UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE LA PLATAFORMA INFORMÁTICA DEL INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y LA PROPIEDAD INTELECTUAL (INDECOPI)

INFORME DE COMPETENCIA PROFESIONAL

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

ALEJANDRO CARBAJAL DIAZ

PROMOCIÓN
2006-I

LIMA-PERÚ
2011

DISEÑO E IMPLEMENTACIÓN DE LA PLATAFORMA INFORMÁTICA DEL INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y LA PROPIEDAD INTELECTUAL (INDECOPI)

A Dios, por inspirar la vocación de ingeniero en mi ser.

A mis padres, por todo el apoyo y amor brindado a lo largo de los años de carrera.

A mis hermanas, por alegrar mis días con su presencia.

A mis amigos, que cumplieron su sueño de ser profesionales al lado mío.

SUMARIO

En el Informe de Competencia Profesional desarrollado en este documento se expone el diseño e implementación de la nueva plataforma informática del Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual (INDECOPI).

El proyecto se justificaba debido a la obsolescencia tecnológica del equipamiento que daba soporte a las aplicaciones que eran utilizadas por INDECOPI para brindar servicios, tanto al público en general, como a los usuarios internos y remotos.

La problemática de la plataforma tecnológica de INDECOPI se resume en lo siguiente: habían islas de información, no existía protección de los datos a nivel de disco, los equipos tenían la garantía vencida, los esquemas de respaldo eran ineficientes, los equipos de cómputo eran inadecuados para su desempeño, eran bajos los niveles de disponibilidad y rendimiento del servicio, la administración era compleja, la escalabilidad era limitada, la red estaba conformada por un solo dominio de colisiones, los puntos de red y equipamiento no estaban identificados, etc.

El proyecto es agrupado en dos aspectos principales y que constituyen los ítems 1 y 3 de la licitación pública. Cada una de ellas se desarrolla en capítulos separados:

- Diseño y renovación de la infraestructura del Data Center (servidores, sistemas de almacenamiento y de respaldo, migración de servicios).
- Diseño y renovación de la infraestructura de redes y comunicaciones (routers y switches bajo un modelo de arquitectura jerárquica de redes, además de la solución de seguridad perimetral y los trabajos relacionados a la renovación del cableado estructurado, migración de servicios).

ÍNDICE

INTRODUCCIÓN

El proyecto de renovación de la plataforma tecnológica se origina en la necesidad de INDECOPI de proporcionar servicios de calidad a sus clientes internos y externos. Para ello procede a la realizar una Licitación Pública denominada "Optimización y Ampliación de la Plataforma Informática del INDECOPI".

La licitación estuvo conformada por tres ítems independientes: ítem1 "Servidores y Almacenamiento", ítem 2 "Adecuación del Data Center", e ítem 3 "Redes y Comunicaciones"; para lo cual COSAPI DATA S.A. fue adjudicado con la Buena Pro en los ítems 1 y 3. El ítem 2 debía ser previamente realizado, aspecto que estuvo a cargo de otro postor.

La problemática a resolver se enfocaba en la obsolescencia tecnológica de INDECOPI y que causaba diversos problemas en su desempeño, y por ende, en asegurar los servicios para la que estaba diseñado brindar. Esta problemática se podría resumir en lo siguiente:

- Infraestructura del Data Center.- Se contaba con una serie de servidores físicos independientes que tenían contratos de mantenimiento vencidos (La mayoría había alcanzando su fin de vida de servicio). La capacidad de los equipos había llegado a su límite (memoria y disco), limitando así la escalabilidad de la plataforma. No existían esquemas de redundancia para las aplicaciones instaladas en los servidores constituyéndose así en puntos únicos de falla, lo que mermaba la disponibilidad de los servicios. Había problemas en la administración de la información crítica de la institución, y los sistemas de respaldo de la información estaban inoperantes. Su cableado estructurado no estaba mapeado, era de una categoría desfasada y los enlaces principales no eran redundantes.
- La infraestructura de redes y comunicaciones.- La red no contaba con un modelo de arquitectura jerárquica (Núcleo, Distribución y Acceso) conformándose así en un solo dominio de colisiones y de broadcast, lo cual implicaba una alta saturación de la red. La seguridad perimetral había estado mal diseñada ya que era fácilmente vulnerable. No se contaba con una solución VPN (Red Virtual Privada), lo cual obligaba a publicar los servicios internos de INDECOPI a Internet. Tampoco se contaba con un sistema de prevención de intrusos de modo que lo hacía vulnerable a ataques directamente a nivel de aplicaciones. El cableado estructurado no había pasado por ningún proceso de

certificación, existían cables de diferente categoría, el cableado no estaba rotulado ni documentado.

Las tecnologías utilizadas para la solución de la infraestructura del Data Center son los siguientes: servidores blades y servidores rackeables, un sistema de almacenamiento con expansión, una librería de respaldo (todos de fabricación IBM) además de un software para consolidación y virtualización,

Las tecnologías utilizadas para la solución de la infraestructura de redes y comunicaciones son: switches multicapa (capas 2 y 3) con puertos GigabitEthernet y FastEthernet (Cisco 3560) usados en las capas de distribución y acceso, y un switch para la capa de núcleo (Cisco 6509 Enhaced), software de administración Cisco Works LMS. Por otro lado, la seguridad perimetral se implementa con equipos dedicados especialmente diseñados para realizar su labor: Firewal Central (Cisco ASA) y un IPS (Sistema de Prevención de Intrusión) Cisco IPS-4240-K9, estableciéndose estrictas políticas de seguridad.

El Informe de Competencia Profesional se divide en cuatro capítulos principales

- Capítulo I.- Se expone y evalúa el problema de ingeniería que experimenta la institución. En dicho capítulo se precisan los objetivos y alcances, se hace una síntesis del trabajo.
- Capítulo II.- Se desarrolla el diseño e implementación de la solución relacionada a la infraestructura del Data Center (servidores y almacenamiento).
- Capítulo III.- Se desarrolla el diseño e implementación de las soluciones de comunicaciones y seguridad informática (arquitectura jerárquica de redes y comunicaciones de la red de área local), además del cableado estructurado. El capítulo concluye con las labores de migración para proveer de funcionalidad a la totalidad del proyecto.
- Capítulo IV.- Se explican las pruebas realizadas además de los resultados obtenidos. Posteriormente se desarrolla lo referente al presupuesto y al cronograma del proyecto de ingeniería (Gantt).

Los capítulos de diseño (II y III) contienen los requerimientos, planteamiento, dimensionamiento, implementación de la solución, además del plan de pruebas. En los mismos capítulos se incluyen los aspectos conceptuales necesarios para el entendimiento de la solución.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema, para ello primeramente se describe el problema y luego se expone el objetivo del trabajo, también se evalúa el problema y se precisan los alcances del informe, para finalmente presentar una síntesis trabajo presentado.

1.1 Descripción del problema

Obsolescencia de la plataforma tecnológica en la cual residen las aplicaciones utilizadas por la institución para brindar servicios al público en general, a los usuarios internos y a las localidades remotas de INDECOPI.

La problemática se resumía en lo siguiente: equipamiento con la garantía vencida, con recursos al límite y sin capacidad de ser escalados; presencia de puntos únicos de falla; sistemas de respaldo de la información inoperantes, información no centralizada; arquitectura de red inadecuada lo que producía alta saturación de la red; sistema de seguridad vulnerable y ausencia de una solución de red virtual privada, cableado estructurado de categoría inadecuada y sin documentar, entre otras deficiencias.

1.2 Objetivos del trabajo

Es la renovación tecnológica y estructural de la plataforma informática de INDECOPI con el fin de dar un óptimo servicio a sus clientes internos y externos, mediante el diseño y puesta en operación de soluciones de servidores, almacenamiento, redes y comunicaciones, que eliminen las deficiencias detectadas en el análisis de la problemática de la plataforma informática.

Este objetivo está orientado a dos aspectos principales, que en resumen son los objetivos secundarios:

- Infraestructura del Data Center (servidores y almacenamiento).- Diseñar una nueva infraestructura para integrar y migrar los servidores existentes a equipos de mayor tecnología, y adicionalmente, proporcionar una solución de almacenamiento y de respaldo.
- Redes y comunicaciones.- Diseñar una nueva infraestructura de red Informática y de seguridad perimetral apoyada en una renovación tecnológica, que garantice la correcta comunicación e intercambio de información.

Para ambas se deben aplicar las mejores políticas de desempeño y seguridad a fin de

optimizar los recursos de la nueva plataforma en beneficio de las labores propias del INDECOPI.

1.3 Evaluación del problema

En la presente sección se describe brevemente a INDECOPI (institución gubernamental) así como a la licitación y los ítems que comprende el proyecto desarrollado. Finalmente, se expone de manera resumida el estado de INDECOPI a nivel de infraestructura tecnológica previa a la solución implementada y con lo que se justifica la necesidad de su renovación.

1.3.1 Acerca de INDECOPI

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) fue creado en noviembre de 1992, mediante el Decreto Ley N° 25868.

Tiene como funciones la promoción del mercado y la protección de los derechos de los consumidores. Además, fomenta en la economía peruana una cultura de leal y honesta competencia, resguardando todas las formas de propiedad intelectual: desde los signos distintivos y los derechos de autor hasta las patentes y la biotecnología.

El INDECOPI es un organismo público especializado adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público interno. En consecuencia, goza de autonomía funcional, técnica, económica, presupuestal y administrativa (Decreto Legislativo Nº 1033).

Como resultado de su labor en la promoción de las normas de leal y honesta competencia entre los agentes de la economía peruana, el INDECOPI es concebido en la actualidad, como una entidad de servicios con marcada preocupación por impulsar una cultura de calidad para lograr la plena satisfacción de sus clientes: la ciudadanía, el empresariado y el Estado [1].

La misión de INDECOPI es promover y garantizar la leal competencia, los derechos de los consumidores y la propiedad intelectual en el Perú, propiciando el buen funcionamiento del mercado, a través de la excelencia y calidad de su personal [2].

1.3.2 La licitación pública

INDECOPI, con los fines de proporcionar servicios de calidad a sus clientes internos y externos, decide renovar su plataforma de informática, para lo cual se procede a la realización de una Licitación Pública denominada "Optimización y Ampliación de La Plataforma Informática del INDECOPI" [3].

Esta licitación comprende tres ítems independientes cuyos objetivos se muestran a continuación [4]:

- El Ítem 1 - Servidores y Almacenamiento.- integración y migración de sus actuales

servidores a equipos con nueva tecnología; e implementar soluciones de almacenamiento en discos, adicionando una solución de "backup" (respaldo) con el fin de dar un óptimo servicio a sus clientes internos y externos.

- El Ítem 2 - Adecuación del Data Center.- acondicionamiento de su actual sala de servidores, a fin de contar con las facilidades necesarias para albergar los equipos de almacenamiento, procesamiento y transporte de datos de la institución dentro de un entorno de seguridad y confiabilidad recomendada por los estándares para centros de cómputo.

- El Ítem 3- Redes y Comunicaciones.- actualizar y reordenar su infraestructura de Red Informática a través de la mejor solución de redes y seguridad perimetral e incluye la renovación de equipamiento de comunicaciones, de tal manera que se obtenga, conjuntamente con las soluciones de cableado, los rendimientos de desempeño y performance adecuado para garantizar la correcta comunicación e intercambio de información.

El postor COSAPI DATA S.A. fue adjudicado con la Buena Pro en los ítems 1 y 3. Para cumplir con las metas, el ítem 2 debía ser previamente realizado, aspecto que estuvo a cargo de otro postor.

1.3.3 Situación previa a la solución

En esta subsección se explica la problemática agrupada en los ítems correspondientes: infraestructura del Data Center, redes y comunicaciones, adecuación física del Data Center

a. Infraestructura del Data Center

Respecto a la Infraestructura del Data Center, INDECOPI contaba con una serie de servidores (19) los cuales poseían contratos de mantenimiento vencidos y serias limitaciones en las renovaciones de las garantías del hardware debido a la antigüedad de los mismos. La mayoría de ellos estaban alcanzando el EOSL (End of Service Life – Fin de Vida de Servicio), lo que significaba que el fabricante de los equipos no podía brindar extensiones de garantía más allá de la fecha del EOSL, lo cual representaba un riesgo elevado para la institución.

Adicionalmente, las capacidades de procesamiento de los equipos estaban llegando sus valores límites, principalmente memoria y disco, lo cual limitaba la escalabilidad de la plataforma.

Así mismo no se manejaban esquemas de redundancia para las aplicaciones instaladas en los servidores (arreglos de discos, fuentes redundantes o esquemas de clusterización a nivel de sistema operativo o de aplicación), los cuales los convertían en puntos únicos de falla (SPF-Single Point of Failure), disminuyendo notoriamente la

disponibilidad de los servicios soportados por el sistema.

INDECOPI no contaba con un sistema de almacenamiento central, de modo que la información estaba dispersa entre todos los servidores generando problemas en la administración de la información crítica de la institución (disponibilidad, continuidad operativa, respaldo). Adicionalmente, los sistemas de respaldo de la información estaban inoperantes.

En cuanto al cableado estructurado. INDECOPI carecía de mapas de red y puntos finales identificado, así mismo el cableado utilizado era de una categoría desfasada. Los enlaces desde el Data Center hacia los usuarios en los edificios contiguos del mismo no eran redundantes, y ante la falta de identificación de puntos, representaban un potencial riesgo en caso de avería de cualquiera de estos enlaces.

b. Redes y Comunicaciones

A nivel de capa de enlace, la red de datos de INDECOPI estaba compuesta por múltiples switches capa 2 sin ningún tipo de configuración, todos ellos en arquitectura tipo "cascada". No había una identificación de la distribución de los switches. La red, en general, trabajaba a 100 Mbps en el Núcleo (Core) y a 10 Mbps en la periferia.

A nivel de capa de red, existía un segmento de servidores publicados a Internet y otro segmento de servidores en la misma subred de la red de usuarios. Sin embargo, y dado que todos los switches trabajaban solamente en capa 2, los dominios de colisiones y de broadcast se propagaban por toda la red sin importar de qué segmento de red provenían. En resumen, la red no contaba con un modelo de arquitectura jerárquica (Núcleo, Distribución y Acceso) conformándose así en un solo dominio de colisiones y de broadcast, lo cual implicaba una alta saturación de la red.

Respecto a la seguridad, el único dispositivo perimetral que tenía INDECOPI, era una PC convencional que contaba con tres tarjetas de red (Internet, Servidores Publicados a Internet, Red Interna). Este equipo tenía por función evitar que los usuarios accedieran a los servidores publicados en Internet y a la publicación de estos últimos. Sin embargo, bastaba con cambiar la dirección IP en una PC convencional de la red del segmento perteneciente a la red de usuarios, a uno perteneciente a la red de servidores publicados en Internet, para tener acceso sin restricciones a estos servidores (debido a que toda la red era un solo dominio de colisiones, como se explicó previamente). La situación inclusive permitía a un usuario tomar una dirección IP pública del rango de direcciones IP disponibles de INDECOPI (mediante una resolución de DNS simple) permitiendo que el usuario tenga salida sin restricciones a Internet

Adicionalmente INDECOPI contaba con una serie de usuarios que necesitaban acceso remoto a los servicios internos de la institución, sin embargo no se contaba con

una solución VPN (Red Virtual Privada), lo cual obligaba a publicar los servicios internos de INDECOPI a Internet.

INDECOPI no contaba con un sistema de prevención de intrusos de modo que lo hacía vulnerable a ataques directamente a nivel de aplicaciones (robo de información, alteración de bases de datos, modificación de los servicios web, denegación de servicios, etc.).

Respecto al cableado estructurado existente, este no había pasado por ningún proceso de certificación, existían cables de diferente categoría, el cableado no estaba rotulado ni documentado.

c. Adecuación física del Data Center

Aunque no fue parte del trabajo realizado por COSAPI DATA, es necesario explicar la situación inicial del Data Center a nivel de infraestructura física.

Los equipos de INDECOPI originalmente fueron acondicionados en un salón ubicado en el cuarto piso del edificio donde se encuentra el área de sistemas. A medida que los sistemas fueron creciendo, se fueron acondicionando servicios adicionales en mesas sobre los cuales se ubicaban los servidores. No existía falso techo, falso piso ni líneas redundantes de energía, tampoco aire acondicionado de precisión (se usaba el mismo que el de las oficinas), no existía un control de acceso electrónico y los UPS (sistema de potencia ininterrumpida) ya habían sido rebasados en capacidad.

Estudios posteriores, determinaron que la infraestructura del Centro de Datos tenía una mala distribución del peso, lo que representaba un alto riesgo de ruptura del piso, por lo que se vio obligado a implementar el nuevo Data Center en el primer piso del edificio en mención.

Este nuevo Data Center, fue implementado previamente a la ejecución de los ítems 1 y 3 de la licitación pública (descritos en a y b de la presente sección). El Data Center fue equipado con falso piso y falso techo adecuados, aire acondicionado de precisión, UPS dimensionados para un crecimiento futuros, sistema contraincendios, gabinetes para montaje de equipos, líneas de energía redundantes y control de acceso electrónico (huella digital).

1.4 Alcance del trabajo

Los trabajos asociados al ítem “Infraestructura Informática del Data Center” comprenden el diseño e implementación de la solución servidores y sistema de almacenamiento, el cual se divide en dos partes:

- Diseño e implementación de la plataforma tecnológica.
- Migración de los servicios generales y de las aplicaciones.

Los trabajos relacionados a “Redes y Comunicaciones” comprenden:

- La mejora de la actual red principal de comunicaciones (backbone) mediante el diseño e implementación de la red de área local (LAN) utilizando un modelo de arquitectura jerárquica (Núcleo, Distribución y Acceso).
- Proporcionar una solución de seguridad de firewall y un sistema de prevención de intrusión (IPS - Intrusion Prevention System).

Lo antes mencionado estuvo supeditado a la implementación de la estructura física del Data Center (obra civil, parte eléctrica, ducterías, gabinetes de montaje, climatización y seguridad de acceso físico), los cuales fueron provistos por INDECOPI.

1.5 Síntesis del trabajo

En esta sección se explica los aspectos que se desarrollan en cada uno de los capítulos principales de diseño.

- Desarrollo de la Infraestructura Informática del Data Center.- Consta del análisis situacional (requerimientos del Data Center, problemática, estrategias de desarrollo de la solución), del diseño, implementación y plan de pruebas (topología de la solución, habilitación y pruebas de la solución de servidores y almacenamiento) y la migración de los servicios generales y de las aplicaciones.
- Desarrollo de la arquitectura jerárquica de redes y comunicaciones.- Consta del análisis situacional (requerimientos, problemática, estrategias de desarrollo de la solución), la solución de comunicaciones (topología de redes, segmentación de VLANs, Gestión centralizada de comunicaciones), la solución de seguridad informática (políticas de seguridad establecidas, esquema final de la red de INDECOPI en función a las políticas establecidas), el cableado estructurado (aspectos normativos y descripción de trabajos), y la migración hacia la nueva red y plan de pruebas de desempeño y continuidad operativa.

CAPÍTULO II
DESARROLLO DE LA INFRAESTRUCTURA INFORMÁTICA DEL DATA CENTER

Como se explicó en el capítulo I. El proyecto desarrollado con COSAPI DATA, respecto a la licitación referida, consistía en los ítems 1 y 3 de las bases integradas. En este capítulo se presenta el desarrollo del ítem 1, es decir el correspondiente a la infraestructura del data center.

Este capítulo se divide en tres partes principales:

- En la primera se realiza el análisis situacional, en donde se exponen requerimientos estipulados y las necesidades de los usuarios. Complementariamente se evalúa la problemática particular y finalmente se plantean las estrategias de solución.
- En la segunda se desarrolla el diseño, implementación y definición del plan de pruebas de la plataforma tecnológica..
- En la tercera se refiere a la migración de módulos de aplicación y bases de datos.

2.1 Análisis situacional

Es necesario primeramente precisar los requerimientos, para luego evaluar la problemática y así plantear las estrategias de desarrollo de la solución (Se resumen al final de esta sección en la Tabla 2.1).

2.1.1 Requerimientos del Data Center

Como fue mencionado, INDECOPI requería de una solución llave en mano para la integración y migración de sus servidores a equipos con nueva tecnología mediante la consolidación de los recursos informáticos de la institución; e implementar soluciones de almacenamiento en discos y respaldo (backup) con el fin de dar un óptimo servicio a sus clientes internos y externos.

Los trabajos de este ítem consistían en la implementación del hardware, software y del cableado del Data Center (implementación de la plataforma tecnológica). A consecuencia de ello, se debía realizar una migración de módulos de aplicación en Web (57 módulos) y sus correspondientes bases de datos (5 Oracle y 4 SQL) a los servidores instalados utilizando soluciones de consolidación de recursos informáticos.

Para la ejecución de este ítem, INDECOPI también licitó la adquisición del hardware y software necesario, según se lista a continuación:

- 1 Chasis para Servidores Blade.
- 4 Servidores Blade (Tipo 1)

- 1 Servidor rackeable (Tipo 1)
- 1 Servidor rackeable (Tipo 2 para Servidor BD)
- 1 Sistema de Almacenamiento.
- 1 Librería de Backup
- Sistema de consolidación.

Las características que debían cumplir estos componentes se describen en el Anexo A "Requisitos para Servidores y Almacenamiento".

Adicionalmente INDECOPI proporcionó licenciamiento para bases de datos Oracle, a ser utilizadas en un servidor especializado para bases de datos.

El plazo para la Implantación del Ítem 1 fue de 105 días calendario desde el día siguiente a la entrega de de equipos.

Con el hardware y software disponibles, se debía diseñar un esquema para la solución. Esta sección se divide en tres subsecciones: análisis situacional, diseño e implementación de plataforma tecnológica; migración de aplicaciones y de los servicios generales.

2.1.2 Problemática

El análisis se realiza en dos campos: Las bases de datos Oracle, y los servicios generales:

a. Bases de datos Oracle

Debido a la criticidad de la información que reside en estos equipos, se observaron los siguientes problemas:

- **Islas de información:** La información crítica se encontraba distribuida entre 2 servidores de producción y uno de desarrollo, haciendo complicada la gestión de la información, y la adecuada asignación de recursos de cómputo para la solución.
- **No existía protección de los datos a nivel de disco:** No había esquemas redundancia de discos en los equipos. Ante la falla de cualquier disco de los servidores, se hubiera perdido información crítica, asimismo, se hubiera generado cortes en los principales servicios de INDECOPI.
- **Equipos con garantía vencida:** Los equipos se encontraban sin garantía del fabricante, ante cualquier avería de componentes, INDECOPI hubiera tenido serios problemas para restaurar el servicio.
- **Esquemas de respaldo ineficientes:** Al contar con islas de información, era complicado y costoso tomar el respaldo de las bases de datos, los que se hacían por la LAN, sin cumplir las ventanas de tiempo requeridas para estas aplicaciones.
- **Requerimientos de escalabilidad:** INDECOPI ha venido interactuando con más entidades privadas y públicas en el transcurso del tiempo, lo cual se ha reflejado en

mayores accesos a sus servicios de bases de datos. En la plataforma actual, no podían seguir escalando de una manera adecuada, tanto en espacio físico como en recursos de cómputo.

b. Servicios generales

INDECOPI estaba integrando mayores usuarios internos de manera remota. Los servicios generales, como el correo, servicios de archivos, Intranet, servicios de antivirus, directorios de usuarios, y algunas bases de datos de producción sobre SQL, encontraban los siguientes desafíos:

- **Equipo de cómputo inadecuado para su desempeño:** Los servicios generales no contaban con equipos adecuados, varios de ellos inclusive estaban montados en PCs convencionales, que no ofrecían ninguna garantía de continuidad operativa.
- **Disponibilidad y rendimiento del servicio:** INDECOPI ya venía presentando cortes en varios servicios críticos, como los de Firewall y los servicios de Correo Electrónico, debido a fallas en el hardware y en afinamiento de la aplicación, así como también problemas de rendimiento general.
- **Complejidad en la administración:** Múltiples servidores físicos, ocupando espacio físico en el centro de datos, hacían complejos los mantenimientos. Algunos equipos tenían problemas de arranque si es que eran reiniciados, o necesitaban acciones manuales de usuario, como conectar teclados para el reinicio de los equipos. Asimismo, no se podía determinar si los problemas de rendimiento que tenían determinadas aplicaciones eran por estar montadas en un equipo inadecuado, o por falta de afinamiento de los servicios.
- **Escalabilidad basada en equipamiento nuevo, se encontraba limitada:** INDECOPI no podía implementar servicios nuevos en su plataforma actual, la única alternativa que tenían disponible era la de agregar equipos nuevos, pese a contar con problemas para ubicar los equipos en su centro de datos original, que no estaba preparado para recibir más equipos, tanto por distribución del espacio físico, problemas con el piso del Datacenter que se encontraba debilitado y no soportaba peso adicional, como por problemas de energía y refrigeración.

2.1.3 Estrategias de desarrollo de la solución

Según el análisis de la problemática se plantea las estrategias que den solución a las deficiencias detectadas. Estas estrategias se resumen en lo siguiente

a. Estrategias para bases de datos

Son las siguientes:

- **Consolidación de la información**: Esto se consigue migrando la data a un sistema de almacenamiento central, de modo que toda la información crítica de la institución se

encuentre en un solo lugar brindado así protección y disponibilidad de los datos

- **Protección de datos a nivel de disco**: Los sistemas de almacenamiento centralizados ofrecen varios niveles de protección de disco, ello implementando arreglos redundantes de discos independientes (RAID - Redundant Array of Independent Disks). Esto hace posible configurar varios de estos arreglos para las aplicaciones de bases de datos, además de brindar un nivel de protección adecuado para un componente determinado de la aplicación. La explicación de los RAID se detalla en el Anexo B.
- **Renovación tecnológica**: Precisamente a raíz del problema de pérdida de garantía se pudo justificar la adquisición de nuevo equipamiento para la plataforma tecnológica de INDECOPI. El equipo especializado para bases de datos y el sistema de almacenamiento se adquirieron con garantía del fabricante por un periodo de 5 años.
- **Arquitectura escalable**: La solución brindada implicó utilizar un equipo especializado para el trabajo con bases de datos, utilizando tecnologías propietarias diseñadas para incrementar el rendimiento de estas aplicaciones, lo cual va en consistencia con los requerimientos de crecimiento de INDECOPI, así mismo al consolidar los datos de las aplicaciones de base de datos en el sistema de almacenamiento central, es simple brindar espacio físico y rendimiento adicional a la aplicación añadiendo discos en "caliente", es decir sin interrupción del servicio.
- **Adición de la solución de backup**: Para solucionar el problema de los respaldos de bases de datos se planteó el uso de una librería de cintas conectada a la red de almacenamiento (SAN) y gestionada por el software de backup de INDECOPI. Esto permitió que los datos fueran respaldados utilizando la red de almacenamiento en lugar de la red LAN, brindando un camino dedicado al respaldo de la información crítica de INDECOPI.

b. Estrategias para servicios generales

Son las siguientes:

- **Renovación tecnológica:** Para los servicios generales se adquirieron servidores basados en tecnología x86 en conjunto con un software de "virtualización" que permitió trabajar con máquinas virtuales sobre los nuevos equipos. Estos servidores también fueron conectados al sistema de almacenamiento para brindar también consolidación de datos y funciones avanzadas de alta disponibilidad, brindadas por el software de virtualización. Estos equipos se adquirieron con 5 años de garantía del fabricante.
- **Solución de virtualización de servidores en alta disponibilidad:** La arquitectura sobre la cual se migraron los servidores originales de INDECOPI proporcionaban varios puntos redundantes ante fallas y crecimiento escalable. En esta nueva plataforma es posible asignar más recursos de cómputo sin necesidad de caída de servicios,

garantizando la disponibilidad de la misma.

- **Administración centralizada:** La plataforma de virtualización habilita la gestión de todos los servidores virtuales desde un solo punto , por tanto las funciones de aprovisionamiento de nuevos servidores o incremento de recursos computacionales para los servidores existentes, despliegue de sistemas operativos y aplicativos, instalación de "parches" en los equipos, y administración personalizada para cada servidor componente de la infraestructura virtual, es ejecutada desde una sola consola gráfica.

- **Escalabilidad basada en equipamiento virtual:** Dado que las máquinas virtuales son paquetes de datos que son cargados en la memoria de los servidores físicos (como un hardware virtual), para poder desplegar nuevo equipamiento de producción basta con hacer una copia basada en una máquina virtual existente a la que se le aplica personalización de su configuración. Esto permite también contener el crecimiento de servidores físicos dado que por concepto la virtualización permite que un servidor físico aprovisione varias máquinas virtuales con distintos sistemas operativos y aplicativos, cada una de ellas.

La Tabla 2.1 resume la problemática y estrategia expuesta.

Tabla 2.1 Problemática y solución planteada (Fuente: Elab. propia)

Problemática	Solución planteada
Base de datos Oracle	
Islas de información	Consolidación de la información en un sistema de almacenamiento central.
Falta de protección de datos a nivel de disco	Protección de datos en función al requerimiento de la aplicación.
Garantía de equipos vencida	Renovación tecnológica (garantía 5 años)
Esquema de respaldo ineficiente	Instalación de una librería de backup conectada a la red de almacenamiento.
Escalabilidad limitada	Implementación de una arquitectura escalable
Servicios generales	
Equipo de cómputo inadecuado	Renovación tecnológica (garantía 5 años)
Disponiblidad y rendimiento del sistema afectados	Virtualización de servidores en alta disponibilidad
Complejidad de la administración	Administración centralizada de la plataforma virtual
Escalabilidad limitada	Escalabilidad basada en infraestructura virtual

2.2 Diseño, implementación y plan de pruebas

Como fue mencionado, los servidores existentes en INDECOPI se encontraban en el límite de su capacidad, alcanzaban la obsolescencia y representaban un riesgo para la continuidad del negocio.

La opción tecnológica se abarcó de la siguiente manera:

- Se contó con un sistema de almacenamiento central, donde se consolidaron todos los

servicios de INDECOPI (bases de datos y servicios generales).

- Para las bases de datos se utilizaron servidores con arquitectura propietaria, que permitía la consolidación de servidores de bases de datos, mediante una técnica llamada particionamiento (LPAR).

- Para los servicios generales se utilizaron servidores de formato físico blade o cuchilla basados en arquitecturas x86, utilizando un software de virtualización de servidores.

Es necesario explicar brevemente los conceptos relacionados

- **Tecnología blade**.- consiste en el uso de servidores de alta densidad física (tipo "cuchillas") de modo tal que permite agrupar varios de ellos en un solo compartimento físico (Chassis o enclosure) compartiendo así recursos tales como energía, comunicaciones LAN y SAN (Storage Area Network) y administración (Figura 2.1). Cada cuchilla es un servidor físico con recursos de procesamiento, memoria y periféricos externos (LAN y SAN) independientes. Estos servidores pueden contar además con discos locales en arreglos de discos, aunque pueden trabajar sin ello cuando se utiliza un sistema de almacenamiento centralizado. El uso de esta tecnología genera ahorros en espacio físico en Data Center, energía, y eficiencia operativa.

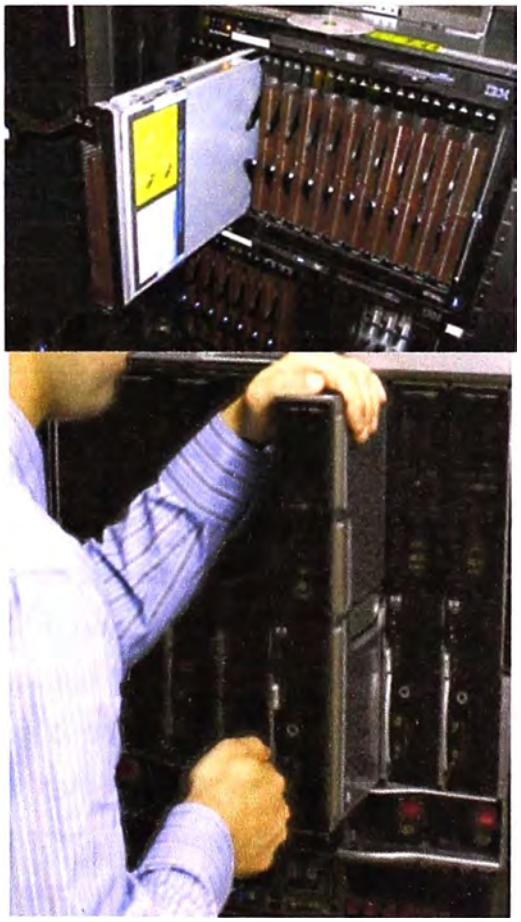

Figura 2.2 Chassis Blade Center y servidores blade (cuchillas) (Fuente: ref [5])

- **Virtualización**.- ésta es una tecnología basada en software que se instala sobre los servidores físicos y que conforman una capa llamada "Hypervisor", que permite agrupar

los recursos de procesamiento, memoria, disco y comunicaciones externas (LAN, SAN) para asignarlos a entes encapsulados llamados "máquinas virtuales", que son archivos cargados en las memorias de los servidores que representan un hardware emulado sobre el cual se puede instalar un sistema operativo tradicional, tal cual se hace sobre un equipo físico convencional. Ello permite instalar múltiples equipos virtuales con diversos sistemas operativos y cada uno de ellos con un aplicativo o aplicativos específicos, lo cual genera consolidación de servidores físicos, reducción del espacio en el Data Center, reducción del consumo de energía, administración centralizada y uso óptimo de los recursos físicos dado que esto aprovecha mejor el rendimiento de hardware más potente. La Figura 2.2 ilustra el esquema general de esta tecnología.

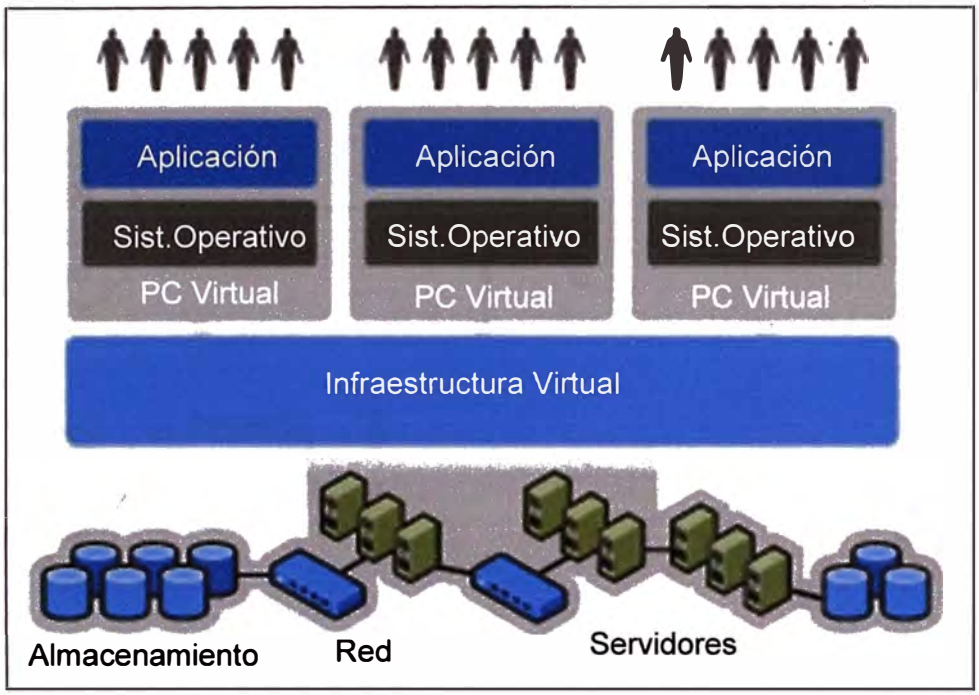

Figura 2.2 Esquema general de la tecnología de virtualización (Fuente: ref. [6])

- **Particionamiento (LPAR)**.- LPAR es un subconjunto de recursos de hardware ubicados dentro del mismo servidor. Una máquina física puede dividirse en múltiples LPAR, cada LPAR se convierte en una máquina virtual independiente y puede contener sistema operativo diferente. El particionamiento lógico se realiza en la capa de hardware, dos LPAR pueden tener acceso a un mismo chip de memoria dentro de los rangos de memoria asignada para que puedan acceder directamente. Varios CPUs pueden usarse para un LPAR o ser compartidos entre varias.

La distribución de los servidores preexistentes en INDECOPI se ilustra en la Figura 2.3. En ella se puede diferenciar a los servidores físicos DMZ (zona desmilitarizada), al servidor firewall, y a los servidores físicos internos. Se puede también apreciar los motores de bases de datos utilizadas en ellas, el servicio que realiza cada una de ellas. Los íconos acompañados de un cilindro indican que contienen bases de datos

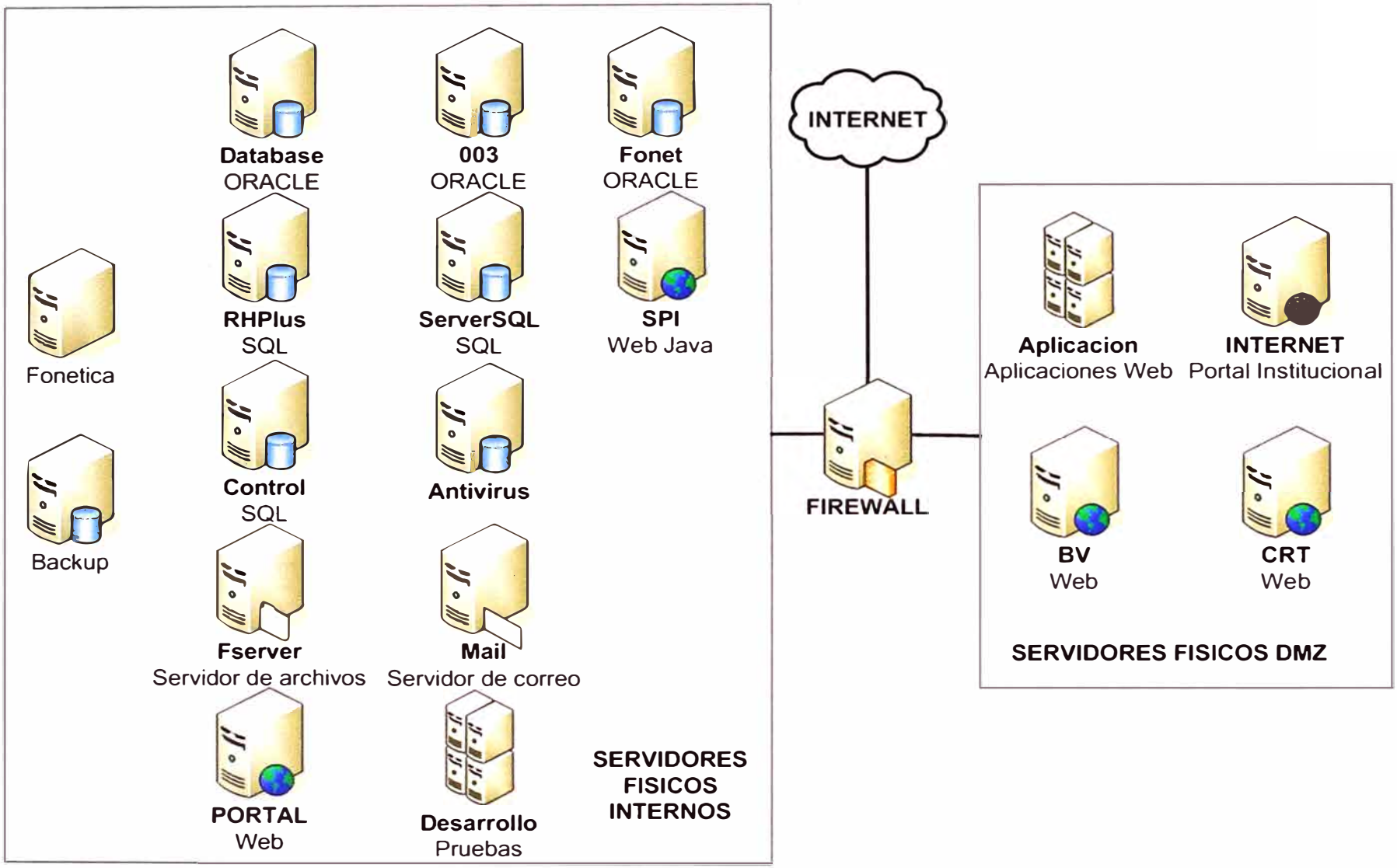

Figura 2.3 Servidores de INDECOPI (Fuente: Elab propia.)

A continuación se describe la solución para servidores y almacenamiento de INDECOPI:

2.2.1 Topología de la solución

Como fue indicado previamente, el equipamiento y software debía cumplir con los requisitos de la licitación para diseñar e implementar un esquema de solución.

Como resultado del análisis de los requerimientos (Anexo A), se determinó que la solución debía ser implementada con los siguientes componentes:

- 1 Chasis para Servidores Blade: Marca IBM, modelo BladeCenter E [7]
- 4 Servidores Blade Tipo 1: Marca IBM, modelo BladeCenter HS21 X [8]
- 1 Servidor rackeable Tipo 1: Marca IBM. modelo System x3550 [9]
- 1 Servidor rackeable Tipo 2: Marca IBM, modelo System p5.520Q [10].
- 1 Sistema de Almacenamiento: Marca IBM, modelo DS4700 + expansión EXP810 [11]
- 1 Librería de Backup: Marca IBM, modelo TS3100 [12]
- Consolidación y virtualización: Software marca VMware [13].

Una breve descripción de las características de estos componentes son presentados en el Anexo C "Equipamiento de Servidores y Almacenamiento Utilizados". Con dichos componentes se planteó e implementó la topología que se muestra en la Figura 2.4 (página siguiente).

En la figura se indica entre paréntesis el orden en el que a continuación se explica la topología mostrada.

(1) Red de Área Local (LAN)

A este nivel aparece como un bloque en el diagrama de servidores y almacenamiento. Representa la conectividad de red de los servidores. Ésta es detallada en el siguiente capítulo.

(2) Red de Área de Almacenamiento (SAN)

Es una red dedicada que provee acceso al almacenamiento compartido a nivel de bloques para los servidores. En el diagrama se muestra una nube esquemática que, típicamente, representa una serie de switches SAN. En la práctica se utilizaron dos switches SAN, los cuales son parte del BladeCenter, pero que para efectos didácticos han sido representados como una nube de red. En el caso de INDECOPI la red SAN está compuesta por conexiones Fibre Channel (FC), a 4Gbps.

Es necesario recalcar que Fibre Channel [14] es un protocolo de red que se utiliza típicamente en la red de almacenamiento para la transferencia de datos entre servidores, sistemas de almacenamiento, dispositivos de respaldo (backup), y otros dispositivos similares. A nivel de la capa física utiliza conexiones de fibra óptica. En la actualidad ofrece tasas de transferencia de 1, 2, 4 y 8 Gbps.

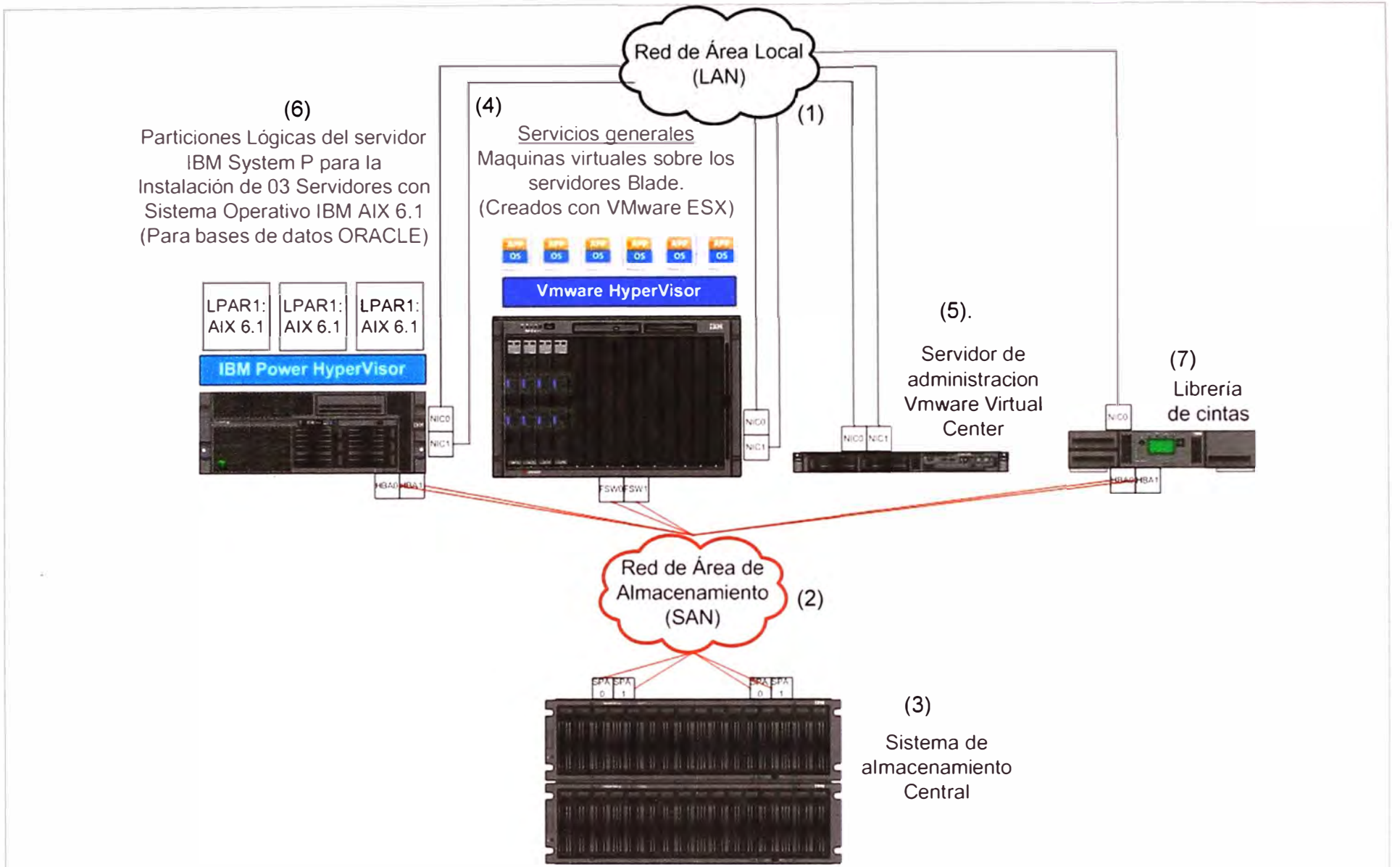

Figura 2.4 Topología de la solución de servidores y almacenamiento (Fuente: Elab. Propia)

(3) Sistema de almacenamiento central

Es de la marca IBM, modelo DS4700 e incluye una bandeja de expansión modelo EXP810. Para INDECOPI el equipo contaba con una capacidad total de 3 TB (Terabytes). El sistema de almacenamiento contiene los volúmenes de disco (lógicos) de los servidores (por ejemplo C:, D:, etc.) también conocidos como LUN (Logical Unit Number) los cuales son asignados a los servidores físicos a través de la SAN. Esto permite consolidar datos y garantizar disponibilidad de información dado que el equipo cuenta con todos sus componentes redundantes. Así mismo habilita a las aplicaciones a contar con funcionalidades de alta disponibilidad, como por ejemplo un cluster físico formado por dos o más servidores.

Se define "cluster" a una agrupación física de servidores físicos diseñados para interactuar en conjunto al servicio de una sola aplicación. Dependiendo de la configuración del cluster, esto brinda alta disponibilidad al servicio (en una configuración activo/pasivo, en la que un solo miembro del cluster se encuentra operativo y el resto de miembros en espera) o adicionalmente puede brindar balanceo de carga (en configuración activo/activo en la que la carga de la aplicación se distribuye entre todos los miembros del cluster). En todos los casos, si un componente activo falla los otros nodos toman la carga y garantizan la continuidad del servicio.

(4) Máquinas virtuales VMware

VMware es una solución de virtualización que opera en infraestructuras de servidores de tecnología x86 (Intel o AMD). La solución de INDECOPI utiliza cuatro cuchillas HS21XM para virtualizar los 16 servidores físicos mencionados previamente. Estas cuatro cuchillas, conectadas al sistema de almacenamiento central, conforman un cluster que agrupa recursos físicos a nivel de memoria, disco, CPU, y red, para asignarlas a las máquinas virtuales según se necesite, brindando además alta disponibilidad. Entre los servicios que se virtualizaron se cuentan las cuatro instancias SQL solicitadas en las bases de la licitación.

(5) Servidor de administración VMware Virtual Center

Esta aplicación está instalada en el servidor marca IBM, modelo System x3550, bajo un sistema operativo Windows. La aplicación administra el Cluster VMware (conformado por las cuatro cuchillas HS21). La aplicación se encarga de gestionar la asignación de recursos de los servidores virtuales así como las funciones de disponibilidad y rendimiento del producto.

(6) Servidor para bases de datos

El equipo IBM modelo System p5.520Q, utiliza una tecnología propietaria que permite dividir lógicamente el hardware entre dos o más particiones lógicas del mismo (LPAR).

Cuando un sistema operativo soportado por este equipo es instalado sobre una de los LPAR, lo que ve el sistema operativo es una emulación real del hardware. Estos sistemas no están basados en tecnología x86; cuentan con procesadores propietarios de IBM. En el caso de INDECOPI, sobre este servidor se crearon **tres LPAR**, en cada una de ellas se instaló el sistema operativo IBM AIX 6.1, para luego instalar las bases de datos basadas en tecnología Oracle. Este equipo se encargó de la consolidación de las cinco bases de datos Oracle indicadas en las bases de la licitación. Ellas en conjunto con las bases de datos SQL virtualizadas sobre VMware soportaban los 57 módulos web indicados en las bases de la licitación.

(7) Librería de backup

Este equipo (marca IBM modelo TS3100) se conectó a la red SAN para permitir el respaldo de las bases de datos Oracle utilizando la red SAN para las transferencia de los datos en lugar de la red LAN, debido al volumen de información que se necesitaba mover para los respaldos. Se menciona que el equipo era controlado por el software de backup del cliente, existente en su infraestructura, y cuya adquisición y configuración no fueron parte del proceso de licitación.

2.2.2 Habilitación y plan de pruebas de la solución de servidores y almacenamiento

El capítulo IV se muestra el diagrama de Gantt integral en donde se puede apreciar las tareas desarrolladas para los ítems de la licitación que son responsabilidad de COSAPI DATA. También se aprecia la duración de las tareas y su relación con las demás actividades. Para esta sección, la Figura 2.5 muestra el detalle de las tareas correspondientes a la habilitación de la plataforma tecnológica.

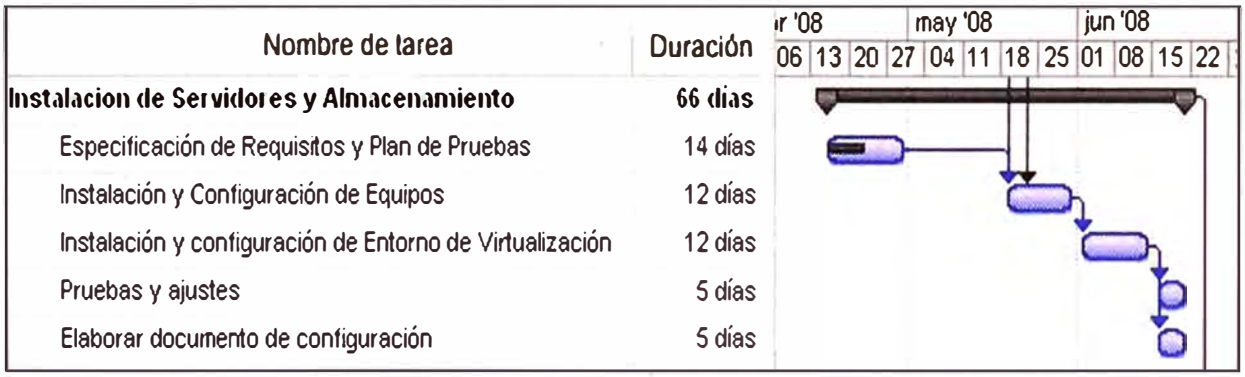

Figura 2.5 Gantt para solución servidores y almacenamiento (Fuente: Elab. Prop)

A continuación se desarrolla lo siguiente: Especificación de requisitos, instalación y configuración de los equipos y del entorno de virtualización, pruebas realizadas previa a la migración.

a. Especificación de requisitos

Está tarea consistió en la evaluación de la problemática y el planteamiento de la topología y la estrategia de despliegue. Basado en ello se determinó la distribución de los

anteriores servidores en la nueva plataforma tecnológica. Esto es mostrado en la Tabla 2.2.

En ella se puede apreciar que tres servidores originales se mantuvieron como equipos físicos: Backup y Fonética permanecieron en sus mismos equipos, en tanto que el Firewall fue reemplazado por un equipamiento de propósito específico (appliance que será descrito en el capítulo siguiente). Las tres bases de datos Oracle fueron consolidadas utilizando la tecnología LPAR. Los restantes 13 servidores fueron virtualizados utilizando VMware.

En la tabla se muestra el nombre del servidor, los recursos con que contaba (procesador, memoria, disco) y el servicio que realizaba, así mismo se indica si el equipo se encontraba en la red interna o en la red protegida (DMZ-Zona desmilitarizada). En la última columna se especifica el servidor de destino, por ejemplo, los servidores Database, 003 y Fonet son consolidados en el equipo IBM System P5, por otro lado, los servidores. RHPLUS ServerSQL, SPI y BV, son virtualizados en la cuchilla (blade) HS21 01.

Tabla 2.2 Distribución de recursos físicos en la nueva plataforma (Elab. Propia)

Nombre de Servidor	Procesador	Memoria (MB)	Disco (GB)			Referencia	LAN / DMZ	Servidor Destino
DATABASE	PIII-3.06 Ghz	2048	72	C:	13.6	Base de Datos Principal - ORACLE	LAN	IBM System P5
				E:	61.82			
			72	D:	67.83			
003	PIII-3.06 Ghz	1024	72	C:	4.0	Base de Datos OSD – Oracle	LAN	
				D:	30.0			
				E:	20.0			
FONET	PIV-3.60 Ghz	1024	73	C:	7.80	Pruebas – Oracle	LAN	
			73	D:	84.90			
				E:	43.90			
BACKUP	PIII-3.06 Ghz	1024	72	C:	20.0	Servidor de Backup	LAN	Servidor gestor de la librería de cintas. Se mantiene como equipo físico
				E:	20.0			
				F:	29.0			
RHPLUS	PIII 600 Ghz	750	9	C:	3.5	Sistema de colas - SQL	LAN	Cuchilla HS21 01
				E:	4.0			
			9	D:	9.0			
			9	G:	9.0			
SERVERSQL	PIII-500 Ghz	512	9	C:	2.0	Sistema de recursos humanos - SQL	LAN	
				E:	7.0			
			9	D:	9.0			

SPI	PIII 1.0 Ghz	1024	18	C:	4.0	Paginas Web en Java	LAN	
				D:	13.0			
			9	E:	9.0			
BV	PII 400 Ghz	512	9	C:	3.0	Portal Web de Biblioteca Virtual	DMZ	
				E:	5.0			
			9	F:	8.0			
CONTROL	PIII-3.06 Ghz	1024	72	C:	6.0	Software de Inventario - SQL	LAN	Cuchilla HS21 02
				E:	25.0			
				F:	5.0			
				G:	25.0			
ANTIVIRUS	PIV-3.60 Ghz	1024	73	C:	20.0	Servidor de administración antivirus	LAN	
			73	E:	20.0			
			73	F:	15.0			
				G:	10.0			
CRT	PIII 1.8 Ghz	512	40	C:	3.5	Sistema de Normalizacion	DMZ	
				E:	34			
FSERVER	PIV-3.60 Ghz	2048	146	C:	15.0	Directorio de usuarios y servidor de archivos	LAN	Cuchilla HS21 03
			146	D:	5.0			
			146	E:	34.0			
			146	F:	410.0			
			146					
			146					
MAIL	PIV-3.60 Ghz	2048	72	C:	20.0	Servidor de correo	LAN	
			72	E:	15.0			
			72	F:	100.0			
			36	G:	38.0			
			36					
APLICACIÓN	PIII-3.06 Ghz	1024	72	C:	6.0	Aplicaciones Web	DMZ	
				D:	30.0			
				F:	10.0			
PORTAL	PIV-3.60 Ghz	1024	73			Portal CLC	LAN	Cuchilla HS21 04
			73					
DESARROLLO	PIV-3.60 Ghz	512	73	C:	8.0	Servidor de Pruebas de Desarrollo	LAN	
			73	D:	64.0			
				E:	65.0			
INTERNET	PIV-3.60 Ghz	1024	73	C:	10.0	Pagina Web de Internet	DMZ	
				D:	48.0			
			73	-				
			73	-				
FIREWALL	PIV 2.2 Ghz	1024	74	C:	4.0	Firewall	N/A	Reemplazado

				E:	30.0			por equipo físico
FONETICA	PIV 3.4 Ghz	1024	80	C: E:	5.9 68.7	Sistema de Busquedas Foneticas	LAN	Se mantiene equipo físico

b. Instalación y configuración de los equipos y del entorno de virtualización

Estas tareas consistieron en lo siguiente:

- Instalación física de equipos.
- Inicialización de equipos.
- Instalación de sistemas operativos.
- Configuración de la librería de cintas.

b.1 Instalación física de equipos

Implica tanto el montaje físico del hardware en los racks instalados en el Datacenter, así como la conexión física de los equipos (energía, red, fibra óptica) en forma redundante.

b.2 Inicialización de equipos

Esto involucra al encendido de equipos, la actualización de BIOS y firmware en los servidores y sistemas de almacenamiento. También implica la inicialización del sistema de almacenamiento y la inicialización del sistema IBM blade center. La Tabla 2.3 describe la descripción de estas tareas.

Tabla 2.3 Inicialización de equipos (Fuente: Elab. Propia)

Tarea	Descripción
Inicialización del sistema de almacenamiento	Configuración inicial: Nombre del host, direcciones IP.
	Preparación de los arreglos de disco para los servidores físicos
	preparación de las LUN y asignación de los mismos a los puertos FC (Fibre Channel) del sistema de almacenamiento.
Inicialización del sistema IBM blade center	configuración inicial: Nombre del host, direcciones IP
	configuración de los switches SAN para el mapeo de las LUN a los servidores HS21 alojados en el blade center y al servidor IBM System P (zonificación).
	asignación de las LUN a los servidores HS21 y System P (presentación de LUNs)

b.3 Instalación de sistemas operativos

Esto se realizó para los siguientes servidores: servidor IBM System P, servidor IBM System X3550 (como servidor de administración de la plataforma VMware), en los cuatro servidores Blade IBM HS21.

Los detalles se describen a continuación.

Tabla 2.4 Inicialización de sistemas operativos (Elab. Propia)

Servidor	Tareas
IBM System P	Particionamiento del equipo en tres LPAR.
	Configuración de las LPAR.
	Parámetros iníciales de las LPAR (porcentaje de hardware asignado a cada una de ellas)
	Instalación del sistema operativo IBM AIX 6.1 de 64 bits las tres LPAR configuradas en el servidor IBM System P.
	Instalación del aplicativo de base de datos Oracle 10g en las tres particiones LPAR ya instaladas con el sistema operativo AIX.
IBM System X3550	Instalación del sistema operativo Microsoft Windows 2003 Server de 32 bits.
	Configuración inicial (nombre del host, direccionamiento IP, parchado del sistema operativo)
	Instalación del software VMware Virtual Center 3.5 en el servidor.
Blade IBM HS21	Instalación del software VMware ESX Server 3.5 en las cuatro cuchillas.
	Configuración Inicial de cada uno de los hosts (nombre del host, direccionamiento IP)
	Adición de los cuatro servidores ESX a la gestión del servidor Virtual Center.
	Creación del Cluster ESX entre las cuatro cuchillas en el servidor del Virtual Center.
	Configuración del Cluster (alta disponibilidad, distribución dinámica de recursos, movimiento dinámico de máquinas virtuales)

b.4 Configuración de la librería de cintas

Esta tarea consistió en la integración con el software de backup de INDECOPI, y en la conexión a la SAN y zonificación para poder respaldar las bases de datos Oracle.

c. Plan de pruebas previas a la migración

Se establecieron las pruebas que debían realizarse para verificar la robustez de la plataforma tecnológica. La Tabla 2.5 resume las pruebas. Luego de alcanzado los resultados esperados (descrito en la sección 4.1.1), la plataforma quedó lista para iniciar las tareas de migración.

Tabla 2.5 Plan de pruebas (Fuente: Elab. Propia)

Prueba	Resultado esperado
Pruebas eléctricas	
Desconexión física de un cable de poder de un equipo aleatorio	El servicio debe continuar a través de la fuente redundante aún en línea.
Deshabilitación de uno de los dos power distribution units (PDU) del rack de servidores	El servicio debe continuar a través del otro PDU del rack
Bajado ordenado de las cuchillas de	Bajada una de las cuchillas los servidores

alimentación del Datacenter	deben mantenerse encendidos a través de la otra línea de alimentación del Datacenter.
Sistema de almacenamiento	
Desconexión física de los cables de FO en uno de los dos procesadores componentes del sistema de almacenamiento.	Las LUN que son propiedad de los puertos desconectados en el primer procesador pasan a ser propiedad del segundo juego de puertos ubicados en el procesador redundante del sistema de almacenamiento
Reinicio ordenado de los procesadores componentes del sistema de almacenamiento.	Las LUN asignadas al procesador que se reinicia pasan a ser propiedad del segundo procesador del sistema de almacenamiento
Retiro en caliente de un disco de un determinado grupo de arreglo (RAID group)	Debe observarse lo siguiente: - Los discos configurados como "discos de espera en caliente" reemplazan al disco retirado - El arreglo afectado mantiene acceso a la data mientras se reconstruye
Switches SAN	
Desconexión física de los cables de FO en el puerto que conecta el switch con el storage	En el sistema de almacenamiento, Las LUN que son propiedad de los puertos desconectados en el primer procesador pasan a ser propiedad del segundo juego de puertos ubicados en el procesador redundante del sistema de almacenamiento
Reinicio o apagado de uno de los switches	Todas las LUN que eran servidas por el camino formado por ese switch mantienen operación a través del otro switch
Plataforma VMware (para ello se preparó una máquina virtual de pruebas)	
Pruebas de alta disponibilidad	
Se coloca la máquina virtual sobre una de las 4 cuchillas HS21 instalado con VMware ESX. A continuación se procede a reiniciar el equipo físico donde se encuentra alojada la máquina virtual	La máquina virtual cae. A continuación comienza a reiniciar automáticamente en una de las tres cuchillas restantes.
Se coloca la máquina virtual sobre una de las 4 cuchillas HS21. A continuación se ejecuta la funcionalidad de vmotion para mover la máquina virtual a otra cuchilla HS21 distinta a la origen.	Durante el movimiento de la máquina virtual no se pierde conectividad de red con la máquina con lo que el servicio se mantiene activo. Se debe observar un estado de "success" al final del movimiento.
Se aloja la máquina virtual en uno de los volúmenes del cluster VMware (Datastore). A continuación se ejecuta la funcionalidad de Storage vmotion y se mueve la máquina virtual a otro volumen (datastore) del cluster vmware.	Durante el movimiento de la máquina virtual no se pierde actividades de lectura y escritura con la máquina, con lo que el servicio se mantiene activo. Se debe observar un estado de "success" al final de movimiento.
Servicios VMware	
Se toma la máquina virtual y se ejecuta	La solución crea una segunda máquina

la funcionalidad de clonación	virtual que es copia de la primera. El sistema debe invitar a efectuar cambios en la configuración del hardware virtual y de la configuración lógica de la máquina antes de proceder. Se debe observar un estado de "success" al final de la copia.
Se toma la máquina virtual y se ejecuta la funcionalidad de snap.	La solución toma una fotografía instantánea del estado de la máquina virtual y lo guarda en disco
Una vez tomado el snap, se ejecuta pruebas intrusivas en la máquina virtual (borrado de archivos aleatorios en la carpeta C:Windows)	Tras el reinicio la máquina debe quedar inutilizable.
Se revisa el inventario de snaps de la máquina virtual y se abre el último snap tomado	La máquina virtual debe restaurarse al estado previo a la manipulación a nivel de sistema operativo.

2.3 Migración de los servicios generales y de las aplicaciones

La migración consiste en trasladar los servicios de INDECOPI desde los servidores originales hacia la nueva plataforma tecnológica. Los servicios consisten en servicios generales y aplicaciones.

2.3.1 Servicios generales

Son los servicios de uso interno de la organización (Por ejemplo: Servicios de correo, servidores de archivo, controlador de dominio, antivirus, servidores web, etc.).

Estos servicios eran ejecutados sobre servidores físicos cuyo detalle se encuentra en la Tabla 2.2, y corresponden a aquellos equipos que fueron virtualizados en cuchillas HS21 con el software de virtualización VMware, en el orden mostrado en la tabla en mención.

Para la migración de estos servicios se ejecutó un procedimiento llamado conversión de físico a virtual (p2v-physical to virtual), cuyo diagrama se muestra en la Figura 2.6. La migración consiste en lo siguiente:

1. Sobre el servidor físico se instala un software llamado agente de conversión. Este software se encarga de analizar el estado de conversión del equipo determinando si el mismo está en condiciones de ser convertido o mostrando alertas en el caso de que presente algún inconveniente.
2. Desde el servidor Virtualcenter se tiene comunicación con el servidor físico el cual ya tiene instalado el agente de conversión, y los servidores ESX, cuyos volúmenes de almacenamiento (Datastore) serán los destinos de la información proveniente de la conversión y albergará la máquina virtual con el servicio proveniente del servidor físico correspondiente (quien ejecutará el mismo sistema operativo y aplicación instalada en el servidor físico origen).

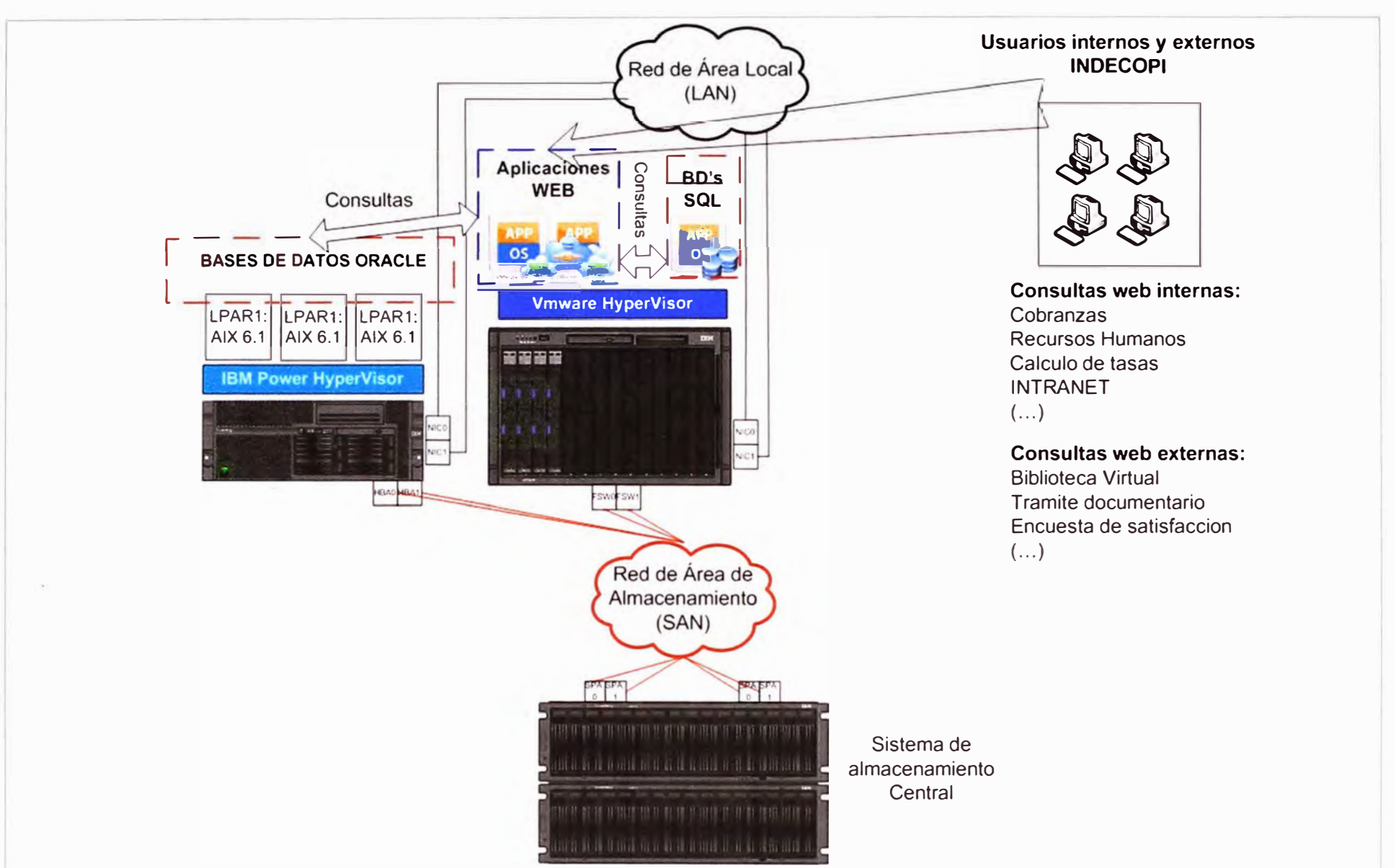

Figura 2.8 Esquema de trabajo de aplicaciones sobre la nueva infraestructura de servidores (Fuente: Elab. Propia)

3. Desde la consola de administración del Virtualcenter se selecciona el Datastore donde se almacenará la máquina virtual y se tiene la opción de modificar el hardware virtual componente de la máquina virtual (lo cual permite, por ejemplo, asignar mayores recursos de cómputo que los originales pertenecientes a la máquina física). Como se observa en la Figura 2.6, es necesario que el servidor físico a convertir, los servidores ESX y el servidor del Virtualcenter tengan conectividad de red. Dado que el flujo de información desde el servidor físico hacia los servidores ESX es masivo se utilizan equipos de red dedicados intermedios durante la conversión. Así mismo, y para evitar que nuevos datos se escriban en el servidor físico mientras es convertido, todos los servicios que están corriendo sobre él son previamente detenidos.

4. Terminada la conversión del servidor ya es posible encender la máquina virtual desde la infraestructura virtual. Para evitar conflictos, antes de encender la máquina virtual, el servidor físico original es retirado de línea, y el servicio se restablece sobre la máquina virtual

La migración estará en función de la cantidad de datos del servidor de origen. Para los servidores con mayor cantidad de datos, es más sencillo tomar una copia de la información de la aplicación y retirarla del servidor físico, efectuar la conversión con todo el grueso de datos retirados del servidor físico y finalmente, la data de la aplicación es copiada a la máquina virtual una vez que esta se encuentre lista.

Observaciones:

- La migración de los servicios se efectuó en horarios fuera de producción.
- La evaluación de los servicios sobre virtual se consideraba exitosa cuando todas las funcionalidades de la aplicación en físico eran equivalentemente probadas sobre virtual, además de las pruebas de alta disponibilidad de VMware detallada en párrafos previos.

2.3.2 Aplicaciones

El flujo de trabajo de las aplicaciones de INDECOPI, es mostrado en la Figura 2.7. Éste se explica a continuación:

- Los clientes internos y externos de INDECOPI interactúan con una serie de portales web de propósito específico (sistemas de cobranza, formularios en línea, consultas en líneas, etc.) y que conformaban las 57 aplicaciones mencionadas en las bases del proceso.
- Estos servicios web cuentan con conectores a nivel de aplicación con las bases de datos de la institución (llámese Oracle o SQL), donde se aloja la data estructurada que es utilizada por los servicios web (formularios, repositorios de datos, etc.) y que almacenan información crítica del negocio (información de usuarios, de proveedores, registro de organizaciones, datos de interacción con otras entidades de gobierno, etc.).

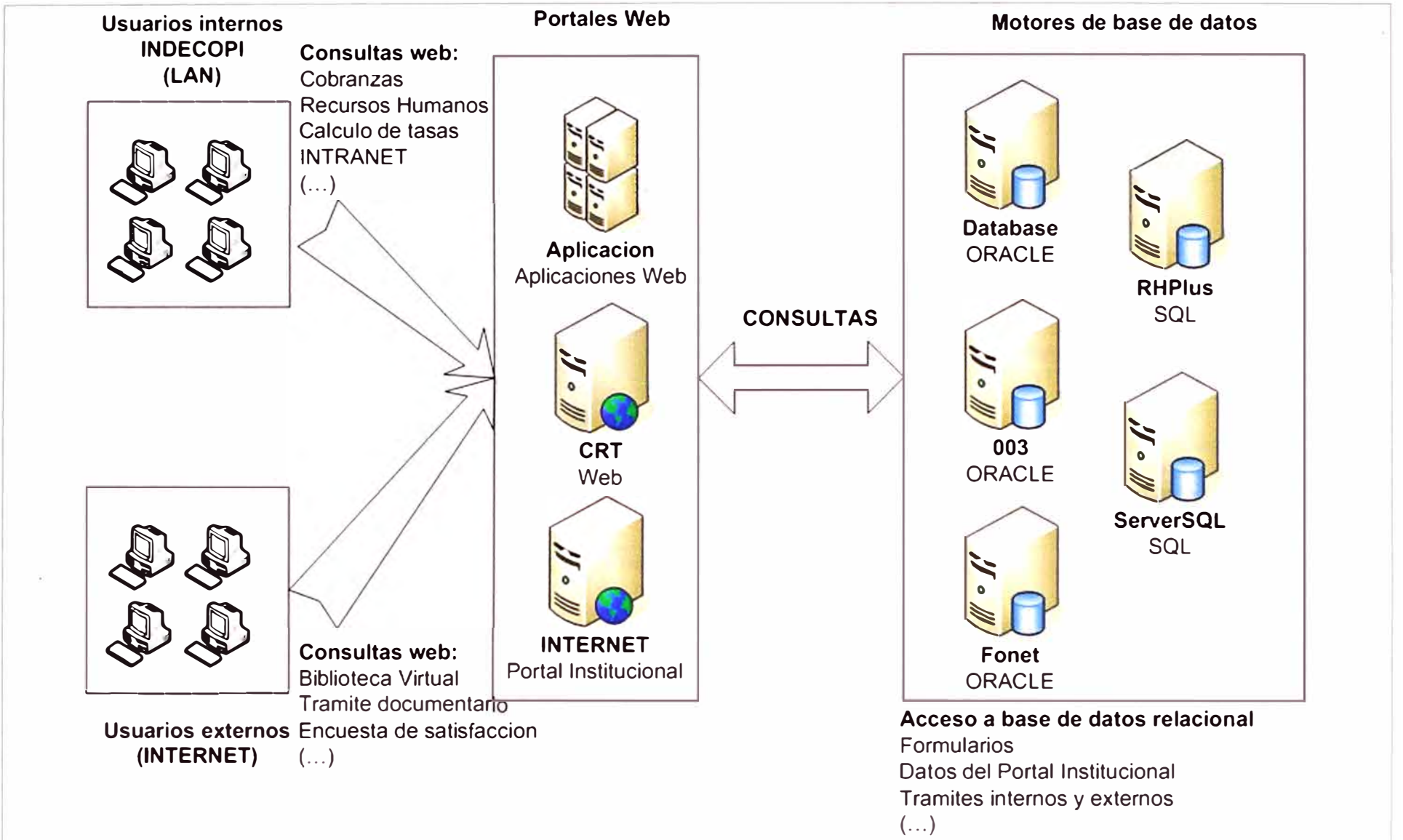

Figura 2.7 Esquema de trabajo de aplicaciones en la infraestructura original (Fuente: Elaboración Propia)

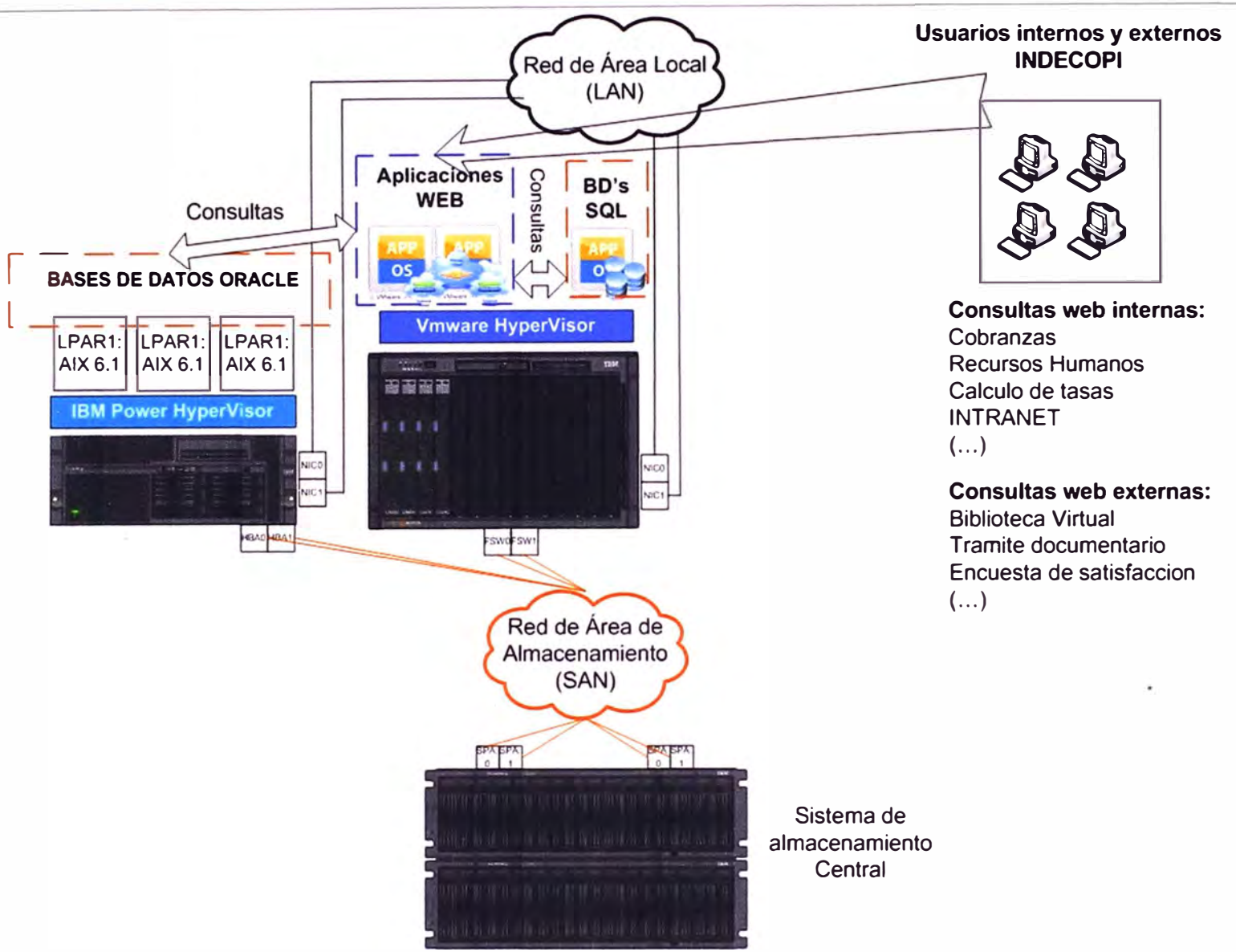

Figura 2.8 Esquema de trabajo de aplicaciones sobre la nueva infraestructura de servidores (Fuente: Elab. Propia)

- Cuando un usuario hace un requerimiento de la aplicación vía web, en pantalla aparecerá los formularios asociados a la aplicación y cuyos campos de interacción provienen de las bases de datos, ello permite interactuar al usuario con los sitemas de INDECOPI.

Dado que en la nueva plataforma este flujo de trabajo se mantiene. La migración consistió en lo siguiente:

a. Migración de las bases de datos Oracle sobre servidores IBM System p

En el caso de las bases de datos Oracle, estas no solamente fueron migradas desde equipos de tecnología inferior a tecnología especializada (System p), sino que también se actualizó la versión del aplicativo de base de datos de la versión 8i a la 10g. Así mismo los sistemas operativos que soportaron la aplicación también cambiaron.

1. Levantamiento de información de las bases de datos creadas sobre el sistema Oracle original.
2. Programación de los cortes de servicio para cada una de las bases de datos.
3. Para cada base de datos, en función a su fecha de migración:

- Bajada de los servicios de la instancia de base de datos particular.
- Respaldo de la base de datos detenida.
- Copia del respaldo en el nuevo servidor IBM System p, en la partición LPAR correspondiente.
- Actualización de parámetros de red.
- Restauración de la base de datos en la nueva versión del aplicativo Oracle.
- Verificación de conectividad con los servidores web a nivel de aplicación.
- Verificación de la operatividad de la aplicación.

b. Migración de las bases de datos SQL sobre servidores VMware

Las bases de datos SQL fueron migradas como máquinas virtuales a la plataforma VMware de la siguiente manera:

1. Levantamiento de información de las bases de datos creadas sobre SQL
2. Programación de los cortes de servicios.
3. Respaldo de las bases de datos previa parada de servicio.
4. Retiro de la data de respaldo del servidor.
5. Conversión de físico a virtual del servidor SQL físico
6. Verificación de la integridad de la conversión en virtual. En caso hubiera falla en el servicio de bases de datos:

- Se instala una máquina virtual limpia con la misma versión del sistema operativo original.
- Se instala el mismo aplicativo de base de datos SQL con la misma versión del equipo

original.

- Se copia la información de respaldo de las bases de datos a la máquina virtual y se ejecuta el proceso de restauración.

7. Verificación de la conectividad con los aplicativos web
8. Pruebas de servicio.

c. Migración de servidores web sobre servidores VMware

Los servidores de portal web también fueron migrados a VMware.

1. Programación de corte de servicio de los servidores web.
2. Conversión de físico a virtual de los equipos.
3. Verificación de conectividad con las bases de datos asociadas.
4. Pruebas integrales de funcionamiento de las aplicaciones cuyos enlaces web estaban alojados en el portal.

Observaciones:

Cabe mencionar que una vez que todos los servidores componentes de las aplicaciones de INDECOPI (web y bases de datos) fueron migrados a la nueva plataforma, el flujo de trabajo (presentado en la Figura 2.7) se mantuvo, como puede observarse en la Figura 2.8.

CAPÍTULO III
DESARROLLO DE LA ARQUITECTURA JERÁRQUICA DE REDES Y COMUNICACIONES

En el presente capítulo se describe la ingeniería del ítem 3 de las bases de licitación. Los aspectos a desarrollar en este capítulo son los siguientes.

- Análisis situacional.
- Solución de comunicaciones.
- Solución de seguridad informática.
- Cableado estructurado.
- Migración a la nueva red y plan de pruebas

3.1 Análisis situacional

Siguiendo la metodología del capítulo anterior, en esta sección se precisarán los requerimientos, para luego evaluar la problemática y así plantear las estrategias de desarrollo de la solución (Se resumen al final de esta sección en la Tabla 3.1).

3.1.1 Requerimientos

El requerimiento básico es actualizar y reordenar la infraestructura de la red informática de INDECOPI proporcionado la mejor solución de redes y seguridad perimetral, incluyendo la renovación de equipamiento de comunicaciones, de tal manera que se garantice la correcta comunicación e intercambio de información para los fines de INDECOPI. Los trabajos a realizar para el ítem 3 de las bases de la licitación, consisten pues en mejorar la red principal de comunicaciones (backbone) actualizando los enlaces y switches de comunicaciones, además de proporcionar la seguridad perimetral mediante una solución de firewall y un sistema de prevención de intrusión (IPS - Intrusion Prevention System). El ítem 3 también involucra la implementación de la solución de cableado estructurado

Para la ejecución de este ítem, INDECOPI también licitó la adquisición del hardware y software necesario, según se lista a continuación:

Equipos de comunicación

- 1 Switch de Núcleo .- Multicapa con arquitectura basada en chasis, con mínimo 8 slots. Con capacidad de operación en capas 2, 3 y 4 del Modelo OSI.
- 3 Switches de Distribución.- Multicapa (capas 2 y 3).
- 14 Switches de Acceso. Multicapa (capas 2 y 3).

- 1 Software de Administración

Equipos de seguridad perimetral

- 1 Firewall Central.
- 1 IPS (Intrusión Prevention System)

Las características que debían cumplir estos componentes se describen en el Anexo D "Requisitos para Equipos de Comunicación y de Seguridad".

3.1.2 Problemática

Se exponen los tres aspectos del ítem 3 de la licitación: Redes y comunicaciones, seguridad informática, y cableado estructurado. La Figura 3.1 ayuda a identificar la problemática que se describe a continuación.

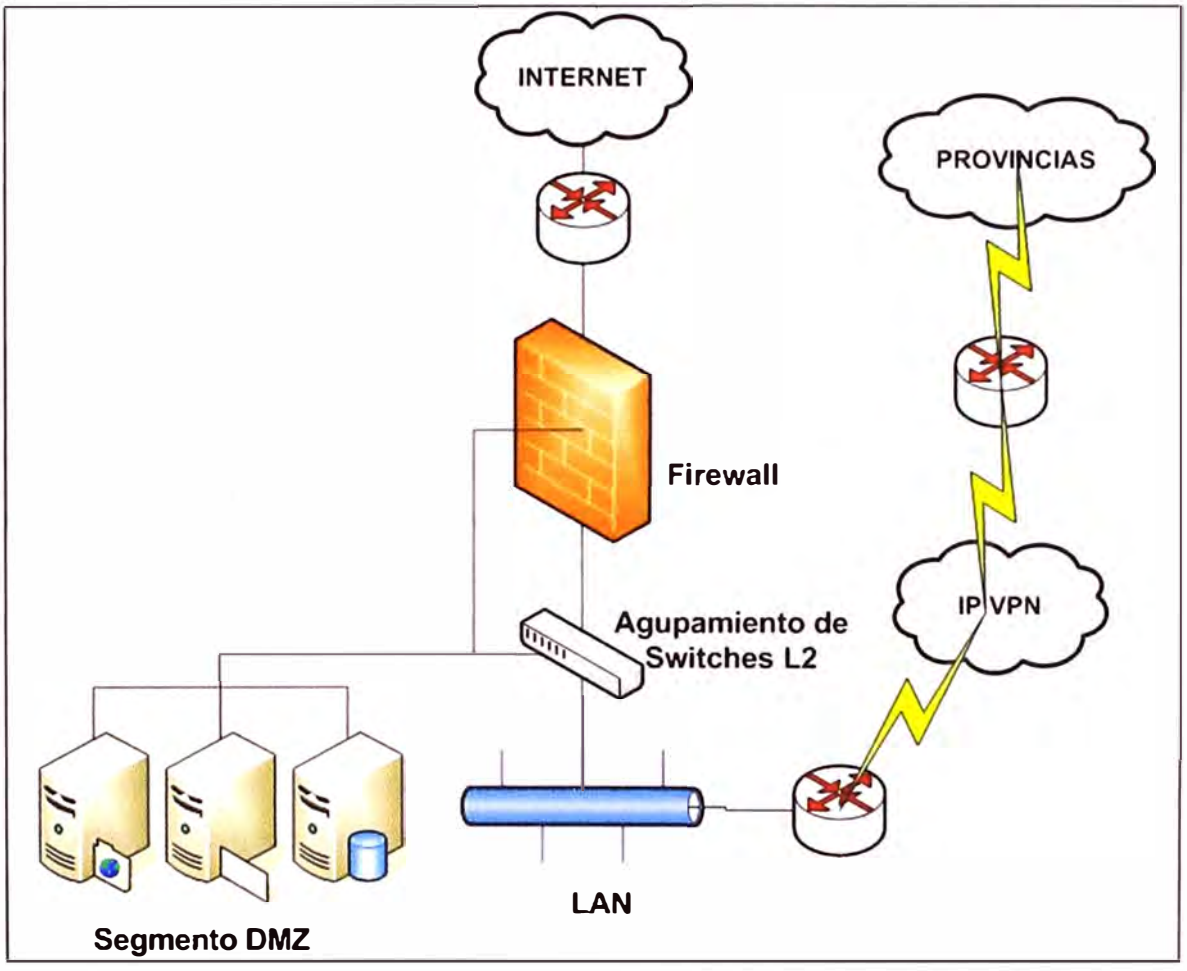

Figura 3.1 Situación inicial (Fuente: Elaboración propia)

a. Redes y comunicaciones

Su problemática se describe a continuación se resume en lo siguiente:

Red conformada por un solo dominio de colisiones

Pese a que la red contaba con 3 segmentos claramente identificados (LAN, DMZ, Internet), todos ellos compartían un mismo dominio de colisiones. Por lo tanto, los broadcasts generados por cada uno de estos segmentos eran transmitidos por toda la red, generando serios problemas de saturación en los enlaces.

Distribución en cascada de los switches

La red estaba compuesta por múltiples switches interconectados unos entre otros, sin una jerarquía definida en la red. Se desconocía la criticidad causada por la falla de un switch determinado (bien podía ser un equipo que interconectara un edificio completo, o conectara solamente algunos equipos puntuales).

Ausencia de identificación de equipamiento y puntos de red

Los puntos de interconexión no estaban documentados, de modo tal que no se sabía a dónde iba un cable de red determinado. Bien a otro switch, a un servidor, a un equipo de usuario final.

Tecnología predominante: Fast Ethernet

La mayoría de switches soportaban enlaces a 100Mbps, incluidas las troncales de interconexión entre edificios, esto, en suma con la saturación causada por los broadcasts generados por los 3 segmentos de red, afectaban seriamente el rendimiento de la red.

Ausencia de gestión

No había manera de medir el consumo de la red, el estado de los equipos, identificar averías o tomar acciones correctivas eficientes ante cualquier eventualidad.

Problemas de enrutamiento IP

Varios servidores críticos de INDECOPI contaban con una incorrecta configuración IP en las interfaces de red que gestionaban. En una adecuada configuración IP de un equipo, los servidores cuentan con una sola puerta de enlace por defecto, y rutas estáticas a otros segmentos de red particulares que precisen alcanzar. INDECOPI contaba con varias puertas de enlace por defecto en sus servidores, para alcanzar las redes remotas.

Debido a que todos los segmentos de red estaban conectados en un mismo dominio de broadcast, todas las direcciones IP de los equipos de enrutamiento eran siempre alcanzadas. Esto generaba indeterminaciones respecto al enrutamiento existente en la red. Equipos intermedios de enrutamiento tenían configuraciones aleatorias para poder enrutar los paquetes IP. Fallas en el enrutamiento tenían múltiples puntos de falla.

Equipos fuera de garantía

Los equipos utilizados por INDECOPI estaban operando con contratos de soporte vencidos, inclusive varios de los switches en uso estaban ya fuera del mercado, por tanto, sin opción alguna a soporte.

La protección de estos equipos era mínima, la gran mayoría de ellos contaban solamente con una sola fuente de poder.

b. Seguridad informática

Su problemática se describe a continuación:

Firewall perimetral: única defensa de red de INDECOPI

El equipo utilizado por INDECOPI para proteger su perímetro de ataques externos, era una computadora con 3 tarjetas Gigabit Ethernet. Cada una de estas interfaces representaba la puerta de enlace por defecto a los equipos de cada segmento de red. Al ser la única defensa, solamente se tenía como protección para los equipos internos de INDECOPI, el bloqueo de puertos a nivel de las capas TCP/UDP.

Desde hace años estas defensas son consideradas insuficientes, debido a que los ataques informáticos han evolucionado de manera que ellos son inyectados utilizando puertos que, típicamente, se encuentran abiertos a nivel de Firewall (Como el puerto 80 TCP (http), o el puerto 53 UDP (dns)). Dado ello, la defensa de INDECOPI a nivel perimetral era sumamente básica, estando expuesta a una indeterminada cantidad de ataques a nivel de aplicación.

Obsolescencia de la solución

El equipo de INDECOPI (una PC), no tenía ninguna clase de garantía. Era un computador basado en el procesador Intel Pentium III, fuera de garantía de cualquiera de sus componentes, sin ninguna clase de redundancia (fuentes o disco).

El software instalado en el computador (basado en Windows), tenía años operando sin soporte del fabricante alguno. El equipo presentaba varias caídas. No había una forma segura de regresar el equipo a operaciones ante estos eventos, generando cortes de servicio generales en INDECOPI.

Compleja administración de la solución de firewall

Debido a que el software utilizado para el firewall estaba desactualizado, no había personal capacitado en INDECOPI para poder brindar una gestión o mantenimiento al equipo. Añadir nuevos servicios, generar nuevas políticas de seguridad, o efectuar una revisión de los registros de auditoría era un serio desafío para INDECOPI.

Red conformada por un solo dominio de colisiones

Si bien es cierto, el firewall tenía una configuración que restringía el acceso a nivel de puertos TCP/UDP a los servidores ubicados en la DMZ, no era complicado tomar un equipo de usuario común y cambiar su dirección IP por una de la DMZ, para tener acceso IP sin restricciones a los servidores DMZ, superando por completo toda defensa ofrecida por la solución de seguridad.

Acceso remoto a la red de INDECOPI brindado de forma insegura

Debido a que INDECOPI contaba con empleados ubicados físicamente en otras ubicaciones fuera de la red interna, era necesario que tuvieran un acceso a los recursos informáticos desde fuera. Dado que no había ninguna opción de acceso seguro, INDECOPI se vio obligado a publicar a Internet los servicios de varios servidores

internos.

Ello representaba un tremendo riesgo a la seguridad de los mismos, dado que bastaba hacer un port sweeping (barrido de puertos) a las direcciones públicas del Firewall de INDECOPI, para descubrir, en función a los puertos publicados, las aplicaciones que INDECOPI utilizaba para brindar sus servicios, exponiéndolas a potenciales atacantes que podrían ganar accesos a estos servicios.

c. Cableado estructurado:

Su problemática se describe a continuación:

Identificación nula de puntos y recorridos

Debido a que la red de INDECOPI fue creciendo sin una logística u orden definido, el cableado se fue aprovisionando en demanda. De modo que no habían diagramas de recorridos de red algunos. Asimismo, los puntos de red no estaban identificados. Ante la falla de un puerto de red en un switch, un cable, o un conector, los administradores de la red tenían que buscar la avería mediante procedimientos basados en prueba y error, tomando tiempos impermisibles para la operación de las actividades de la institución

Instalación no certificada

El cableado de la institución no estaba uniformizado, es decir, mientras en determinadas zonas se encontraba cableado UTP categoría 5, en otros, se encontraba categoría 5E. Las recomendaciones de diseño para los recorridos de los cableados no eran respetadas, así por ejemplo, muchos cables compartían recorridos en forma paralela a cableado eléctrico o tuberías de agua. Las reglas básicas de recorridos de cableado, longitudes recomendadas del cableado horizontal y vertical, longitudes de reserva, conectores, u otras, no eran respetadas. Todo ello generaba atenuaciones en las señales de datos, degradando el servicio general de la red.

Enlaces no redundantes

Los enlaces a los edificios interconectados con el centro de datos principal no contaban con conexiones redundantes. Una falla en el puerto del switch, el conector, o el cable, dejaba sin servicio a uno o a más de un edificio de la red de INDECOPI.

3.1.3 Estrategias de desarrollo de la solución

A continuación se describe el planteamiento de la solución para resolver la problemática expuesta en la anterior sección (3.1.2)

a. Redes y comunicaciones

Se describen a continuación:

- **Segmentación de los dominios de colisiones mediante el uso de VLANs.-** Para contener los broadcasts a los dominios de colisiones definidos por cada VLAN y así optimizar la red, se plantea crear jerarquías de red, para habilitar la creación de

determinadas VLANs para los segmentos LAN, DMZ y red de servidores internos, así como VLANs para los accesos a Internet y para la administración de los equipos. También se plantea establecer políticas adecuadas de enrutamiento. Esta solución se consigue con la nueva distribución de los servidores sobre sus plataformas consolidadas en soluciones de virtualización (descritas en capítulo anterior), así como la adquisición de equipos de comunicaciones.

- **Distribución jerárquica de dispositivos de red.-** Con el nuevo equipamiento instalar una nueva arquitectura basada en un Switch de Núcleo (Core), Switches de distribución y Switches de acceso, de modo que se entrega una arquitectura de comportamiento predecible, escalable, y de alto rendimiento.

- **Adecuada documentación de los equipos de red.-** Se plantea realizar un registro detallado en donde se identifique claramente el equipo de comunicaciones y sus aspectos funcionales dentro de la red, así mismo de todos los puntos de la red principal. De este modo se podrá llevar a cabo un control de la red de manera precisa. Esta identificación debe ser realizada a nivel de switch y de puntos de interconexión en el switch. Este planteamiento permite determinar la criticidad de los switches, y con ello, entregarle a cada componente una estrategia de contingencia adecuada ante fallas.

- **Tecnología Core Gigabit Ethernet**.- Para uniformizar la tecnología de interconexión central, la conexión a servidores, y la conexión a edificios aledaños, se plantea actualizarla con enlaces Gigabit Ethernet soportados sobre tecnologías de cableado UTP categoría 6, y tendidos de fibra óptica para la interconexión a los edificios aledaños al centro de datos.

- **Gestión centralizada de la solución integral de comunicaciones**.- Para lograr una adecuada gestión se plantea una solución basada en software que permita tomar control de todos los equipos de la red desde una sola consola administrativa, pudiéndose así revisar la configuración y el estado de salud de cada uno de los equipos involucrados en la solución de comunicaciones. Con este planteamiento se pretende tener la capacidad de tomar el control de cualquier puerto de red de cualquiera de los switches componentes de la solución, y de modificar según se precise la configuración de cualquier parámetro de operación de cualquiera de los switches involucrados.

- **Enrutamiento IP basado en la previa identificación de las redes de INDECOPI.-** Para evitar los problemas de enrutamiento se plantea rediseñar el enrutamiento IP en la red de INDECOPI, aprovechando la implementación de VLANs. Para las redes LAN, se plantea crear VLANs por edificios y por piso de edificio, cada uno de ellos con un segmento de red determinado. También se plantea mantener los segmentos de red de los servidores, pero aislándolas en VLANs independientes. Así mismo configurar los

switches capa 3 (con capacidad de enrutamiento), de forma tal que los paquetes de datos sigan un camino previamente diseñado. Estos switches deben interactuar con la solución de seguridad perimetral a implementar, brindando una estrategia de enrutamiento integral escalable, diseñada para el crecimiento de futuros segmentos de red, y con procedimientos de adecuación correctamente definidos.

- **Renovación tecnológica**.- Dada la obsolescencia tecnológica, se plantea la adquisición de nuevos equipos con 3 años de garantía brindada por el fabricante, con posibilidad de extensión de garantía. Esto le da a la solución vigencia tecnológica en el tiempo. El switch de núcleo (Core) debe contar con partes actualizables, que le permitan escalar modularmente a tecnologías superiores a las implementadas, como 10Gb Ethernet.

b. Seguridad informática

Se describen a continuación:

- **Robustecer la seguridad perimetral mediante un Firewall y un Sistema de Prevención de Intrusos (IPS) basado en dispositivos de propósito específico**.- Habiendo identificado la problemática de la solución de seguridad, se plantea la adquisición e implementación de "appliances" (dispositivos de propósito específico) para soluciones de Firewall e IPS. Esto permite brindar modelos de seguridad adaptables a los requerimientos y, que al mismo tiempo, esté en congruencia con la implementación de la red Core Gigabit Ethernet. Estos equipos deben ser incluidos dentro de la estrategia de comunicaciones, tomando un rol protagónico en el enrutamiento de la información de la institución, brindando protección a nivel de puertos y de aplicación a los servicios y clientes de la red. Esto también soluciona el problema de la obsolescencia, y por ello se plantea que los equipos cuenten con una garantía de 3 años de parte del fabricante.

- **Administración centralizada basada en web.-** Se plantea que los equipos a adquirir trabajen de manera integrada, manteniendo una configuración conjunta consistente con los requerimientos. La gestión debe ser centralizada e intuitiva basada en web, habilitando así a los administradores a tomar el control de la estrategia de seguridad, permitiéndoles controlar cambios y auditoría, así como la detección proactiva de amenazas en la red.

- **Interconexión de los equipos de seguridad en el contexto de los nuevos segmentos de colisiones, brindando distintos niveles de seguridad a cada segmento**.- Se plantea una nueva infraestructura que brinde una adecuada segmentación y protección de los servidores y usuarios de INDECOPI. Los accesos deben estar correctamente asignados, y de esa manera solucionar el problema de accesos no autorizados a los segmentos privados de la red.

- **Implementación de VPNs personales basadas en tecnologías SSL**.- El Firewall debe

ser configurado además como un servidor VPN SSL (Secure Socket Layer), que permita a los usuarios externos de INDECOPI, acceder en forma segura desde cualquier ubicación en Internet, mediante un canal cifrado utilizando SSL y certificados digitales para el cifrado de las comunicaciones a los recursos internos de la red. Así mismo, las políticas de acceso deben brindar las restricciones adecuadas en función al perfil del usuario externo que acceda a la red. Para contactar a los recursos internos de INDECOPI, los usuarios externos deberán iniciar las conexiones seguras desde un navegador de Internet cualquiera.

c. Cableado estructurado

Se describen a continuación:

- **Adecuada identificación de puntos y recorridos**.- Todos los componentes de red, activos y pasivos, deben ser correctamente identificados. El cableado anterior debe reemplazado por cableado de categoría 6, con un diseño de recorrido y de identificación de puntos documentado adecuadamente. Con ello, se soluciona el serio problema de identificación de puntos ante averías de red, asimismo. También se deben planificar las estrategias de contingencia para actuar ante fallas de los componentes involucrados.
- **Cableado certificado**.- El nuevo cableado a implementar en INDECOPI debe ser instalado cumpliendo los estándares exigidos para este tipo de trabajo, para así pasar exitosamente el proceso de certificación, asegurando una garantía de 25 años a la nueva infraestructura de cableado estructurado.
- **Enlaces redundantes**.- Todos los enlaces de interconexión a equipamiento y edificios críticos deben ser conectados de manera redundante, de modo tal que ante la falla de un enlace, se mantenga la comunicación mediante enlaces auxiliares.

La Tabla 3.1 resume la problemática y estrategia expuesta.

Tabla 3.1 Problemática y solución planteada (Fuente: Elab. propia)

Problemática	Solución planteada
Redes y comunicaciones	
Red conformada por un solo dominio de colisiones	Segmentación de los dominios de colisiones mediante el uso de VLANs
Distribución en cascada de los switches	Distribución jerárquica de dispositivos de red (Núcleo, Distribución, Acceso)
Ausencia de identificación de equipamiento y puntos de red	Adecuada documentación de los equipos de red
Tecnología predominante: Fast Ethernet	Tecnología Core Gigabit Ethernet
Ausencia de gestión	Gestión centralizada de la solución integral de comunicaciones
Problemas de enrutamiento IP	Enrutamiento IP basado en la previa identificación de las redes de INDECOPI

Equipos fuera de garantía	Renovación tecnológica (3 años)
Seguridad informática	
Firewall perimetral: única defensa de red de INDECOPI	Robustecer la seguridad perimetral mediante un Firewall y un Sistema de Prevención de Intrusos (IPS) basado en dispositivos de propósito específico, con garantía a 3 años.
Obsolescencia de la solución	
Compleja administración de la solución de firewall	Administración centralizada basada en web
Red conformada por un solo dominio de colisiones	Interconexión de los equipos de seguridad en el contexto de los nuevos segmentos de colisiones, brindando distintos niveles de seguridad a cada segmento
Acceso remoto a la red de INDECOPI brindado de forma insegura	Implementación de VPNs personales basadas en tecnologías SSL
Cableado estructurado	
Identificación nula de puntos y recorridos	Adecuada identificación de puntos y recorridos
Instalación no certificada	Cableado certificado
Enlaces no redundantes	Enlaces redundantes

3.2 Solución de comunicaciones

Como fue mencionado, la solución de comunicaciones se basa en la distribución de los switches en una estructura jerárquica, en la segmentación por medio de VLANs e implementación de enlaces troncales (802.1q), la redefinición de las tablas de enrutamiento en la institución, además de la implementación de la gestión centralizada de comunicaciones. Es necesario explicar brevemente algunos aspectos importantes.

La estructura jerárquica

Es la que posee niveles o capas en los que cada uno se enfoca en una función específica, permitiendo al diseñador de la red escoger los sistemas y características correctos para el nivel específico. La estructura jerárquica provee una estructura de trabajo modular que permite flexibilidad en el diseño de la red y facilita la implementación así cómo la resolución de problemas. La estructura jerárquica consta de las siguientes capas: acceso, distribución, y núcleo (core) con sus características asociadas [15]:

a. Capa de acceso: Usado para garantizar el acceso a la red a los usuarios, servidores, y dispositivos de conexión a otras redes. El nivel de acceso incorpora generalmente switches con puertos que proveen conectividad a estaciones de trabajo, servidores, impresoras, APs (puntos de acceso inalámbricos) etc.

b. Capa de distribución: Interconecta a los cuartos de comunicación, utilizando switches para segmentar grupos de trabajo y aislar problemas de la red. Similarmente, la capa de distribución agrega conexiones a las áreas más alejadas y provee nivel de seguridad. A menudo, la capa de distribución actúa como un facilitador para la comunicación ente las

capas de acceso y la de núcleo.

c. Capa de núcleo (core): Es un backbone (red principal) de alta velocidad, diseñada para conmutar paquetes tan rápido como sea posible. Debido a que el núcleo da la conexión critica, debe proveer un alto nivel de disponibilidad y adaptarse rápidamente a los cambios. Este diseño de capas también provee escalabilidad y rápida convergencia.

Modelo de Capas

En la Figura 3.2 se muestran el modelo OSI, el cual es el modelo de referencia para la definición de arquitecturas de interconexión de sistemas de comunicación en general. A su lado se muestra el modelo TCP/IP que es la referencia para arquitecturas de interconexión de dispositivos que utilizan IP (protocolo de Internet)

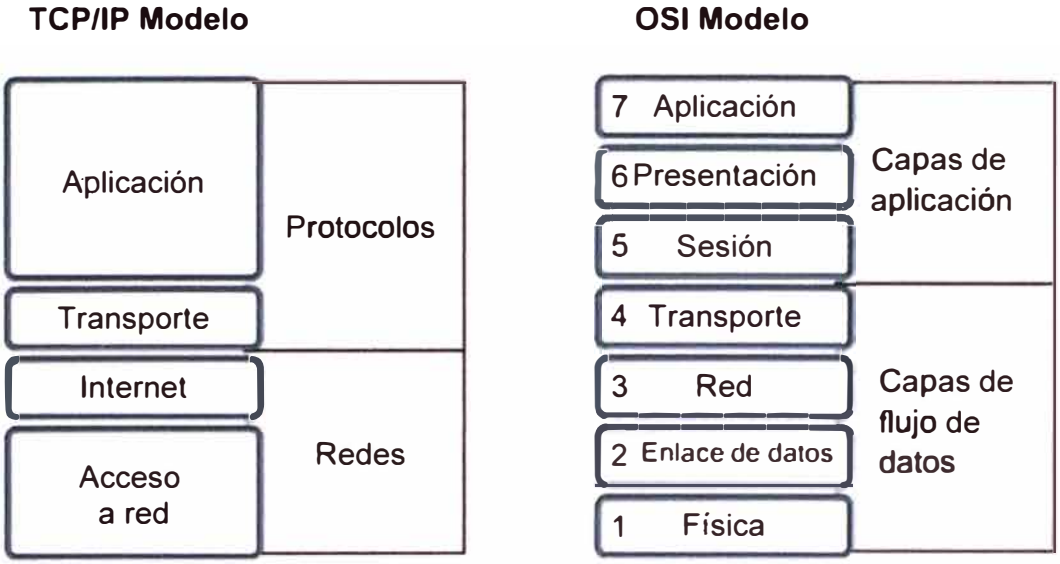

Figura 3.2 Modelos de Capa OSI y TCP/IP (Fuente: Ref [16])

Ambos modelos se ponen uno al lado del otro para hacer referencia a uno u otro en función al contexto en que se esté trabajando.

A continuación se describen las capas que son utilizadas para hacer el diseño de la rede de INDECOPI:

- Capa de acceso a red: Esta capa consolida la capa 1 y 2 del modelo OSI. La capa 1 hace referencia a la conexión física de los dispositivos (cableado de red) y la capa 2 hace referencia a los protocolos de interconexión físicos entre dispositivos de red (para los efectos del caso, Ethernet 802.1). Los dispositivos de capa 2 son aquellos que se encargan de interconectar físicamente las tarjetas de acceso de los computadores en red basados en las direcciones físicas de dichas tarjetas (para Ethernet las direcciones MAC). Los switches capa 2 están asociados a esta capa.

- Capa de Internet.- Esta capa está asociada a la capa 3 del modelo OSI y hace referencia a los protocolos de interconexión lógica entre dispositivos de red. En este caso particular, el protocolo utilizado es IPV4. Los dispositivos de capa 3 son aquellos a los

que se les configura direcciones lógicas en sus tarjetas de red (direcciones IP), son agrupadas en segmentos lógicos llamadas redes, las que típicamente son segmentadas en subredes y que tienen capacidades de enrutamiento (trasladar paquetes IP pertenecientes a una red o subred lógica a otras y viceversa). Los dispositivos con capacidad de enrutamiento (routers, switches capa 3, etc.) están asociados a esta capa

- Capa de transporte.- Esta capa está asociada a la capa 4 del modelo OSI y hace referencia a los protocolos que brindan interconexión de punto a punto para las aplicaciones entre dos dispositivos de red pertenecientes a una red local (donde los dispositivos pertenecen a la misma red o subred) o a una red remota (donde los dispositivos pertenecen a distintas redes o subredes). En el modelo TCP/IP se hace referencia al protocolo TCP (Protocolo de Capa de Transporte) y al UDP (Protocolo de Datagrama de Usuario), donde dependiendo de la aplicación se hará uso de uno o de otro. Estos protocolos permiten la comunicación de las aplicaciones mediante el uso de puertos. Los dispositivos que tengan la capacidad de gestionar puertos están en esta capa (Firewall).
- Capa de aplicación.- Esta capa está asociada a las restantes capas del modelo OSI y están referidas a las aplicaciones que hacen uso de las capas inferiores del modelo TCP/IP. Existen múltiples aplicaciones como por ejemplo HTTP (Hypertext Transfer Protocol, FTP (File Transfer Protocol), DNS (Domain Name Server), entre otros, que habilitan la interacción práctica de los usuarios de la red. Dado que estos protocolos están compuestos por diversas cabeceras, particulares a cada uno de ellos, los dispositivos de la capa de aplicación deben poder entender estas cabeceras. Los IPS (sistema de prevención de intrusión) caen dentro de dicha definición.

Ethernet

Ethernet es la tecnología LAN de uso más frecuente. Un grupo formado por las empresas Digital, Intel y Xerox, conocido como DIX, fue el primero en implementar Ethernet. DIX creó e implementó la primera especificación LAN Ethernet, la cual se utilizó como base para la especificación 802.3 del Instituto de Ingenieros Eléctrica y Electrónica (IEEE), publicada en 1980. Más tarde, el IEEE extendió la especificación 802.3 a tres nuevas comisiones conocidas como 802.3u (Fast Ethernet), 802.3z (Gigabit Ethernet transmitido en fibra óptica) y 802.3ab (Gigabit Ethernet en UTP) [17].

VLAN y enlaces troncales (802.1q)

La segmentación de las LAN es un aspecto muy importante. Son dos los motivos fundamentales para dividir una LAN en segmentos: la primera es aislar el tráfico entre segmentos; la segunda es lograr más ancho de banda por usuario mediante la creación de dominios de colisión más pequeños.

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico. Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

La implementación de las VLAN combina la conmutación de Capa 2 y las tecnologías de enrutamiento de Capa 3 para limitar tanto los dominios de colisión como los dominios de broadcast. Las VLAN también ofrecen seguridad con la creación de grupos VLAN que se comunican con otras VLAN a través de routers [18].

Referente al 802.1q, el enlace troncal es un conducto para las VLAN entre los switches y los routers. El enlace troncal proporciona un método eficaz para distribuir la información del identificador de VLAN a otros switches. Es importante entender que un enlace troncal no pertenece a una VLAN específica [19].

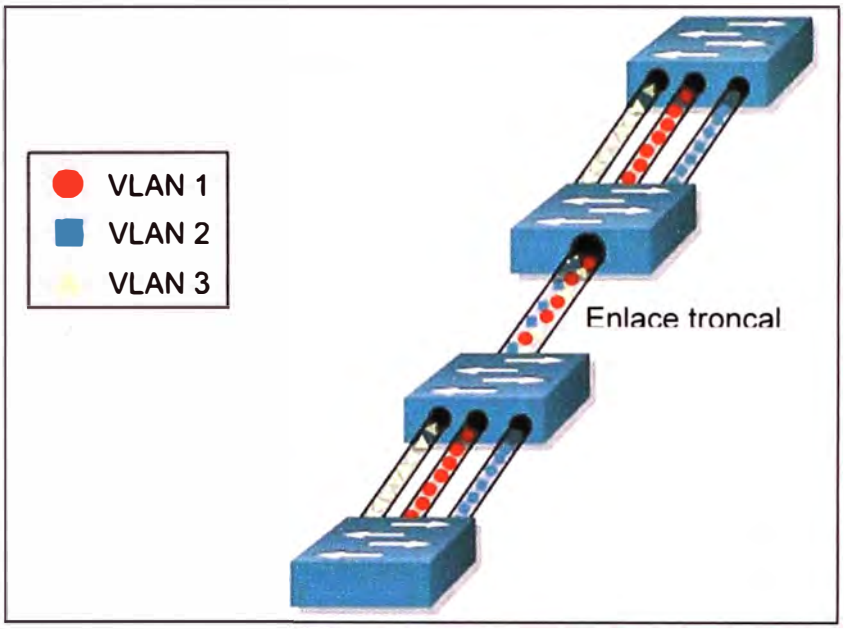

Figura 3.3 Enlace troncal (Fuente: Referencia [19])

Enrutamiento

La Figura 3.4 ayuda a explicar el enrutamiento. El enrutamiento permite que los paquetes IP provenientes de los equipos que conforman la red, encuentren una ruta lógica a una red de destino remota. Estas rutas son configurables, y pueden ser estáticas (donde los caminos se definen manualmente) o dinámicas (donde los caminos se definen automáticamente basados en una serie de parámetros previos que son utilizados por determinados protocolos de enrutamiento).

La figura muestra las capas que son involucradas en el proceso de enrutamiento de un paquete IP. La figura hace evidente que la comunicación de enlace de datos tiene un contexto local, y la comunicación de capa de red, un contexto interredes

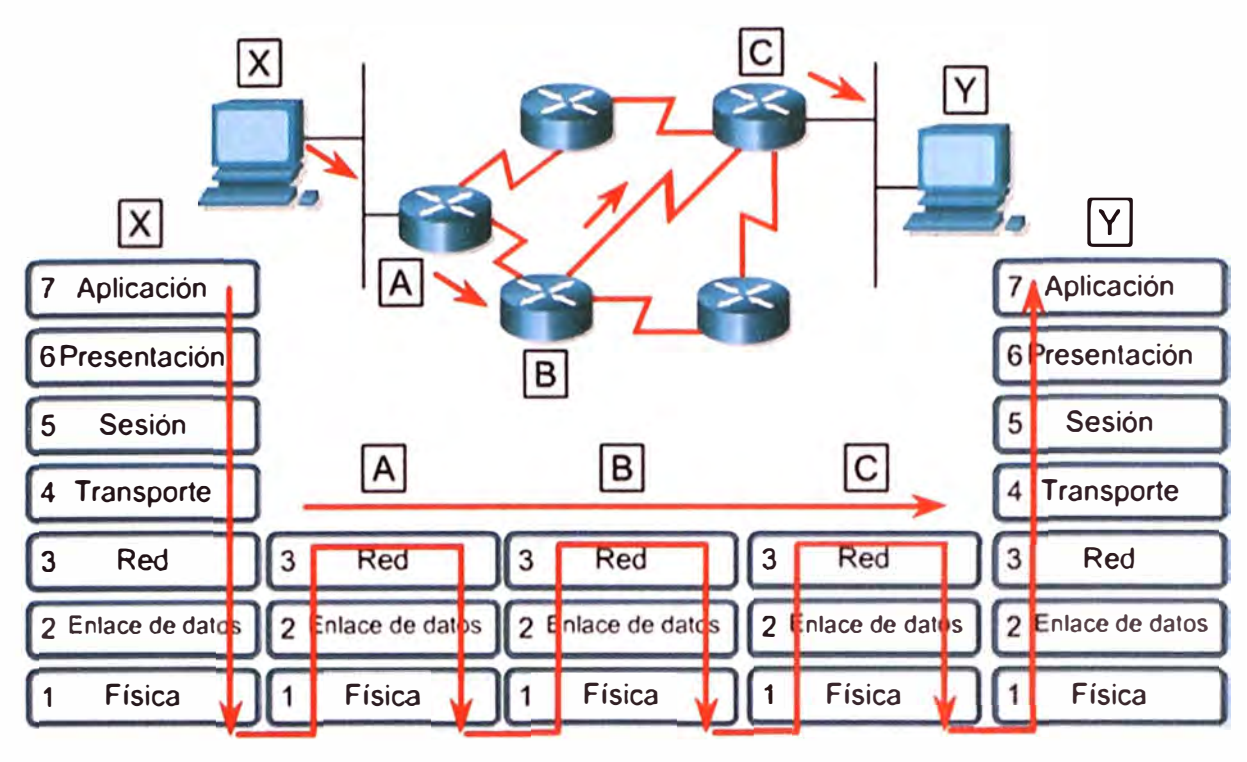

Figura 3.4 Enrutamiento IP (Fuente: Referencia [20])

3.2.1 Topología de la solución de redes

La Figura 3.1 y 3.2 muestran la topología de la solución de comunicaciones y la segmentación de la LAN en VLANs para las redes de usuarios y la de los servidores.

Cumpliendo con los requerimientos de la licitación se proporcionaron los siguientes dispositivos y elementos para la solución de comunicaciones:

- 1 Switch de Núcleo Cisco Catalyst 6509 Enhanced [21].
- 3 Switch de Distribución Cisco Catalyst 3560G-48PS [22].
- 14 Switch de Acceso Cisco Catalyst 3560-48PS [Ibídem].
- 1 Software de Administración Cisco Works LAN Management Solution [23].

El detalle de estos elementos es descrito en el Anexo E.

Es necesario hacer notar que durante el desarrollo de la solución se determinó la necesidad de utilizar uno de los switch de acceso como de distribución, por tal motivo se tuvo que adicionar un adaptador para conexión de fibra (Pabellón F de la Figura 3.1). Como puede observarse en la Figura 3.1, la topología de la red posee una estructura jerárquica. Por otro lado la Figura 3.2 ilustra el esquema de conexiones de la sección de la capa de núcleo de la red de INDECOPI. Estas figuras son utilizadas en las secciones siguientes (secciones 3.2.2 y 3.2.3) para explicar lo correspondiente a la segmentación de las VLAN y a la gestión centralizada de comunicaciones.

Es necesario recalcar, que por aspecto de confidencialidad exigidos por INDECOPI no se precisan la nomenclatura real de las VLAN, así como tampoco los verdaderos valores de las direcciones IP, para cada caso.

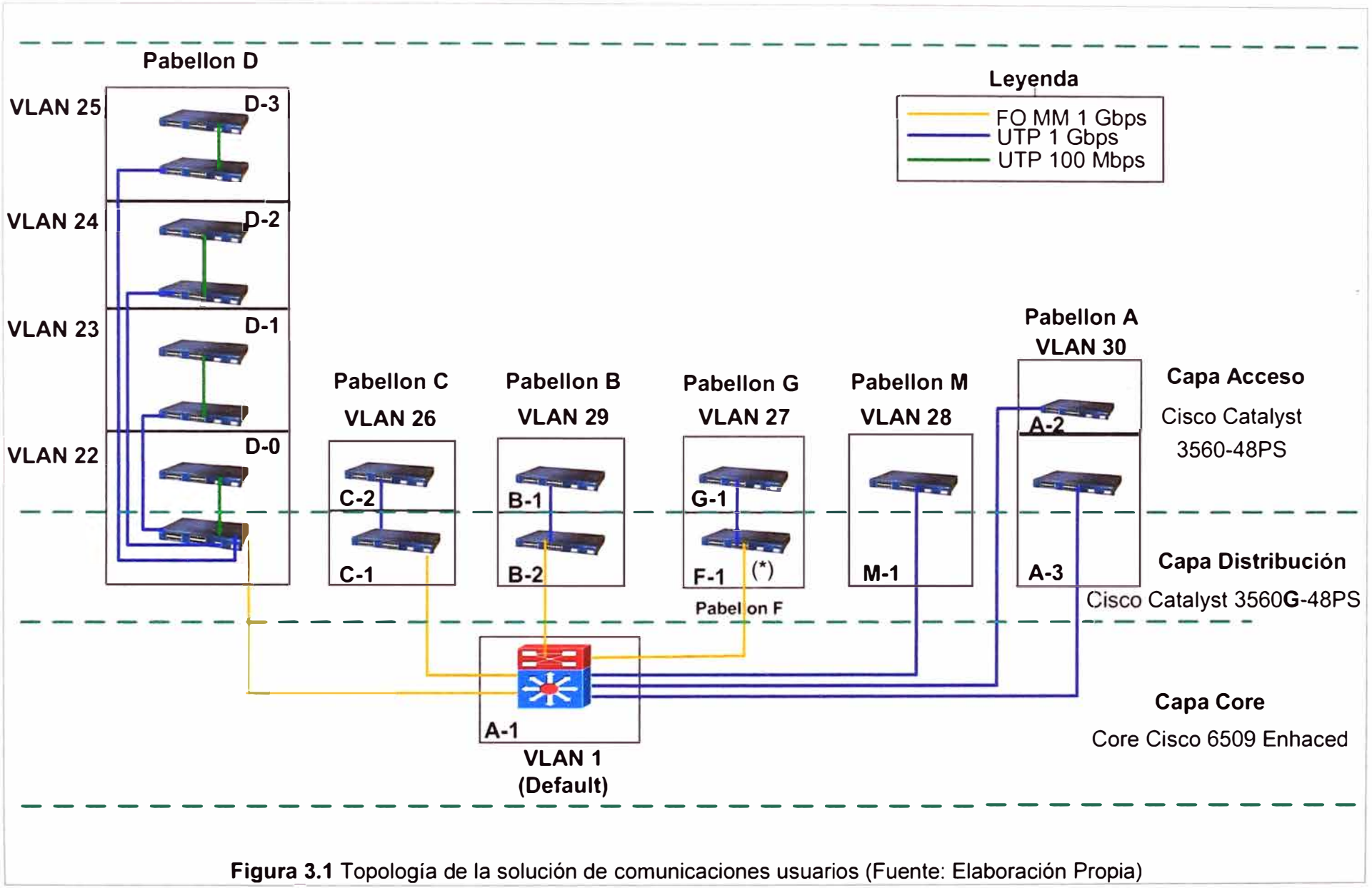

Figura 3.1 Topología de la solución de comunicaciones usuarios (Fuente: Elaboración Propia)

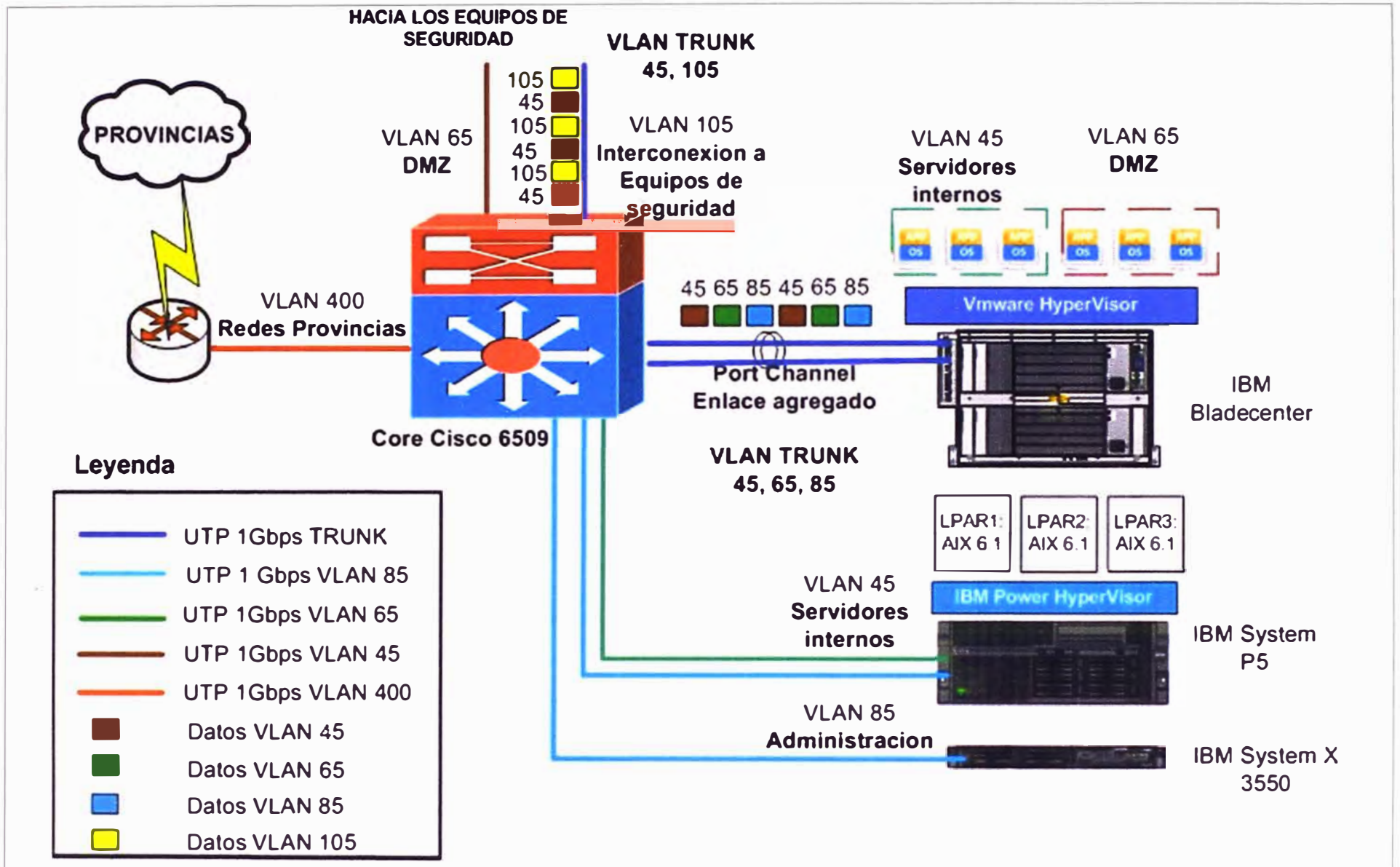

Figura 3.2 Topología de la solución de comunicaciones para Servidores (Fuente: Elaboración Propia)

3.2.2 Segmentación de VLANs

A continuación, se hace una descripción de la arquitectura planteada (capas núcleo, distribución y acceso):

a. Capa de Núcleo (core).

Está conformada por el switch Cisco 6509– E. Las Figura 3.1 y 3.2 ayudan a mostrar las funciones de esta capa de la arquitectura, las cuales son las siguientes:

- Interconexión con los pabellones de INDECOPI, mediante enlaces troncales.
- Interconexión con los servidores de INDECOPI, mediante enlaces troncales o enlaces asociados a una VLAN determinada.
- Interconexión con los equipos de seguridad perimetral mediante enlaces troncales o enlaces asociados a una VLAN determinada (Los componentes de seguridad perimetral y su interacción con la red será explicada más adelante).
- Interconexión con el equipo de enrutamiento que brindaba conectividad a la sede principal de INDECOPI, con las sedes remotas en provincias.

En la presente capa se realiza la gestión de la totalidad de VLANs configuradas en INDECOPI, las cuales son las siguientes:

- Para los usuarios de la red interna.
- De administración.
- Para el acceso seguro a servidores.
- Para el acceso a Internet
- Para el acceso a las sedes remotas.

Esta capa también es el enrutador central de INDECOPI. La estrategia completa de enrutamiento será explicada en conjunto con los equipos de seguridad perimetral, dado que ellos complementan el esquema de enrutamiento de la institución.

Esta capa brinda alta disponibilidad mediante equipamiento redundante (supervisoras de gestión y fuentes de poder), así como enlaces redundantes a los equipos más críticos de la arquitectura. (Enlaces agregados, o enlaces que actúan en paralelo, incrementando la confiabilidad de la solución, y duplicando el ancho de banda disponible para los servicios que se conecten utilizando los mismos). Nótese el detalle de interconexión en la Figura 3.2 donde se ven los datos de las diferentes VLANs de servidores y firewall..

b. Capa de Distribución

Está conformada por:

- 3 Switches Cisco Catalyst 3560**G**-48PS, los cuales tienen 48 puertos Gigabit Ethernet (10/100/1000 Mbps), 4 de esos puertos con opción de ser adaptados a fibra óptica para distancias mayores a 100m,
- 1 Switch Cisco Catalyst 3560-48PS, el cual posee 48 puertos FastEthernet (10/100

Mbps), pero 4 de esos puertos tienen la capacidad de poder ser adaptados fibra óptica Gigabit Ethernet (10/100/1000 Mbps) para interconexión a distancias mayores a 100m.

Las funciones de esta capa son las siguientes:

- Interconexión de los pabellones principales con el switch de núcleo, mediante enlaces de fibra óptica a 1 Gbps con los pabellones a una distancia mayor a 100m del switch de núcleo, y mediante enlaces de cobre a 1Gbps con los pabellones a una distancia menor a 100m del mencionado switch.
- Distribución de las VLANs correspondientes a cada grupo de pabellones servidos por esta capa, de acuerdo al diagrama de distribución mostrado en la figura 3.1
- Estos equipos, además de gestionar las VLANs correspondientes para los pabellones que se interconectan a la red a través de ellos, gestionaban la VLAN de administración, de modo que estos equipos y los equipos de acceso tuvieran la opción de ser gestionados remotamente desde una VLAN particular a la cual tenían acceso solamente los administradores de la red.

c. Capa de Acceso

Conformada por los switches Cisco 3560-48PS, con 48 puertos FastEthernet (10/100). Las funciones de esta capa son las siguientes:

- Brindar la interconexión en una VLAN respectiva a cada pabellón de la red de INDECOPI. Cada VLAN contaba con un direccionamiento de red distinto al de otro edificio, lo cual permitió ordenar la ubicación de cada subred, haciendo una asociación de la VLAN asignada al piso de un pabellón particular, y el rango de direcciones IP brindado en dicha VLAN. Esto generó un impacto muy positivo en cuanto a la identificación de problemas de red en INDECOPI, debido a la mayor facilidad de detectar problemas de red en un determinado segmento de la red.
- Brindar la conectividad de los equipos del pabellón, a través de switches en cascada conectados a los switches de esta capa, cuya única función es la de interconectar puntos finales de red (usuarios). Esto también generó un tremendo impacto en INDECOPI, debido a que el reordenamiento de los switches permitió brindar a la red el nivel de servicio adecuado en función a la criticidad y requerimiento de los servicios de la red. Así pues, switches con bajas capacidades ya no se encontraban cerca a la parte central de la red sosteniendo servicios críticos.

3.2.3 Gestión centralizada de comunicaciones

La gestión centralizada de las comunicaciones en INDECOPI se logró mediante el uso de la herramienta CISCO WORKS, que es una solución basada en software, que fue instalada en una máquina virtual sobre la infraestructura virtual VMware, con conectividad en la VLAN de administración de equipos.

Esta herramienta permite la gestión de todos los equipos de comunicaciones de INDECOPI (Incluyendo los equipos de seguridad perimetral). De este modo no solo se tiene el control de todas las opciones de configuración de un determinado equipo en la red, sino también se conoce el estado de salud de cada uno de los equipos (actividad de los puertos, monitoreo de los procesadores y memoria de los equipos, entre otros), brindándose así a INDECOPI una visibilidad total del desempeño de la red.

3.3 Solución de seguridad informática

En esta sección se describen las políticas de seguridad y la funcionalidad completa de la red, en función a los planteamientos de diseño que fueron tomados en consideración para este proyecto.

3.3.1 Políticas de seguridad establecidas

Se establecieron tres tipos de políticas:

- Para los usuarios internos de la red de INDECOPI (Entre los que se contaban también a los usuarios de provincias).
- Para los servidores de la red de INDECOPI.
- Para los usuarios remotos pertenecientes a INDECOPI.- Son ubicados fuera de la red interna de la institución.

a. Políticas para los usuarios internos de la red de INDECOPI

Como se mencionó, entre estos usuarios también se consideran a los usuarios de provincias. Las políticas que se están cumpliendo son las siguientes:

- Cada VLAN de usuario debe contar con su propia subred, y las direcciones IP de dicha subred deben ser asignadas de manera dinámica a los equipos de dicha VLAN. (utilizando servicios de distribución dinámica de asignación de direcciones de red). Para este caso se considera utilizar el protocolo DHCP (Dynamic Host Configuration Protocol-Configuración Dinámica de Equipo) [24] (se explica en 4.1.3.a).
- La comunicación entre VLANs de usuarios debe ser efectuada vía enrutamiento IP simple, es decir, sin ninguna clase de filtrado IP o de capas superiores. INDECOPI con ello logra que los usuarios de la red puedan comunicarse entre ellos de manera eficiente, es decir, conteniendo el tráfico de Broadcast en la red origen. Lo mismo se aplica para la comunicación de los usuarios internos con las provincias, y viceversa.
- La comunicación entre VLANs de usuarios y las VLANs de servidores debe contar con restricciones de acceso, de modo tal que se garantice que los usuarios puedan acceder solamente a servicios específicos de los servidores, y no posean capacidad de acceso sin restricciones, como ocurría en la red original de INDECOPI. Asimismo, los usuarios que acceden a los servidores de INDECOPI, deben contar con protección a nivel de la capa de aplicaciones, es decir, con la capacidad de detectar anomalías en los protocolos

de aplicación empleados para el acceso a los servicios (entre los que se pueden encontrar códigos maliciosos, como virus o inyección malintencionada de código, buscando explotar alguna vulnerabilidad de los servicios brindados por la red de INDECOPI).

- El acceso a Internet de los usuarios internos, debe ocultar las direcciones IP de la red interna de la institución detrás de un grupo determinado de direcciones IP públicas enrutables a Internet, de este modo se evita la comunicación a nivel de IP o de puertos desde fuera de la red de INDECOPI hacia un equipo particular interno. Solamente los servicios básicos deben ser permitidos para los usuarios (por ejemplo, navegación web o consultas a servidores de transferencia de archivos externos). Asimismo, se debe brindar protección a nivel de las capas de aplicaciones, para poder detectar las aplicaciones maliciosas que puedan establecer conexiones malintencionadas fuera de la red de INDECOPI, desde equipos internos que hubieran podido verse afectados por eventos como, por ejemplo, la descarga de un archivo infectado.

b. Políticas para los servidores de la red de INDECOPI

Los servidores se clasifican dos grupos:

- **Servidores internos**: Son aquellos que brindan servicios exclusivamente a la red interna de INDECOPI, como servicios de Intranet, impresión, compartición de archivos y gestión de permisos en la red. Los servidores de bases de datos (Oracle y SQL), también se encuentran en este segmento.

- **Servidores DMZ**: Estos servidores brindan servicios, no solo a la red interna de INDECOPI, sino también al público en general a través de Internet. Están compuestos básicamente por los servidores de aplicaciones. Ellos necesitan determinados servicios de conectividad con los equipos de bases de datos de la red Interna, y algunos servicios particulares adicionales de dicha red – pero no acceso sin restricciones.

Para estos segmentos, las políticas son las siguientes:

a. Servidores Internos

Dado que estos equipos no brindan acceso a usuarios fuera de la red de INDECOPI, ellos no precisan exponer sus servicios a Internet. Si bien ello es aplicable, cuentan deben contar con salida a Internet para mantener actualizados sus sistemas operativos y aplicaciones. Por lo tanto, solo determinados puertos de salida deben estar definidos para estos equipos.

Solamente los puertos de servicio de las aplicaciones alojadas en dichos servidores deben estar a disposición de los usuarios de la red interna. El resto de puertos deben estar restringidos. Los servidores de aplicaciones ubicados en el segmento DMZ deben acceder a puertos especiales de las bases de datos (Oracle y SQL), por ello deben estar

habilitados puertos específicos solo para ellos.

Toda comunicación (entrante o saliente), debe contar obligatoriamente con protección a nivel de la capa de aplicación, dada la criticidad de los servicios alojados en este segmento de red.

b. Servidores DMZ

Estos equipos brindan servicios al público en general, por lo tanto, sus servicios están expuestos a Internet. Algunos de estos servicios también deben estar habilitados para los usuarios internos.

Al igual que los servidores de la red Interna, estos equipos deben poseer determinados accesos a Internet para mantenerse actualizados.

Estos equipos deben poseer acceso a determinados servicios de la red de servidores internos, sobre todo aquellos necesarios para las consultas a las bases de datos (Oracle y SQL).

Toda comunicación (entrante o saliente), debe contar obligatoriamente con protección a nivel de la capa de aplicación, dada la criticidad de los servicios alojados en este segmento de red.

c. Políticas para los usuarios remotos pertenecientes a INDECOPI

Son aquellos ubicados fuera de la red interna de la institución. Las políticas son las siguientes:

Toda comunicación de estos usuarios debe ser auditada por INDECOPI. Por lo tanto, los accesos a los recursos internos de la red, como los accesos a INTERNET, deben gestionarse en la red de INDECOPI.

La comunicación hacia los recursos de INDECOPI debe utilizar métodos de acceso seguros, de modo que no hubiera compromiso de la información que se transfiriese entre los usuarios remotos y la red interna de la institución.

3.3.2 Esquema final de la red de INDECOPI en función a las políticas establecidas

En la Figura 3.3 se muestra el esquema final de la red de INDECOPI, la cual ayudará a explicar la funcionalidad completa de la solución, tanto para la parte de enrutamiento interno, como de las políticas de seguridad previamente definidas.

a. Firewall Cisco ASA

Las funciones del Firewall indicado (1) en la red de INDECOPI son las siguientes [25]:

- Gestión de las políticas de seguridad perimetrales de INDECOPI (filtrado de puertos y restricción de acceso entre redes de INDECOPI).
- Enrutamiento de las redes internas hacia otras redes distintas a ellas:
  - hacia los servidores, brindando filtrado de puertos.
  - hacia Internet usando traducción de direcciones de red (NAT).

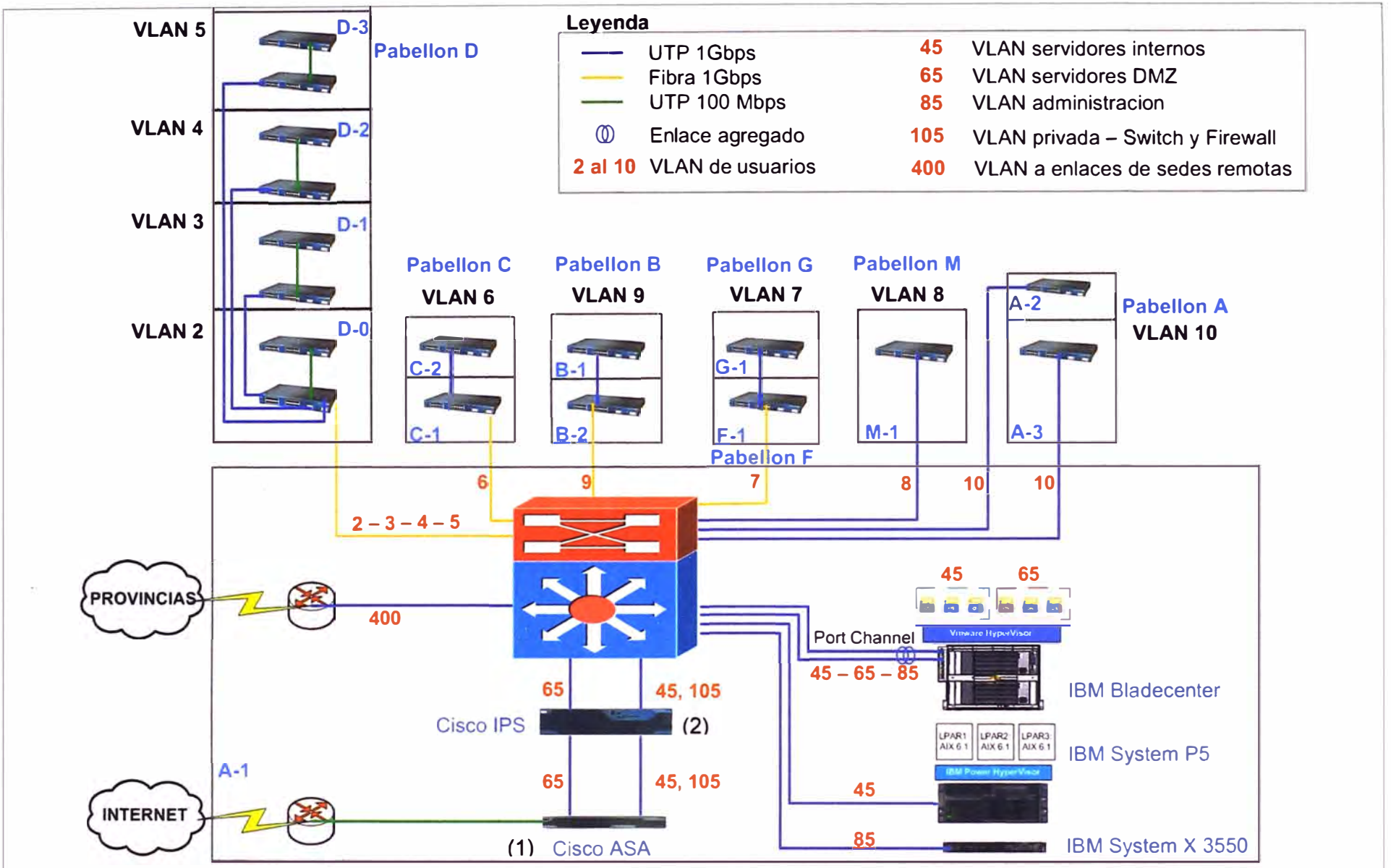

Figura 3.3 Esquema final de la red de INDECOPI (Fuente: Elab. Propia)

- Enrutamiento de los servidores:

o Hacia los servidores internos retornando las solicitudes de conexión de las redes internas.

o Entre los servidores DMZ y los servidores de la red interna para acceder a los servicios requeridos para el trabajo de las aplicaciones.

o Acceso a Internet para servicios de actualización de aplicaciones y sistemas operativos instalados en los servidores.

o Publicación de servicios a Internet para servicio al público en general.

- Gestión de las conexiones remotas SSL (Secure Socket Layer) para los usuarios externos (VPN SSL).

Nota:

El NAT (Network Adress Translation) [26] es una técnica definida por la IETF (Internet Engineering Task Force) en la RFC 3022 [27] (Request for Comment). Consiste en la traducción de las direcciones privadas (definidas en el RFC 1918 [28]) en direcciones públicas enrutables a Internet.

b. Sistema de prevención de intrusos (IPS)

El equipo indicado (2) es el Cisco IPS-4240-K9. Éste brinda seguridad en todas las capas del modelo TCP/IP. Tiene las siguientes funcionalidades [29]:

- El equipo cuenta con una máquina de inspección que normalmente es un software basado en códigos cerrados o propietarios que permite el análisis de paquetes de red y la toma de acciones en función a los resultados de la detección. Entre estas acciones se cuenta el bloqueo de las conexiones mediante envíos de paquetes de reinicio de sesiones (TCP reset), alertas, presentación al usuario de páginas informativas en sus navegadores web sobre potenciales amenazas y retroalimentación inteligente mediante el aprendizaje de las amenazas que va detectando (ello se consigue con actualizaciones del software brindado por el fabricante). En adición a ello el IPS tiene la capacidad de detectar y tomar acción frente a comportamientos anómalos en la red, como por ejemplo, incrementos sospechosos del consumo del tráfico de la red proveniente de un usuario o usuarios internos, o desde Internet, lo cual puede representar desde infecciones de virus hasta ataques orientados a consumir los recursos computacionales de los equipos de la red (DoS - Denegación de Servicio).

- El equipo puede trabajar de tres modos:

o Inline (modo en línea).- Un par de interfaces del equipo (que pueden provenir de un enlace simple o de un enlace troncal) se colocan de tal manera que el equipo IPS esté en línea con el tráfico de red, de modo tal que el tráfico es inspeccionado al atravesar el equipo. Si el equipo falla (pérdida de energía o falla en la máquina de inspección) el

servicio no se ve comprometido, ya que éste se comporta como un cable. Este es el modo de trabajo configurado en INDECOPI.

- Blocking (modo de bloqueo).- Este modo es similar al modo inline con la única diferencia de que ante la falla de la máquina de inspección el equipo se comporta como un relé abierto de modo que el tráfico de red no circula.
- IDS (Intrusion Detection System) o modo out of line.- En este modo el equipo no se encuentra en línea con el tráfico, sino que tiene conectada una interfaz de red proveniente de un puerto promiscuo de la red de producción (un puerto promiscuo o espejado, es aquel del cual se puede analizar todo el tráfico de determinados segmentos de red). Ello permite al IPS inspeccionar los paquetes pero no toma ninguna acción de seguridad excepto el envío de alertas.

c. Enrutamiento diseñado para la red de INDECOPI

El esquema de conexión mostrado en la Figura 3.3 es consecuencia de la definición de todas las políticas de seguridad y de enrutamiento precisadas para INDECOPI.

Para poder entender el funcionamiento de la red es necesario hacer referencia a las Tablas 3.2 y 3.3 (esquema general de enrutamiento Switch de Core y de Firewall, respectivamente). Para todo efecto la VLAN X representa a cualquier VLAN Interna (2 al 10) cualquiera, y la VLAN Y a cualquiera otra pero VLAN interna distinta a la VLAN X.

Ambas tablas están organizadas de la siguiente manera. Por un lado se muestra el origen y destino de la conexión, por otra parte los equipos por donde ingresas y egresan las conexiones, y finalmente las VLANs de ingreso y egreso. Este último punto es importante porque permite identificar las redes que se están intercomunicando en el proceso de transporte de los paquetes IP a través de la red, y permite ubicar al lector en un punto específico del gráfico mostrado previamente. El objetivo es encontrar un camino para todos los paquetes IP en las diferentes subredes de INDECOPI que cumplan con las políticas e seguridad previamente definidas.

Se debe tomar en consideración que, cuando los paquetes se dirigen hacia el Firewall o retornan de él hacia las redes internas, el IPS se encarga de brindar servicios de análisis de paquetes asegurando protección hasta el nivel de aplicaciones. Así mismo todo paquete que sea enrutado en el firewall cuenta con filtrado de puertos que son definidos particularmente para cada segmento destino de la red.

Para ilustrar la lectura de las siguientes tablas se decribirá como ejemplo la primera fila de la Tabla 3.2. En ella se puede apreciar que el origen de la conexión son las redes internas locales (VLAN X), y el destino de la conexión cualquier otra VLAN interna distinta (VLAN Y). Para este caso el equipo de ingreso y de egreso es el switch de core quien enruta los paquetes entre VLANs distintas (X e Y).

Tabla 3.2 Rutas: Switch de Core (Fuente: Elab. Propia)

Origen	Destino	Equipo		VLAN		Comentarios
		de ingreso	de egreso	de Ingreso	de egreso	
Redes Internas Locales VLAN X	Redes Internas Locales VLAN Y	Switch de Core	Switch de Core	X	Y	Enrutamiento entre redes internas efectuado exclusivamente en el Switch de core
Redes Internas Locales VLAN X	Redes Provincias	Switch de Core	Router Provincias	X	400	Enrutamiento entre redes internas y redes de provincias efectuado exclusivamente en el switch de core
Redes Provincias	Redes Internas Locales VLAN X	Router Provincias	Switch de Core	400	X	
Redes Internas Locales VLAN X	Red Servidores (Internos y Externos)	Switch de Core	Firewall	X	105	Enrutamiento hacia las redes de servidores, enviado al Firewall (Siguiente Salto), vía la VLAN 105
Redes Provincias	Red Servidores (Internos y Externos)	Switch de Core	Firewall	400	105	Enrutamiento hacia las redes de servidores, enviado al Firewall (Siguiente Salto), vía la VLAN 105
Red Servidores (Internos y DMZ)	Redes Internas Locales VLAN X	Firewall	Switch de Core	105	X	Enrutamiento desde las redes de servidores hacia la red Interna, efectuado en el Switch de Core
Red VPN SSL (Usuarios remotos)	Redes Internas Locales VLAN X	Firewall	Switch de Core	105	X	Los usuarios VPN SSL también cuentan con sus rutas de acceso a los equipos internos
Red VPN SSL (Usuarios remotos)	Redes Provincias	Firewall	Switch de Core	105	400	
Ruta por defecto	Cualquier red	Switch de Core	Firewall	Cualquiera	105	Cualquier otra red se enruta hacia el Firewall

Para el caso del firewall, se sigue la misma metodología de la tabla anterior. En la primera fila de la Tabla 3.3 el origen de conexión son las redes internas y el destino la red de servidores internos, desde el contexto del firewall la conexión ingresa por la VLAN 105 de firewall y egresa por la VLAN 45 dirigiéndose de vuelta al switch de core. Nótese en la

Figura 3.3 que la conexión troncal que consolida las VLAN 105 y 45, que interconectan firewall y switch, transportan datagramas ubicadas en VLANs distintas y que necesitan un dispositivo de enrutamiento intermedio para poder comunicarse.

Tabla 3.3 Rutas: Firewall (Fuente: Elab. Propia)

Origen	Destino	Equipo		VLAN		Comentarios
		de ingreso	de egreso	de Ingreso	de egreso	
Redes Internas (Locales y Provincias)	Red Servidores Internos	Firewall	Switch de Core	105	45	El tráfico proveniente de las redes internas es filtrado y enrutado a la VLAN 45 (Servidores Internos), en el firewall.
Redes Internas (Locales y Provincias)	Red Servidores DMZ	Firewall	Switch de Core	105	65	El tráfico proveniente de las redes internas es filtrado y enrutado a la VLAN 65 (Servidores DMZ), en el firewall.
Redes Internas (Locales y Provincias)	Internet	Firewall	Router Internet	105	Internet	El tráfico proveniente de las redes internas es enviado hacia Internet por medio del Firewall
Red Servidores Internos	Redes Internas (Locales y Provincias)	Firewall	Switch de Core	45	105	Enrutamiento desde la red de servidores internos hacia los usuarios vía la VLAN 105.
Red Servidores Externos	Redes Internas Locales VLAN X	Firewall	Switch de Core	65	105	Enrutamiento desde la red de servidores DMZ hacia los usuarios internos a las VLAN respectivas en la parte interna de la red
Red Servidores Externos	Redes Provincias	Firewall	Switch de Core	65	105	
Red VPN SSL (Usuarios remotos)	Redes Internas (Locales y Provincias)	Router Internet	Firewall	Internet	105	Enrutamiento de los usuarios VPN SSL externos hacia las redes internas
Red VPN SSL (Usuarios remotos)	Red Servidores Internos	Router Internet	Firewall	Internet	45	Enrutamiento de los usuarios VPN SSL externos hacia los servidores internos
Red VPN SSL (Usuarios remotos)	Red Servidores DMZ	Router Internet	Firewall	Internet	65	Enrutamiento de los usuarios VPN SSL externos hacia los servidores DMZ
Ruta por defecto	Cualquier red	Firewall	Router Internet	Cualquiera	Internet	Cualquier otra red se enruta a Internet

Se puede notar que físicamente el paquete ingresa y retorna por la misma interfaz de firewall pero lógicamente se ha efectuado el enrutamiento entre las VLANs (con su correspondiente aplicación de política de seguridad al momento de enrutarse).

3.4 Cableado estructurado

Esta solución consiste en todos los trabajos relacionados con la conectividad de los equipos de comunicaciones considerando los aspectos normativos actuales. La Figura 3.4 muestra la distribución de los edificios y el tipo de cableado utilizado.

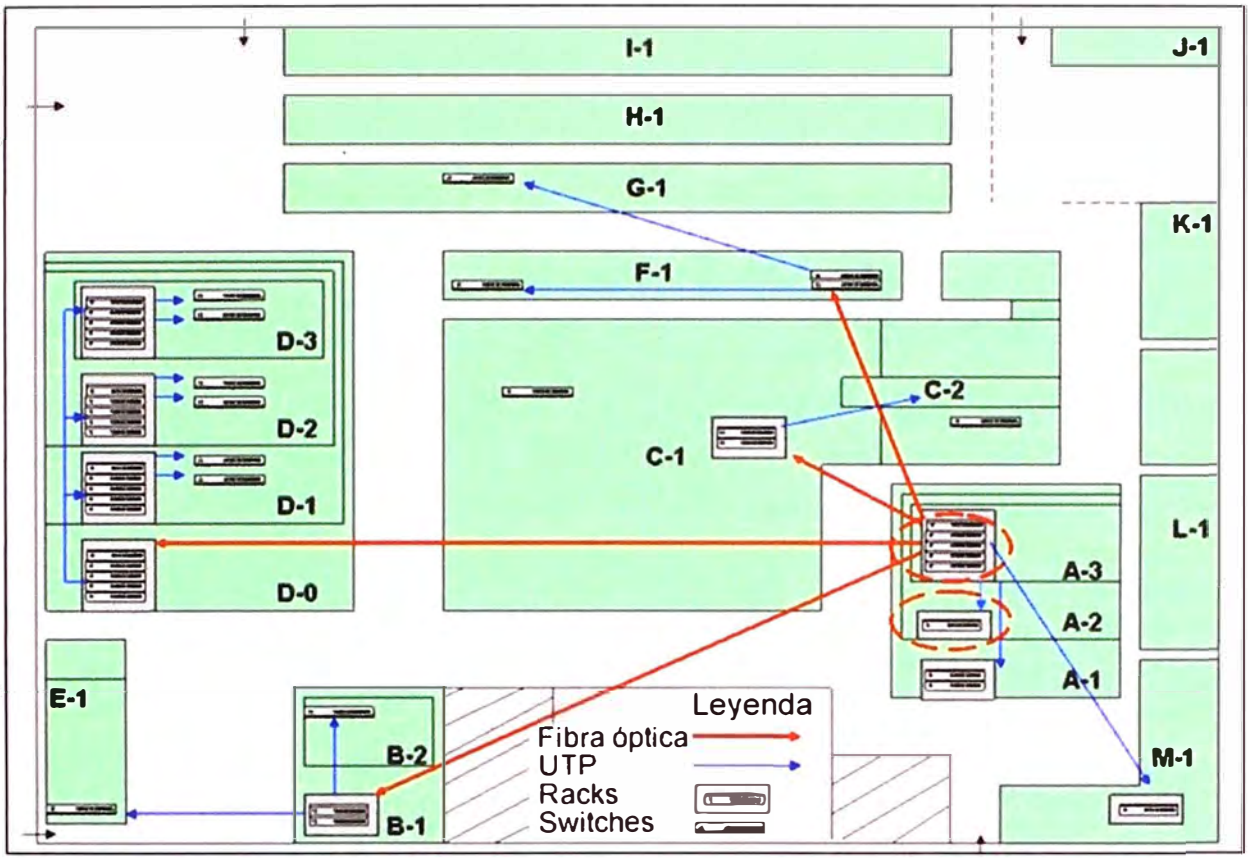

Figura 3.4 Distribución de los edificios y el tipo de cableado utilizado (Fuente: Ref. [3])

3.4.1 Aspectos normativos

Los trabajos relativos al cableado estructurado se enmarcaron dentro de las normas y estándares en lo que se refiere a: Conectividad, canalización/enrutamiento, identificación, uniones y conexiones a tierra. Las siguientes son las últimas versiones de las normas, adendas y estándares considerados por ANSI/TIA/EIA, para categoría 6.

- **ANSI/TIA/EIA-568-B** [30].- Permite el planeamiento y la instalación de un sistema de cableado estructurado para edificios comerciales. Especifica los requerimientos mínimos para los componentes de cableados estructurados

- **ANSI/TIA/EIA-569-B** [31].- Brinda especificaciones de diseño para todas las estructuras de las edificaciones relacionadas a los sistemas de cableado de telecomunicaciones y sus componentes. El estándar identifica seis componentes de la infraestructura del edificio: el ingreso al edificio, cuartos de equipamiento, recorridos del backbone

(verticales), cuartos de telecomunicaciones, recorrido horizontal y áreas de trabajo.

- **ANSI/TIA/EIA-606(A)** [32].- Provee lineamientos y alternativas de las clases de administración para mantener una infraestructura de telecomunicaciones. Cuatro clases de administración son especificadas. Estas clases están basadas en la complejidad de la infraestructura que es gestionada y permiten una implementación modular y escalable.
- **J-STD-607** [33].- Especifica los requerimientos para una infraestructura de aterramiento y montaje uniforme que puede ser aplicada en los edificios comerciales donde los equipos de telecomunicaciones sean instalados.
- **ANSI/TIA/EIA-526-14A** [34].- Establece el procedimiento a ser utilizado para medir la pérdida óptica entre dos puntos conectados pasivamente, incluidas las terminaciones finales, de una planta de cableado de fibra óptica multimodo. La planta de cable de fibra óptica puede consistir en cables de fibra óptica, conectores, paneles montables, jumpers, y otros componentes pasivos (no se consideran los componentes activos).
- **ANSI/TIA/EIA-758(A)** [35].- Especifica los requerimientos mínimos para los equipamientos de telecomunicaciones de planta externa propiedad del cliente, en un entorno de campus. Este estándar especifica el cableado, recorridos y espacios para soportar el cableado.
- **ISO/IEC 11801** [36].- Especifica el cableado genérico para ser usado entre locales, el cual puede comprender uno o varios edificios. Cubre cableado balanceado y cable de fibra óptica.
- **ISO/IEC 14763-1** [37].- Identifica principios fundamentales de tal forma que los individuos y organizaciones que son propietarios, o responsables de una infraestructura de telecomunicaciones, puedan, desarrollar un sistema de administración que encaje en sus necesidades. Este estándar internacional no recomienda un tipo específico de sistema de administración.
- **ISO/IEC 14763-2** [38].- Resalta temas relevantes al planeamiento y la instalación de cableado genérico, que ha sido diseñado en concordancia con ISO/IEC 11801.
- **ISO/IEC 14763-3** [39].- Detalla los procedimientos de inspección y pruebas del cableado de fibra óptica diseñado en concordancia con ISO/IEC 11801 y estándares equivalentes, e instalado acorde con los requerimientos y recomendaciones del ISO/IEC 14763-2.
- **IEC 61935-1** [40].- Especifica los procedimientos de medida de los parámetros de cableado así como los requerimientos de precisión de los instrumentos de medición de campo.

3.4.2 Descripción de trabajos

El cableado estructurado incluyó lo siguiente:

- Se instaló un gabinete de comunicaciones de 42 RU (unidades de rack) con kit de ventiladores para el área de sistemas.

- Se instalaron 20 puntos de red en el Data Center para servidores adicionales.

- Se proveyó el cableado y accesorios necesarios para interconectar el gabinete de comunicaciones y los gabinetes de servidores del centro de cómputo.

- Se instaló un gabinete de comunicaciones de pared de 15 RU con kit de ventiladores para el 2do. Piso del Edificio A, además se trasladó los puntos de red de este piso que llegaban al gabinete del primer piso.

- Se reordenó, identificó y etiquetó los gabinetes de comunicaciones ubicados en las zonas A-3, A-1, B-1, C-1, D-0, D-1, D-2, D-3, M-1. Incluyendo los ordenadores power rack y los accesorios de fijación. Se consideró el uso de los patch panel y patch cord existentes en todos los cuartos de comunicaciones de los edificios a interconectar que no perjudicaran la conectividad.

También se instalaron tubos y ductería subterránea para enlaces de fibra óptica y cable UTP que son descritos en la Tabla 3.4:

Tabla 3.4 Enlaces instalados en la red central de INDECOPI (Fuente: Ref [3])

Tipo enlace	Locales enlazados	Distancia (m)
04 enlaces de fibra óptica 10G para interconexión de edificios	Datacenter → 1er Piso Edificio B	120
	Datacenter → 1er Piso Edificio C	95
	Datacenter → hacia Sótano Edificio D	120
	Datacenter → 1er Piso Edificio F	115
Tendido de enlaces UTP categoría 6 para interconexión de edificios y entre pisos	Datacenter → 1er Piso Edificio A	50
	Datacenter → 2do Piso Edificio A	40
	Datacenter → 1er Piso Edificio M	50
	1er Piso Edificio B → 2do Piso Edificio B	40
	1er Piso Edificio B → 1er Piso Edificio E	50
	1er Piso Edificio C → 2do Piso Edificio C	30
	Sótano Edificio D → 1er Piso Edificio D	35
	Sótano Edificio D → 2do Piso Edificio D	45
	Sótano Edificio D → 3er Piso Edificio D	55
	1er Piso Edificio F → 1er Piso Edificio G	40

Nota: Data Center está en el 3er piso del edificio A.

3.5 Migración hacia la nueva red y plan de pruebas

Con esta sección concluye el capítulo 3 "Desarrollo de la arquitectura jerárquica de redes y comunicaciones" (ítem 3 de las bases de licitación). La sección se divide en dos subsecciones: Migración de la nueva red y plan de pruebas (desempeño y continuidad).

3.5.1 Migración hacia la nueva red

La migración se explica en dos partes:

- Equipos de comunicaciones
- Equipos de seguridad informática.

a. Equipos de comunicaciones

La migración de los equipos de comunicaciones constó de lo siguiente:

a.1 Configuración inicial

Básicamente constó de lo siguiente:

- Instalación de la última versión de firmware en los switches de core, distribución y acceso.
- Asignación de hostname (nombre del equipo), y direcciones IP de gestión iniciales.

a.2 Primera configuración del switch de Core

El switch de Core se preparó en primera instancia fuera de línea, de modo tal que no interfiriese con las operaciones de la red en producción. Los primeros equipos a conectarse fueron los nuevos servidores, quienes también se encontraban fuera de línea.

Para iniciar a migrar la red, se tendieron enlaces temporales que comunicaban la red de producción con la nueva red en configuración, y un servicio que era brindado en la red original, era dado de baja para ser activado en los nuevos equipos, de modo que no hubiese inconvenientes de duplicidad del mismo servicio en la red.

Se realizó lo siguiente:

1. Configuración de las siguientes VLAN en el switch de Core: VLAN de servidores Internos, VLAN de servidores DMZ, VLAN de pruebas y VLAN por defecto.
2. Conexión de los servidores IBM Bladecenter, IBM SystemX e IBM SystemP al switch de Core. Dependiendo de si contaban con servicios de la red interna, o de la DMZ, se conectaban en la VLAN determinada. En detalle fue lo siguiente:

- Conexión de servidores IBM Bladecenter mediante 4 enlaces, agrupados en 2 enlaces agregados Gigabit Ethernet, configurados en modo troncal para el traslado de múltiples VLANs (Servidores Internos, DMZ, Pruebas)
- Conexión de servidores IBM System P e IBM SystemX en sus VLANs correspondientes mediante enlaces simples.

3. Conexión temporal del Switch de Core con la red original.- Debido a que la nueva red solamente alojaba la nueva infraestructura de servidores (aún sin servicios, dado que todos ellos se encontraban en la red original), y dado que la red original era un mismo dominio de colisiones con varios segmentos lógicos en él. Para brindar conectividad temporal adecuada, bastó con conectar un punto de la VLAN de Servidores y otro de la VLAN DMZ a la red original (Figura 3.5).

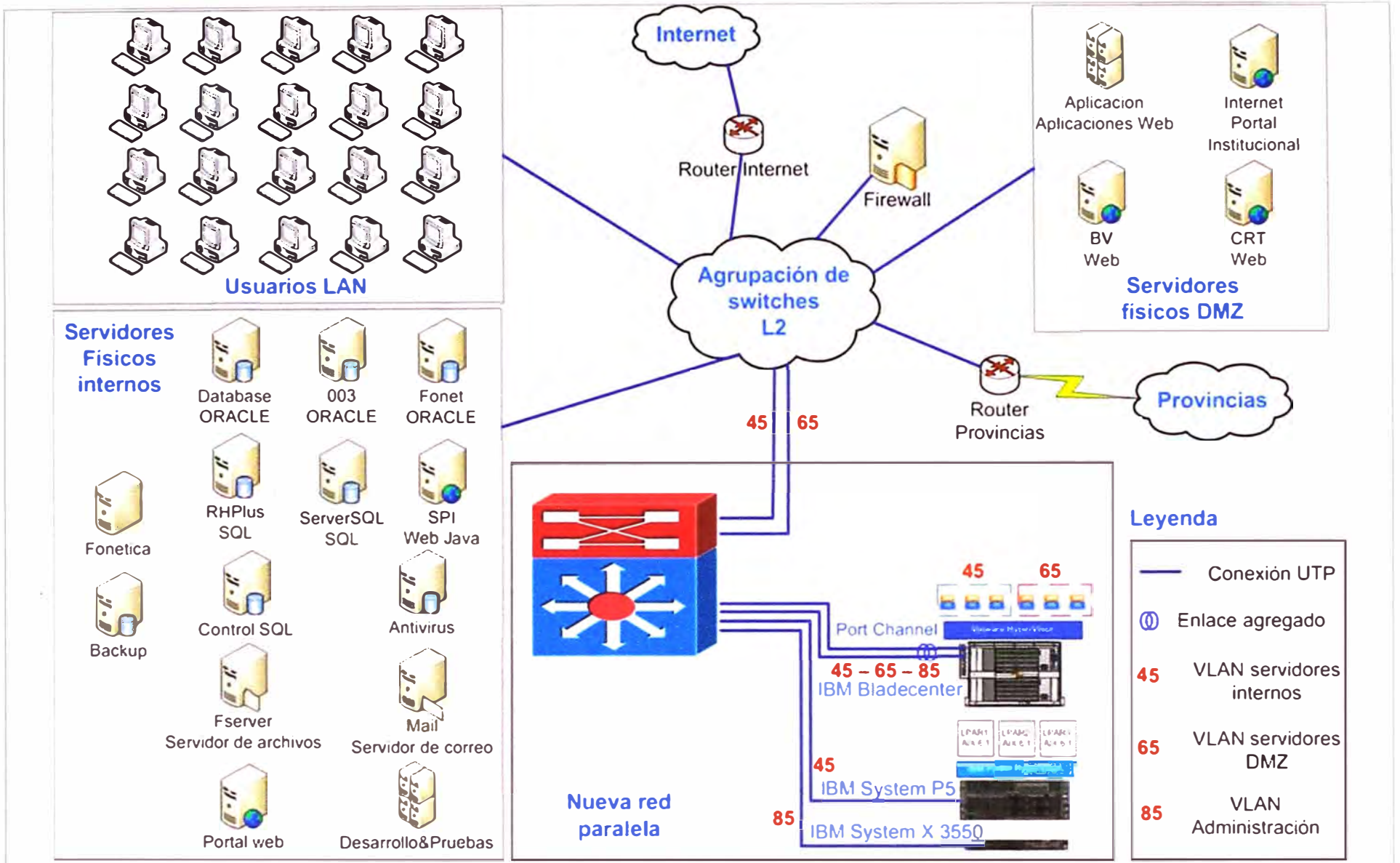

Figura 3.5 Diagrama de conexión temporal para la migración de la red (Fuente: Elaboración propia)

4. Migración de servidores de la red original a la nueva red.- Cuando un servicio era migrado a la nueva red de servidores, el mismo era desactivado en la red original, de modo que pasaba a ser servido desde la nueva red de servidores.

a.3 Segunda configuración del switch de Core. Adición de las VLANs internas en los edificios

Antes que los usuarios de los edificios empezaran a utilizar la red inicial, los nuevos equipos fueron conectados al Core, de acuerdo a lo indicado en los diagramas de red previamente mostrados. Esta etapa se llevó a cabo una vez que todos los servidores fueran migrados a la nueva infraestructura de servidores.

Los siguientes pasos se iteraron para cada una de las VLANs que entraron en producción.

1. Modificación temporal del enrutamiento interno de INDECOPI.- El siguiente cambio permitió el enrutamiento temporal de los usuarios por el switch de Core. Ello era necesario para permitir que las nuevas VLANs que se fueran agregando, pudieran enrutarse a la red original a medida que eran agregadas:

- Configuración de la VLAN por defecto del switch de core, con la dirección IP de la puerta de enlace por defecto configurada en INDECOPI. (Que era la dirección IP Interna del Firewall original).
- Cambio de la interfaz interna del firewall por una dirección cualquiera del segmento interno de INDECOPI.
- Configuración de una ruta por defecto en el switch de core, a la nueva dirección del firewall
- Cambio de la ruta por defecto en el router de provincias, para que apuntase al switch de core
- Adición de todas las rutas de provincias en el switch de core, para que se enrutaran de retorno vía el router de provincias.

2. Instalación de los nuevos equipos de distribución y acceso en los edificios de INDECOPI.- Constó de lo siguiente:

- Interconexión del switch de Core con el nuevo switch de distribución en el edificio correspondiente.
- Identificación de puntos de red en el edificio correspondiente.
- Programación del corte de servicio en dicho edificio. Migración de puntos de red, de la red original a la nueva red.
- Etiquetado y documentación.

3. Cambio del esquema de trabajo de direcciones IP en la red de INDECOPI.- Los usuarios internos de INDECOPI trabajaban con direcciones fijas. Ello era perjudicial para

las labores de migración. Antes de iniciar cualquier labor, INDECOPI efectuó los siguientes cambios:

- Configuración de un servidor DHCP temporal en INDECOPI
- Cambio mediante política global de grupo en los computadores de INDECOPI, de las direcciones fijas a direcciones DHCP. La política de grupo se configuró de manera tal que el equipo buscara una nueva dirección IP cada 30 segundos, de modo tal que si no tuviera una, recuperase una dirección en un tiempo no mayor a 30 segundos.
- Reinicio de los computadores de INDECOPI, mediante política global de grupo.

4. Configuración de la nueva VLAN.- Para que una VLAN determinada entrara en servicio, se identificaba los grupos usuarios que se verían afectados con los cambios, para programar sus horas de corte de servicio. Los siguientes pasos son disruptivos:

- Configuración de un servidor DHCP temporal en el switch de core, con las direcciones IP preparadas para la nueva VLAN. Este servidor brindaba servicio solamente a la VLAN en cuestión, y bloqueaba los requerimientos del servidor DHCP temporal previamente configurado, y estaba configurado para que los requerimientos de dirección IP se efectuaran una vez al día.
- Configuración de VLANs en el switch de core y en los switches de acceso y distribución.
- Configuración de la puerta de enlace por defecto en la nueva VLAN creada, en el switch de core.

Dado que los usuarios ya se encontraban conectados a los nuevos equipos, después de 30 segundos recibían un nuevo direccionamiento IP correspondiente a la nueva VLAN donde habían sido instalados. Esta dirección IP no solicitaba cambios cada 30 segundos, la estrategia se planteó para minimizar el tiempo fuera de línea de los equipos.

b. Equipos de seguridad informática

La migración de los equipos de seguridad informática constó de lo siguiente:

b.1 Configuración inicial

Se realizó lo siguiente:

- Instalación de la última versión de firmware el firewall e IPS
- Configuración del hostname, y las direcciones IP de gestión iniciales.
- Actualización de firmas en el IPS

b.2 Tercera configuración del switch de Core

Los siguientes pasos definen la migración de toda la red al nuevo esquema de trabajo de INDECOPI:

1. Configuración de la troncal de interconexión del Firewall y el Switch de Core.- Esta troncal tiene por objetivo enrutar todos los paquetes de la red interna de INDECOPI hacia las redes de servidores. También contiene la información correspondiente a la red de

Servidores Internos:

- Configuración del enlace troncal entre el firewall y el switch de core.
- Para garantizar el enrutamiento de los servidores al firewall, la puerta de enlace de los servidores se configuró en el firewall. Todas las redes internas contaban ya con una puerta de enlace por defecto en el switch de core.
- Instalación de políticas de seguridad iniciales en el Firewall de INDECOPI:
  - Políticas para el segmento INTERNO
  - Políticas para el segmento SERVIDORES INTERNOS
  - Políticas para el segmento SERVIDORES DMZ
  - Políticas de acceso a INTERNET

2. Migración final de la red.- Los siguientes pasos son disruptivos e implican cortes de servicio en toda la red de INDECOPI:

- Deshabilitación de los servicios DHCP en el switch de core.
- Reconfiguración del servidor DHCP de INDECOPI, para que entregue direcciones IP a cada uno de los nuevos segmentos. Para que esto trabaje, se precisaron configuraciones especiales en el firewall y en el switch de core, de modo tal que los broadcasts generados por el servidor DHCP puedan atravesar los dispositivos de enrutamiento, para poder recibir las súplicas de los clientes, y ellos puedan recibir una dirección IP.
- Deshabilitación de las rutas hacia la red original de INDECOPI.
- Desconexión física de los enlaces hacia la red de servidores.
- Reconfiguración del switch de core, para que tuviera como puerta por defecto, al firewall.
- Adición en el nuevo firewall de las rutas correspondientes.
- Configuración de una VLAN para la interconexión del router de Provincias, y su adición al nuevo esquema de red.
- Conexión física del Firewall en las interfaces configuradas en el switch de core: Troncal para servicios internos, conexión para el segmento DMZ, y conexión con el router de Internet para el acceso a las redes externas.
- Pruebas de conectividad. Afinamiento de políticas de seguridad.
- Monitoreo de la red.

3. Instalación de la VPN SSL en el Firewall.-

   Fueran las siguientes:

- Instalación de un certificado Web SSL en el firewall de INDECOPI
- Configuración del segmento privado VPN:
  - Definición de la red VPN SSL.
  - Configuración del enrutamiento en el firewall y en el switch de core.

- Configuración de políticas de acceso en el firewall.
- Configuración de la autenticación de usuarios.

- Pruebas de conectividad. Afinamiento de políticas de seguridad.

4. Inclusión del equipo Cisco IPS en línea.- Este equipo se conectó al final, debido a que su configuración es delicada y constantemente iterativa. Una mala configuración de este equipo puede generar problemas de conexión a nivel de aplicaciones, de modo tal que se instaló al final, y se fue adecuando a la nueva red gradualmente.

- Configuración de los pares de las interfaces del equipo IPS:
  - Par 1: Troncal de interconexión para los servicios internos.
  - Par 2: Enlace de interconexión DMZ.
- Configuración inicial fuera de línea del equipo.
- Instalación física del equipo en modo INLINE – MONITOR ONLY.- En este modo, el equipo se coloca en línea con el tráfico de producción, pero no toma acciones, solamente envía alertas.
- Afinamiento de las políticas de seguridad en función a las alertas emitidas por el equipo.
- Activación del modo INLINE.
- Monitoreo y afinamiento de las políticas de seguridad.

3.5.2 Plan de pruebas de desempeño y continuidad operativa

La Tabla 3.5 resume las pruebas que debían realizarse para verificar que la solución implementada en INDECOPI cumpliera con los aspectos relacionados al desempeño de la red y la continuidad que debía poseer. Los resultados son descritos en la sección 4.1.2.

Tabla 3.5 Plan de Pruebas (Fuente: Elab. Propia)

Prueba	Resultado esperado
Switch de Core	
Pruebas eléctricas	
Desconexión física de un cable de poder	El servicio debe continuar a través de la fuente redundante aún en línea.
Deshabilitación de uno de los dos power distribution units (PDU) del rack de comunicaciones	El servicio debe continuar a través del otro PDU del rack
Apagado ordenado de las cuchillas de alimentación del Datacenter	Bajada una de las cuchillas, el switch de Core debe mantenerse encendidos a través de la otra línea de alimentación del Datacenter.
Redundancias	
Desconexión de un cable de un enlace agregado determinado	El otro par del enlace agregado debe mantener el servicio
Desactivación de una de las dos controladoras del switch	La supervisora restante debe recuperar el servicio en la red. La gestión del switch debe recuperarse después de un par de minutos.

Reactivación de la controladora previamente desactivada	La supervisora reconectada debe recuperar la gestión del servicio
Enrutamiento	
Envío de paquetes ICMP (ver nota al final de la tabla) desde una red particular hacia las otras redes	El switch debe enrutar los paquetes hacia el destino esperado, de acuerdo a lo indicado a la tabla de enrutamiento configurada.
Configuraciones adicionales	
El servidor DHCP debe brindar una dirección IP a un usuario en una VLAN específica	El usuario debe recibir correctamente la dirección IP en el rango de red que le corresponde según la VLAN en la que se encuentre.
Los usuarios no pueden tener conexión con la VLAN de administración de equipos, exceptuando a los admisnistradores	Los intentos de conexión desde una VLAN de usuario hacia las direcciones IP de las VLAN de administración, fallan. Los administradores tienen conexión exitosa a dicha VLAN.
Switches de distribución y acceso	
Los equipos de distribución identifica al switch de Core y a los switches de acceso que tiene conectados, en los puertos específicos de cada switch.	La identificación adecuada coincide con los mapas de diseño previamente documentados.
El usuario conectado al switch de acceso en una VLAN determinada, debe recibir una dirección IP en el segmento correspondiente a dicha VLAN	El usuario recibe una dirección IP consistente con la VLAN en dicho segmento.
Firewall	
Enrutamiento	
Envío de paquetes ICMP a través del Firewall	El enrutamiento de los paquetes desde una red particular hacia otra debe estar según lo diseñado.
Network Address Translation (NAT)	
Las redes internas deben esconderse detrás de una dirección pública configurada en el firewall	Mediante el uso de herramientas de verificación de IP pública (como www.direccionip.com), se verifica en el computador de la red interna cualquiera la dirección IP que utiliza el equipo.
Redirección de puertos desde Internet hacia los servidores DMZ, en los puertos de servicios solamente	Se verifica operatividad de los servicios desde Internet. Acceso a portales y sistemas de consulta.
Políticas de acceso a red	
Acceso a Internet de los servidores para los servicios permitidos para ellos.	Los servidores muestran en sus sistemas operativos y en sus aplicaciones, condiciones exitosas de actualizaciones de seguridad. Otros servicios de red no son accesibles.
Acceso a Internet de los usuarios de la red en los servicios permitidos para ellos.	Los usuarios cuentan con navegación web, sistemas de correo y servicios de consulta a instituciones externas. Otros servicios de red no son accesibles.
Acceso de los usuarios a los servidores	Las aplicaciones de los usuarios funcionan. Acceso a otros servicios en los servidores no se encuentran disponibles.

Acceso de los servidores DMZ a los servidores de la red interna	Las aplicaciones funcionan tanto desde la red interna, como desde Internet, incluyendo los servicios de consultas de formularios. (Bases de datos). Otros servicios no se encuentran disponibles.
VPN SSL	
Autenticación de usuario	El usuario ingresa desde Internet al portal VPN SSL, utilizando un navegador web. El sistema exige autenticación. Si la autenticación falla, el usuario no accede a la VPN.
Parámetros de conexión concedidos al usuario	Si el usuario tiene una autenticación exitosa, recibe una dirección IP correspondiente a su grupo de configuración.
Políticas de acceso para cada grupo de autenticación	El usuario recibe distintos niveles de acceso a la red, dependiendo del perfil de usuario que posea. Así, un administrador tiene acceso a toda la red, mientras que un usuario de aplicaciones solamente puede entrar a las aplicaciones que tiene permitidas.
Acceso a Internet de usuarios remotos	Los usuarios remotos deben tener las mismas restricciones de acceso a Internet que los usuarios internos de INDECOPI, al estar conectados a la VPN.
	IPS
Pruebas asociadas al sistema	
Actualización de firmas	El sistema debe mostrar la última versión del firmware, asociado a la fecha en la que fue descargado.
El sistema se configura como modo Inline. Se desactiva vía software la máquina de inspección.	El tráfico de red no debe detenerse. Los usuarios continúan accediendo a red
El sistema se configura como modo Inline. Se activa vía software la máquina de inspección.	El tráfico de red no debe detenerse. El sistema IPS debe indicar que la inspección está activada.
Políticas de seguridad	
El sistema debe emitir alertas ante determinados umbrales configurados en el equipo: Tráfico de red, consumo de la máquina de inspección, interfaces.	Se configura el IPS en un umbral muy bajo, de modo que sea sencillo rebasar dicho umbral. El equipo envía alertas a los administradores vía email.
El sistema debe estimar la criticidad de una amenaza detectada	Se hace una inyección de código diseñado para lanzar alertas de seguridad en los equipos IPS. Se muestra una alerta indicando la criticidad de la acción. (Leve, Moderada, Alta)
El sistema debe bloquear un ataque determinado e informar al respecto	Se hace una inyección de código diseñado para lanzar alertas de seguridad en los equipos IPS. La alerta debe especificar que el ataque fue bloqueado. En el equipo desde donde se lanzó la prueba, debe evidenciarse la falla de conexión mediante

	un aviso de la aplicación.
El sistema debe bloquear las conexiones que rebasen determinado umbral.	Se configura al sistema para que bloquee el paso de un determinado protocolo de red que se emita desde el mismo host un número de veces en un período de tiempo definido. El sistema IPS detecta el comportamiento y bloquea el paso del protocolo desde el equipo origen. Una alerta informa la acción tomada.

Nota: ICMP (Internet Control Message Protocol- Protocolo de Mensajes de Control de Internet) [41] es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Es utilizado para el envío de mensajes de error, por ejemplo para indicar que un determinado servicio no está disponible o de la imposibilidad de localización de un dispositivo de la red (router o host). ICMP es definido por el IETF RFC792 [42] y 950 [43];

CAPÍTULO IV
PRUEBAS, CRONOGRAMA Y COSTOS

En el presente capítulo se explican las pruebas realizadas (en el Data Center y en los equipos de comunicaciones y seguridad) además de los resultados obtenidos. Posteriormente se desarrolla lo referente al presupuesto y al cronograma del proyecto de ingeniería.

4.1 Pruebas realizadas

Para la explicación de esta sección se hará uso de las Tablas 2.5 y 3.5 (subsecciones 4.1.1 y 4.1.2 respectivamente) de los capítulos anteriores. Las pruebas se agrupan en pruebas en el Data Center, y pruebas en los equipos de comunicaciones y de seguridad.

4.1.1 Pruebas en el Data Center

Estas pruebas se organizan de la siguiente manera:

- Pruebas eléctricas en los equipos
- Sistema de almacenamiento
- Switches SAN
- Plataforma VMware (para ello se preparó una máquina virtual de pruebas)

a. Pruebas eléctricas en los equipos

Se explican a continuación:

- Desconexión física de un cable de poder de un equipo aleatorio.- El objetivo de la prueba fue verificar que dicho equipo se mantiene encendido a través de la fuente redundante que posee. De no ser así, se descartan problemas eléctricos en las fuentes o en el equipo. La prueba se repitió con todos los equipos. La prueba se diói por aprobada al verificarse el objetivo con todas las fuentes de todos los equipos.
- Deshabilitación de uno de los dos power distribution units (PDU) del rack de servidores.- El objetivo de la prueba fue verificar que el servicio eléctrico es redundante en el rack de servidores. Al deshabilitar uno de los dos PDU del rack, esto es, al deshabilitar uno de los dos tomacorrientes del rack, el servicio continuaba mediante el PDU restante en el rack. La prueba se dio por aprobada ya que todos los equipos permanecieron operativos al desactivar un PDU y quedarse activo el otro. La prueba se repitió con ambos PDU.
- Bajado ordenado de las cuchillas de alimentación del Datacenter.- Debido a que el centro de datos de INDECOPI cuenta con 2 líneas de energía independientes, el objetivo de la prueba fue demostrar que se mantenía la continuidad operativa con una de las dos

líneas activas. La prueba se dio por aprobada al verificarse que todos los equipos permanecían operativos al desactivar una línea y dejar activa la otra. La prueba se repitió con ambas líneas.

b. Sistema de almacenamiento

Se explican a continuación:

- Desconexión física de los cables de FO en uno de los dos procesadores componentes del sistema de almacenamiento.- Los procesadores del sistema de almacenamiento mantienen configuraciones redundantes y espejadas, de modo tal que ante cualquier falla de un componente cualquiera en uno de los procesadores (por ejemplo, interfaces de conexión, memorias, CPU u otros), el otro debe tomar la carga correspondiente al miembro averiado. Al desconectarse los cables de fibra óptica en uno de los procesadores, los volúmenes (LUN) que se sirven a través de dichos puertos, pasaron a ser servidos desde los puertos del procesador de almacenamiento sobreviviente. La prueba se dio por aprobada al verificarse que todas las LUN se seguían sirviendo desde el procesador de almacenamiento sobreviviente. La prueba se repitió para cada procesador de almacenamiento.

- Reinicio ordenado de los procesadores componentes del sistema de almacenamiento.- Debido a que el reinicio constituye un evento de avería de uno de los procesadores de almacenamiento, se espera que el servicio se mantenga vía el procesador de almacenamiento sobreviviente. Asimismo, al reiniciar el otro procesador, la carga debe balancearse. La prueba se dio por aprobada al verificarse que todas las LUN se seguían sirviendo desde el procesador de almacenamiento sobreviviente, y se volvían a balanceaban cuando el procesador reiniciado regresaba a operación. La prueba fue repetida para cada procesador de almacenamiento.

- Retiro en caliente de un disco de un determinado grupo de arreglo (RAID group).- Para verificar la funcionalidad de los discos de espera en caliente, o discos que entran a operación ante la falla de un disco de tecnología similar, se escoge un arreglo físico de discos configurado en el equipo, y se retira un disco cualquiera. Además que no debe percibirse pérdida de datos, se debe apreciar que el disco retirado es reemplazado por uno de los discos en espera en caliente, y el arreglo debe reconstruir su integridad una vez que el disco en espera entra en operación. La prueba se dio por aprobada al apreciarse que el disco de espera en caliente tomaba la carga al retirarse un disco de un arreglo, y que la data se mantenía operativa, además de que al colocar el disco retirado, la data era copiada al disco inicialmente retirado, y el disco de espera en caliente volvía a su estado de espera. La prueba fue repetida para cada disco de almacenamiento del arreglo de discos RAID.

c. Switches SAN

Se explican a continuación:

- Desconexión física de los cables de FO en el puerto que conecta el switch con el storage.- Al representar una avería en el camino de acceso a los procesadores de almacenamiento del storage, se debe verificar que se mantiene el acceso a los volúmenes (LUN) por el camino sobreviviente. La prueba se dio por aprobada al permanecer el acceso a los volúmenes luego de desconectadas las conexiones de un switch al storage. La prueba fue repetida para cada switch.

- Reinicio o apagado de uno de los switches.- La intención de esta prueba fue la de verificar que, mientras uno de los switches estaba inoperativo, permanecía el acceso a los volúmenes desde el switch sobreviviente. Asimismo, la carga debía rebalancearse en el sistema de almacenamiento cuando el switch averiado regresaba a su condición de operativo. La prueba se dio por aprobada al verificarse que permanecía el acceso a las LUN en el storage al apagarse un switch, y también cuando se apreciaba que la carga se rebalanceaba al regresar el switch a operaciones. La prueba fue efectuada para cada switch.

d. Plataforma VMware

Para efectuar las pruebas con VMware, es necesario contar con una máquina virtual de pruebas, que se mantenga encendida. Estas pruebas se subdividen en pruebas de alta disponibilidad y pruebas de servicios VMware.

d.1 Pruebas de alta disponibilidad

Se explican a continuación:

- Se coloca la máquina virtual sobre una de las 4 cuchillas HS21 instalado con VMware ESX y a continuación se procede a reiniciar el equipo físico donde se encuentra alojada la máquina virtual.- VMware cuenta con la funcionalidad de Alta Disponibilidad (High Availabilty o HA), que permite que las máquinas virtuales que estaban cargadas en la memoria de un servidor físico, puedan ser reiniciadas en otro equipo sobreviviente de la arquitectura. El reinicio del servidor donde se encuentra la máquina virtual representa un escenario de avería, y se espera que la máquina virtual reinicie por si sola en otro equipo miembro de la solución. La prueba se dio por aprobada al verificarse que la máquina virtual se reiniciaba en otro host una vez que un equipo fallaba. La prueba fue repetida con las 4 cuchillas físicas.

- Se coloca la máquina virtual sobre una de las 4 cuchillas HS21 y a continuación se ejecuta la funcionalidad de Vmotion para mover la máquina virtual a otra cuchilla HS21 distinta a la origen.- VMware Vmotion es una funcionalidad del producto, que permite a una máquina virtual, ser movida desde un equipo físico a otro, de modo tal que pueda

liberarse el equipo origen para labores de mantenimiento, actualización o reemplazo. Una vez que se terminan las labores de servicio en el equipo origen, es posible regresar la máquina virtual previamente desplazada utilizando Vmotion. Vmotion permite que el servicio de la máquina virtual se mantenga ininterrumpido mientras se efectúa el movimiento. La prueba se dio por aprobada al verificarse que la máquina virtual se desplazaba, sin perder conectividad, hacia otro equipo de la plataforma. Al finalizar el desplazamiento, aparecía el estado de "Success" en la consola. La prueba fue realizada con las 4 cuchillas físicas.

- Se aloja la máquina virtual en uno de los volúmenes del cluster VMware (Datastore) y a continuación se ejecuta la funcionalidad de Storage Vmotion y se mueve la máquina virtual a otro volumen (datastore) del cluster vmware.- Mware Storage Vmotion permite mover los datos entre un volumen de almacenamiento de VMware (DataStore) a otro, sin que genere interrupción del servicio en la máquina virtual que es movida. Esto es útil para migraciones de datos, reemplazo de sistemas de almacenamiento y balanceo de carga.

La prueba se dio por aprobada al verificarse que la máquina virtual se desplazaba, sin perder conectividad, hacia otro volumen (DataStore) de la plataforma. Al finalizar el desplazamiento, aparecía el estado de "Success" en la consola. La prueba fue realizada con los DataStores seleccionados por INDECOPI.

d.2 Pruebas de servicios VMware

Se explican a continuación:

- Se toma la máquina virtual y se ejecuta la funcionalidad de clonación.- La funcionalidad de clonación permite contar con una copia de una máquina virtual, que puede ser utilizada para desplegar un nuevo servicio rápidamente. El administrador debe poder hacer cambios en la configuración del hardware virtual de la nueva máquina, brindando flexibilidad en la administración de la plataforma virtual. La prueba se da por aprobada al encender la nueva máquina virtual, con los nuevos parámetros de hardware virtual aplicados por el ejecutor de la prueba.

- Se toma la máquina virtual y se ejecuta la funcionalidad de snap.- Un Snap es una instantánea en el tiempo del estado de una máquina virtual. Esta instantánea graba el estado de la máquina virtual en el momento de la toma del snap, y lo almacena en disco. Esta instantánea permite efectuar pruebas sobre una máquina virtual, como la ejecución o instalación de nuevos programas. Si por alguna razón la máquina virtual se corrompe a raíz de los cambios efectuados en ella, el snap le permite regresar al estado previo a la ejecución de los cambios, ahorrando tremendamente el tiempo de reaprovisionamiento de la máquina virtual. La prueba se dio por aprobada al verificarse la creación del snap de manera exitosa.

- Una vez tomado el snap, se ejecuta pruebas intrusivas en la máquina virtual (borrado de archivos aleatorios en la carpeta C:Windows).- Esta prueba pretende poner a prueba la efectividad del snap, y consiste en la corrupción de la máquina virtual tras haber tomado el snap. Tras el reinicio la máquina virtual debe quedar inutilizable, esto es necesario para verificar la recuperación (ver siguiente párrafo).
- Se revisa el inventario de snaps de la máquina virtual y se abre el último snap tomado.- El objetivo de esta prueba es buscar el snap tomado previamente a la corrupción de la máquina virtual, y restaurar el estado anterior a la acción destructiva. La prueba se dio por aprobada al verificarse que la máquina virtual aparece operativa en el estado previo a la acción destructiva.

4.1.3 Pruebas en los equipos de comunicaciones y de seguridad

Estas pruebas se organizan de la siguiente manera:

- Switch de Core
- Switches de distribución y acceso
- Firewall
- IPS

a. Switch de Core

Estas a su vez se subdividen en pruebas eléctricas, redundancias, enrutamiento, configuraciones adicionales

a.1 Pruebas eléctricas

Se explican a continuación:

- Desconexión física de un cable de poder.- De manera similar a los servidores y almacenamiento, al retirar un cable de poder, el servicio debía mantenerse a través de la fuente redundante. La prueba se dio por aprobada al permanecer el servicio con una sola fuente. La prueba fue realizada con cada una de las fuentes.
- Deshabilitación de uno de los dos power distribution units (PDU) del rack de comunicaciones.- El objetivo de la prueba fue verificar que el servicio eléctrico es redundante en el rack de comunicaciones. Al deshabilitar uno de los dos PDU del rack, esto es, al deshabilitar uno de los dos tomacorrientes del rack, el servicio debía mantenerse mediante el PDU restante en el rack. La prueba se dio por aprobada al comprobarse que el switch de Core permanecía operativo al desactivarse un PDU y dejar activo el otro. La prueba fue realizada con ambos PDU.
- Bajado ordenado de las cuchillas de alimentación del Datacenter.- Debido a que el centro de datos de INDECOPI cuenta con 2 líneas de energía independientes, el objetivo de la prueba fue demostrar que se mantenía la continuidad operativa con una de las dos líneas activas. La prueba se dio por aprobada al verificarse que el switch de Core

permanecía operativo al desactivarse una línea y dejarse activa la otra. La prueba fue realizada con ambas líneas.

a.2 Redundancias

Se explican a continuación:

- Desconexión de un cable de un enlace agregado determinado.- Los enlaces agregados son asociaciones de dos o más puertos que trabajan como uno solo, para brindar mayor capacidad de acceso de datos, y redundancia. Si uno falla, el servicio debe mantenerse por el miembro sobreviviente. La prueba se dio por aprobada al comprobarse que el servicio permanecía al retirarse uno de los dos miembros de un enlace agregado cualquiera. La prueba fue realizada para cada par del enlace agregado, y para todos los enlaces agregados.
- Desactivación de una de las dos controladoras del switch.- Las controladoras de gestión del Swtich de Core se denominan Supervisoras. Su función es la de mantener la operación general del equipo, así como también cumplir todas las tareas de gestión. Si una de ellas cae y se cuenta con una supervisora auxiliar, esta debe iniciar operaciones ante la caída de la supervisora averiada. Por tanto, los servicios de Core deben estar disponibles una vez que la supervisora de respaldo haya iniciado operaciones. La prueba se dio por aprobada al verificarse que, ante una avería programada de la supervisora principal, se recuperaban las operaciones y el control del switch de core mediante la supervisora de respaldo. La prueba fue repetda para cada supervisora.
- Reactivación de la controladora previamente desactivada.- Cuando la supervisora averiada es regresada a operaciones, debe tomar la responsabilidad de las operaciones del equipo. Este requisito garantiza que la supervisora de respaldo regrese a su estado de espera, y pueda reaccionar ante cualquier falla. La prueba se dio por aprobada al verificarse que la supervisora principal recuperaba el control del switch una vez que reiniciaba.

a.3 Enrutamiento

Se explican a continuación:

- Envío de paquetes ICMP desde una red particular hacia las otras redes.- Debido a que el switch de core cuenta con capacidades de capa 3, permite el enrutamiento de paquetes IP. El envío de paquetes ICMP permite determinar la ruta que toma un determinado paquete IP en su recorrido por la red, de modo que se puede evaluar si los recorridos del paquete son según se esperan. La prueba consiste en el envío de paquetes ICMP por la red, de modo que pueda apreciarse que sigan el camino impuesto por las rutas configuradas en el switch de Core. La prueba se dio por aprobada al verificarse la integridad de la tabla de enrutamiento del switch de Core.

a.4 Configuraciones adicionales

Se explican a continuación:

- El servidor DHCP debe brindar una dirección IP a un usuario en una VLAN específica El protocolo DHCP está basado en el envío de paquetes IP a direcciones de Broadcasts determinadas. Por concepto, estos paquetes no son enrutados en los dispositivos de enrutamiento, llámese routers o switches capa 3. Para que ellos puedan enrutarse y alcanzar a un usuario en una VLAN determinada, es necesario configurar los equipos de enrutamiento, de modo tal que permitan el paso solamente de determinados paquetes de broadcast, como los que caracterizan al protocolo DHCP. La prueba se dio por aprobada al verificarse que un un usuario en una VLAN determinada recibía la dirección IP planificada en el diseño de la solución. La prueba fue realizada para todas las VLAN de usuarios.

- Los usuarios no pueden tener conexión con la VLAN de administración de equipos, exceptuando a los administradores.- Debido a que los equipos de operaciones de INDECOPI (sean servidores o equipos de comunicaciones), son críticos para la institución, no se permite que los usuarios comunes puedan alcanzar la red donde se encuentran las direcciones IP de administración de los equipos. Solamente los administradores de red pueden alcanzar esta red. Para ello, se configuraron listas de bloqueo en el switch de Core. La prueba se dio por aprobada al verificarse que no hay acceso desde una VLAN de usuario a la VLAN de administración. La prueba fue repetida desde todas las VLAN de usuario. Asimismo, para complementar la prueba, se verificó la validación del acceso desde la VLAN donde residen los administradores de la red.

b. Switches de distribución y acceso

Se explican a continuación:

- Los equipos de distribución identifican al switch de Core y a los switches de acceso que tiene conectados, en los puertos específicos de cada switch.- Este descubrimiento permite validar que el mapa de distribución de los equipos, es acorde al diseño de la red, y a lo indicado en el plan de documentación de la red. La prueba se dio por aprobada al visualizarse, desde un switch de distribución, la información de los puertos del switch de Core a los que se encuentra conectado, así como también la identificación de todos los switches de acceso a los que se encuentre conectado. La prueba debe se repitió para todos los switches de distribución.

- El usuario conectado al switch de acceso en una VLAN determinada, debe recibir una dirección IP en el segmento correspondiente a dicha VLAN.- Esta prueba complementa a la prueba efectuada en el switch de Core, permite verificar que el plan de conectividad entre el switch de Core y los switches de distribución y acceso, es según diseño. La

prueba se dio por aprobada al verificarse que el usuario recibía una dirección IP consistente con la VLAN en dicho segmento. Esta prueba se repetida con otros usuarios.

c. Firewall

Las pruebas en el Firewall, se subdividen en enrutamiento, NAT, políticas de acceso a red y VPN SSL.

c.1 Enrutamiento

Consiste en el envío de paquetes ICMP a través del Firewall. Nuevamente, el objetivo es evaluar si la tabla de enrutamiento del Firewall es consistente con lo diseñado. La prueba se dio por aprobada al verificarse la integridad de todas las rutas del Firewall.

c.2 Network Address Translation (NAT)

Se explican a continuación:

- Las redes internas deben esconderse detrás de una dirección pública configurada en el firewall.- Esto es necesario para que las direcciones internas de INDECOPI, puedan acceder a Internet, ocultas detrás de una dirección IP pública enrutable en Internet. La prueba se da por aprobada cuando se comprueba que un equipo interno puede acceder a Internet, y se verifica, mediante el uso de herramientas en línea, que la dirección IP pública que utiliza para el acceso, es la configurada en el firewall.

- Redirección de puertos desde Internet hacia los servidores DMZ, en los puertos de servicios solamente.- La redirección de puertos permite que el puerto de una dirección pública se cambie (traduzca) al mismo puerto de una dirección IP privada. Esto permite que los servicios que residen en un servidor con una dirección IP privada, puedan ser publicados a Internet para el servicio al público en general. La prueba se dio por aprobada al comprobarse que se obtiene acceso a los servicios públicos de INDECOPI desde Internet.

c.3 Políticas de acceso a red

Se explican a continuación:

- Acceso a Internet de los servidores para los servicios permitidos para ellos..- La política de acceso a Internet de los servidores debe ser tal, que permita que sus sistemas operativos y aplicaciones se mantengan actualizados. La prueba se da por aprobada si los servidores tienen la capacidad de descargar sus actualizaciones desde Internet, y otros servicios no son accesibles.

- Acceso a Internet de los usuarios de la red en los servicios permitidos para ellos.- De manera similar, los usuarios deben contar solamente con determinados servicios de acceso a Internet, como navegación, correo electrónico y consultas a determinadas instituciones, otros servicios no deben permitirse. La prueba se dio por aprobada al verificarse el cumplimiento de la política previamente descrita en los usuarios internos de

la red.

- Acceso de los usuarios a los servidores.- Los usuarios contaban con acceso a determinados servicios en los servidores, pero no a otros servicios no autorizados que pudiesen estar habilitados en dichos equipos. La prueba se dio por aprobada al comprobarse que los usuarios podían acceder solamente a las aplicaciones que residen en los servidores.
- Acceso de los servidores DMZ a los servidores de la red interna.- Debido a que los servidores DMZ necesitaban determinados accesos a los servidores de bases de datos de la red de servidores internos, se debieron habilitar los accesos en el firewall de manera exclusiva para dichos propósitos. La prueba se dio por aprobada al verificarse que los servicios de aplicaciones asociados a bases de datos funcionaban tanto desde la red interna como desde Internet.

c.4 VPN SSL

Se explican a continuación:

- Autenticación de usuario.- Debido a que el acceso a los recursos internos de INDECOPI debe ser autenticado, se le entrega a cada usuario una determinada credencial de acceso. Ante un evento de autenticación fallida, el usuario no gana acceso a la VPN. La prueba se dio por aprobada al comprobarse que el usuario consigue acceso a la VPN solamente si sus credenciales son correctas.
- Parámetros de conexión concedidos al usuario.- Ya que es posible contar con varios grupos de usuarios, cada uno de ellos con distintos privilegios de acceso, la prueba está orientada a verificar que la configuración de la política para cada grupo de usuarios es correcta. La prueba se dio por aprobada al verificar que un usuario de un grupo determinado recibe los privilegios de acceso y direcciones IP distintivas de su grupo. La prueba se repitió para todos los grupos de usuarios configurados.
- Políticas de acceso para cada grupo de autenticación.- Debe verificarse la diversidad de accesos a los sistemas internos que cada grupo posee, de modo tal que un usuario en un grupo podría no poder acceder a un recurso determinado, a menos que cuente con otra cuenta de usuario de mayores privilegios. La prueba se dio por aprobada cuando se verifica la validación de la integridad de acceso de cada política de seguridad configurada.
- Acceso a Internet de usuarios remotos.- Los usuarios VPN SSL deben ser tratados como usuarios internos, y como tales, deben tener controles de acceso a Internet según las políticas de INDECOPI. Para ello, se configura el equipo para que el usuario VPN SSL remoto no use los servicios de Internet de su red local, sino que su tráfico de Internet se redirija a la central antes de ir a Internet, de modo que pueda ser controlado. La prueba

se dio por aprobada al verificarse que cualquier usuario VPN SSL accede a Internet bajo las restricciones de las políticas de su grupo.

d. IPS

Finalmente, las pruebas para el IPS se subdividen en pruebas asociadas al sistema, y pruebas para la evaluación de las políticas de seguridad.

d.1 Pruebas asociadas al sistema

Se explican a continuación:

- Actualización de firmas.- Si el sistema se encuentra configurado adecuadamente, debe tener acceso a Internet y mantenerse al día con la última versión de las firmas de seguridad, las que se actualizan periódicamente. La prueba se dio por aprobada al verificarse que se cumplía la condición descrita previamente.

- El sistema se configura como modo Inline. Se desactiva vía software la máquina de inspección.- Al efectuar esta acción, se espera que el tráfico de red no se vea interrumpido. Cualquier otro resultado debe ser inmediatamente revisado. La prueba se dio por aprobada al comprobarse que el tráfico de red permanecía, pese a desactivarse la máquina de inspección.

- El sistema se configura como modo Inline, se activa vía software la máquina de inspección.- Tras haber desactivado la máquina de inspección, al reactivarla, se debe mantener el tráfico, al mismo tiempo que todas las inspecciones de seguridad configuradas se activan. La prueba se dio por aprobada al verificarse el cumplimiento de la condición descrita previamente.

d.2 Políticas de seguridad

Se explican a continuación:

- El sistema debe emitir alertas ante determinados umbrales configurados en el equipo: Tráfico de red, consumo de la máquina de inspección, interfaces.- Para poder evaluar al equipo, se disminuyen intencionalmente los umbrales de detección, de modo tal que con una menor cantidad de tráfico pueda verse la activación de las alertas de seguridad del sistema. La prueba se dio por aprobada al comprobarse la alerta y la criticidad para cada grupo de políticas de seguridad a evaluar.

- El sistema debe estimar la criticidad de una amenaza detectada.- Una alerta debe informar al administrador si es informativa, intermedia o crítica, y las acciones y recomendaciones respecto a la misma. La prueba se dio por aprobada cuando se pudo verificar la criticidad de ataques previamente preparados.

- El sistema debe bloquear un ataque determinado e informar al respecto.- Para poder determinar la eficacia del producto, se lanzan ataques que son conocidos como potenciales amenazas, pero de manera controlada. El equipo debe reaccionar tomando

acciones de bloqueo. Asimismo, el equipo desde donde se lanza el ataque, debe evidenciar problemas de conexión. La prueba se dio por aprobada al verificarse que se cumplía la condición descrita previamente.

- El sistema debe bloquear las conexiones que rebasen determinado umbral.- Esta prueba permite demostrar la efectividad del IPS para la detección y bloqueo de eventos anómalos, como el incremento del consumo de los recursos de la red. Para ello, se utiliza un equipo de pruebas desde donde se busca saturar el tráfico de red con un determinado protocolo. El IPS debe notar el protocolo que satura la red, el equipo que lo genera, y tomar la acción configurada (alerta y bloqueo). La prueba se dio por aprobada al verificarse que se cumplía la condición descrita previamente.

4.2 Estimación de costos

A continuación se muestra (Tabla 4.1) los "Topes mínimos y máximos al valor referencial por ítem" de la licitación. Solo se está considerando los ítems en los que COSAPI DATA obtiene la buena pro (ítem 1 e ítem 3 de la licitación pública).

Nota: El IGV era 19 % en la fecha en que el proyecto fue ejecutado.

Tabla 4.1 Topes mínimos y máximos al valor referencial por ítem (Fuente: Ref. [3])

Item	Denominación	Monto en soles (s/.)		
		Valor	110%	70%
1	Servidores y almacenamiento	808 118.18 (Ochocientos ocho mil ciento dieciocho con 18/100 Nuevos Soles)	888 929.99	565 682.73
			Ochocientos ochenta y ocho mil novecientos veinte y nueve con 99/100 Nuevos Soles	Quinientos sesenta y cinco mil seiscientos ochenta y dos con 73/100 Nuevos Soles
3	Redes y comunicaciones	757 451.40 (Setecientos cincuenta y siete mil cuatrocientos cincuenta y uno con 40/100 Nuevos Soles)	833 196.54	530 215.98
			Ochocientos treinta y tres mil ciento noventa y seis con 54/100 Nuevos Soles	Quinientos treinta mil doscientos quince con 98/100 Nuevos Soles

De acuerdo al pronunciamiento de la Buena Pro para este proceso, en la Tabla 4.1 se muestran los costos para los ítems 1 y 3 de la Licitación Pública en mención.

Tabla 4.2 Costos Buena pro otorgada a COSAPI DATA (Fuente: Buena Pro)

ítem	Denominación	Monto en soles (s/.) valor
1	Servidores y almacenamiento	779 900.00 (Setecientos Setenta y Nueve mil Novecientos y 00/100 Nuevos Soles)
3	Redes y comunicaciones	642 900.00 (Seiscientos cuarenta y dos mil novecientos y 00/100 Nuevos Soles)

Para la referencia, se adjunta el cuadro de componentes involucrados con los precios de lista (que incluyen IGV), en el momento en el que se desarrolló la licitación.

Para el momento del proceso de las órdenes de compra para este proyecto (Febrero 2008), el tipo de cambio del dólar americano fue de S./ 2.89 [44].

A continuación se muestra los costos referentes al ítem 1 (Tabla 4.3), y los referentes al ítem 3 (Tabla 4.4)

Tabla 4.3 Costos ítem 1 - Servidores y almacenamiento (Fuente: Elab. Propia)

EQUIPAMIENTO			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
86773RU	IBM eServer BladeCenter™ Chassis with 2x2000W PSU	1	93 720.40
32R1860	Nortel Networks Layer 2/3 Copper GbE Switch Module for Bladecenter		
32R1812	Brocade® 20-port 4Gb SAN Switch Module for IBM Bladecenter™		
39M4575	IBM Bladecenter 2000W Power Supplies 3 & 4		
22R4897	4 Gbps SW SFP Transceiver 4 Pack		
43W6555	IBM remote Deployment Manager 4.4. BladeCenter Chasis		
24R9418	RDM for Server 2YR software suscription renewal		
7995C2U	HS21, 2xXeon Quad Core E5345 2.33 Ghz/1333Mhz/8MB x 04	1	49 975.04
39M5791	4GB Kit (2x 2GB DIMM) PC2 5300 DDR2 x 08		
26R0890	Qlogic 4Gb SFF Fibre Channel Expansion Card for IBM Bladecenter x 04		
7978EDU	x3350 Xeon Quad Core E5355 2.66Ghz/1333Mhz/2x4Mb L2, 2x2GB	1	25 547.60
40K1251	x3350 Xeon Quad Core E5355 2.66Ghz/1333Mhz/2x4Mb L2		
39M5791	4GB Kit (2x 2GB DIMM) PC2 5300 DDR2		
39Y6126	Intel PRO 1000 PT Dual port server adapter		
40C2071	Emulex 4GB FC HBA PCI-E Controller Dual Port for IBM System X		
39M5697	5m Fiber Optic cable LC-LC x 04		
39Y8940	DPI 60 amp/250V Front End PDU with IEC 309 2P+ Gnd Connector x 02	1	10 656.64
39Y8951	DPI Universal Rack PDU with Nema L5-20P and L6-20P (US line cord) x 04		
31R3132	3m console switch cable (USB) x 03		

17351LX	IBM 1x8 Console switch x 01		
EX-GAR	EXTENSION DE GARANTIA A 5 AÑOS	6	21 500.37
1814-72A	DS4700 Express Model 74 (4GB Cache)	1	190 038.77
1812-81A	DS4000 EXP810 Expansion Unit Model 81	1	60 411.03
EX-GAR	EXTENSION DE GARANTIA A 5 AÑOS	1	102 814.79
3573-L2U	TS3100 Tape Library Express	1	23 600.09
3589-010	800 GB Ultrium Tape Cartridges Labeled	1	12 300.97
EX-GAR	EXTENSION DE GARANTIA A 5 AÑOS	1	20 733.79
9131-52A	IBM SystemP5 520 Express	1	137 730.06
EX-GAR	EXTENSION DE GARANTIA A 5 AÑOS	1	48 684.78
SOFTWARE DE VIRTUALIZACION			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
VI-AK-C	Vmware Infrastructure Acceleration Kit for 8 Processors	1	100 772.21
VI-AK-G-SSS-C	Gold Support/Suscription Vmware Infrastructura Acceleration Kit for 8 Processors	5	115 554.25
OTROS			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
N/A	Cursos y capacitación	1	5 000.00
N/A		1	10 000.00

Tabla 4.4 Costos ítem 3 - Redes y Comunicaciones (Fuente: Elab. Propia)

EQUIPAMIENTO			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
WS-C3560G-48PS-S	Catalyst 3560 48 10/100/1000 Base T PoE + 04 SPF	3	62 965.01
GLC-SX-MN	GE SFP LC Connector SX Transceiver	3	3 316.28
COV-SMBS-3560G48S	SMBSA 8x5xNext Business Day	3	8 444.86
WS-C3560-48PS-S	Catalyst 3560 48 10?100 PoE + 04 SFP	12	172 313.65
GLC-T	1000 Base-T SFP	12	10 479.43
COV-SMBS-356048PS	SMBSA 8x5xNext Business Day	12	24 771.54
Server (SSL)	Certificado Digital SSL	1	736.95
WS-C6509-E	Catalyst 6500 Enhanced 9 Slots Chassis	1	21 003.08
WS-SUP720	Catalyst 6500/Cisco 7600	1	61 903.80

	Supervisor		
WS-X6748-GE-TX	Cat6500 48 port 10/100/1000 GE	1	33 162.75
WS-X6408A-GBIC	Catalyst 6000 8 Port GE Enhanced	1	22 097.45
WS-G5484	1000 Base-SX Short Wavelength Gbic	5	5 527.13
WS-C6509-E-FAN	Catalyst 6509-E Chassis Fan Tray	1	1 094.37
WS-CAC-6000W	Catalyst 6000W AC Power Supply	1	11 054.25
COV-SNT-WS-C6509	8x5 NBD Service - Catalyst 6509	1	55 283.09
WS-C3560-48PS-S	Catalyst 3560 48 10/100 PoE + 4 SFP	2	28 718.94
GLC-SX-MM	GE SFP, LC Connector SX-Transceiver	2	2 210.85
GLC-T	1000 Base-T SFP	2	1 746.57
COV-SMBS-356048PS	SMBSA 8x5xNext Business Day	2	4 128.59
CW LMS-3.0-100-K9	LMS 3.0 Windows Only 100 Device Restricted	1	22 097.45
ASA5510-SSL50-K9	ASA 5510 VPN Edition N/50 SSL User	1	16 570.32
ASA5510-SEC-PL	ASA 5510 Security Plus License W/HA, GE	1	2 210.85
ASA-ADV-END-SEC	ASA 5500 Advanced Endpoint Assessmnt	1	2 199.80
COV-SNT-ASIBUNK9	Smartnet 8x5x Next Bussiness Day ASA 5510 N/50	1	3 392.92
IPS-4240-K9	IPS4240 Appliance Sensor	1	26 519.15
COV-SUI-IPS4240	IPS SVC AR Next Bussiness Day IPS 4240 Appliance	1	17 490.97
EQUIPAMIENTO PARA CABLEADO			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
8-1664164-S	AMP Cable para Enlace de FO	500	7 762.54
6754399-3	AMP Patch cord de FO	8	996.36
1657014-1	Bandeja deslizable para Rack 1RU	1	294.04
1657229-7	Panel FO para Gabinete IE 06 Acopladores SC	2	47.165
1657229-1	Panel FO ciego para Gabinete	1	23.58
6457567-4	Módulo acoplador LC Duplex FO	12	308.34
1657014-1	Bandeja deslizable para Rack 1RU	4	1 176.17
1657229-7	Panel FO para Gabinete IE 06 Acopladores SC	4	94.33
1657229-1	Panel FO ciego para Gabinete	8	188.66

6457567-4	Módulo acoplador LC Duplex FO	16	411.12
6588706-1	AMP Conector de Fibra Óptica tipo LC	48	1 108.37
6754399-2	AMP Patch cord de FO LC/LC	8	910.28
SFK-P-06-2SD-M	Spider FAN-OUT para FO Multimodo 6	8	3 530.68
6-1427200-4	Cable UTP 4 pares categoría 6 CMR 23	6	3 979.53
6-0219590-6	Cable UTP 4 pares categoría 5E 24 AWG	2	862.23
1375055-1	Modulo jack Rj-45 Categoría 6	160	3 820.35
557505-1	Placa Multimedia 2 Módulos Simétrica	40	430.38
0B-6049	Caja de Montaje Cable Canal Universal	40	216.17
1375291-1	Patch panel 24 módulos Multimedia	5	678.73
1375158-1	Ordenador de cables Horizontal Frontal	45	12 033.66
219884-3	Patch cord UTP RJ-45 Cat 6	80	1 764.75
1-219884-0	Patch cord UTP RJ-45 Cat 6 Multi	20	583.66
GF-2140	Gabinete de piso 45 RU 2"x22.5"x32"	1	3276.48
K2V220V	Kit de 2 Ventiladores para Gabinete 220V	1	196.52
MH-4713	Multitoma Eléctrica 10 Tomas Línea	1	157.21
GW-2066	Gabinete de pared 16 RU 31"x20.5"x23"	1	1241.51
K2V220V	Kit de 2 ventiladores para gabinete	1	196.52
MH-4713	Multitoma Eléctrica 10 Tomas Línea	1	157.21
OTROS			
Part Number	**Descripción**	**Cantidad**	**Costo total de lista + IGV (19%) (S./)**
N/A	Cursos y capacitación	1	2 700.00
N/A	Servicios de implementación	1	79 000.00

4.3 Cronograma

La relación de tareas realizadas para la implementación del proyecto de ingeniería se resume en el diagrama de Gantt mostrado en las figuras siguientes (Figura 4.1 y 4.2).

En resumen los trabajos tomaron un total de 187 días. El diagrama de Gantt presentado indica lo propia para la implementación de cada ítem (Servidores y Almacenamiento= ítem 1; Redes y Comunicaciones= ítem 3).

Id	Nombre de tarea	Duración1
1	**OPTIMIZACIÓN Y AMPLIACIÓN DE LA PLATAFORMA INFORMÁTICA DEL INDECOPI**	**187 días**
2	**Eventos y Entregables Previos del Proyecto**	**98 días**
3	Acto Público de otorgamiento de la Buena Pro	1 día
4	Confirmación de la adjudicación	1 día
5	Firma del contrato	1 día
6	**Plan de Gestión del Proyecto Item 1 e Item 3**	**30 días**
9	**Entrega de Equipos y Datacenter**	**68 días**
10	Entrega de equipos Servidores y de Almacenamiento	25 días
11	Entrega de Equipos de Comunicaciones	35 días
12	Adecuación del DataCenter (hito externo de otro proveedor)	68 días
13	Recepción de Equipos Servidores y de Almacenamiento	0 días
14	Recepción de equipos de Comunicaciones	0 días
15	Entrega de Datacenter adecuado	0 días
16	Implantación Item 1: Servidores y Almacenamiento	**157 días**
17	**Instalacion de Servidores y Almacenamiento**	**66 días**
18	Especificación de Requisitos y Plan de Pruebas	14 días
19	Instalación y Configuración de Equipos	12 días
20	Instalación y configuración de Entorno de Virtualización	12 días
21	Pruebas y ajustes	5 días
22	Elaborar documento de configuración	5 días
23	**Migración de Modulos Web y Bases de Datos**	**148 días**
34	**Conformidad de Equipos Servidores y de Almacenamienrto**	**7 días**
36	**Puesta en Producción**	**9 días**
40	Implantación Item 3: Redes y Comunicaciones	96 días
41	**Cableado Estructurado**	**63 días**
42	**Especificación de Requisitos y Plan de Instalación**	**3 días**
45	**Instalación del Cableado**	**52 días**
60	**Capacitación y documentación**	**11 días**
65	Acta de Cierre - Instalación de Cableado Estructurado INDECOPI	1 día
66	**Equipamiento de Comunicaciones**	**69 días**
67	Especificación de Requisitos y Plan de Instalación	7 días
68	Plan de Pruebas	7 días
69	**Instalación y Configuración de equipos**	**51 días**
70	Instalacion y Configuracion de Switches de Distribucion	2 días
71	Instalacion y Configuracion de Switches de Borde	7 días
72	Configuracion de Switches de Distribucion 1GB	3 días
73	Configuracion de Switches de Borde 1GB	7 días

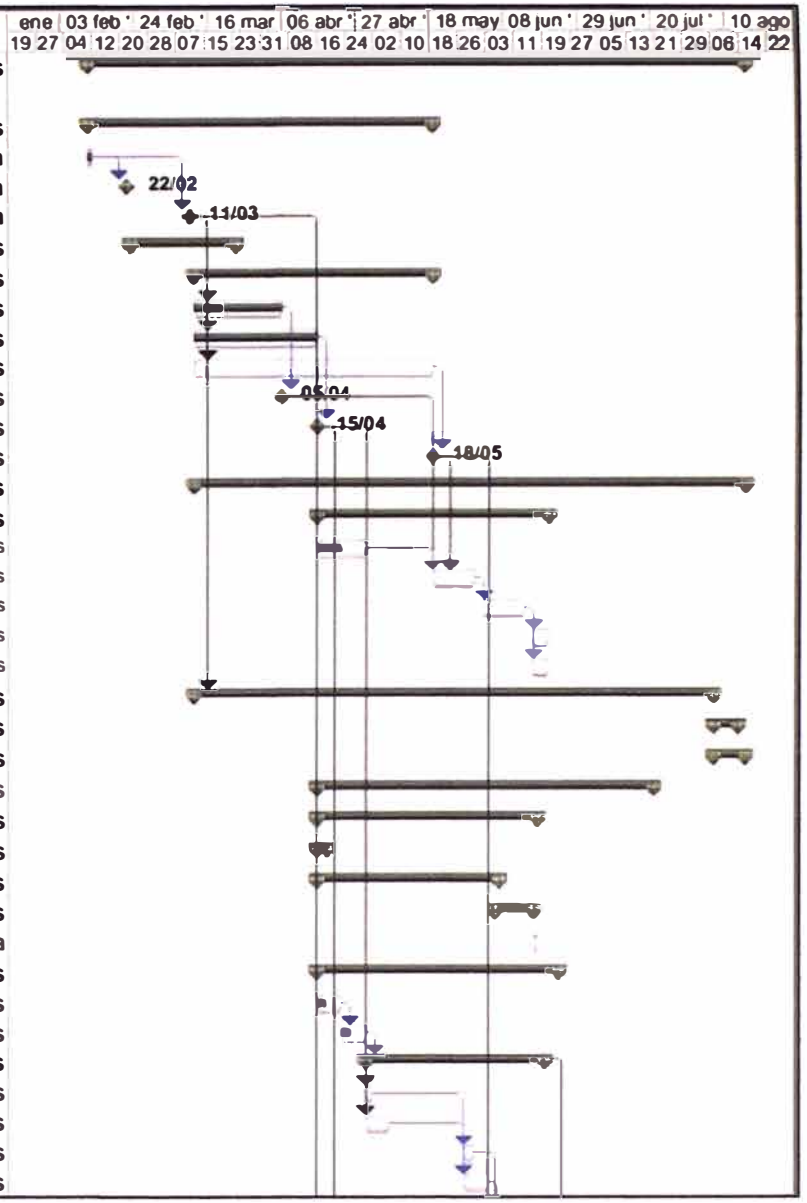

Figura 4.1 Diagrama de Gantt del proyecto de ingeniería- Parte 1/2 (Fuente: Elab. Propia)

Id	Nombre de tarea	Duración1
74	Instalación del Switch de Core	1 día
75	Configuración del Switch de Core	1 día
76	Configuracion de IP´s por nuevas VLANs en las PCs de INDECOPI	11 días
77	Instalacion de Software de Gestion de Switches Cisco	2 días
78	Pruebas y ajustes	1 día
79	Documentacion de la Solucion de Redes	7 días
80	**Conformidad - Equipos de Comunicaciones**	**4 días**
81	Pruebas de conformidad	4 días
82	**Implementación Sistema de seguridad perimetral - INDECOPI**	**96 días**
83	**Instalación del Firewall e IPS**	**3 días**
84	Especificación de Requisitos y Plan de Pruebas	2 días
85	Entrega del plan de instalación	2.5 días
86	Levantamiento de información relevante	2 días
87	**Instalación y actualización del Firewall**	**69 días**
88	Actualización del Firewall	1 día
89	**Configuración del Firewall**	**4 días**
90	Configuracion inicial, rutas y reglas de seguridad	2 días
91	Configuración de VPN SSL con certificados	2 días
92	**Puesta en producción**	**7 días**
93	Pruebas de servicio en Producción	1 día
94	Pruebas de aceptación	1 día
95	Monitoreo de Firewalls	5 días
96	**Instalación y configuración del IPS**	**86 días**
97	Activación de licencias	1 día
98	Configuración inicial y actualización de firmas	1 día
99	**Puesta en producción**	**14 días**
100	Instalación en modo IDS (Transparente)	1 día
101	Pruebas de servicio en producción	1 día
102	Monitoreo en modo transparente	5 días
103	Activación en modo IPS (Habilitación de firmas)	1 día
104	Pruebas de servicio en producción	1 día
105	Monitoreo en modo activo	5 días
106	Curso de capacitación Seguridad	3 días
107	**Documentación de la solución de seguridad**	**6 días**
108	Documentación Técnica de Firewall	2 días
109	Documentación Técnica IPS	2 días
110	Procedimientos de mantemineto	2 días
111	Acta de aceptación - Instalación de seguridad perimetral INDECOPI	1 día

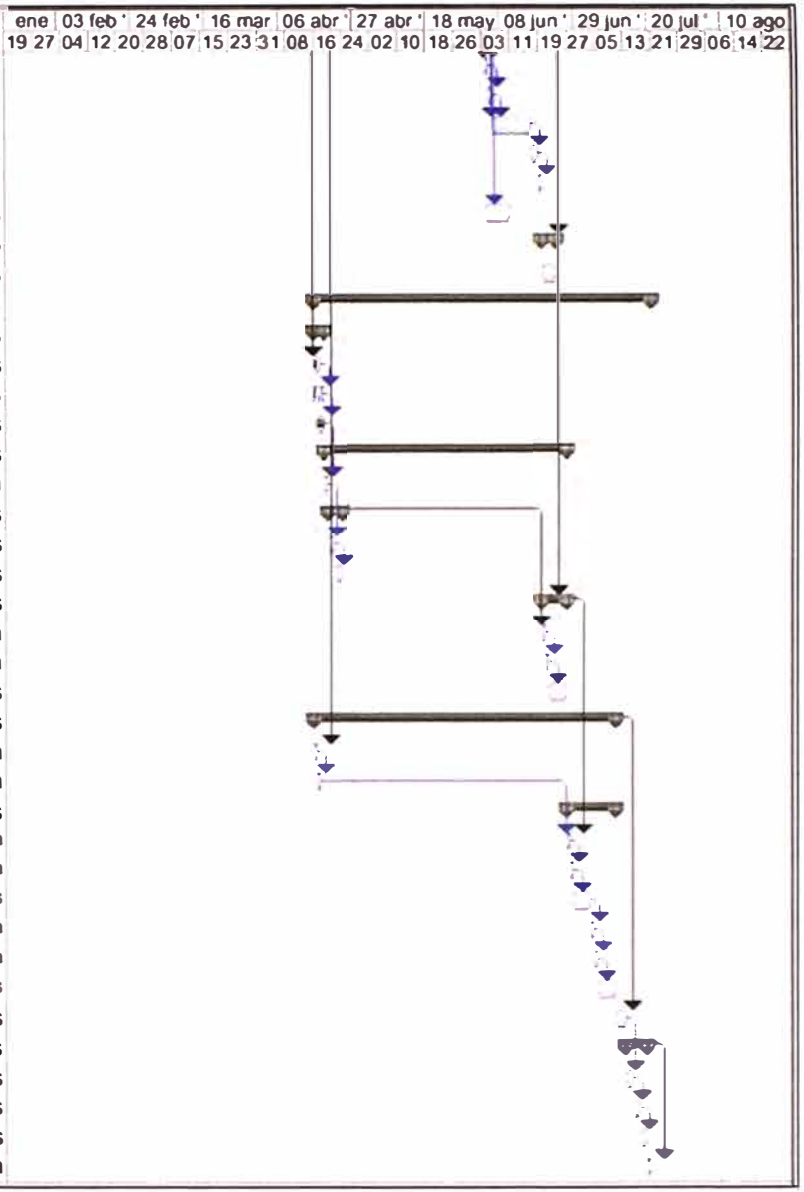

Figura 4.2 Diagrama de Gantt del proyecto de ingeniería- Parte 2/2 (Fuente: Elab. Propia)

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La renovación tecnológica y estructural de la plataforma informática de INDECOPI, mediante soluciones de servidores, almacenamiento, redes y comunicaciones, eliminaron las deficiencias existentes previas al proyecto. INDECOPI es capaz ahora de brindar servicios generales de manera óptima, garantizando continuidad operativa, y respuesta ante fallas por parte de los fabricantes que componen la solución.

2. Se eliminó la saturación de la red al segmentarse los dominios de colisiones mediante el uso de VLANs. La adecuada segmentación de la red, en grupos de redes identificables en el contexto de trabajo del área de sistemas de INDECOPI logra la contención del tráfico no deseado, optimizando la transferencia de datos en la red.

3. La administración centralizada, tanto para los servicios de infraestructura de servidores, como para la parte de comunicaciones y seguridad informática, proporcionan una facilidad de gestión, mantenimiento y aprovisionamiento de servicios de producción de la red. Al mismo tiempo, permite una real aplicación de las políticas de seguridad en la institución, controles de cambios auditables y documentables, monitoreo continuo, además de la flexibilidad en la administración de la seguridad de la información para nuevos servicios que ingresen a la red.

4. El diseño implementado fue orientado a asegurar la escalabilidad de los servicios y la red, facilitando el crecimiento en recursos computacionales a medida que los servicios los exijan. La virtualización a su vez, permite aprovisionar nuevos servicios sin que ello implique, obligatoriamente crecer en equipamiento física.

5. Se aseguró la continuidad de los servicios operativos de INDECOPI mediante una plataforma diseñada para tolerar fallas en los componentes más críticos, de modo tal que, mientras el fabricante cubre la avería física en función a los compromisos asumidos con la institución en sus contratos de soporte, las redundancias de la solución la mantienen operativa mientras el fabricante repone el componente averiado.

6. La consolidación de la información crítica eliminó las islas de información permitiendo contar con información sensible de la institución en sistemas altamente confiables y redundantes que brindaban además rendimiento optimizado a los servicios y facilidad de

gestión y respaldo de la información.

7. Se efectuó la adecuada documentación, tanto de los puntos y recorridos del cableado estructurado, así como de los equipos de red, determinándose los puntos críticos en la red, estableciéndose distintas estrategias de contingencia de acuerdo a la criticidad de los puntos.

8. La nueva arquitectura de red, que incluye en el diseño equipos de seguridad perimetral (firewall e IPS), brinda una estrategia de seguridad a nivel de red acorde a los requerimientos de los servicios que tiene, mediante: restricciones de acceso a servidores, protección a nivel de aplicaciones, acceso remoto (VPN) y políticas de seguridad granulares en función a la criticidad de los servicios.

Recomendaciones

1. Dado que el firewall cumple funciones críticas de enrutamiento y de acceso a los servicios de INDECOPI, se recomienda contar con un equipo adicional para brindar alta disponibilidad a nivel de firewall. En el mismo tenor, se recomienda contar con un equipo IPS redundante.

2. Se recomienda que las soluciones de bases de datos Oracle cuenten con un segundo equipo IBM System p que permita brindar redundancia a nivel de las bases de datos Oracle Los servicios principales de bases de datos de INDECOPI se encuentran montados sobre el servidor IBM System p, y aunque fue implementada adecuadamente esta solución, esta se hizo sobre un solo equipo físico de alta confiabilidad por temas presupuestales.

3. Se recomienda habilitar enlaces redundantes, como mínimo para todos los equipos que conformen las capas de distribución acceso y core. Si bien es cierto que se cuenta con enlaces redundantes en la red de INDECOPI, por temas presupuestales el diseño entregado consideró redundancia de conexiones solamente para los puntos más críticos (interconexión de servidores virtuales a la red y enlaces entre edificios).

ANEXO A
REQUISITOS PARA SERVIDORES Y ALMACENAMIENTO

Tabla A.1 Chasis para Servidores Blade (Fuente: Referencia [3])

Característica	Descripción
Factor de Forma	Chasis Rackeable, máximo 10U
Capacidad	Para 8 Servidores tipo blade similares a los solicitados en el presente concurso como mínimo. En caso de necesitar más de un chasis blade estos deben incluir las mismas características de conexión LAN y SAN, fuente de poder, ventiladores y módulos de administración indicados en el presente cuadro.
Conexión LAN (*)	Dos (2) switches Gigabit Ethernet Capa 2/3 Hot-swap redundantes con soporte a LACP y de administración vía web y telnet con 6 puertos externos y 14 internos.
Conexión SAN (*)	Dos (2) switches (redundantes) de 4Gbps (conector LC) que sean necesarios para conectar como mínimo 4 Blades de 02 Puertos Fibre Channel de 4Gbps. Deberán tener como mínimo 6 puertos externos y 14 internos cada uno.
Arquitectura de Midplane	Redundante
Media	DVD-ROM y disketera 3.5" 1.44MB (interno o externo)
Fuente de Poder	Fuentes de poder redundantes internas al chasis y de cambio en caliente que soporten la máxima configuración del equipo.
Ventiladores	Internos al chasis y de cambio en caliente que soporten la máxima configuración de servidores del equipo.
Módulo de Administración	02 módulos (redundante) con capacidad de cambio en caliente. También debe incluir puertos para teclado, Mouse, video (pueden ser remotos) y un RJ-45 para administración remota
Soporte de Monitoreo Remoto	A través de puerto dedicado con soporte de HTTPS, SNMP
Software de Instalación remota	Herramienta de instalación remota vía Ethernet de Sistemas Operativos (Windows y Linux) e imágenes de clonación para el total de servidores blade que soporte el (o los) chasis.
Software de Administración	De la misma marca del servidor que permita administrar los equipos solicitados en la presente, obtener inventario de HW, definir usuarios con diferentes niveles de acceso y analizar los principales componentes de HW para el envío de alertas predictivas de fallas en por lo menos procesador, memoria y discos. Presentar carta del fabricante indicando que el SW de Administración incluido cumple con todas las funciones indicadas.
Garantía y Soporte	Debe contar con soporte de HW y SW por 3 años con atención 24x7.
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha la solución blade. La instalación se realizará en el Rack Standard de 19" y 42U proporcionado por INDECOPI (El SWITCH KVM debe ser proporcionado por el postor)

(*) Nota: según la respuesta a la observación Nº 8, respecto al número de puertos internos para los switches LAN Y SAN, Se podrá ofertar switches de capa 2/3 con 5 puertos externos como mínimo siempre y cuando se cubra la necesidad de puertos

internos para la capacidad de servidores del chasis.

Tabla A.2 Servidor Blade Tipo 1 (Fuente: Ibídem)

Característica	Descripción
Factor de Forma	Formato Blade (Full-height)
Procesadores Soportados	(02) Dos
Procesadores Instalados	(02) Dos procesadores Intel Xeon Quad Core de 2.33GHz como mínimo.
Memoria Cache	8MB
Front Side Bus	1333MHZ
Memoria RAM	8GB RAM DDR2/667MHz ECC. Capacidad para crecer a 32GB como mínimo. Incluir todos los componentes y slots de memoria necesarios para soportar los 32 GB.
Sistemas Operativos Soportados	Windows Server 2003 (32-bit y 64-bit), Red Had Linux (v3, v4), SuSE Linux y UNIX (opcional). Sustentar con documento técnico el soporte de los sistemas operativos solicitados y adjuntar carta del fabricante.
Puertos Ethernet	Mínimo 2 puertos Gigabit Ethernet
Puertos Fiber Channel	Tarjeta con 2 puertos de 4Gbps instalados
Memoria de video	16MB integrado
SW de administración y monitoreo	Debera incluir la licencia de Software con capacidad para monitorear los componentes de HW y SW. Deberá contar con la capacidad de levantar el inventario de sus componentes. Deberá permitir realizar actualizaciones de firmware, BIOS y drives.
Alertas predictivas de falla	Indicar por medio de una carta del fabricante que los servidores blade, por medio del SW de administración y HW, cuentan con alertas predictivas de fallas de los siguientes componentes: procesador, memoria y discos (se debe poder solicitar la garantía de dichas partes con dicha alerta inclusive antes de que se de la falla).
Garantía y Soporte	Integral, tres (03) años on site (mano de obra y repuestos), respaldado por el fabricante para todo el equipo con atención 24x7.
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha la solución blade. La instalación se realizará en el Rack Standard de 19" y 42U proporcionado por INDECOPI

Tabla A.3 Servidor Rackeable Tipo 1 (Fuente: Ibídem)

Característica	Descripción
Factor de Forma	Rack 1U como máximo.
Procesadores Soportados	(02) Dos
Procesadores Instalados	(02) Dos procesadores Intel Xeon Quad Core de 2.66GHz como mínimo.
Memoria Cache	8MB
Front Side Bus	1333MHZ
Memoria RAM	8GB RAM DDR2/667MHz ECC. Capacidad para crecer a 32GB como mínimo.
Sistemas Operativos Soportados	Windows Server 2003 (32-bit y 64-bit), Red Had Linux (v3, v4), SuSE Linux ES
Media	CD-RW / DVD-ROM
Fuente de Poder	Fuentes de poder redundantes y de cambio en caliente.
Ventiladores	Ventiladores redundantes y de cambio en caliente.
Puertos Ethernet	4 puertos Gigabit Ethernet RJ-45
Puertos Fibra Canal	Tarjeta con 2 puertos de 4Gbps instalados.
Memoria de video	16MB integrado
SW de administración y monitoreo	Deberá contar con la capacidad de monitorear los componentes de HW y SW. Deberá contar con la capacidad de levantar el inventario de sus componentes. Deberá permitir realizar actualizaciones de firmware, BIOS y drives.
Alertas predictivas de falla	Indicar por medio de una carta del fabricante que el servidor rackeable, por medio del SW de administración y HW, cuentan con alertas predictivas de fallas de los siguientes componentes: procesador, memoria y discos (se debe poder solicitar la garantía de dichas partes con dicha alerta inclusive antes de que se de la falla).
Garantía y Soporte	Integral, tres (03) años on site (mano de obra y repuestos), respaldado por el fabricante para todo el equipo con atención 24x7.
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha el servidor.

Tabla A.4 Servidor Rackeable Tipo 2 -Servidor de BD (Fuente: Ibídem)

Característica	Descripción
Arquitectura	RISC SMP 64Bits EPIC siempre y cuando se cumpla con la capacidad de procesamiento mínimo requerido(160,000 TPM-C) evidenciando dicho requerimiento. Así mismo, por tratarse de nuevas tecnologías, consideramos necesario que la propuesta de este tipo de tecnologías (EPIC) incluya un contrato de soporte (GOLD o su equivalente) mínimo por un año del fabricante, que garantice el rendimiento especificado y atenciones de alta prioridad ante fallas del producto.
Particionamiento	02 particiones lógicas o 02 Servidores Virtuales.
Sistema Operativo	Sistema Operativo Unix última versión,64 bits nativos (adjuntar documento técnico que certifique el Oracle DB, sea compatible con el sistema operativo ofertado).
Capacidad de procesamiento	160,000 TPM-C
	Cada partición deberá hacer uso dinámico del total de los recursos.
Discos Duros	02 Discos Duros cambio en caliente de 72 GB de 15,000 RPM (como mínimo), Tecnología SCSI o superior.
	La capacidad efectiva del sistema deberá ser 72 GB en espejo mínimo (Raid 1) y será distribuida a las dos particiones para Sistema Operativo. Una de las Particiones tendrá conectividad al Sistema de Almacenamiento por medio de un adaptador HBA de Fibra Canal de doble puerto de 4 Gbps.
Puertos Fibra Canal	El sistema deberá contar con un adaptador de Fibra Canal de 4 Gbps de dos puertos, el cual será conectado a una de las particiones para ampliar su capacidad de almacenamiento y manejar los arreglos del almacenamiento externo.
Memoria RAM	08 GB de memoria RAM Como mínimo en total con crecimiento a 32 GB
Unidad de DVD	El servidor propuesto deberá contar con una Unidad de DVD
Puertos Gigabit Ethernet	4 Puertos Ethernet 1 Gibabit (2 integrado y 2 en una tarjeta adicional)
Fuentes de poder y ventilación	Redundantes. 220 VAC y 60 Hz.
Consola de administración	Consola Administración de que incluya pantalla TFT 17", teclado, y mouse. Esta consola deberá permitir la administración de las particiones manejando la configuración y la distribución de recursos de las particiones.
Fuentes de poder y ventilación	Redundantes. 220 VAC y 60 Hz.
Reconfiguración dinámica de recursos	Capacidad de asignación dinámica de los recursos del servidor (procesador, memoria, tarjetas de I/O) sin necesidad de reiniciar las particiones involucradas.

Característica	Descripción
Soporte de componentes cambio en caliente	Capacidad de agregar o remover discos magnéticos, fuentes de poder, ventiladores y/o tarjetas de I/O sin necesidad de reiniciar el servidor.
Licencias de software	UniX (última versión comercial de 64 bits). Lenguaje C. Software de administración
Instalación	El servidor y la consola de Administración deben ser instalados en un gabinete estándar para servidores de (19") 42U, suministrado por Indecopi
Garantía y soporte	Integral, tres (03) años on-site (mano de obra y repuestos), respaldado por el fabricante para todo el equipo con atención 24x7 (Adjuntar carta del fabricante).
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha el servidor en el gabinete suministrado.

Tabla A.5 Sistema de Almacenamiento (Fuente: Ibídem)

Característica	Descripción
Capacidad requerida (total)	3.0 TB de capacidad efectiva total.
Tipo de Discos	Tecnología: fibra canal de 4Gbps nativa de tipo Hot Swap ó Hot plug que cumpla con la misma características del Hot swap.
Capacidad de Discos	Capacidades que deberá soportar: 146 y 300 GB FC y 500 GB SATA o FATA
	Capacidad de discos solicitada: 146 GB FC.
	Velocidad: 15,000 RPM.
Desempeño	Mínimo 120,000 IOPS a caché. (número de operaciones de entrada y salida en un segundo) El postor debe incluir una carta emitida por el fabricante o subsidiaria local certificando el nivel de rendimiento indicando los IOPS y documentación técnica.
Compatibilidad	El subsistema deberá conectarse de manera directa y redundante a dos Switches de FC de 4 Gbps del chasis de Servidores Blade ofertado.
	Deberá ser compatible con los siguientes sistemas operativos: AIX, HP-UX, SUN Solaris, Windows 2000/2003, Linux SUSE, Linux Red Hat.
Capacidad de expansiones de discos	Las expansiones de discos deberán tener un mínimo de 14 bahías y deben poder adicionar discos sin interrumpir el funcionamiento del sistema
Configuración de arreglo de discos	La configuración y distribución de los arreglos de discos deberán considerar lo siguiente: discos de datos + disco de paridad + disco de Spare.
	Arreglo: Tipo RAID-5 con Hot Spare o equivalentes
Conectores de discos a	La conectividad entre discos y controladoras debe ser de 4 Gbps en total.

Característica	Descripción
Controladoras internas	Conectividad a los servidores deberá realizarse de manera redundante y utilizando los switches del chasis de los Servidores tipo Blade ofertados.
Memoria caché	El subsistema propuesto deberá tener un total de 4 GB de memoria caché
	El subsistema de discos propuesto deberá tener 2 controladoras redundantes, cada una con 2 GB de memoria caché
Licencia de Software de Administración	El subsistema deberá incluir una licencia de software de administración que permita realizar la configuración y administración de los arreglos Raid de discos internos.
	El software de administración deberá tener Interfase GUI y la capacidad de acceso remoto.
Funcionalidades incluidas	Adición de discos a arreglos RAID de manera dinámica - On Line.
	Las licencias de particionamiento del sistema de almacenamiento deberá tener cobertura de uso para 16 particiones con conexión redundante como mínimo.
Fuentes de Poder y Ventilación	Redundantes y hot swap. 220 VAC y 60 Hz.
Garantía y Soporte	Integral, tres (03) años on site (mano de obra y repuestos), respaldado por el fabricante para todo el equipo con atención 24x7.
Otros	**Cables**: De tipo Fibra Canal LC – LC Suficientes y completos para conectar los equipos ofertados. **Accesorios**: El storage deberá contar con todos los accesorios, hardware y software requeridos para su correcto funcionamiento con los equipos ofertados.
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha el sistema de almacenamiento en le Gabinete Standard de 19" y de 42 U suministrado por INDECOPI.

Tabla A.6 Librería de Backup (Fuente: Ibídem)

Característica	Descripción
Equipo a Adquirir	Librería automática de cintas
Tipo de Tecnología	Ultrium LTO4 ó Tipo SAS
Cantidad de Drives	Uno (01)
Tipo de Drive	SCSI LVD tape Drive.
Número de Cartuchos	Mínimo 22 cartuchos
Capacidad Física	800 GB de capacidad por cartucho en modo nativo (sin compresión)
	Mínimo 17.6 TB en total (sin compresión)
Velocidad de transferencia de datos	Mínimo 80 Mbps nativo

Característica	Descripción
Modelo o factor de Forma	Tipo Rack
Voltaje	220 V AC
Conectividad	Conectividad de tipo SCSI-LVD, con capacidad de conexión a la SAN (opcional). Este equipo será conectado a un servidor con procesador Intel y slots PCI-Express propiedad de INDECOPI. Se deberá suministrar el adaptador y cables correspondientes.
Opción de lectora de Código de Barras	Incluida
Accesorios a Incluir	Kit de montaje en Rack Standard de 19"
	Dos (02) cartuchos de limpieza
	Veinte (20) cartuchos LTO4 con código de barras
Compatibilidad de Software y Sistemas Operativos	Windows 2003 Server Software de BackUp: Brightstore ARC Server BackUp 11.1 y 11.5
Garantía y soporte	Integral, tres (03) años on site (mano de obra y repuestos), respaldado por el fabricante para todo el equipo con atención 24x7.
Servicios de Instalación y Re-Configuración	El postor deberá proveer la instalación física, configuración y poner en marcha la librería de backup en un rack Standard de 19" y 42U proporcionado por INDECOPI

Tabla A.7 Sistema de consolidación y virtualización (Fuente: Ibídem)

Descripción General	- El Software de Virtualización deberá ser de clase EMPRESARIAL, el cual debe ser LICENCIADO y Preinstalado en los 04 Servidores Blade ofertados, los cuales estarán ubicados en el Data Center de INDECOPI. - El Software de Virtualización debe de ejecutarse directamente sobre los niveles más bajos de Hardware de los equipos en modo "BARE METAL" como Sistema Operativo dedicado al manejo y administración de máquinas virtuales. - El Software de Virtualización deberá contar con una consola de administración centralizada y esta debe estar LICENCIADA para ser instalada en un Servidor (INDECOPI proporcionará dicho Servidor).
Sistemas Operativos Soportados	- El Software de Virtualización deberá tener soporte en sus Máquinas Virtuales para los siguientes Sistemas Operativos: o Windows 2000 Server - Service Pack 4 o Windows Server 2003 Standard Edition Service Pack 2 o Windows Server 2003 R2 Standard Edition Service Pack 2 o Suse Linux Enterprise Server 9 o Suse Linux Enterprise Server 10 o Red Hat Enterprise Linux 4.0 o Red Hat Enterprise Linux 5.0 o Novell NetWare 6.0 Server Support Pack 5

	o Novell NetWare 5.1 Server Support Pack 8 - El Software de Virtualización deberá tener compatibilidad completa con el Storage Ofertado. Tanto el fabricante de Software de Virtualización como el fabricante del Storage deben tener publicados en sus respectivas Guías de compatibilidad lo mencionado anteriormente. - El Software de Virtualización deberá tener un probado funcionamiento con la SAN Fibre Channel de 4GB a implementarse. - El Software de Virtualización deberá soportar las siguientes configuraciones: Multipathing (incluyendo licencias para el maximo numero de servidores a conectar que soporta el arreglo), HBA Failover, Storage Port Failover en la SAN Fibre Channel. - El Software de Virtualización deberá soportar Boot desde la SAN.
Alta Disponibilidad	- El Software de Virtualización deberá soportar funcionalidades de espejado y replicación de SAN para mantener copias actualizadas de las Máquinas Virtuales permitiendo Alta Disponibilidad en una recuperación ante desastres. - El Software de Virtualización deberá permitir configurar Alta Disponibilidad para las máquinas Virtuales más críticas de INDECOPI. De modo que si un Servidor físico queda fuera de servicio, las máquinas virtuales afectadas puedan reiniciarse automáticamente en otros servidores operativos con recursos disponibles.
Migración De Máquinas Virtuales	- El Software de Virtualización debe soportar migración de Máquinas Virtuales apagadas (POWER OFF) de un Servidor Físico a otro tan solo arrastrando y soltando el Icono de la Maquina Virtual seleccionada en la Consola de Administración. - El Software de Virtualización deberá soportar Migración de Máquinas virtuales en ejecución o encendidas (POWER ON) desde un servidor físico a otro similar, sin alterar la disponibilidad del servicio y la integridad de la transacción.
Optimización Dinámica De Recursos	- El Software de Virtualización deberá permitir definir reglas y políticas avanzadas de asignación de recursos para máquinas virtuales asegurando CPU y Memoria, para ello las Máquinas Virtuales deberán tener la capacidad de moverse automáticamente a otros servidores físicos con disponibilidad de recursos, para asegurar y mejorar los niveles de servicio de las diferentes aplicaciones de INDECOPI. - El Software de Virtualización debe soportar activar un Modo de Mantenimiento de Servidor de tal modo que cada vez se requiera realizar mantenimiento a un Servidor Físico, las Máquinas Virtuales se muevan automáticamente a Servidores Físicos alternativos.
Administración	- El Software de Virtualización deberá soportar Administración centralizada multinodo de todos los servidores. - El Software de Virtualización deberá soportar

	Administración de máquinas virtuales con jerarquía para acceso de múltiples usuarios. - El Software de Virtualización deberá contar con una consola de administración centralizada con interfase grafica GUI sobre plataforma Windows. - El Software de Virtualización deberá soportar Administración basada en la Web. - La administración deberá soportar un repositorio de información en base de datos relacional. - La administración deberá proveer reportes de carga de CPU, Memoria y Red y estos deben ser exportables a formato Excel.
Licenciamiento	- El Software de Virtualización y todos sus funcionalidades como Backup, Alta Disponibilidad, Migración de Máquinas Virtuales, Optimización Dinámica de Recursos, la consola de administración centralizada u otros deberán tener LICENCIAMIENTO a nombre de INDECOPI.
Otros	- El Software de Virtualización deberá soportar la creación rápida de nuevas Máquinas Virtuales usando plantillas de Máquinas Virtuales. - El Software de Virtualización deberá permitir implementar Clustering Basado en Máquinas Virtuales. - El Software de Virtualización deberá permitir realizar instalaciones de software en las Máquinas Virtuales directamente desde el CD-ROM de una computadora (Desktop). - El Software de Virtualización deberá soportar la configuración de VLANs entre las Máquinas Virtuales. - El Software de Virtualización deberá permitir asignar hasta 8GB de memoria RAM a una Máquina Virtual. - El Software de Virtualización deberá permitir que cada Máquina Virtual pueda trabajar hasta con 2 procesadores físicos simultáneamente.

ANEXO B
NIVELES DE RAID

Los siguientes son los tipos de RAID (Redundant Array Of Independent Disks) "Arreglos Redundantes de Discos Independientes". Estos serán explicados en este anexo

- RAID 0: Striping sin paridad
- RAID 1: Mirror sin paridad
- RAID 10: Mirror con Strip
- RAID 5: Stripping con paridad distribuída
- RAID 6: Stripping con paridad doble distribuida

Las características en cuanto a Mínimo numero de discos necesarios, Eficiencia en el espacio y Tolerancia a fallos (Discos), se resume en la Tabla B.1 al final del anexo.

RAID 0: Striping sin paridad

Provee rendimiento mejorado y almacenamiento adicional, pero no ofrece redundancia o tolerancia a fallas. Debido a que no existe redundancia, este nivel no es realmente un Arreglo Redundante de Discos Independientes (RAID). Sin embargo, por las similitudes que guarda con los arreglos RAID (especialmente por la necesidad de un controlador de distribuir la data entre los múltiples discos), normalmente se refiere como RAID 0.

Cualquier falla de disco destruye el arreglo, que tiene mayores consecuencias cuando hay más discos en el arreglo (como mínimo, la pérdida de datos es hasta dos veces más severa que en discos simples sin RAID). Una sola falla de disco destruye el arreglo porque cuando la data es escrita a un arreglo RAID 0, la data es partida en fragmentos. El número de fragmentos es dado por la cantidad de discos en el arreglo. Los fragmentos son escritos a sus respectivos discos simultáneamente en el mismo sector. Esto permite secciones más pequeñas de todo el bloque de datos para que sea leído en paralelo de varios discos, incrementando el rendimiento.

RAID 0 no implementa corrección de errores, así que cualquier error es irrecuperable. Más discos en el arreglo significa mayor tráfico, pero mayor riesgo de pérdida de datos.

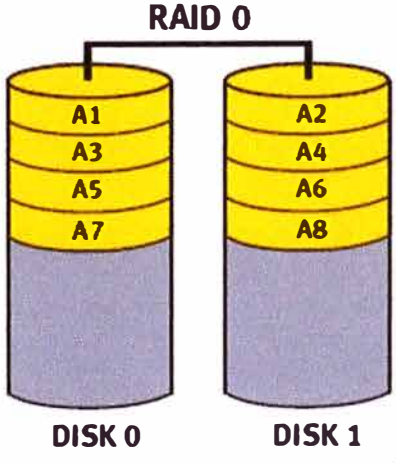

Figura B.1 RAID 0 (Fuente: Referencia [45])

RAID 1: Mirror sin paridad

Provee tolerancia a fallos de errores de disco y falla de hasta todos excepto uno de los discos. Incrementos de performance en las lecturas ocurren cuando se usa un sistema operativo Multi-Thread, que soporta búsquedas divididas, así como también una pequeña reducción en el rendimiento cuando se escribe. El arreglo sigue trabajando mientras al menos un disco siga funcionando.

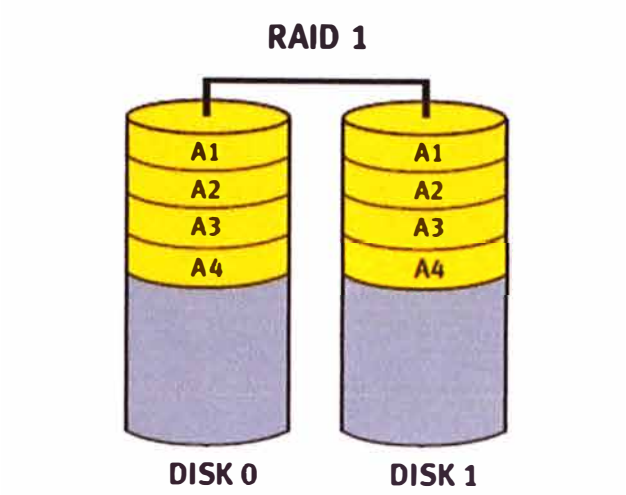

Figura B.2 RAID 1 (Fuente: ibídem)

RAID 10: Mirror con Strip

Provee la replicación de datos y la división de la misma, brindando los beneficios combinados de RAID 1 y RAID 0.

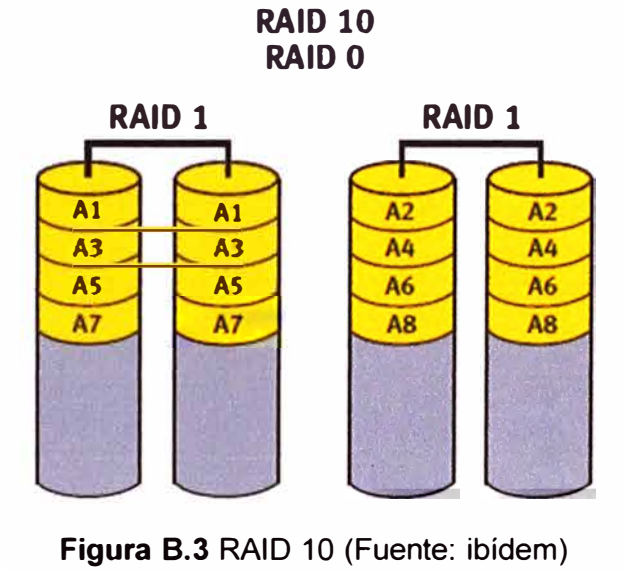

Figura B.3 RAID 10 (Fuente: ibídem)

RAID 5: Stripping con paridad distribuida

Paridad distribuida requiere que todos los discos excepto uno estén presentes para seguir operando, la falla de un disco requiere reemplazo, pero el arreglo no es destruido por una sola falla de disco. Luego de la falla del disco, cualquier lectura subsecuente puede ser calculada de la paridad distribuida. El arreglo perderá data en el caso de un

segundo fallo de disco y es vulnerable hasta que la data que estaba en el disco averiado haya sido reconstruida en el disco de reemplazo. La falla de un disco generará reducción en el rendimiento de todo el arreglo hasta que el disco averiado haya sido reemplazado y reconstruido.

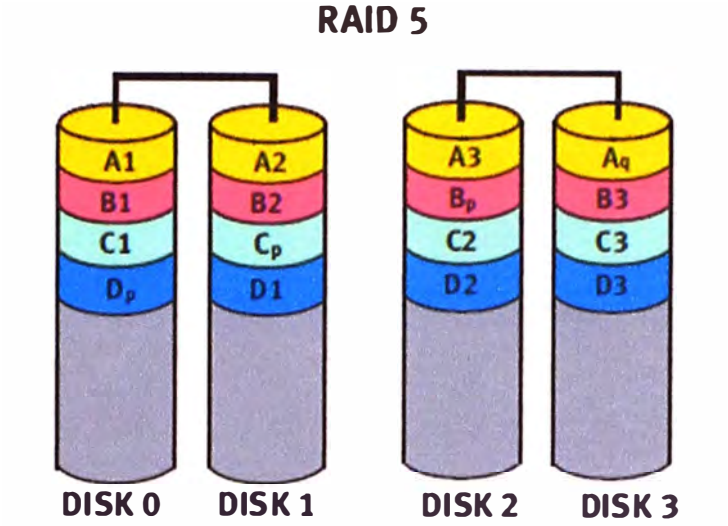

Figura B.4 RAID 5 (Fuente: ibídem)

RAID 6: Stripping con paridad doble distribuida

Provee tolerancia a fallos de hasta dos fallas de discos, el arreglo sigue operando hasta con dos discos averiados. Esto hace el crear RAID groups más largos mucho más prácticos, especialmente para sistemas que requieran alta disponibilidad. Eso se vuelve muy importante porque los discos de gran capacidad incrementan el tiempo necesario para recuperarse de la falla de un solo disco. Los niveles de protección RAID de paridad simple son vulnerables a pérdida de datos, hasta que disco averiado haya sido reconstruido. Paridad doble ofrece tiempo para reconstruir el arreglo sin que la data se ponga en riesgo si un solo disco adicional falla antes que la reconstrucción se complete.

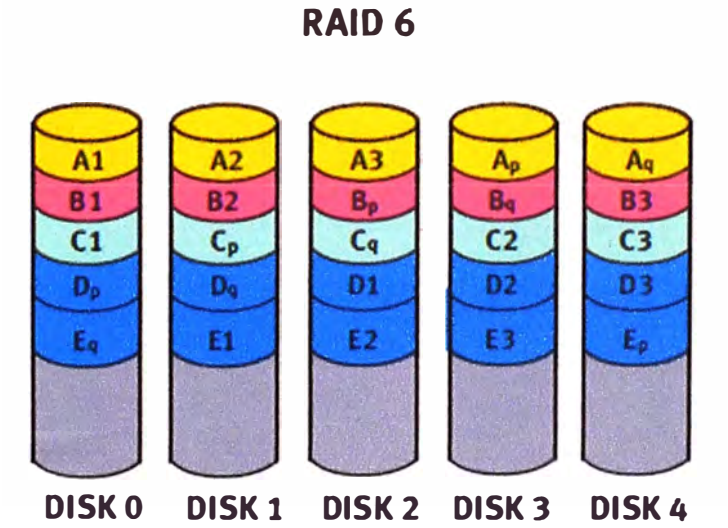

Figura B.6 RAID 6 (Fuente: ibídem)

Tabla B.1 Comparación de características RAID (Fuente: Elaboración propia)

	RAID 0	RAID 1	RAID 10	RAID 5	RAID 6
Mínimo numero de discos necesarios	2	2	4	3	4
Eficiencia en el espacio	N	1 (Tamaño del disco más pequeño)	N/2	N-1	N-2
Tolerancia a fallos (Discos)	0	N-1	N/2 (uno de cada mirror set)	1	2

ANEXO C
EQUIPAMIENTO DE SERVIDORES Y ALMACENAMIENTO UTILIZADOS

Tabla C.1 Chasis para Servidores Blade IBM BlaceCenter E (Fuente: Ref. [7])

Características	Descripción
Factor de Forma	Chasis Rackeable, 7U
Capacidad	Para 14 Servidores tipo blade similares a los solicitados en la Licitación de INDECOPI
Conexión LAN	Dos (2) switches Gigabit Ethernet Capa 2/3 Hot-swap redundantes con soporte a LACP y de administración vía web y telnet con 6 puertos externos y 14 internos.
Conexión SAN	Dos (2) switches (redundantes) de 4Gbps (conector LC) con 6 puertos externos y 14 internos cada uno.
Arquitectura de Midplane	Redundante
Media	DVD-ROM y disketera 3.5" 1.44MB (interno)
Fuente de Poder	Fuentes de poder redundantes internas al chasis y de cambio en caliente.
Ventiladores	Internos al chasis y de cambio en caliente.
Módulo de Administración	02 módulos (redundantes) con capacidad de cambio en caliente.
Soporte de Monitoreo Remoto	A través de puerto dedicado con soporte de HTTPS, SNMP
Software de Instalación remota	Herramienta de instalación remota vía Ethernet de Sistemas Operativos (Windows y Linux) e imágenes de clonación para el total de servidores blade que soporte el chasis.
Software de Administración	De la misma marca del servidor (IBM Director) que permite administrar los equipos solicitados por INDECOPI, obtener inventario de HW, definir usuarios con diferentes niveles de acceso y analizar los principales componentes de HW para el envío de alertas predictivas de fallas en procesador, memoria, discos, fuentes de poder y ventiladores.

Figura C.1 Chasis para Servidores Blade IBM BlaceCenter E (Fuente: ibídem)

Tabla C.2 Servidor Blade IBM BladeCenter HS21 XM (Fuente: Ref. [8])

Característica	Descripción
Factor de Forma	Formato Blade (Full-height)
Procesadores Soportados	(02) Dos
Procesadores Instalados	(02) Dos procesadores Intel Xeon Quad Core de 2.33GHz.
Memoria Cache	8MB
Front Side Bus	1333MHZ
Memoria RAM	8GB RAM DDR2/667MHz ECC. Capacidad para crecer a 32GB
Sistemas Operativos Soportados	Windows Server 2003 (32-bit y 64-bit), Red Had Linux (v4, v5), SuSE Linux.
Puertos Ethernet	2 puertos Gigabit Ethernet.
Puertos Fiber Channel	Tarjeta con 2 puertos de 4Gbps instalados.
Memoria de video	16MB integrado
SW de administración y monitoreo	Incluye la licencia de software IBM Director con capacidad para monitorear los componentes de HW y SW. Cuenta con la capacidad de levantar el inventario de sus componentes. Permite realizar actualizaciones de firmware, BIOS y drives.
Alertas predictivas de falla	Los servidores blade, por medio del SW de administración y HW, cuentan con alertas predictivas de fallas de los siguientes componentes: procesador, memoria y discos.

Figura C.2 Servidor Blade IBM BladeCenter HS21 XM (Fuente: Ibídem)

Tabla C.3 Servidor Rackeable IBM SystemX 3550 (Fuente: Ref. [9])

Característica	Descripción
Factor de Forma	Rack 1U.
Procesadores Soportados	(02) Dos
Procesadores Instalados	(02) Dos procesadores Intel Xeon Quad Core de 2.66GHz.
Memoria Cache	8MB
Front Side Bus	1333MHZ
Memoria RAM	8GB RAM DDR2/667MHz ECC. Capacidad para crecer a 32GB.
Sistemas Operativos Soportados	Windows Server 2003 (32-bit y 64-bit), Red Had Linux (v3, v4), SuSE Linux ES
Media	CD-RW / DVD-ROM
Fuente de Poder	Fuentes de poder redundantes y de cambio en caliente.
Ventiladores	Ventiladores redundantes y de cambio en caliente.
Puertos Ethernet	4 puertos Gigabit Ethernet RJ-45
Puertos Fibra Canal	Tarjeta con 2 puertos de 4Gbps instalados.
Memoria de video	16MB integrado
SW de administración y monitoreo	Incluye la licencia de software IBM Director con capacidad para monitorear los componentes de HW y SW. Cuenta con la capacidad de levantar el inventario de sus componentes. Permite realizar actualizaciones de firmware, BIOS y drives.
Alertas predictivas de falla	El servidor rackeable, por medio del SW de administración y HW, cuenta con alertas predictivas de fallas de los siguientes componentes: procesador, memoria y discos.

Figura C.3 Servidor Rackeable IBM SystemX 3550 (Fuente: Ibídem)

Tabla C.4 Servidor Rackeable (Servidor de BD) IBM System p5 520Q (Fuente: Ref [10])

Característica	Descripción
Arquitectura	RISC SMP 64Bits
Particionamiento	02 particiones lógicas.
Sistema Operativo	Sistema Operativo AIX 6.1, 64 bits
Capacidad de procesamiento	167,255 TPM-C (Transacciones por minuto) (http://www.tpc.org/information/benchmarks.asp)
Discos Duros	02 Discos Duros cambio en caliente de 72 GB de 15,000 RPM, Tecnología SCSI.
	La capacidad efectiva del sistema es de 72 GB, sin formato, en espejo (Raid 1). Una de las Particiones tendrá conectividad al Sistema de Almacenamiento por medio de un adaptador HBA de Fibra Canal de doble puerto de 4 Gbps.
Puertos Fibra Canal	Cuenta con un adaptador de Fibra Canal de 4 Gbps de dos puertos.
Memoria RAM	08 GB de memoria RAM con crecimiento a 32 GB
Unidad de DVD	Incluida
Puertos Gigabit Ethernet	4 Puertos Ethernet 1 Gibabit (2 integrado y 2 en una tarjeta adicional)
Fuentes de poder y ventilación	Redundantes. 220 VAC y 60 Hz.
Consola de administración	Consola Administración que incluye pantalla TFT 17", teclado, y mouse.
Fuentes de poder y ventilación	Redundantes. 220 VAC y 60 Hz.
Reconfiguración dinámica de recursos	Capacidad de asignación dinámica de los recursos del servidor (procesador, memoria, tarjetas de I/O) sin necesidad de reiniciar las particiones involucradas.
Soporte de componentes cambio en caliente	Capacidad de agregar o remover discos magnéticos, fuentes de poder, ventiladores y/o tarjetas de I/O sin necesidad de reiniciar el servidor.
Licencias de software	AIX 6.1 (última versión comercial de 64 bits). Lenguaje C. Software de administración

Figura C.4 Servidor Rackeable (Servidor de BD) IBM System p5 520Q (Fuente: Ibídem)

Tabla C.5 Sist. de Almacenamiento IBM DS4700 + Expansión EXP810 (Fuente: Ref. [11])

Característica	Descripción
Capacidad requerida (total)	3.0 TB de capacidad efectiva total.
Tipo de Discos	Tecnología: fibra canal de 4Gbps nativa de tipo Hot Swap.
Capacidad de Discos	Capacidades soportadas: 146 y 300 GB FC y 500 GB SATA
	Velocidad: 15,000 RPM.
Desempeño	121,500 IOPS a caché. (número de operaciones de entrada y salida en un segundo)
Compatibilidad	Es compatible con los sistemas operativos: AIX, HP-UX, SUN Solaris, Windows 2000/2003, Linux SUSE, Linux Red Hat.
Capacidad de expansiones de discos	Las expansiones de discos tienen 16 bahías y pueden adicionar discos sin interrumpir el funcionamiento del sistema
Configuración de arreglo de discos	La configuración y distribución de los arreglos de discos incluye: discos de datos + disco de paridad + disco de Spare.
	Arreglo: Tipo RAID-5 con Hot Spare
Conectores de discos a Controladoras internas	La conectividad entre discos y controladoras es de 4 Gbps en total.
	Conectividad a los servidores se realizará de manera redundante y utilizando los switches del chasis de los Servidores tipo Blade ofertados.
Memoria caché	El subsistema tiene un total de 4 GB de memoria caché
	El subsistema de discos propuesto tiene 2 controladoras redundantes, cada una con 2 GB de memoria caché
Licencia de Software de Administración	El subsistema incluye una licencia de software de administración (Storage Manager) que permite realizar la configuración y administración de los arreglos Raid de discos internos.
	El software de administración tiene interfase GUI y la capacidad de acceso remoto.
Funcionalidades incluidas	Adición de discos a arreglos RAID de manera dinámica - On Line.
	Las licencias de particionamiento del sistema de almacenamiento tienen cobertura de uso para 16 particiones con conexión redundante.
Fuentes de Poder y Ventilación	Redundantes y hot swap. 220 VAC y 60 Hz.

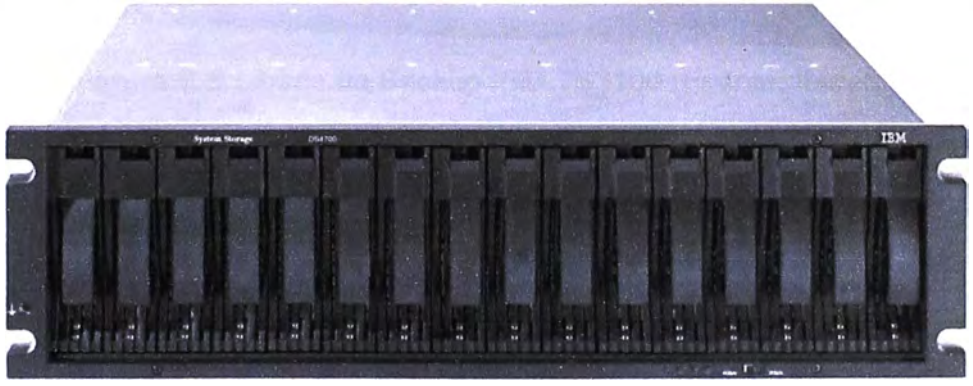

Figura C.5 Sistema de Almacenamiento IBM DS4700 (Fuente: Ibídem)

Tabla C.6 Liberia de Backup IBM TS3100 (Fuente: Referencia [12])

Característica	Descripción
Equipo a Adquirir	Librería automática de cintas
Tipo de Tecnología	Ultrium LTO4
Cantidad de Drives	Uno (01)
Tipo de Drive	SCSI LVD tape Drive.
Número de Cartuchos	24 cartuchos
Capacidad Física	800 GB de capacidad por cartucho en modo nativo (sin compresión)
	19.6 TB en total (sin compresión)
Velocidad de transferencia de datos	120 Mbps nativo
Modelo o factor de Forma	Tipo Rack
Voltaje	220 V AC
Conectividad	Conectividad de tipo SCSI-LVD.
Opción de lectora de Código de Barras	Incluida
Accesorios incluidos	Kit de montaje en Rack Standard de 19"
	Dos (02) cartuchos de limpieza
	Veinte (20) cartuchos LTO4 con código de barras
Compatibilidad de Software y Sistemas Operativos	Windows 2003 Server Software de BackUp: Brightstore ARC Server BackUp 11.1 y 11.5

Figura C.6 Liberia de Backup IBM TS3100 (Fuente: Ibídem)

Tabla C.7 Sist. de consolidación y virtualización VMware ESX Server (Fuente: Ref: [13])

vmware®	
Descripción General	El **Software de Virtualización VMware ESX Server** es de clase EMPRESARIAL, el cual fue LICENCIADO y Preinstalado en los 04 Servidores Blade solicitados por INDECOPI. El Software de Virtualización VMware ESX Server se ejecuta directamente sobre los niveles más bajos de Hardware de los equipos en modo "BARE METAL" como Sistema Operativo dedicado al manejo y administración de máquinas virtuales. El Software de Virtualización VMware ESX Server cuenta con una consola de administración centralizada VMware VirtualCenter y esta LICENCIADA para ser instalada en un Servidor (INDECOPI proporcionó dicho Servidor).
Sistemas Operativos Soportados	El Software de Virtualización VMware ESX Server tiene soporte en sus Máquinas Virtuales para los siguientes Sistemas Operativos: o Windows 2000 Server - Service Pack 4 o Windows Server 2003 Standard Edition Service Pack 2 o Windows Server 2003 R2 Standard Edition Service Pack 2 o Suse Linux Enterprise Server 9 o Suse Linux Enterprise Server 10 o Red Hat Enterprise Linux 4.0 o Red Hat Enterprise Linux 5.0 o Novell NetWare 6.0 Server Support Pack 5 o Novell NetWare 5.1 Server Support Pack 8 - El Software de Virtualización VMware ESX Server tiene compatibilidad completa con el Storage Ofertado a INDECOPO (DS4700). Tanto el fabricante de Software de Virtualización VMware ESX Server VMware como el fabricante del Storage tienen publicados en sus respectivas Guías de compatibilidad lo mencionado anteriormente. - El Software de Virtualización VMware ESX Server tiene un probado funcionamiento con la SAN Fibre Channel de 4GB implementada en INDECOPI. - El Software de Virtualización VMware ESX Server soporta las siguientes configuraciones: Multipathing (incluyendo licencias para el máximo número de servidores a conectar que soporta el arreglo), HBA Failover, Storage Port Failover en la SAN Fibre Channel. - El Software de Virtualización VMware ESX Server soporta Boot desde la SAN.
Alta Disponibilidad	- El Software de Virtualización VMware ESX Server soporta funcionalidades de espejado y replicación de SAN para mantener copias actualizadas de las Máquinas Virtuales permitiendo Alta Disponibilidad en una recuperación ante desastres. - El Software de Virtualización VMware ESX Server permite configurar Alta Disponibilidad para las máquinas Virtuales más críticas de INDECOPI. De modo que si un Servidor físico queda fuera de servicio, las máquinas virtuales afectadas puedan reiniciarse automáticamente en otros servidores operativos con recursos disponibles.
Migración De Máquinas	- El Software de Virtualización VMware ESX Server soporta migración de Máquinas Virtuales apagadas (POWER OFF) de un

Virtuales	Servidor Físico a otro tan solo arrastrando y soltando el Icono de la Maquina Virtual seleccionada en la Consola de Administración. - El Software de Virtualización VMware ESX Server soporta Migración de Máquinas virtuales en ejecución o encendidas (POWER ON) desde un servidor físico a otro similar, sin alterar la disponibilidad del servicio y la integridad de la transacción.
Optimización Dinámica De Recursos	- El Software de Virtualización VMware ESX Server permite definir reglas y políticas avanzadas de asignación de recursos para máquinas virtuales asegurando CPU y Memoria, para ello las Máquinas Virtuales deberán tener la capacidad de moverse automáticamente a otros servidores físicos con disponibilidad de recursos, para asegurar y mejorar los niveles de servicio de las diferentes aplicaciones de INDECOPI. - El Software de Virtualización VMware ESX Server soporta activar un Modo de Mantenimiento de Servidor de tal modo que cada vez se requiera realizar mantenimiento a un Servidor Físico, las Máquinas Virtuales se muevan automáticamente a Servidores Físicos alternativos.
Administración	- El Software de Virtualización VMware ESX Server soporta Administración centralizada multinodo de todos los servidores. - El Software de Virtualización VMware ESX Server soporta Administración de máquinas virtuales con jerarquía para acceso de múltiples usuarios. - El Software de Virtualización VMware ESX Server cuenta con una consola de administración centralizada con interfase grafica GUI sobre plataforma Windows. - El Software de Virtualización VMware ESX Server soporta Administración basada en la Web. - La administración soporta un repositorio de información en base de datos relacional. - La administración provee reportes de carga de CPU, Memoria y Red y estos son exportables a formato Excel.
Licenciamiento	- El Software de Virtualización VMware ESX Server y todos sus funcionalidades como Backup, Alta Disponibilidad, Migración de Máquinas Virtuales, Optimización Dinámica de Recursos, la consola de administración centralizada u otros tienen LICENCIAMIENTO a nombre de INDECOPI.
Otros	- El Software de Virtualización VMware ESX Server soporta la creación rápida de nuevas Máquinas Virtuales usando plantillas de Máquinas Virtuales. - El Software de Virtualización VMware ESX Server permite implementar Clustering Basado en Máquinas Virtuales. - El Software de Virtualización VMware ESX Server permite realizar instalaciones de software en las Máquinas Virtuales directamente desde el CD-ROM de una computadora (Desktop). - El Software de Virtualización VMware ESX Server soporta la configuración de VLANs entre las Máquinas Virtuales. - El Software de Virtualización VMware ESX Server permite asignar hasta 8GB de memoria RAM a una Máquina Virtual. - El Software de Virtualización VMware ESX Server permite que cada Máquina Virtual pueda trabajar hasta con 2 procesadores físicos simultáneamente.

ANEXO D
REQUISITOS PARA EQUIPOS DE COMUNICACIÓN Y DE SEGURIDAD

Tabla D.1 Switch de Núcleo (Fuente: Referencia [3])

Característica	Descripción
Interfaces y puertos	El equipo deberá soportar al menos 20 interfaces de 10Gbps. Las interfaces deben estar disponibles en el mercado al momento de presentar la oferta.
	El equipo deberá incluir 48 puertos 10/100/1000 BaseT RJ45.
	04 puertos Gigabit Ethernet, 1000BaseSX, incluidas las interfaces.
	Switch fabric instalado y operativo de 500 Gbps mínimo. Tasa de envío de 30 Mpps instalados y operativos, escalable al menos hasta 300 Mpps, tanto en Capa 2 como en Capa 3.
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT, IEEE 802.3ae.
	LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del switch del mismo tipo y velocidad
Funcionalidades en capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Soporte de IPv4 e IPv6.
	Multicast IGMPv1, v2 y v3 y PIMv1 y v2.
Funcionalidades en Capa 2	Soporte de 4,000 VLAN's mínimo. VLAN trunk IEEE 802.1Q.
	Soporte de 30,000 direcciones MAC como mínimo.
	Soporte de Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.
Soportar redundancia en	- Módulo de procesamiento o Supervisor - Switch Fabric La redundancia de estos elementos debe operar de manera que ante la falla de uno, el redundante garantice que el equipo continuará operando al 100%, tanto en su capacidad como en sus funcionalidades en capa 2 y 3. Todas las tarjetas de interfaz y administración deberán ser Hot-Swap.
Soporte de Calidad de Servicio	IEEE 802.1p CoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP
	Limitación de ancho de banda basada en direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones IP de origen y destino y puertos TCP/UDP.
	Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2 y SCP.

Característica	Descripción
	Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como "MAC Address Flooding", "VLAN. Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
Mecanismos de gestión	Puerto de consola para gestión local
	Soporte de Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporte de SNMP v2 y v3
	Soporte de RMON
	Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporte de protocolos NTP, DHCP, DNS.
	Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.
	Soporte de multiples sesiones de "port mirroring" así como "port mirroring" remoto.
Otros	Fuente de poder con alimentación a 220Vac 60Hz. Montable en rack 19" Software actualizable. Incluir la última versión disponible

Tabla D.2 Switch de distribución (Fuente: Ibídem)

Característica	Descripción
Interfaces y puertos	48 puertos 10/100/1000 Autosensing con PoE IEEE 802.3af.
	04 puertos Gigabit modulares GBIC o SFP, con soporte de interfaces 1000BaseSX, 1000BaseLX y 10/100/1000BaseT. Incluir por los menos una interfase 1000BaseSX.
	Switch Fabric de 30 Gbps.
	Tasa de envío de 38 Mpps en Capa 2 y Capa 3.
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT.
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
Funcionali-dades capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Capacidad de ampliación a IPv6 sin cambio de hardware
	Multicast IGMPv1, v2 y v3 Snooping, con posibilidad de agregar PIMv1, PIMv2 y DVMRP sin cambio de hardware.
Funcionali-dades capa 2	1,000 VLANs. VLAN trunk IEEE 802.1Q.
	8,000 direcciones MAC.
	Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.
Soporte de Calidad de Servicio	IEEE 802.1p CoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP.
	Limitación de ancho de banda basada en direcciones MAC de origen

Característica	Descripción
	y destino, direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
	Asignación dinámica de filtros por usuario vía 802.1x.
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2, SSL y SCP.
	Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como "MAC Address Flooding", "VLAN" "Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
Mecanismos de gestión	Puerto de consola para gestión local
	Soporte de Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporte de SNMP v2 y v3
	Soporte de RMON
	Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporte de protocolos NTP, DHCP, DNS.
	Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.
	Soporte de múltiples sesiones de "port mirroring" así como "port mirroring" remoto.
	El puerto de monitoreo deberá permitir colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de sesiones TCP a través del mismo puerto (puerto bidireccional).
Otros	Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante. Montable en rack 19" Software actualizable. Incluir la última versión disponible.

Tabla D.3 Switch de Acceso (Fuente: Ibídem)

Característica	Descripción
Interfaces y puertos	48 puertos 10/100 Autosensing con PoE IEEE 802.3af.
	04 puertos Gigabit modulares GBIC o SFP, con soporte de interfaces 1000BaseSX, 1000BaseLX y 10/100/1000BaseT. Incluir por lo menos una interfaz 10/100/1000BaseT.
	Switch Fabric mínimo de 17.6 Gbps.
	Tasa de envío de 12 Mpps en Capa 2 y Capa 3.

Característica	Descripción
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000Base.
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
Funcionalidades capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Capacidad de ampliación a IPv6 sin cambio de hardware
	Multicast IGMPv1, v2 y v3 Snooping, con posibilidad de agregar PIMv1, PIMv2 y DVMRP sin cambio de hardware.
Funcionalidades capa 2	1,000 VLANs. VLAN trunk IEEE 802.1Q.
	8,000 direcciones MAC.
	Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.
Soporte de Calidad de Servicio	IEEE 802.1p CoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP.
	Limitación de ancho de banda basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
	Asignación dinámica de filtros por usuario vía 802.1x.
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2, SSL y SCP.
	Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como "MAC Address Flooding", "VLAN", Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
Mecanismos de gestión	Puerto de consola para gestión local
	Soporte de Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporte de SNMP v2 y v3
	Soporte de RMON
	Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporte de protocolos NTP, DHCP, DNS.
	Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.

Característica	Descripción
	Soporte de multiples sesiones de "port mirroring" así como "port mirroring" remoto.
	El puerto de monitoreo debe permitir colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de sesiones TCP a través del mismo puerto (puerto bidireccional).
Otros	Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante. Montable en rack 19" Software actualizable. Incluir la última versión disponible.

Tabla D.4 Software de Administración (Fuente: Ibídem)

Descripción
- La aplicación debe permitir administrar los dispositivos de distribución y acceso, desde cualquier lugar de la intranet/internet. - Debe tener la posibilidad de realizar múltiples tareas de configuración sin usar comandos de interfaz de línea de comandos. - Asimismo debe aplicar acciones a múltiples dispositivos y puertos al mismo tiempo para configuraciones de VLAN y Calidad de Servicio (QoS), supervisión de enlaces, reportes de tráfico y actualizaciones de software.

Tabla D.5 Firewall (Fuente: Ibídem)

Característica	Descripción
Capacidades	El equipo deberá incluir capacidad de firewall con una inspección de paquetes no menor de 300 mbps.
	Soporte de 48,000 conexiones concurrentes como mínimo.
	Deberá Incluir 3 Puertos Fast Ethernet y 2 Gigabit Ethernet
	Sistema Operativo en codigo cerrado y certificado.
	Chasis diseñado (Tipo Apliance) para su instalación en rack.
Licenciamiento	El licenciamiento del Software cliente VPN deberá ser ilimitado y proporcionado sin costo.
	El sistema de seguridad ofertado deberá poseer licenciamiento ilimitado de usuarios, hosts y tiempo de uso como firewall.
Capacidades L2	Deberá incluir manejo de 802.1q para el manejo de Virtual LANs.
Capacidades L3	Deberá incluir manejo de IGMPv2, Stub multicast routing, y configuración de rutas multicast.
	Deberá incluir manejo de filtros para trafico multicast.
	Deberá incluir manejo de NAT y PAT sobre multicast source address.
	Soporte de algoritmos de ruteo dinámico como RIP y OSPF.
Inspección de tráfico y soporte de protocolos	El equipo deberá permitir inspección detallada tráfico web, para controlar comandos, URI, MIME, anomalías del protocolo, y cumplimiento de RFC.
	Control de aplicación tunel sobre port 80: mensajeria instantánea, aplicaciones p2p, tunelización, entre otros.
	Deberá Incluir manejo de NAT, PAT, y mapeo de múltiples hosts internos en una dirección global para servicios TCP y UDP.
	Deberá incluir manejo de PAT para trafico ESP, H.323v3, H.323v4, SIP.

Característica	Descripción
	Deberá incluir manejo de inspección de estado para tráfico ICMP via NAT.
	Deberá incluir manejo DHCP como relay, server y cliente.
	Soporte de Inspección de Estado para: - Protocolos Básicos: DNS, FTP, HTTP, ICMP, IPSEC, PPTP, SMTP,TFTP, ESMTP - Voice over IP: CTIQBE, H.323v3/4, TAPI/JTAPI, MGCP, SIP - Multimedia: Netshow, RTSP, VDO Live - Database y Directory: ILS, LDAP, Sun RPC, - Management: ICMP, RSH, SNMP
Métodos de cifrado	Deberá Incluir mecanismos de encriptación DES, 3DES y AES, 150 Mbps AES.
	Deberá Incluir manejo de IPSec y SSL para el acceso remoto.
	El equipo deberá permitir trabajar en modo cluster de vpn tanto para IPSec como SSL con otros equipos de las mismas características.
Soporte de certificados digitales	Deberá Incluir soporte de certificados digitales emitidos por la entidad de certificación DST(Digital Signature Trust) y el uso de tokens de seguridad para la autenticación de conexiones VPN SSL. Si para lograr la autenticación de las sesiones VPN SSL usando certificados de DST es necesario que el equipo ofertado tenga instalado un certificado de servidor emitido por esta entidad (DST), el costo de este certificado deberá ser asumido totalmente por el postor.
Soporte IPSec	Deberá Incluir manejo de tuneles IPSec red a red, para conexión con routers, firewalls similares, o equipos vpn en configuraciones donde las IPs de los equipos remotos: son estáticas o dinámicas.
	Deberá Incluir soporte de 250 tuneles IPSec concurrentes.
Soporte VPN SSL	La solución deberá permitir funcionar como un redireccionador de puertos a través de protocolo SSL.
	En SSL el usuario remoto deberá poder ingresar mediante un navegador WEB, permitiendo que acceda a diferentes recursos de la intranet utilizando distintos tabs definidos en su portal inicial. No será necesaria la instalación manual de ningún software en la PC del cliente.
	En SSL deberá permitir el ingreso de usuarios mediante VPN L3. Esto es, asignando al usuario externo una nueva dirección IP y encapsulando, en forma transparente para el usuario y la aplicación, cualquier protocolo a través del túnel.
	El Software cliente VPN proporcionado deberá permitir trabajar sobre equipos NAT, permitiendo split ip y dns.
Gestión de políticas	Deberá poseer un modelo de políticas de seguridad basada en usuarios y/o grupos, debiendo ser esto de forma granular.
	Deberá permitir asignar recursos a los usuarios dependiendo del nivel de autorización, incluyendo control granular sobre URL permitidos.
	Deberá permitir la autenticación de usuarios a través de tokens, y certificados X.509
Calidad de servicio	Manejo de Calidad de servicio: priorización y limitación de ancho de banda por aplicación atravesando el equipo.
Administración	Capacidad de administración y gestión basada en los protocolos telnet, SSH, https, radius.
	El equipo deberá contar con una interface WEB gráfica interna, accesible en modo seguro, que permita la configuración de las

Característica	Descripción
	funciones de firewall-vpn.
	Deberá incluir el manejo de niveles administrativos para la operación y manejo del equipo, personalizables mínimo 12.
	Deberá incluir mecanismos de inspección de estado para http, ftp, smtp, icmp, tcp, y udp en IPv6.
	El equipo deberá incluir protocolos de administración seguros: https, sshv2, SNMPv2c, NTP v3.
	El equipo debe enviar alarmas vía Syslog.
	Soporte de multiples softwares y configuraciones, sobre el equipo como backups o restauración ante cambios.
Alta disponibilidad	Debe soportar alta disponibilidad active/active y active/stand bye, fail over

Tabla D.5 IPS (Fuente: Ibídem)

Característica	Descripción
Capacidades	Se deberá ofrecer una solución de hardware y software basado en appliance, el cual realice monitoreo y prevención en línea.
	Deberá contar con un mínimo 4 interfaces 10/100/1000 en cobre y proporcionar un throughput de 230 Mbps para el análisis del tráfico.
	Deberá contar con al menos un puerto de administración ethernet 10/100 o en su mejor caso 10/100/1000, adicional a las interfaces de análisis solicitadas.
	Las Interfaces utilizadas para sensar tráfico deben trabajar en modo stealth, sin stack de TCP/IP en la interfaz.
	Montaje físico en rack 19".
	Alimentación 220V
Licenciamiento	Deberá disponer de licencias para monitorear todos los servidores
Modos de trabajo	El monitoreo debe de ser transparente para los usuarios.
	El equipo podrá configurarse en modo transparente; es decir, de prevención en línea, pero sin bloquear tráfico. El sistema sólo alerta que eventos serían bloqueados. La característica de modo transparente es equivalente al modo de simulación; siempre que el equipo este en línea, pero sin bloquear tráfico. El sistema sólo alerta qué eventos serían bloqueados si estaría en producción.
	El equipo deberá permitir la configuración de modo transparente para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo y VLAN ID (se aceptarán soluciones que no consideren VLAN ID como un parámetro para manejar políticas durante el despliegue inicial, siempre que exista el compromiso de actualizar el sistema para incluir esta funcionalidad durante el primer trimestre de operación).
	El equipamiento soportará el bloqueo dinámico de intrusos pudiendo bloquear el tráfico del ataque a partir de la dirección IP y puerto del atacante, dirección IP y puerto del atacado o una combinación de ambos por un período específico de tiempo a partir de un ataque detectado. Deberá ser posible visualizar las conexiones bloqueadas y remover las reglas automáticas de bloqueo en cualquier momento.
	Soportará funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
	Soportará combinación de las modalidades IDS (pasivo) y IPS (en

Característica	Descripción
	línea) dentro de un mismo equipo.
Manejo de protocolos	Capacidad de identificar y bloquear tráfico de aplicaciones instant messenger y P2P.
	Análisis de tráfico de voz sobre IP.
	Deberá tener módulos de prevención de spyware, impidiendo la instalación de módulos de spyware; el cual podrá estar basado en firmas u otro mecanismo.
Gestión de políticas	Deberá asegurar que se manejen políticas por dispositivo, puerto, VLAN tag, IP y rango de IP's.
Capacidades L2	El producto deberá soportar trabajar en capa 2 como Bridge.
	Deberá soportar monitoreo de VLANs, incluyendo frames 802.1q.
Capacidades L3	Deberá soportar monitoreo de IPv6.
Certificaciones	El producto ofertado debe de contar la Certificación de NSS Group u otros
Detección de amenazas	Deberá incluir mecanismo para personalizar firmas.
	Deberá soportar monitoreo stateful inspection.
	La detección de ataques deberá ser independiente al sistema operativo.
	Deberá permitir la detección de comportamientos de WORM.
	La solución deberá permitir la detección de comportamientos malicioso, propagación de gusanos y ataques dentro de la red.
	Deberá poder detectar patrones de tráfico que sean diferentes a comportamientos predeterminados.
	El equipo deberá poder reconocer cambios abruptos de tráfico.
	Deberá poder detectar ataques de red y amenazas como spyware, phishing, troyanos y otros tipos de malware.

ANEXO E
EQUIPAMIENTO DE COMUNICACIÓN Y DE SEGURIDAD UTILIZADOS

Tabla E.1 Switch de Núcleo Cisco Catalyst 6509 Enhanced (Fuente: Ref: [17])

Característica	Descripción
Interfaces y puertos	El equipo soporta 20 interfaces de 10Gbps.
	El equipo incluye 48 puertos 10/100/1000 BaseT RJ45.
	04 puertos Gigabit Ethernet, 1000BaseSX
	Switch fabric instalado y operativo de 720 Gbps Tasa de envío de 30 Mbps instalados y operativos, escalable al menos hasta 300 Mbps, tanto en Capa 2 como en Capa 3.
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT, IEEE 802.3ae.
	LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del switch del mismo tipo y velocidad
Funcionalidades en capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Soporta IPv4 e IPv6.
	Multicast IGMPv1, v2 y v3 y PIMv1 y v2.
Funcionalidades en Capa 2	Soporta 4,000 VLAN's, VLAN trunk IEEE 802.1Q.
	Soporta 64 000 direcciones MAC
	Soporta Spanning Tree IEEE 802.1d así como RST 802.1w y MST 802.1s.
Redundancia soportadas en	- Módulo de procesamiento o Supervisor - Switch Fabric La redundancia de estos elementos opera de manera que ante la falla de uno, el redundante garantice que el equipo continuará operando al 100%, tanto en su capacidad como en sus funcionalidades en capa 2 y 3. Todas las tarjetas de interfaz y administración son Hot-Swap.
Soporte de Calidad de Servicio	IEEE 802.1p QoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP
	Limitación de ancho de banda basada en direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones IP de origen y destino y puertos TCP/UDP.
	Soporta autentificación 802.1x, con asignación dinámica de VLAN.
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2 y SCP.
	Soporta mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como “MAC Address Flooding”,

Característica	Descripción
	"VLAN. Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
Mecanismos de gestión	Puerto de consola para gestión local
	Soporte de Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporta SNMP v2 y v3
	Soporta RMON
	Soporta protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporta protocolos NTP, DHCP, DNS.
	Soporta "port mirroring" por puerto o grupo de puertos y por VLAN.
	Soporta multiples sesiones de "port mirroring" así como "port mirroring" remoto.
Otros	Fuente de poder con alimentación a 220Vac 60Hz. Montable en rack 19" Software actualizable.

Figura E.1 WS-C6509-E (Fuente: Ibídem)

Tabla E.2 Switch de distribución Cisco Catalyst 3560**G**-48PS (Fuente: Ref. [18])

Característica	Descripción
Interfaces y puertos	48 puertos 10/100/1000 Autosensing con PoE IEEE 802.3af.
	04 puertos Gigabit modulares GBIC o SFP, con soporte de interfaces 1000BaseSX, 1000BaseLX y 10/100/1000BaseT.
	Switch Fabric de 32 Gbps.
	Tasa de envío de 38.7 Mpps en Capa 2 y Capa 3.
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT.
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda

Característica	Descripción
	usar cualquier puerto del mismo tipo y velocidad.
Funcionali-dades capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Capacidad de ampliación a IPv6 sin cambio de hardware
	Multicast IGMPv1, v2 y v3 Snooping, con posibilidad de agregar PIMv1, PIMv2 y DVMRP sin cambio de hardware.
Funcionali-dades capa 2	1024 VLANs. VLAN trunk IEEE 802.1Q.
	12000 direcciones MAC.
	Spanning Tree IEEE 802.1d así como RST 802.1w y MST 802.1s.
Soporte de Calidad de Servicio	IEEE 802.1p QoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP.
	Limitación de ancho de banda basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	Soporta autentificación 802.1x, con asignación dinámica de VLAN.
	Asignación dinámica de filtros por usuario vía 802.1x.
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2, SSL y SCP.
	Soporta mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como “MAC Address Flooding”, “VLAN” “Hopping”, “DHCP Rogue Server”, “ARP Poisoning” y “IP Spoofing”.
Mecanismos de gestión	Puerto de consola para gestión local
	Soporte de Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporta SNMP v2 y v3
	Soporta RMON
	Soporta protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporta protocolos NTP, DHCP, DNS.
	Soporta “port mirroring” por puerto o grupo de puertos y por VLAN.
	Soporta múltiples sesiones de “port mirroring” así como "port mirroring" remoto.
	El puerto de monitoreo permite colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de

Característica	Descripción
	sesiones TCP a través del mismo puerto (puerto bidireccional).
Otros	Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante. Montable en rack 19" Software actualizable.

Figura E.2 Imagen del WS-C3560**G**-48PS-S (Fuente: Ibídem)

Tabla E.3 Switch de Acceso Cisco Catalyst 3560-48PS (Fuente: Ibídem)

Característica	Descripción
Interfaces y puertos	48 puertos 10/100 Autosensing con PoE IEEE 802.3af.
	04 puertos Gigabit modulares GBIC o SFP, con soporte de interfaces 1000BaseSX, 1000BaseLX y 10/100/1000BaseT
	Switch Fabric de 32 Gbps.
	Tasa de envío de 13.1 Mpps en Capa 2 y Capa 3.
Estándares relacionados	IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000Base.
	Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
Funcionalidades capa 3	Enrutamiento entre VLANs.
	Enrutamiento estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
	Capacidad de ampliación a IPv6 sin cambio de hardware
	Multicast IGMPv1, v2 y v3 Snooping, con posibilidad de agregar PIMv1, PIMv2 y DVMRP sin cambio de hardware.
Funcionalidades capa 2	1024 VLANs. VLAN trunk IEEE 802.1Q.
	12000 direcciones MAC.
	Spanning Tree IEEE 802.1d así como RST 802.1w y MST 802.1s.
Soporte de Calidad de Servicio	IEEE 802.1p QoS.
	Cuatro colas de salida por puerto.
	Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	DSCP.
	Limitación de ancho de banda basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
Mecanismos de Seguridad	Seguridad por puerto en base a la dirección MAC.
	Filtros aplicables por puerto y por VLAN.
	Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
	Soporta autentificación 802.1x, con asignación dinámica de VLAN.
	Asignación dinámica de filtros por usuario vía 802.1x.

Característica	Descripción
	Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
	6 niveles de privilegios de acceso para administración por consola o por Telnet.
	Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2, SSL y SCP.
	Soporta mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como "MAC Address Flooding", "VLAN", Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
Mecanismos de gestión	Puerto de consola para gestión local
	Soporta Telnet, http y SSHv2 para gestión remota
	Registro de eventos vía Syslog
	Soporta SNMP v2 y v3
	Soporta RMON
	Soporta protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
	Soporta protocolos NTP, DHCP, DNS.
	Soporta "port mirroring" por puerto o grupo de puertos y por VLAN.
	Soporta multiples sesiones de "port mirroring" así como "port mirroring" remoto.
	El puerto de monitoreo permitir colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de sesiones TCP a través del mismo puerto (puerto bidireccional).
Otros	Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante. Montable en rack 19" Software actualizable.

Figura E.3 WS-C3560-48PS-S (Fuente: Ibídem)

Tabla E.4 Cisco Works LAN Management Solution (Fuente: Ref. [19])

Descripción del Software de Administración CWLMS-3.0-100-K9
- La aplicación permite administrar los dispositivos de distribución y acceso, desde cualquier lugar de la intranet/internet. - Puede realizar múltiples tareas de configuración sin usar comandos de interfaz de línea de comandos. - Permite aplicar acciones a múltiples dispositivos y puertos al mismo tiempo para configuraciones de VLAN y Calidad de Servicio (QoS), supervisión de enlaces, reportes de tráfico y actualizaciones de software.

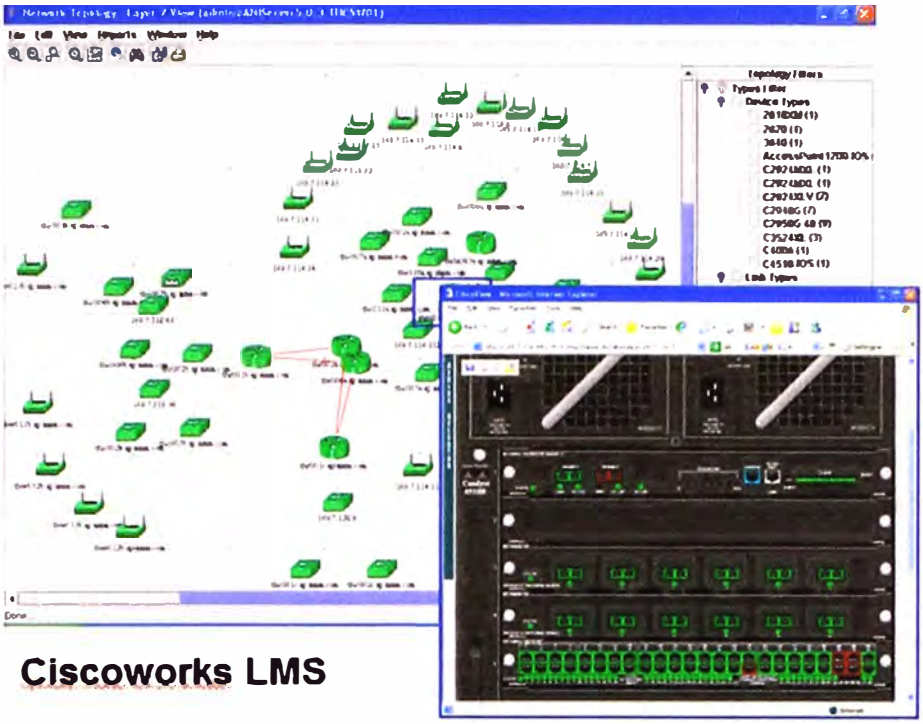

Figura E.4 Vistas del CWLMS-3.0-100-K9 (Fuente: Ibídem)

Tabla E.5 Firewall Cisco ASA 5510 (Fuente: Ref. [v])

Característica	Descripción
Capacidades	El equipo incluye capacidad de firewall con una inspección de paquetes de 300 Mbps.
	Soporta de 50,000 conexiones concurrentes.
	Incluye 5 Puertos Fast Ethernet y 2 Gigabit Ethernet
	Sistema Operativo en codigo cerrado y certificado.
	Chasis diseñado (Tipo Apliance) para su instalación en rack.
Capacidades L2	Incluye manejo de 802.1q para el manejo de Virtual LANs.
Capacidades L3	Incluye manejo de IGMPv2, Stub multicast routing, y configuración de rutas multicast.
	Incluye manejo de filtros para trafico multicast.
	Incluye manejo de NAT y PAT sobre multicast source address.
	Soporta algoritmos de ruteo dinámico como RIP y OSPF.
Inspección de tráfico y soporte de protocolos	El equipo permite inspección detallada tráfico web, para controlar comandos, URI, MIME, anomalías del protocolo, y cumplimiento de RFC.
	Control de aplicación tunel sobre port 80: mensajeria instantánea, aplicaciones p2p, tunelización, entre otros.
	Incluye manejo de NAT, PAT, y mapeo de múltiples hosts internos en una dirección global para servicios TCP y UDP.
	Incluye manejo de PAT para trafico ESP, H.323v3, H.323v4, SIP.
	Incluye manejo de inspección de estado para tráfico ICMP via NAT.
	Incluye manejo DHCP como relay, server y cliente.
	Soporta Inspección de Estado para: - Protocolos Básicos: DNS, FTP, HTTP, ICMP, IPSEC, PPTP, SMTP,TFTP, ESMTP

Característica	Descripción
	- Voice over IP: CTIQBE, H.323v3/4, TAPI/JTAPI, MGCP, SIP - Multimedia: Netshow, RTSP, VDO Live - Database y Directory: ILS, LDAP, Sun RPC, - Management: ICMP, RSH, SNMP
Métodos de cifrado	Incluye mecanismos de encriptación DES, 3DES y AES, 170 Mbps AES.
	Incluye manejo de IPSec y SSL para el acceso remoto.
	Permite trabajar en modo cluster de vpn tanto para IPSec como SSL con otros equipos de las mismas características.
Soporte de certificados digitales	Incluye soporte de certificados digitales emitidos por la entidad de certificación DST (Digital Signature Trust) y el uso de tokens de seguridad para la autenticación de conexiones VPN SSL.
Soporte IPSec	Incluye manejo de tuneles IPSec red a red, para conexión con routers, firewalls similares, o equipos vpn en configuraciones donde las IPs de los equipos remotos: son estáticas o dinámicas.
	Incluye soporte de 250 tuneles IPSec concurrentes.
Soporte VPN SSL	La solución permite funcionar como un redireccionador de puertos a través de protocolo SSL.
	En SSL el usuario remoto ingresa mediante un navegador WEB, permitiendo que acceda a diferentes recursos de la intranet utilizando distintos tabs definidos en su portal inicial. No es necesaria la instalación manual de ningún software en la PC del cliente.
	En SSL permite el ingreso de usuarios mediante VPN L3. Esto es, asignando al usuario externo una nueva dirección IP y encapsulando, en forma transparente para el usuario y la aplicación, cualquier protocolo a través del túnel.
	El Software cliente VPN proporcionado permite trabajar sobre equipos NAT, permitiendo split ip y dns.
Gestión de políticas	Posee un modelo de políticas de seguridad basada en usuarios y/o grupos, esto, en forma granular.
	Permite asignar recursos a los usuarios dependiendo del nivel de autorización, incluyendo control granular sobre URL permitidos.
	Permite la autenticación de usuarios a través de tokens, y certificados X.509
Calidad de servicio	Priorización y limitación de ancho de banda por aplicación atravesando el equipo.
Administración	Capacidad de administración y gestión basada en los protocolos telnet, SSH, https, radius.
	Cuenta con una interface WEB gráfica interna, accesible en modo seguro, que permita la configuración de las funciones de firewall-vpn.
	Incluye el manejo de niveles administrativos para la operación y manejo del equipo, mínimo 12.
	Deberá incluir mecanismos de inspección de estado para http, ftp, smtp, icmp, tcp, y udp en IPv6.
	El equipo deberá incluir protocolos de administración seguros: https, sshv2, SNMPv2c, NTP v3.
	El equipo debe enviar alarmas vía Syslog.
	Soporta multiples softwares y configuraciones, sobre el equipo como backups o restauración ante cambios.
Alta disponibilidad	Soporta alta disponibilidad active/active y active/standby, fail over

Figura E.5 Firewall Cisco ASA 5510-SSL50-K9 (Fuente: Ibídem)

Tabla E.6 Intrusion Prevention System Cisco IPS 4240 (Fuente: Ref. [x])

Característica	Descripción
Capacidades	Solución de hardware y software basado en appliance, el cual realiza monitoreo y prevención en línea.
	Cuenta con 4 interfaces 10/100/1000 en cobre y proporciona un throughput de 250 Mbps para el análisis del tráfico.
	Cuenta con un puerto de administración ethernet 10/100, adicional a las interfaces de análisis.
	Las Interfaces utilizadas para sensar tráfico trabajan en modo stealth, sin stack de TCP/IP en la interfaz.
	Montaje físico en rack 19".
	Alimentación 220V
Modos de trabajo	El monitoreo es transparente para los usuarios.
	El equipo puede configurarse en modo transparente; es decir, de prevención en línea, pero sin bloquear tráfico. El sistema sólo alerta qué eventos serían bloqueados. La característica de modo transparente es equivalente al modo de simulación; siempre que el equipo este en línea, pero sin bloquear tráfico. El sistema sólo alerta qué eventos serían bloqueados si estaría en producción.
	El equipo permite la configuración de modo transparente para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo y VLAN ID.
	El equipamiento soporta el bloqueo dinámico de intrusos pudiendo bloquear el tráfico del ataque a partir de la dirección IP y puerto del atacante, dirección IP y puerto del atacado o una combinación de ambos por un período específico de tiempo a partir de un ataque detectado. Es posible visualizar las conexiones bloqueadas y remover las reglas automáticas de bloqueo en cualquier momento.
	Soporta funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
	Soporta combinación de las modalidades IDS (pasivo) y IPS (en línea) dentro de un mismo equipo.
Manejo de protocolos	Capacidad de identificar y bloquear tráfico de aplicaciones instant messenger y P2P.
	Análisis de tráfico de voz sobre IP.
	Cuenta con módulos de prevención de spyware, impidiendo la instalación de módulos de spyware.
Gestión de políticas	Asegura que se manejen políticas por dispositivo, puerto, VLAN tag, IP y rango de IP's.
Capacidades	Soporta trabajar en capa 2 como Bridge.

Característica	Descripción
L2	Soporta monitoreo de VLANs, incluyendo frames 802.1q.
Capacidades L3	Soporta monitoreo de IPv6.
Certificaciones	Cuenta con la Certificación de NSS Group
Detección de amenazas	Incluye mecanismos para personalizar firmas.
	Soporta monitoreo stateful inspection.
	La detección de ataques es independiente al sistema operativo.
	Permite la detección de comportamientos de WORM.
	La solución permite la detección de comportamientos maliciosos, propagación de gusanos y ataques dentro de la red.
	Permite detectar patrones de tráfico que sean diferentes a comportamientos predeterminados.
	Puede reconocer cambios abruptos de tráfico.
	Puede detectar ataques de red y amenazas como spyware, phishing, troyanos y otros tipos de malware.

Figura E.6 IPS-4240-K9 (Fuente: Ibídem)

ANEXO F
GLOSARIO DE TÉRMINOS

ANSI	Instituto Nacional Estadounidense de Estándares
AP	Puntos de acceso inalámbrico
Backbone	Red principal de comunicaciones
Backup	respaldo
Core	Núcleo
Datastore	Volúmenes de almacenamiento.
DHCP	Dynamic Host Configuration Protocol-Configuración Dinámica de Equipo
DMZ	Zona desmilitarizada.
DNS	Domain Name Server
DoS	Denegación de Servicio.
DST	Digital Signature Trust
EIA	Alianza de Industrias Electrónicas
EOSL	End of Service Life – Fin de Vida de Servicio)
FC	Fibre Channel
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol - Protocolo de Mensajes de Control de
IDS	Intrusion Detection System- - Sistema de detección de intrusos
IEEE	Instituto de Ingenieros Eléctrica y Electrónica
IETF	Internet Engineering Task Force
INDECOPI	Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual.
IP	Protocolo de Internet.
IPS	Intrusion Prevention System – sistema de prevención de intrusión.
LAN	Red de Área Local.
LPAR	Particionamiento.
LUN	Logical Unit Number
NAT	Network Adress TranslationInternet
TIA	Asociación de la Industria de Telecomunicaciones
PDU	Power Distribution Units
RAID	Redundant Array of Independent Disks.
RFC	Request for Comment.
SAN	Storage Area Network - Red de almacenamiento
SSL	Secure Socket Layer
SPF	Single Point of Failure - puntos únicos de falla
TCP	Protocolo de Capa de Transporte
UDP	Protocolo de Datagrama de Usuario

UPS	Sistema de potencia ininterrumpida
VPN	Red Virtual Privada)

BIBLIOGRAFÍA

[1] Página Institucional de INDECOPI. "Sobre el INDECOPI". http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=600

[2] Ibídem, "Misión y Visión de INDECOPI".

[3] INDECOPI, "Bases Integradas", Licitación Pública-0003-2007-INDECOPI .

[4] Ibídem, "Anexo 2: Especificaciones Técnicas".

[5] IBM, Blade Center, http://www-03.ibm.com/systems/bladecenter/

[6] VMware, "Virtual Infrastructure". http://www.vmware.com/virtualization/virtual-infrastructure.html

[7] IBM BladeCenter E, http://public.dhe.ibm.com/common/ssi/ecm/en/bld03018usen/BLD03018USEN.PDF

[8] IBM BladeCenter HS21, http://www.spectra.com/pdfs/BC-HS21.PDF

[9] IBM System X 3550 M2, http://www-05.ibm.com/es/id/resources/System_x_3550_M2.pdf

[10] IBM SystemP 5 – 520, http://www.greenbell.com/korean/brochure/pSeries/entrylevel/p5_520_Express&p5520Q_Express.pdf

[11] IBM DS4700, http://www.spectra.com/pdfs/ds4700.pdf; IBM EXP810, http://media.techdata.fr/000TDF2/BS3683/docs/EXP810.pdf

[12] IBM TS3100, http://public.dhe.ibm.com/common/ssi/ecm/en/tsd03015usen/TSD03015USEN.PDF

[13] VMware Vsphere Enterprise and Enterprise Plus Editions, http://www.vmware.com/files/pdf/products/vsphere/VMware-vSphere-Enterprise-DataSheet-DS-EN.pdf

[14] Javvin Technologies Inc.," Network Protocols Handbook", 2004, Segunda Edición. Pag. 228

[15] Cisco, "CCNA 4.0 Exploration, LAN Conmutación y conexión inalámbrica", Módulo 1.

[16] Cisco, "CCNA 3, Módulo 1 – Conceptos básicos sobre, Capítulo 9.

[17] Ibídem, Capítulo 5 (sección 5.1.2)

[18] Cisco, "CCNA 3, Módulo 3 - Principios básicos de Conmutación y enrutamiento intermedio v3.1", Capítulo 8.

[19] Ibídem, Capítulo 9.

[20] Referencia [16], Capítulo 10 (sección 10.1.3)

[21] Cisco Catalyst Series 6500 y 6500-E

http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916.pdf

[22] Cisco Catalysy 3560 Series
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.pdf

[23] Cisco Works LAN Management CWLMS-3.0-100-K9
http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/data_sheet_c78-534877.pdf

[24] "DHCP, Dynamic Host Configuration Protocol", Referencia [14], página 15.

[25] Cisco ASA 5510-SSL50-K9
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.pdf

[26] "NAT, Network Address Translation", Referencia [14] página 27. NAT: Network Address Translation

[27] IETF, Traditional IP Network Address Translator (Traditional NAT)
http://www.apps.ietf.org/rfc/rfc3022.html

[28] RFC 1918 - Asignación de direcciones para Internet privadas (Address Allocation for Private Internet) http://www.rfc-es.org/rfc/rfc1918-es.txt

[29] Cisco IPS-4240-K9
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/ps9157/product_data_sheet09186a008014873c.pdf

[30] ANSI, 568-B "Commercial Building Telecommunications Cabling Standard: General Requirements".
http://webstore.ansi.org/FindStandards.aspx?SearchString=CSA+T568&SearchOption=0&PageNum=0&SearchTermsArray=null|CSA+T568|null

[31] ANSI, 569-B "Commercial Building Standard for Telecommunications Pathways and Spaces". http://www.belden.com/pdfs/Techpprs/2030.pdf.

[32] ANSI, 606(A), "The Administration Standard for the Telecommunications Infrastructure of Commercial Buildings".
http://www.belden.com/pdfs/Techpprs/2060.pdf

[33] TIA, J-STD-607 "A Commercial Building Grounding and Bonding Requirements for Telecommunications", http://standardsdocuments.tiaonline.org/tia-j-std-607-a.htm

[34] ANSI, 526-14A "Measurement of Optical Power Loss of Installed Multimode Fiber Cable Plant", http://standardsdocuments.tiaonline.org/tia-526-14-a-ofstp-14.htm.

[35] ANSI, 758(A) "Customer-Owned Outside Plant Telecommunications Cabling Standard". http://standardsdocuments.tiaonline.org/tia-758-a.htm.

[36] ISO/IEC, 11801 "Information technology – Generic cabling for customer premises"

[http://webstore.iec.ch/preview/info_isoiec11801%7Bed2.0%7Den.pdf]

[37] ISO/IEC, 14763-1 "Information technology – Implementation and operation of customer premises cabling – Part 1: Administration".
http://webstore.iec.ch/preview/info_isoiec14763-1%7Bed1.0%7Den.pdf

[38] ISO/IEC, 14763-2.- "Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation".
http://webstore.iec.ch/preview/info_isoiec14763-2%7Bed1.0%7Den.pdf.

[39] ISO/IEC, 14763-3 "Information technology – Implementation and operation of

customer premises cabling – Part 3: Testing of optical fibre cabling". http://webstore.iec.ch/preview/info_isoiec14763-3%7Bed1.0%7Den.pdf

[40] IEC, 61935-1, "Specification for the testing of balanced and coaxial information technology cabling. Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards". http://webstore.iec.ch/preview/info_iec61935-1%7Bed3.0%7Den.pdf

[41] "ICMP, Internet Message Control Protocol", Referencia [14], página 68.

[42] RFC792, "Protocolo de Mensajes de Control Internet", http://www.rfc-es.org/rfc/rfc0792-es.txt

[43] RFC950, "Procedimiento Estándar para División en Subredes en Internet" http://www.rfc-es.org/rfc/rfc0950-es.txt

[44] Tipo de cambio oficial, http://www.sunat.gob.pe/cl-at-ittipcam/tcS01Alias

[45] RAID Iomega® Storcenter™, "px12-350r Storage Provisioning and RAID Migration Configuration Guide", http://www.backupworks.com/pdf/px12350r_provisioning_raid_migration.pdf