11. Gestión de los riesgos del Proyecto				
	11.1 Planificación de la gestión de los riesgos. 11.2 Identificación de riesgos. 11.3 Análisis cualitativo de riesgos. 11.4 Análisis cuantitativo de riesgos. 11.5 Planificación de la respuesta a los riesgos.		11.6 Seguimiento y control de riesgos.	
12. Gestión de las adquisiciones del Proyecto				
	12.1 Planificar las compras y adquisiciones. 12.2 Planificar la contratación.	12.3 Solicitar respuestas de vendedores. 12.4 Selección de vendedores.	12.5 Administración del contrato.	12.6 Cierre del contrato.

Tabla 10. Correspondencia o mapeo de los procesos de la gestión de proyectos con los grupos de procesos y las áreas del conocimiento según la Guía PMBOK Tercera Edición. Imagen adaptada de la Guía PMBOK, *Third Edition*, 2004, p.70 [Imagen]

Tecnologías de almacenamiento de datos

Grabación helicoidal

Este método de grabación es utilizado en la tecnología DAT, es no-lineal (a diferencia del usado en la tecnología LTO), en el cual la información es escrita diagonalmente a lo ancho de la cinta, la ventaja de este concepto es que se obtienen más pistas contiguas que si se escribiera a 90° con respecto de la cinta. Para poder hacer la grabación de manera diagonal, los drives de DAT cuentan con un tambor giratorio inclinado que contiene cuatro cabezas (2 de escritura y 2 de lectura). Por cada giro del tambor se graban dos pistas y las cabezas lectoras verifican que la información haya sido almacenada y el drive la re-escribe si es necesario.

Figura 32. Trayectoria seguida para la grabación helicoidal de datos.

Grabación lineal

Este método de grabación es utilizado en la tecnología LTO, es lineal/serpenteado, en el que la información es grabada como una secuencia de pistas (similares a las de un disco LP) que corren alternadamente hacia delante y hacia atrás a lo largo de toda la cinta, teniendo como ventaja que para cuando se llegue al final lógico de la cinta, la cinta en sí estará físicamente al inicio para continuar grabando de manera ininterrumpida; es decir, graba de “ida y de vuelta”.

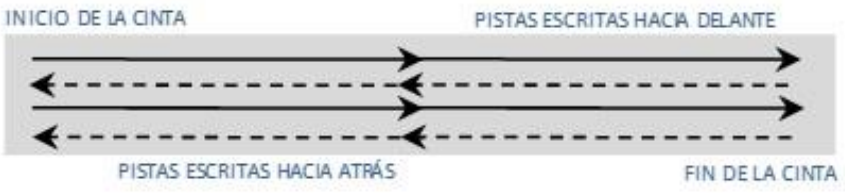


Figura 33. Trayectoria seguida para la grabación lineal de datos.

Resumen de características de los equipos activos de red

A continuación, se muestra un par de tablas que resumen las características más relevantes de los equipos activos de red elegidos para el proyecto reportado, de acuerdo con sus fichas técnicas. 3Com SuperStack 3 Switch 4924 and SuperStack 3 Switch 4950 (2002) [Ficha Técnica]; 3Com SuperStack 3 Switch 4200 Family (2002) [Ficha Técnica]; y Enterprise-Class 3Com Wireless LAN Access Points 7250/8250/8500/8750 (2004) [Ficha Técnica]. Obtenidas originalmente en 2002, de http://www.3com.com, la cual ya no es vigente al momento de la elaboración de este documento, debido principalmente a la antigüedad del producto y a que la marca 3Com fue adquirida en abril del 2010 por Hewlett Packard (hoy Hewlett Packard Enterprise), perdiéndose algunas referencias sobre productos que –en esa fecha- ya habían completado su ciclo de vida.

Modelo	Puertos 10/100	Puertos 10/100/1000	Capacidad de *switcheo*	Colas por puerto	Prioridad de tráfico	Permite
4950	-	12	56 Gbps	4	SI	▪ Link Aggregation ▪ Resilient Links ▪ Spanning Tree ▪ Rapid Spanning Tree ▪ Siete grupos RMON
4924	-	24	56 Gbps	4	SI	▪ Link Aggregation ▪ Resilient Links ▪ Spanning Tree ▪ Rapid Spanning Tree ▪ Siete grupos RMON
4250T	48	2	13.6 Gbps	2	SI	▪ Link Aggregation ▪ Resilient Links ▪ Spanning Tree ▪ Rapid Spanning Tree
4228G	24	2/2 GBIC	12.8 Gbps	2	SI	▪ Link Aggregation ▪ Resilient Links ▪ Spanning Tree ▪ Rapid Spanning Tree

Tabla 11. Resumen de especificaciones de los equipos de *switcheo* propuestos.

Modelo	Número de usuarios	Velocidad Máxima	Cumple con	Permite
AP 7250	253	54 Mbps	▪ Wi-Fi ▪ WEP ▪ WPA ▪ IEEE 802.11bag ▪ IEEE 802.3af ▪ CSMA/CA	▪ 802.11x RADIUS ▪ Validación por dirección MAC ▪ WEP de 40/64, 128 y 154 bits ▪ DHCP

Tabla 12. Resumen de especificaciones del equipo de acceso inalámbrico (Access Point) propuesto.

Especificaciones detalladas del dispositivo firewall y sus componentes

En la sección 2.4.3.1, se indicó la elección del firewall Astaro TimeNET SecuRACK P-8/100. Antes de revisar al detalle las capacidades técnicas de este *firewall*, resultó –y continúa siéndolo- interesante conocer las opiniones a nivel mundial de los expertos en temas de tecnologías de información sobre el producto que finalmente elegimos. Estos expertos se dedican a realizar evaluaciones exhaustivas en busca de los mejores productos en el mercado. Algunos de los factores de decisión considerados, se describen a continuación.

- Astaro era considerada entonces como una de las 100 mejores compañías privadas de acuerdo con Insight Venture Partners, lo cual garantizaba cierta permanencia en el mercado.
- El *firewall* de Astaro había obtenido en esas fechas, los siguientes reconocimientos y/o premios:
  - "Mejor *Firewall*" elegido por los lectores de Linux Enterprise
  - "Mejor Solución de Seguridad" Premio de excelencia de productos durante la exposición y conferencias Linux World
  - "Excelente" por la revista Infoworld
  - "Muy Bueno" por los editores de PC Magazine
  - "Elección de los Editores" de PC Magazine
  - "La más alta clasificación" por SC (Secure Computing) Magazine
  - "Mejor Solución de Seguridad Empresarial del Año" por PC Magazine
  - Certificado como "Excede las Especificaciones" por The Tolly Group
  - "El grado más alto posible" por Nätverk & Kommunikation Magazine
- Adicionalmente, al ser evaluado por InfoWorld Magazine, derrotó a CISCO y a CheckPoint; y al ser evaluado durante el Linux World, derrotó a IBM y a Computer Associates.
- Provee el motor de *firewall* para otros productos como Novell Security Manager.

- La opción elegida se basa en la utilización del *firewall* Astaro Security Linux V5 instalado en un hardware Nexcom NSA1080L; esta combinación es conocida como TimeNET SecuRACK P-8/100.

Las características principales de este equipo se detallan en la siguiente tabla

Especificación	Valor
Diseño	19” presentación de 1 Unidad de rack
CPU	Intel Pentium III@1.26 GHz
Memoria	512 MBytes SDRAM
Disco Duro	20 GBytes
Sistema de enfriamiento	2 ventiladores de 40 mm
Interfaces de red	8 del tipo 10/100 Base-TX
Conectores	2 seriales
Fuente de voltaje	180W tipo ATX
Desempeño de red	95 Mbps
Desempeño de correo electrónico	2.2 Mi por día SMTP
VPN 3DES/AES	57/90 Mbps
Certificaciones	CE, FCC
Arquitecturas de VPN soportadas	Red-a-Red, Nodo-a-Red y Nodo-a-Nodo
Algoritmos de encriptación	AES (Rjindael), DES, 3DES, Blowfish, Serpent de 128 bits, Twofish de 128 bits, y MPPE de 40 y 128 bits
Tipos de VPN soportados	PPTP e IPSec
Clientes de VPN soportados	Cliente PPTP nativo de Windows Cliente IPSec nativo de Windows Cliente Astaro Secure Tros clientes del estándar IPSec Cliente VPN de MacOS
Métodos de encriptación	PSK (Passphrase), Certificados (X.509v3), llaves RSA, CHAP, MSCHAP, MSCHAPv2, PAP, y RADIUS (para IPSec L2TP y PPTP)
Protocolos IPSec	Interchange Key Exchange (IKE), Encapsulated Security Payload (ESP) y Layer 2 Tunneling Protocol (L2TP)

Tabla 13. Características de diseño y operación del firewall Astaro TimeNET SecuRACK P-8/100.

Una característica relevante de este equipo, es que el VPN de Astaro incluye una autoridad de gestión de certificados interna con autentificación basada en PKI-trustchain. Esto permite el uso de certificados digitales sin que éstos tengan que ser generados centralmente y distribuidos a los sitios remotos.

Tal como se menciona en el apartado 2.4.3.5, *Definición del esquema de seguridad en el acceso a Internet*, el dispositivo firewall se compone de cuatro elementos, los cuales se detallan a continuación.

El *firewall* examina los encabezados de paquetes individuales para asegurarse de que éstos cumplen con las reglas del protocolo apropiado (filtrado de paquetes), y rastrea la secuencia de eventos durante las conexiones corrientes para detectar violaciones a los procesos normales (inspección de paquetes por estado).

El *firewall* de Astaro utiliza *proxies* de nivel de aplicación para revisar el contenido relacionado con las aplicaciones en los paquetes de comunicaciones. Astaro provee *proxies* que permiten habilitar o deshabilitar protocolos y funcionalidades tales como el filtrado de contenido, caché, filtrado por extensión de archivos, así como revisión de errores MIME. Los *proxies* están disponibles para los protocolos HTTP, DNS, SOCKS, POP3, Ident, y SMTP.

Este módulo proporciona cuatro funcionalidades importantes:

- NAT y Masquerading: Ambas técnicas esconden direcciones IP internas detrás de direcciones IP “públicas” para prevenir que los *hackers* lleguen a tener conocimiento de las redes internas, servidores y usuarios.
- Protección DoS: Protege contra ataques comunes de DoS (Denial of Service) como inundación TCP SYN, inundación ICMP, inundación UDP, Smurf, y Trinoo.
- Moldeo del tráfico y QoS: Permite incremento o decremento de la prioridad otorgada a los diferentes tipos de tráfico entre puntos específicos, proporcionando calidad de servicio (QoS) a transacciones críticas.

- Reporteo detallado: Astaro genera reportes detallados sobre el tráfico de la red, conexiones, violaciones al filtrado de paquetes, así como la utilización del hardware por el sistema *firewall*.

Gateway de VPN: Este módulo permite una fácil implementación de VPN con un alto nivel de seguridad. Utiliza una gran variedad de métodos avanzados de encriptación para proteger la información, y permite que la organización utilice una combinación de clientes VPN que satisfagan las necesidades de conveniencia y seguridad de los diferentes usuarios.

Entre las arquitecturas de VPN soportadas por este *gateway* están: Red-a-Red, Nodo-a-Red, y Nodo-a-Nodo. Los algoritmos de encriptación utilizados incluyen a: AES (Rjindael), DES, 3DES, Blowfish, Serpent de 128 bits, Twofish de 128 bits, y MPPE de 40 y 128 bits.

El *gateway* soporta VPN tanto PPTP como IPSec, entre los clientes permitidos están: El cliente PPTP nativo de Windows, el cliente IPSec nativo de Windows, el cliente Astaro Secure, otros clientes que manejen el estándar IPSec, y clientes VPN de MacOS. Adicionalmente ofrece los siguientes métodos de encriptación: PSK (Passphrase), Certificados (X.509v3), llaves RSA, CHAP, MSCHAP, MSCHAPv2, PAP, y RADIUS (para IPSec L2TP y PPTP).

Dentro de los protocolos IPSec, utiliza Interchange Key Exchange (IKE), Encapsulated Security Payload (ESP) y Layer 2 Tunneling Protocol (L2TP).

El VPN de Astaro incluye una autoridad para certificados interna con autentificación basada en PKI-trustchain. Esto permite el uso de certificados digitales sin que éstos tengan que ser generados centralmente y distribuidos a los sitios remotos.

Protección de navegación: Esta protección se compone básicamente de dos técnicas: el filtrado de contenido o de URL, y la protección anti-*spyware*.

El filtrado de contenido o de URL funciona bajo la premisa de que el administrador del sistema especifique los tipos de páginas *web* que son inapropiadas para los grupos de usuarios de la compañía. De esta forma, conforme el usuario solicita páginas *web*, el software revisa en una base de datos compuesta de 20 millones de direcciones *web* para, finalmente, registrar o bloquear el acceso al sitio solicitado.

Astaro resulta muy flexible para la creación de políticas de forma rápida y sencilla, así como la definición de perfiles de sitios inapropiados de entre cerca de 60 categorías diferentes. Los administradores pueden también crear listas blancas y listas negras de los sitios *web* que deberán estar accesibles o bloqueados según sea el caso.

El filtrado de contenido es proveído por Cobion, empresa mundialmente reconocida por su alto desempeño. Cobion se dedica a categorizar y a mantener la base de datos de 20 millones de direcciones de sitios *web*, siendo la base de datos más grande disponible para cualquier sistema comercial de filtrado de URL.

Las páginas *web* son analizadas utilizando sofisticadas técnicas de clasificación, tales como:

- Clasificación del texto: Las páginas *web* son calificadas utilizando factores tales como la frecuencia de ocurrencia de palabras y combinaciones de palabras.
- Reconocimiento óptico de caracteres: El texto es capturado y analizado.
- Reconocimiento visual de objetos: Los símbolos, logotipos, y marcas registradas son utilizados para categorizar los sitios *web*.
- Detección de pornografía: Se usa el reconocimiento de imágenes crudas y de caras para identificar fotografías con altas concentraciones de piel no facial.
- Comparación de similitudes: Las imágenes son comparadas con imágenes similares provenientes de sitios *web* ya clasificados.

La base de datos clasifica páginas *web* en 15 idiomas y si un usuario solicita una página que no está incluida en la base de datos, el URL es enviado a Cobion en donde será clasificada en las siguientes 24 horas.

El módulo de protección anti-*spyware* no sería implementado, ya que se analizó el escenario en el peor de los casos y se determinó que en conjunto los demás esquemas de seguridad contrarrestarían cualquier intento de ataque por medio de elementos del tipo *spyware*.

Protección de intrusiones: Realiza la detección de vulnerabilidades que indiquen:

- Sondeo de hostilidades, revisión de puertos, sondeo de "puertas traseras", cuestionamientos ilegítimos, barridos de clientes y otras actividades.
- Ataques DoS tales como inundación SYN.
- Explotación de protocolos, aprovechamiento de debilidades en DNS, FTP, ICMP, IMAP, POP3, RPC, SNMP, x11 y otros protocolos de red.
- Ataques a aplicaciones aprovechando errores de programación en software desarrollado internamente y código CGI, y en aplicaciones y bases de datos populares como ORACLE, MySQL Server, Coldfusion y Frontpage.
- Ataques dirigidos que aprovechen la vulnerabilidad del tráfico de mensajes y Chat, y conexiones punto a punto (P2P).

Al utilizar esta funcionalidad, nos aseguramos que todo el tráfico de Internet y de VPN es inspeccionado, y que no existan retrasos por el hecho de re-*enrutar* el tráfico a un sensor diferente. Información adaptada de ASL-V5 (2004). *User Manual*. Obtenida originalmente en 2004, de http://www.astaro.com, la cual ya no es vigente al momento de la elaboración de este documento, debido principalmente a la antigüedad del producto y a que la marca Astaro fue adquirida a mediados del 2011 por Sophos, perdiéndose algunas referencias sobre productos que –en esa fecha- ya habían completado su ciclo de vida.

Especificaciones de operación del antivirus

Antivirus para buzones de correo electrónico de Exchange: Al utilizar Microsoft Exchange Server, los buzones de correo electrónico de cada usuario se encuentran en un servidor centralizado, por lo que es en ese servidor donde los mensajes serán recibidos. Mientras el usuario final no abra su visor de correo electrónico, en este caso Microsoft Outlook, los mensajes estarán únicamente en el servidor en el que se alberga el buzón del usuario; siendo así, la suite antivirus realiza un análisis de los mensajes de correo electrónico y de sus archivos adjuntos cuando aún se encuentran en el servidor, limpiándolos, bloqueándolos o eliminándolos, de acuerdo a como se haya configurado la respuesta de la suite antivirus en caso de detectar amenazas. Bajo este esquema de protección, resultaría prácticamente imposible que un virus detectado en este punto, pudiese continuar su camino hasta llegar a la computadora o periféricos del usuario final.

En el caso de BDT todos los buzones de correo electrónico se ubicaban en un servidor del tipo Microsoft Exchange, por lo que el esquema de protección a nivel servidor, cubría perfectamente con este requerimiento.

Analizador en tiempo real y protección de acceso: Esta protección revisa todos los archivos que circularían en la red de datos de la compañía. Esta funcionalidad opera tanto a nivel servidor como a nivel de equipo de escritorio, ya que analiza los archivos descargados por medio de los navegadores haciendo uso de protocolos estándar de *web* (HTTP y FTP), así como aquellos que procedan de algún medio de almacenamiento que se encuentre conectado a la computadora del usuario final, ya sea localmente o por medio de la red local de datos, e igualmente analiza los archivos descargados por los usuarios con servicios de correo electrónico basados en *web*, tales como Hotmail, Yahoo, GMX, y muchos más.

La suite se instala localmente en cada computadora de la compañía, esta suite incluye un agente ePO (ePolicy Orchestrator), el cual es el enlace entre el software VirusScan y la herramienta de gestión ePO. El agente recibe comunicación de ePO central para saber cuándo y cómo deberá instalar la suite VirusScan, calendarizar búsquedas y análisis de virus, y actualizar las definiciones de virus.

El contar con un punto de control principal donde los virus puedan ser bloqueados rápidamente antes de que éstos puedan infectar la red interna brinda un alto nivel de confianza contra este peligro informático; de igual forma, representa un complemento de la solución antivirus implementada en el resto de la plataforma.

Características y configuración de los servidores

En el apartado 2.4.3.1, se mencionó la decisión de utilizar servidores marca Hewlett Packard modelo ProLiant ML370 G3 para los servidores de categoría crítica. Algunas de las características por las cuales se optó por este modelo se enlistan a continuación en las tablas 14 y 15.

Especificación	Valor
Procesador	Uno o dos procesadores Intel Xeon @ 2.8GHz con bus frontal de 533MHz.
Cache	1MB ECC L3 por cada procesador.
Controladora de arreglos de discos	Controladora de arreglos de discos HP Smart Array de doble canal para RAID 0, 1, 3, 5, 10, 30, y 50.
Sistema de almacenamiento masivo	6 bahías de tipo *hot-swap* para discos duros Ultra320 SCSI de 10,000 y 15,000 rpm. 2 bahías opcionales.
Almacenamiento interno máximo	6 discos de 300GB *hot-plug*, más 2 discos opcionales de 300GB, para un total de 2.34TB posibles.
Vídeo	Integrado, ATI Rage XL resolución de 1920 x 1200.
Tarjeta de red	Integrada, 10/100/1000 Gigabit.
Presentación	Compatible físicamente con los gabinetes y bastidores estándar de 19”.
Temperatura de operación	5° a 35°C
Fuente de voltaje	Una o dos fuentes de voltaje de tipo hot-swap con un consumo continuo de 500W cada una.

Tabla 14. Características físicas (hardware) de los servidores primarios seleccionados.

Especificación	Valor
Instalación y configuración	Navegador HP SmartStart, el cual realiza una instalación y configuración automatizada y guiada, facilitando estas actividades.
Software de monitoreo	▪ HP Insight Manager (HP SIM), software que facilita la solución de problemas, administración y monitoreo. Muestra información de inventario detallado, así como administración remota. ▪ Integrated Lights-Out (iLO)
Sistemas Operativos compatibles	▪ Microsoft Windows NT Server 3.51 y 4.0 ▪ Microsoft Windows 2000 Server ▪ Windows Server 2003 Server ▪ Novell NetWare ▪ Red Hat Linux ▪ SCO OpenServer y OpenUNIX ▪ SuSE Linux ▪ United Linux
Seguridad	▪ Contraseña de arranque ▪ Contraseña de administrador ▪ Botón de bloqueo de reinicio-apagado y teclado. ▪ Detección de intrusión al chasis del equipo ▪ Llave de acceso-bloqueo a las bahías de los discos duros.

Tabla 15. Características operativas de los servidores primarios seleccionados.

En el apartado 2.4.3.1, también se mencionó la decisión de utilizar servidores marca Hewlett Packard modelo ProLiant ML330 G3 para los servidores de categoría secundaria. Algunas de las características por las cuales se optó por este modelo se enlistan a continuación en las tablas 16 y 17.

Especificación	Valor
Procesador	Uno o dos procesadores Intel Xeon @ 2.8GHz o @ 3.06GHz, con bus frontal de 533MHz.
Cache	512KB ECC L2 por cada procesador.
Controladora de arreglos de discos	Controladora de arreglos de discos HP Smart Array de un solo canal capaz de manejar RAID 0, 1, 3, 5, 10, 30, y 50.
Sistema de almacenamiento masivo	3 bahías no *hot-plug* y 2 bahías opcionales *hot-plug* para discos duros Ultra320 SCSI de 10,000 y 15,000 rpm.
Almacenamiento interno máximo	3 discos de 146.8GB no *hot-plug*, más 2 discos opcionales *hot-plug* de 300GB, para un total de 1.04TB posibles.
Vídeo	Integrado, ATI Rage XL resolución de 1920 x 1200.
Tarjeta de red	Integrada, 10/100/1000 Gigabit.
Presentación	Compatible físicamente con los gabinetes y bastidores estándar de 19”.
Temperatura de operación	10° a 35°C
Fuente de voltaje	Una fuente de voltaje con un consumo continuo de 300W con Factor de Corrección de Potencia.

Tabla 16. Características físicas (hardware) de los servidores secundarios seleccionados.

Especificación	Valor
Instalación y configuración	Navegador HP SmartStart, el cual realiza una instalación y configuración automatizada y guiada, facilitando estas actividades.
Software de monitoreo	▪ HP Insight Manager (HP SIM), software que facilita la solución de problemas, administración y monitoreo. Muestra información de inventario detallado, así como administración remota. ▪ Integrated Lights-Out (iLO)
Sistemas Operativos compatibles	▪ Microsoft Windows NT Server 3.51 y 4.0 ▪ Microsoft Small Business Server 2000 ▪ Microsoft Small Business Server 2003 ▪ Windows Server 2003 ▪ Novell NetWare / Small Business Server 6.0 ▪ Linux (Red Hat, SuSE, United Linux)
Seguridad	▪ Contraseña de arranque ▪ Contraseña de instalación ▪ Detección de intrusión al chasis del equipo

Tabla 17. Características operativas de los servidores secundarios seleccionados.

La configuración de los siete servidores propuesta en el apartado 2.4.4.1, cubriría básicamente dos aspectos: el procesamiento, y el almacenamiento interno.

Para el procesamiento de los servidores de categoría crítica, la configuración propuesta fue la utilización de dos procesadores Intel Xeon @ 2.8GHz, con 1GB (512MB por procesador) de memoria RAM con monitoreo y corrección de errores.

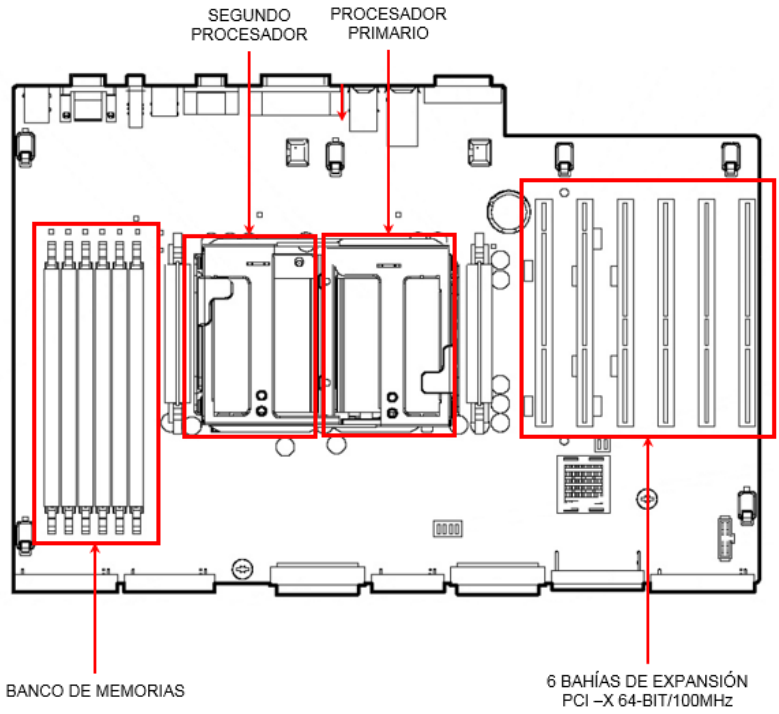


Figura 34. Configuración de la tarjeta madre de los servidores de categoría crítica, mostrando la configuración de doble procesador y las bahías de expansión.

Un aspecto importante de este modelo es la disponibilidad de seis bahías de expansión PCI-X para fines de conectividad con la SAN por medio de tarjetas de fibra óptica.

El almacenamiento interno de los servidores de categoría crítica fue manejado de la siguiente manera: para los servidores PDC, de los sistemas ERP y MES, y de redundancia, se generaron dos arreglos de discos independientes.

El primer arreglo consistió de tres discos duros de 18.2GB a 15,000 rpm cada uno, configurados en RAID 5, con lo que se obtenía una capacidad de almacenamiento disponible de 36GB (contra los 54.6GB en bruto), dos veces la velocidad de lectura y la posibilidad de falla de un disco duro sin perder información o detener la operación.

El segundo arreglo se realizó a partir de los cinco discos duros restantes (de los 8 posibles) con capacidad de 36.4GB a 15,000 rpm cada uno, configurados en RAID 5, con lo que se conseguía una capacidad total máxima de 144GB (contra los 182GB en bruto). Este segundo arreglo sería utilizado para almacenamiento de documentos en el caso del servidor PDC, y para contener las bases de datos operativas de tipo Oracle en el caso de los servidores de los sistemas ERP y MES. En la figura 35 se muestra la implementación física de dicha configuración.

Figura 35. Implementación física de los arreglos de discos para almacenamiento interno de los servidores PDC y de archivos, sistemas ERP y MES y de respaldo.

En el caso del servidor de correo electrónico, el primer arreglo se realizó con tres discos duros de 36.4GB cada uno, configurados también en RAID 5, resultando en una capacidad de almacenamiento disponible de 72GB (contra los 109.2GB en bruto). Este arreglo, sería utilizado para instalar el sistema operativo y para la utilización de los archivos de paginación, entre otras cosas.

El segundo arreglo se realizó a partir de ocho discos duros con capacidad de 72.8GB a 15,000 rpm cada uno, configurados en RAID 5, con lo que se conseguía una capacidad total máxima de 511GB (contra los 582.4GB en bruto). Este segundo arreglo sería utilizado para almacenamiento de las bases de datos de Exchange. En la figura 36 se muestra la implementación física de dicha configuración.

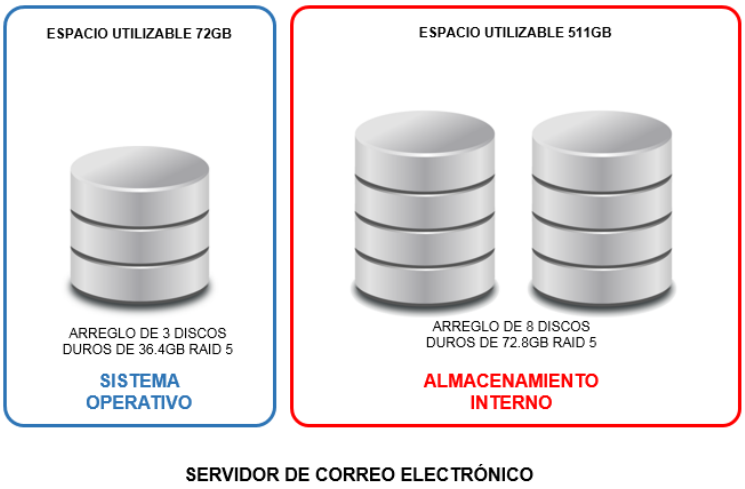


Figura 36. Implementación física de los arreglos de discos para almacenamiento interno del servidor de correo electrónico.

Para los servidores de categoría secundaria, la configuración propuesta fue la utilización de un solo procesador Intel Xeon @ 2.8GHz para el servidor de respaldos, e Intel Xeon @ 3.06GHz para el servidor de aplicaciones financieras y de recursos humanos; ambos con 1GB de memoria RAM con monitoreo y corrección de errores. Este modelo dispone de cuatro bahías de expansión PCI para fines de conectividad con la SAN por medio de tarjetas de fibra óptica en caso de ser necesario.

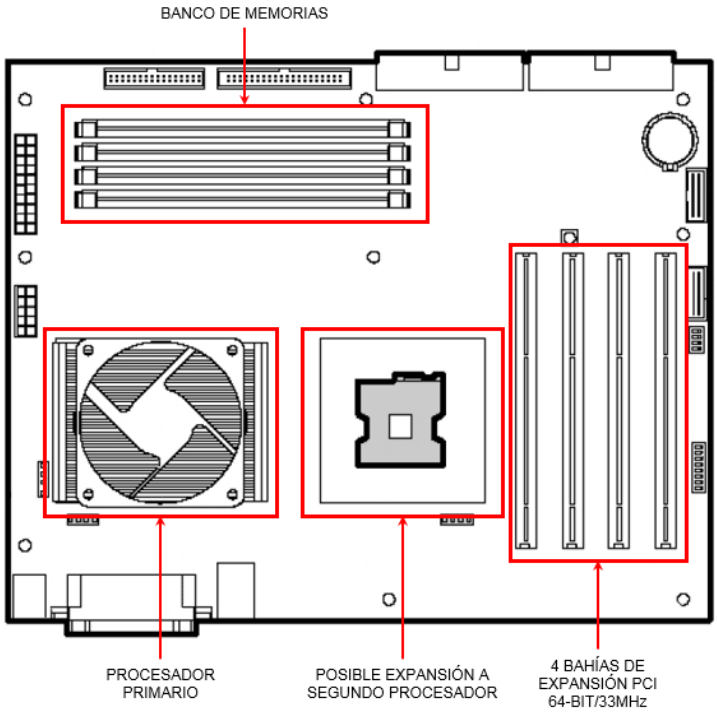


Figura 37. Configuración de la tarjeta madre de los servidores de categoría secundaria, mostrando la configuración de un solo procesador y las bahías de expansión.

El almacenamiento interno en los servidores de categoría secundaria constaría de un solo disco duro, ya que el software instalado en ellos podría ser reinstalado fácilmente y el volumen de información manejado no resultaba excesivo como para requerir una configuración más robusta. Los discos duros utilizados para este fin, serían de 36.4GB a 10Krpm de tipo SCSI U320;

Las imágenes y tablas de esta sección son adaptaciones de HP ProLiant ML370 (G3) Quick Specs (2005) [Guía rápida de especificaciones], obtenida de

https://h10057.www1.hp.com/ecomcat/hpcatalog/specs/emeapsg/99/HP_ProLiant_ML370_Generation_3.pdf,

y de HP ProLiant ML330 (G3) Quick Specs (2005) [Guía rápida de especificaciones], obtenida de https://www.hpe.com/h20195/v2/getpdf.aspx/c04283012.pdf

Características y configuraciones física y lógica de la SAN

De acuerdo con HP StorageWorks Modular Smart Array family (2004) [Ficha técnica], obtenida de https://www.senetic.ro/i/objects/HP_literature_emea_en_DA-12095.pdf algunas de las características que hicieron de la MSA1000 nuestra mejor opción fueron:

- Controladores de alto desempeño
- Chasis modular cuyo diseño permite su instalación en gabinete o bastidor, ocupando 4U, combinando el controlador con la caja de discos (14 discos) en una misma unidad. Escalabilidad de 1 a 42 discos por medio de cajas externas MSA30 (14 discos cada una) de 3U, ocupando 10U si se implementara la configuración máxima de este equipo.
- Conexiones de FC de 2Gb. Las pruebas independientes de desempeño demostraban una velocidad de transmisión de hasta 30,000 IOPS[39] y un ancho de banda de hasta 200 MB/s con un solo controlador MSA1000.
- *Switch* de Fibra Canal integrado de 8 puertos
- Utilización de discos de clase empresarial HP Ultra2 (velocidad de transferencia de 80 MB/s), Ultra3 (160 MB/s), y Ultra320 (320 B/s), todos de tipo SCSI de 1" a 15K rpm, que, al reducir la saturación, permiten las velocidades de transferencia indicadas para cada tipo de disco. Todos estos discos se ofrecían en formato *hot plug*, es decir que podían ser insertados o retirados aun estando el equipo en funcionamiento.
- Compatible con software de respaldos y recuperación ISV y Veritas, entre otros.
- Interfaz gráfica de configuración de arreglos (*Array Configuration Utility*, ACU), así como de monitoreo de los controladores y de detección de fallas potenciales (*Array Diagnostics Utility*, ADU), ambas sumamente amigables con el usuario.

[39] Input/Output Operations Per Second (IOPS). Es una unidad de referencia que se utiliza para medir el rendimiento relativo de dispositivos tales como unidades de disco duro, e indica el número total de operaciones de entrada/salida (combinación de pruebas de lectura y escritura en dichas unidades) por segundo observables en esos dispositivos.

- Compatible con sistemas operativos tales como Windows Server 2003 (32 y 64 bits), Windows 2000, Windows NT, NetWare y Linux (32 y 64 bits), y de manera limitada con HP-UX, SCO, Tru64 Unix y OpenVMS. Gracias a esta característica, se podría continuar utilizando este equipo –y no perder la inversión-, en caso de que la compañía llegase a modificar su preferencia de sistema operativo y optase por uno diferente al indicado en la sección 2.4.2.1, *Elección del sistema operativo de red*.
- Opción de un paquete de alta disponibilidad que proveía el hardware necesario para brindad redundancia.
- Posibilidad de implementación del nivel máximo de tolerancia a fallas en la configuración de los arreglos de disco por medio de RAID[40] 6 (RAID ADG[41]), el cual ubica dos conjuntos de información de paridad a través de los discos y permite operaciones simultáneas de escritura. Este nivel de tolerancia a fallas, permite la falla simultánea de dos discos sin que esto ocasione tiempos muertos o pérdida de información.

Tanto el equipo MSA 1000 como el MSA 30, elegidos para cubrir las demandas de almacenamiento compartido, fueron habilitados con 14 discos duros de 72.8GB c/u, obteniéndose un espacio de almacenamiento en bruto de 2TB; sin embargo, al crearse los arreglos de discos, este espacio se redujo en proporción de dos discos por cada uno de los equipos.

Recordemos que se utilizaron arreglos RAID 6, por lo que el espacio final disponible para utilización resultó ser de 1.7TB (1,752GB). Posteriormente se realizaron los volúmenes que estarían visibles para los usuarios y las aplicaciones.

[40] Redundant Array of Inexpensive Disks (RAID): Un sistema RAID está compuesto por múltiples discos usados en paralelo. Este arreglo proporciona redundancia al distribuir los bits de paridad a través del rango completo de discos, haciendo posible reconstruir la información encontrada en un disco en particular en caso de que éste falle.

[41] Advanced Data Guarding (ADG): En este tipo de arreglo, la paridad es generada y almacenada con la finalidad de protegerse contra la pérdida de información causada por daños físicos en los discos duros. ADG genera dos conjuntos diferentes de paridad para cada bloque de información en una lista, entonces los dos bloques de paridas son almacenados en diferentes discos físicos, permitiendo conservar la información aun cuando dos discos fallen simultáneamente. Se requieren al menos cuatro discos duros para implementar un arreglo ADG.

La figura 38 muestra la vista física de los discos duros disponibles para la creación de un arreglo utilizando la Interfaz gráfica de configuración de arreglos (Array Configuration Utility, ACU).

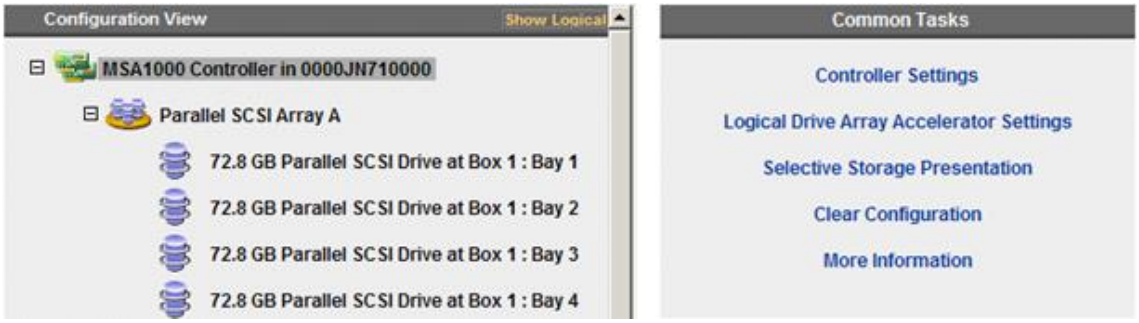


Figura 38. Vista **física** de los discos duros utilizables para la creación de un arreglo por medio de la herramienta ACU; es posible observar la capacidad de cada disco duro y la bahía en la que se encuentra instalado.

La figura 39 muestra la vista lógica de los discos lógicos (volúmenes) realizados a partir de los discos duros disponibles.

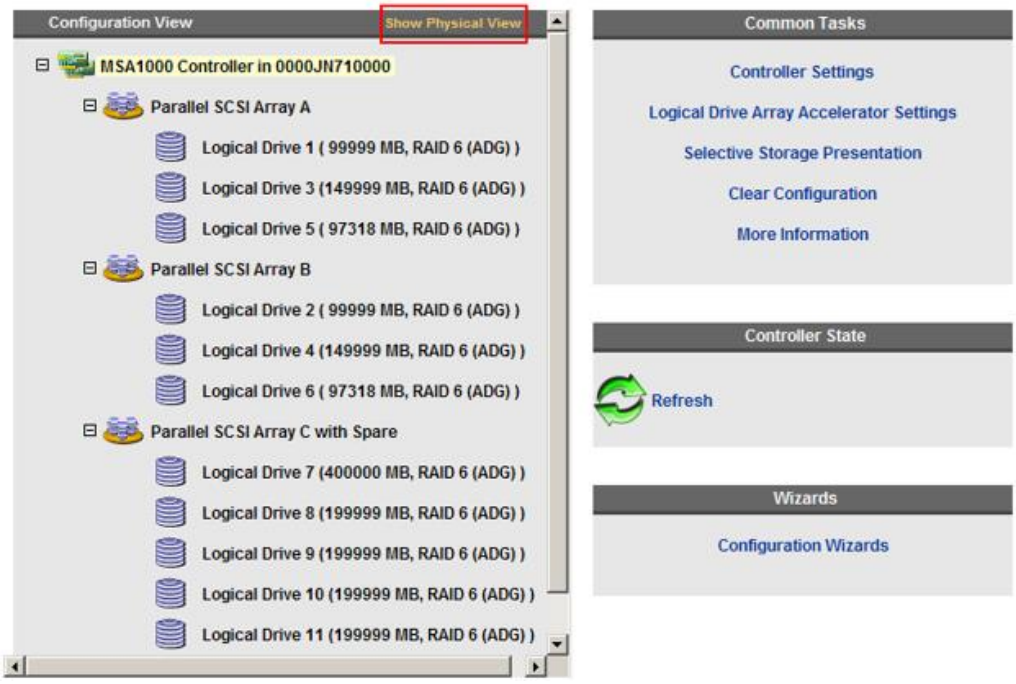


Figura 39. Vista **lógica** de los volúmenes realizados a partir de los discos duros de la vista física por medio de la herramienta ACU; es posible observar la capacidad final de cada volumen.

Posteriormente, gracias a la presentación selectiva de la herramienta ACU, al poder revisar cuáles volúmenes (discos lógicos) estarían disponibles, sería posible asignar su acceso por determinado servidor, tal como lo muestra la figura 40.

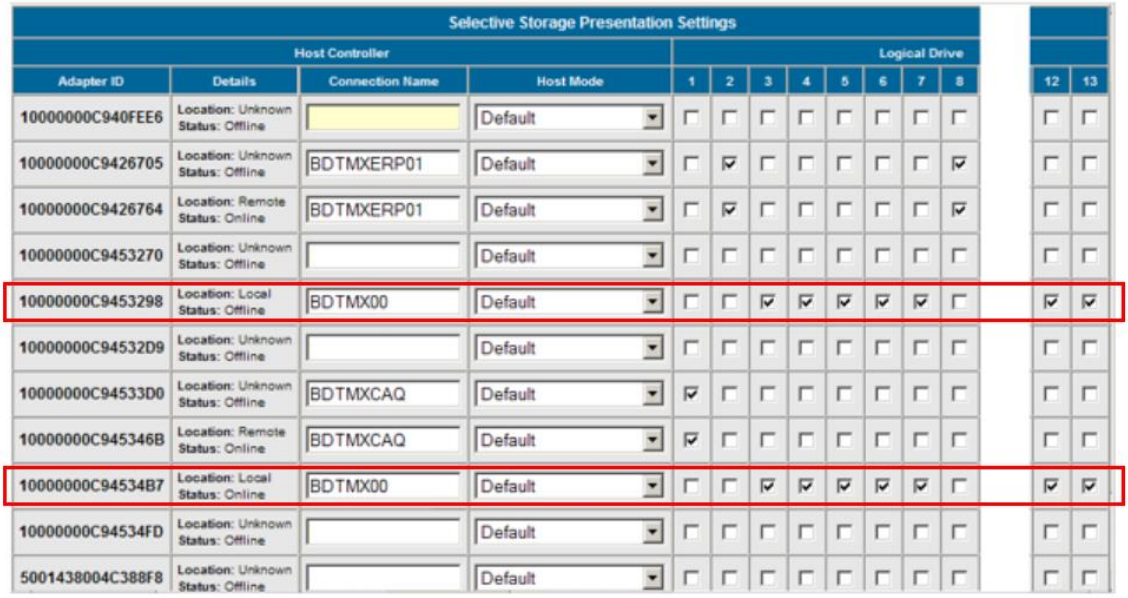


Figura 40. Presentación **selectiva** de los volúmenes y los posibles servidores por medio de los cuales se puede tener acceso a ellos. Nótese la existencia de dos conexiones para cada servidor.

Características de los componentes del cableado de red

A continuación, se muestran las características relevantes del cable, paneles de conexión y conectores utilizados en el cableado de red.

	Margen del peor par (1-250 MHz)	
	Garantizado	**Típico**
Pérdida de inserción	5.0%	6.5%
Pr-Pr NEXT	6.0 dB	9.4 dB
PSNEXT	7.5 dB	10.6 dB
Pr-Pr ELFEXT	6.0 dB	11.3 dB
PSELFEXT	8.0 dB	12.7 dB
Pérdida del retorno	4.0 dB	5.7 dB

Tabla 18. Capacidades del cable UTP categoría 6 no pleno.

	Panel de parcheo 1100GS3	Cable de parcheo modular GS8E
	Margen del peor par	**Margen garantizado**
Pérdida de inserción	64.3%	5.0%
NEXT	6.6 dB	6.0 dB
PSNEXT	7.3 dB	7.5 dB
ELFEXT	6.4 dB	6.0 dB
PSELFEXT	6.1 dB	8.0 dB
Pérdida del retorno	6.6 dB	4.0 dB
Rango de frecuencia	1-250 MHz	1-250 MHz

Tabla 19. Capacidades del panel de parcheo y del cable de parcheo modular.

	Conector de telecomunicaciones MGS400	Cable de parcheo modular GS8E
	Margen del peor par	**Margen garantizado**
Pérdida de inserción	29.9%	5.0%
NEXT	5.4 dB	6.0 dB
PSNEXT	4.7 dB	7.5 dB
ELFEXT	10.5 dB	6.0 dB
PSELFEXT	10.8 dB	8.0 dB
Pérdida del retorno	8.0 dB	4.0 dB
Rango de frecuencia	1-250 MHz	1-250 MHz

Tabla 20. Capacidades de los conectores de telecomunicaciones y del cable de parcheo modular.

Trayectorias de cableado por área operativa

A continuación, se muestran los planos sin escala del resto de las trayectorias de cableado de red, la ubicación de sus IDF correspondientes, y la ubicación de los nodos de red de cada una de esas áreas operativas.

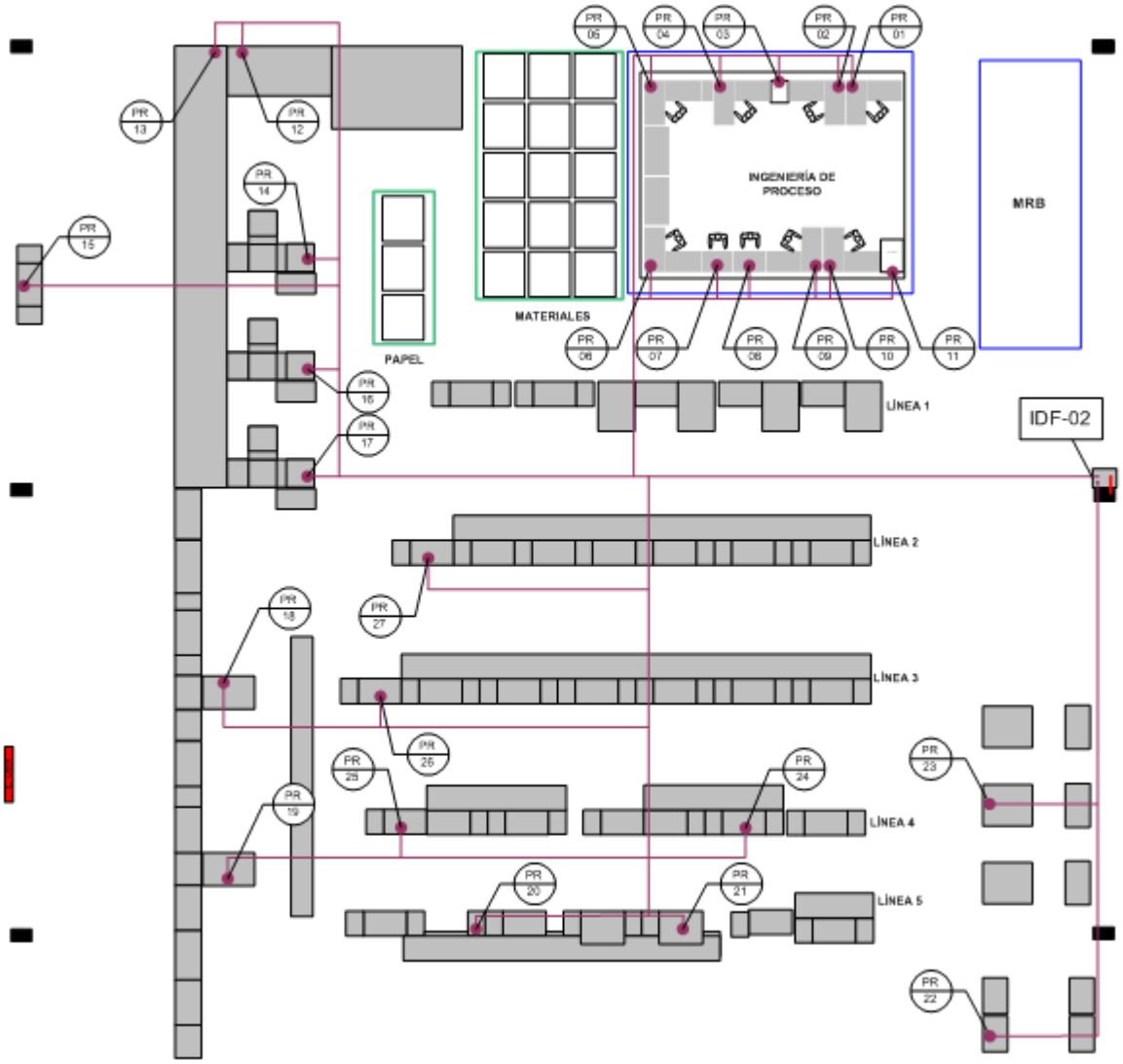


Figura 41. Diagrama de conexiones de los servicios de la red de datos desde el IDF02 hasta las diferentes ubicaciones del área de manufactura de productos *Paper Handling*, así como del área de Ingeniería de Procesos.

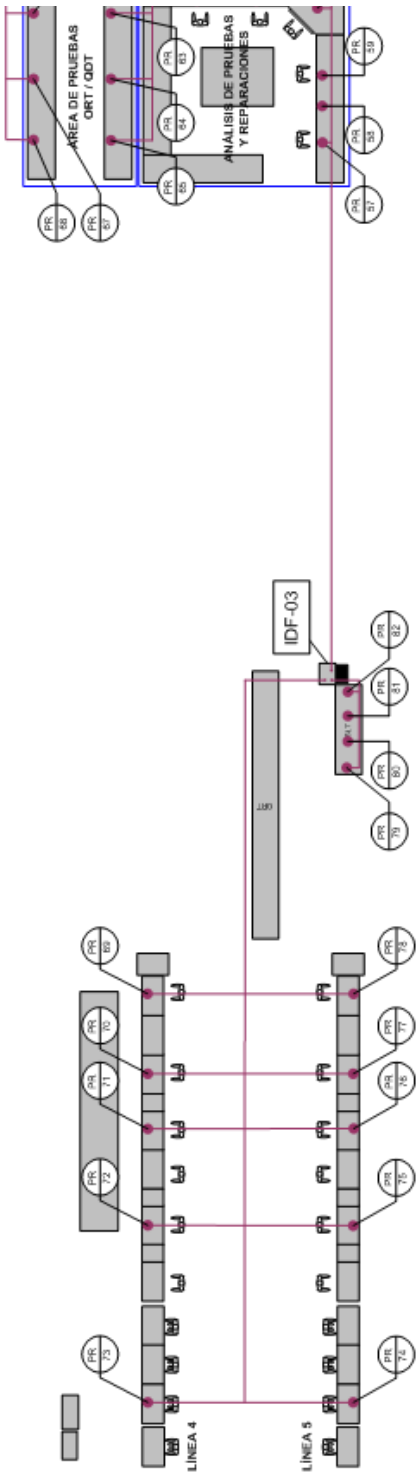


Figura 42. Diagrama de conexiones de los servicios de la red de datos desde el IDF03 hasta los equipos ubicados en las líneas de producción 4 y 5 del área de manufactura de productos Storage y se análisis de fallas y reparaciones.

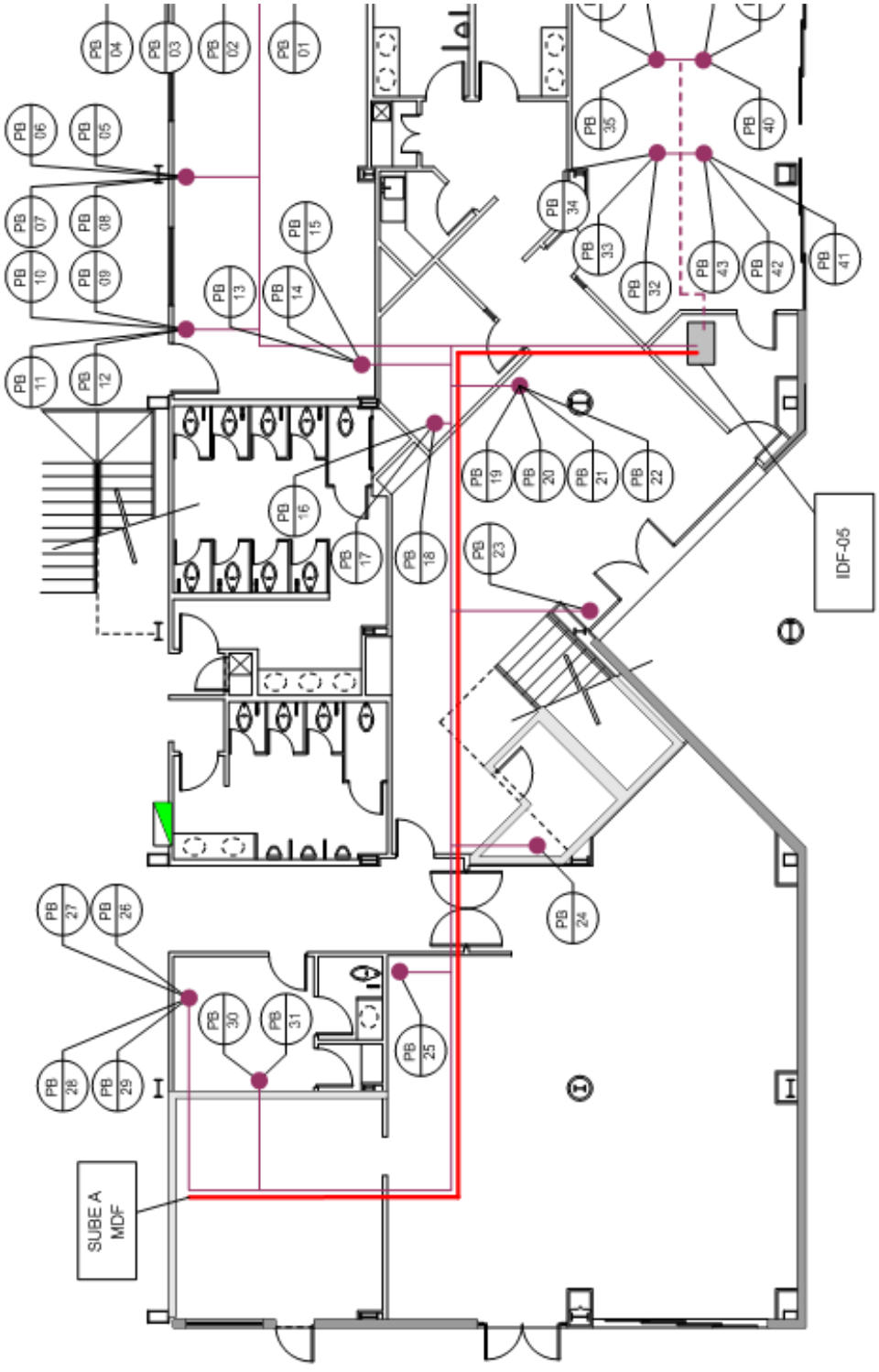


Figura 43. Diagrama de conexiones de los servicios de la red de datos desde el IDF05 hasta los equipos ubicados en la planta baja del edificio.

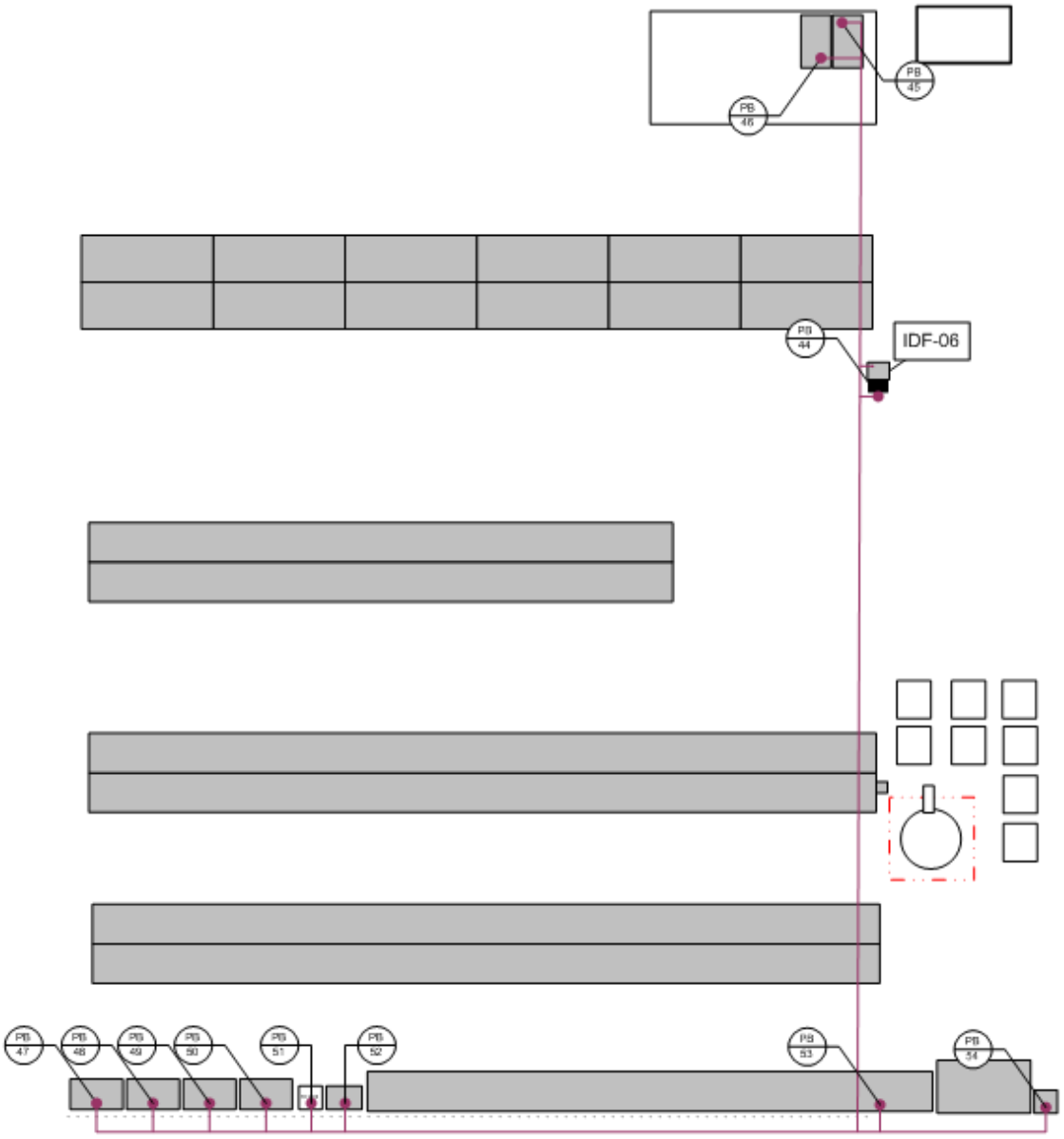


Figura 44. Diagrama de conexiones de los servicios de la red de datos desde el IDF06 hasta las diferentes ubicaciones del área de almacén.

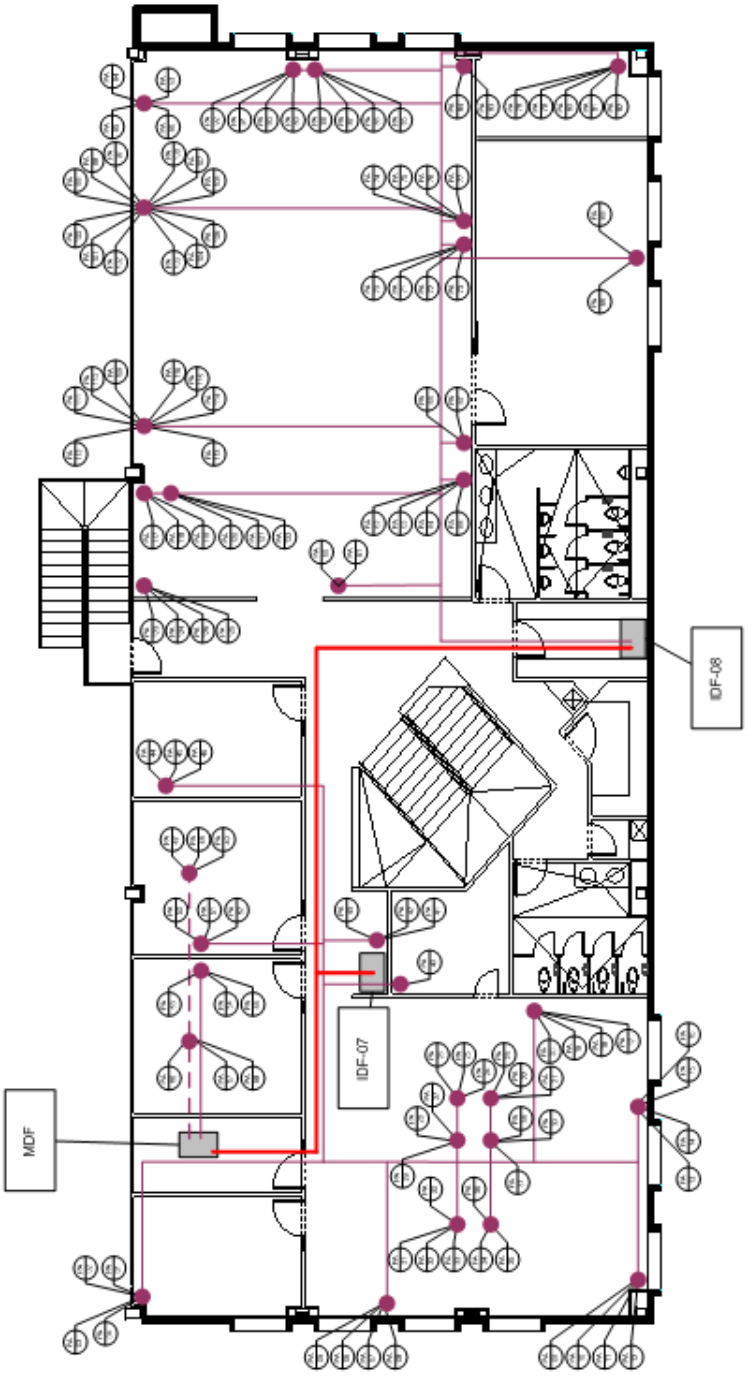


Figura 45. Diagrama de conexiones de los servicios de la red de datos desde los IDF07 e IDF08 hasta las diferentes ubicaciones de la planta alta.

Tablas de referencia de conectividad de los diferentes nodos de red

IDF – 01		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PR28	I01-01-01	14.6
PR29	I01-01-02	17.0
PR30	I01-01-03	19.0
PR31	I01-01-04	16.3
PR32	I01-01-05	21.0
PR33	I01-01-06	31.0
PR34	I01-01-07	33.5
PR35	I01-01-08	36.0
PR36	I01-01-09	38.5
PR37	I01-01-10	41.0
PR38	I01-01-11	14.6
PR39	I01-01-12	16.3
PR40	I01-01-13	17.9
PR41	I01-01-14	19.5
PR42	I01-01-15	21.2
PR43	I01-01-16	23.0
PR44	I01-01-17	24.5
PR45	I01-01-18	26.0
PR46	I01-01-19	20.0
PR47	I01-01-20	23.4
PR48	I01-01-21	25.6
PR49	I01-01-22	27.8
PR50	I01-01-23	30.0
PR51	I01-01-24	35.4
PR52	I01-01-25	33.8
PR53	I01-01-26	30.0
PR54	I01-01-27	27.8
PR55	I01-01-28	25.6
PR56	I01-01-29	23.4
Total de nodos conectados al IDF-01		29

Tabla 21. Cantidad de nodos de red conectados al IDF-01, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

IDF – 02		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PR01	I02-01-01	40.0
PR02	I02-01-02	38.8
PR03	I02-01-03	37.0
PR04	I02-01-04	35.5
PR05	I02-01-05	33.0
PR06	I02-01-06	25.5
PR07	I02-01-07	27.0
PR08	I02-01-08	28.0
PR09	I02-01-09	30.0
PR10	I02-01-10	31.0
PR11	I02-01-11	33.0
PR12	I02-01-12	41.0
PR13	I02-01-13	42.6
PR14	I02-01-14	34.2
PR15	I02-01-15	39.0
PR16	I02-01-16	30.0
PR17	I02-01-17	26.5
PR18	I02-01-18	40.6
PR19	I02-01-19	42.5
PR20	I02-01-20	37.0
PR21	I02-01-21	35.5
PR22	I02-01-22	26.0
PR23	I02-01-23	20.0
PR24	I02-01-24	37.0
PR25	I02-01-25	36.0
PR26	I02-01-26	35.5
PR27	I02-01-27	27.0
Total de nodos conectados al IDF-02		27

Tabla 22. Cantidad de nodos de red conectados al IDF-02, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

IDF – 03		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PR57	I03-01-01	23.4
PR58	I03-01-02	24.5
PR59	I03-01-03	26.0
PR60	I03-01-04	28.5
PR61	I03-01-05	30.0
PR62	I03-01-06	31.4
PR63	I03-01-07	33.4
PR64	I03-01-08	35.0
PR65	I03-01-09	37.0
PR66	I03-01-10	37.5
PR67	I03-01-11	39.0
PR68	I03-01-12	41.0
PR69	I03-01-13	20.5
PR70	I03-01-14	22.5
PR71	I03-01-15	24.5
PR72	I03-01-16	27.0
PR73	I03-01-17	31.0
PR74	I03-01-18	31.0
PR75	I03-01-19	27.0
PR76	I03-01-20	24.5
PR77	I03-01-21	22.5
PR78	I03-01-22	20.5
PR79	I03-01-23	17.3
PR80	I03-01-24	16.0
PR81	I03-01-25	15.0
PR82	I03-01-26	14.0
Total de nodos conectados al IDF-03		26

Tabla 23. Cantidad de nodos de red conectados al IDF-03, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

El IDF-04 fue omitido intencionalmente ya que éste fue reservado para un uso posterior durante el crecimiento de la red de datos en el área de manufactura de los productos de *almacenamiento*.

IDF – 05		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PB01	I05-01-01	32.0
PB02	I05-01-02	32.0
PB03	I05-01-03	32.0
PB04	I05-01-04	32.0
PB05	I05-01-05	29.0
PB06	I05-01-06	29.0
PB07	I05-01-07	29.0
PB08	I05-01-08	29.0
PB09	I05-01-09	25.5
PB10	I05-01-10	25.5
PB11	I05-01-11	25.5
PB12	I05-01-12	25.5
PB13	I05-01-13	30.5
PB14	I05-01-14	30.5
PB15	I05-01-15	30.5
PB16	I05-01-16	21.0
PB17	I05-01-17	21.0
PB18	I05-01-18	21.0
PB19	I05-01-19	21.0
PB20	I05-01-20	21.0
PB21	I05-01-21	21.0
PB22	I05-01-22	21.0
PB23	I05-01-23	28.5
PB24	I05-01-24	32.5
PB25	I05-01-25	34.0
PB26	I05-01-26	49.5
PB27	I05-01-27	49.5
PB28	I05-01-28	49.5
PB29	I05-01-29	49.5
PB30	I05-01-30	46.0
PB31	I05-01-31	46.0
PB32	I05-01-32	14.5
PB33	I05-01-33	14.5
PB34	I05-01-34	14.5
PB35	I05-01-35	16.0
PB36	I05-01-36	16.0
PB37	I05-01-37	16.0
PB38	I05-01-38	16.0
PB39	I05-01-39	16.0
PB40	I05-01-40	16.0
PB41	I05-01-41	14.5
PB42	I05-01-42	14.5
PB43	I05-01-43	14.5
Total de nodos conectados al IDF-05		43

Tabla 24. Cantidad de nodos de red conectados al IDF-05, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

IDF – 06		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PB44	I06-01-01	08.0
PB45	I06-01-02	24.7
PB46	I06-01-03	21.5
PB47	I06-01-04	47.8
PB48	I06-01-05	46.0
PB49	I06-01-06	44.5
PB50	I06-01-07	42.6
PB51	I06-01-08	40.0
PB52	I06-01-09	38.4
PB53	I06-01-10	29.0
PB54	I06-01-11	36.0
Total de nodos conectados al IDF-06		11

Tabla 25. Cantidad de nodos de red conectados al IDF-06, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

IDF – 07		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PA22	I07-01-22	25.0
PA23	I07-01-23	25.0
PA24	I07-01-24	24.0
PA25	I07-01-25	24.0
PA26	I07-01-26	24.0
PA27	I07-01-27	22.5
PA28	I07-01-28	22.5
PA29	I07-01-29	22.5
PA30	I07-01-30	24.0
PA31	I07-01-31	24.0
PA32	I07-01-32	24.0
PA33	I07-01-33	24.0
PA34	I07-01-34	25.0
PA35	I07-01-35	25.0
PA36	I07-01-36	25.0
PA37	I07-01-37	22.5
PA38	I07-01-38	22.5
PA39	I07-01-39	22.5
PA40	I07-01-40	16.0

La tabla continúa en la página siguiente.

Continuación de la tabla en la página anterior.

IDF – 07		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PA41	I07-01-41	16.5
PA42	I07-01-42	16.5
PA43	I07-01-43	16.5
PA44	I07-01-44	21.0
PA45	I07-01-45	21.0
PA46	I07-01-46	21.0
PA47	I07-01-47	18.0
PA48	I07-01-48	18.0
PA49	I07-01-49	18.0
Total de nodos conectados al IDF-07		49

Tabla 26. Cantidad de nodos de red conectados al IDF-07, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.

IDF – 08		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PA60	I08-01-01	23.5
PA61	I08-01-02	23.5
PA62	I08-01-03	23.5
PA63	I08-01-04	23.5
PA64	I08-01-05	23.5
PA65	I08-01-06	23.5
PA66	I08-01-07	25.5
PA67	I08-01-08	25.5
PA68	I08-01-09	33.5
PA69	I08-01-10	33.5
PA70	I08-01-11	29.0
PA71	I08-01-12	29.0
PA72	I08-01-13	29.0
PA73	I08-01-14	29.0
PA74	I08-01-15	30.0
PA75	I08-01-16	30.0
PA76	I08-01-17	30.0
PA77	I08-01-18	30.0
PA78	I08-01-19	38.0
PA79	I08-01-20	38.0
PA80	I08-01-21	38.0

La tabla continúa en la página siguiente.

Continuación de la tabla en la página anterior.

IDF – 08		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PA81	I08-01-22	38.0
PA82	I08-01-23	38.0
PA83	I08-01-24	33.5
PA84	I08-01-25	33.5
PA85	I08-01-26	37.0
PA86	I08-01-27	37.0
PA87	I08-01-28	37.0
PA88	I08-01-29	37.0
PA89	I08-01-30	37.0
PA90	I08-01-31	37.0
PA91	I08-01-32	37.0
PA92	I08-01-33	37.0
PA93	I08-01-34	40.5
PA94	I08-01-35	40.5
PA95	I08-01-36	40.5
PA96	I08-01-37	40.5
PA97	I08-01-38	38.0
PA98	I08-01-39	38.0
PA99	I08-01-40	38.0
PA100	I08-01-41	38.0
PA101	I08-01-42	38.0
PA102	I08-01-43	38.0
PA103	I08-01-44	38.0
PA104	I08-01-45	38.0
PA105	I08-01-46	38.0
PA106	I08-01-47	38.0
PA107	I08-01-48	38.0
PA108	I08-02-01	38.0
PA109	I08-01-02	33.0
PA110	I08-01-03	33.0
PA111	I08-01-04	33.0
PA112	I08-01-05	33.0
PA113	I08-01-06	33.0
PA114	I08-01-07	33.0
PA115	I08-01-08	33.0
PA116	I08-01-09	33.0
PA117	I08-01-10	31.0
PA118	I08-01-11	31.0
PA119	I08-01-12	31.0
PA120	I08-01-13	31.0

La tabla continúa en la página siguiente.

Continuación de la tabla en la página anterior.

IDF – 08		
NODO	**CONEXIÓN (IDF-PANEL-PUERTO)**	DISTANCIA AL IDF (EN METROS)
PA121	I08-01-14	31.0
PA122	I08-01-15	31.0
PA123	I08-01-16	29.0
PA124	I08-01-17	29.0
PA125	I08-01-18	29.0
PA126	I08-01-19	29.0
Total de nodos conectados al IDF-08		67

Tabla 27. Cantidad de nodos de red conectados al IDF-08, indicando la distancia de cada uno de ellos respecto al IDF, así como su identificación única dentro de la red de datos.