ESTUDIO DE LA EVOLUCIÓN DE LA RED DE COMUNICACIONES DE UN OPERADOR LOGÍSTICO

PROYECTO DE FINAL DE CARRERA ETSETB

Joan Herráez Balanzat

DIRECTOR DE PROYECTO

Joan Francesc Marchan García-Moreno

A mi familia, con cariño

Desde diferentes vertientes, la globalización y deslocalización han tenido como consecuencias entre otras el incremento exponencial de mercadería, personas y como no información.

Por otro lado la necesidad de conseguir una mayor eficiencia de los sistemas de transporte al tiempo de mantener un respeto al medio ambiente ha provocado que en la última década del siglo pasado y durante lo que llevamos de la actual hayan proliferado diferentes sistemas de operadores logísticos, centros de intercambios modales, almacenes reguladores…

Una de las herramientas sin duda para conseguir mayor rendibilidad y respetabilidad con el medio ambiente son las TICs, que se van a aplicar a los procesos de la cadena de suministro.

El proyecto propuesto es un estudio de mejoras de un operador nacido hace 15 años que ha ido creciendo sin ningún orden o planificación y que busca incorporar nuevas aplicaciones y mejoras de las que hay en la actualidad.

ABSTRACT

Estudio de la implantación de nuevas tecnologías en el sí de un operador logístico, al menos se pretende una rendibilidad y una eficiencia al tiempo que seguridad y respeto al medio ambiente.

RESUMEN

Este proyecto surge a raíz de la aparición de nuevas posibilidades tecnológicas en el campo de las infraestructuras logísticas. El documento contiene una descripción actual de un operador logístico y realiza una propuesta de innovación tecnológica a partir de las debilidades detectadas. Se define que funciones tiene actualmente un operador y se coge como punto de partida uno en concreto.

A partir de aquí se define primero la propuesta de red corporativa realizando el dimensionado de voz y datos para definir el esquema de red en la que se integran voz y datos. En el cuarto capítulo se propone un sistema de posicionamiento y control de flota que compone el operador con el objetivo de automatizar el proceso de entrega y trazar mediante aplicaciones de control y posicionamiento de la flota las rutas más rápidas y eficientes. En el quinto capítulo se definirá una solución de video vigilancia y centralización de alarmas que permitirá mecanizar y centralizar la seguridad de todas las sedes en la sede principal del operador.

Posteriormente se realizará un plan de implantación en el tiempo de todas las innovaciones propuestas en el que se detallará los pasos realizados en la puesta en marcha de las propuestas del presente proyecto.

En el capítulo siete se define un plan de explotación, mantenimiento y monitorización basados en los principios ITL de buenas prácticas. Se desarrollan los procesos y funciones necesarios para la gestión de la nueva infraestructura. En el octavo capítulo se ha detallado un plan de contingencia que servirá para amortiguar el impacto de las posibles fallidas tecnológicas en el desarrollo del negocio.

Por último se realiza un análisis del impacto económico que tendrá este despliegue tecnológico en el operador y se sacan conclusiones.

ÍNDICE

Estudio de la evolución tecnológica de la red de comunicaciones de un operador logístico

Estudio de la evolución tecnológica de la red de comunicaciones de un operador logístico.

1. Definición de un operador logístico

- “operador logístico es aquella empresa que por encargo de su cliente diseña los procesos de una o varias fases de su cadena de suministro (aprovisionamiento, transporte, almacenaje, distribución e, incluso, ciertas actividades del proceso productivo), organiza, gestiona y controla dichas operaciones utilizando para ello infraestructuras físicas, tecnología y sistemas de información, propios o ajenos, independientemente de que preste o no los servicios con medios propios o subcontratados. En este sentido, el operador logístico responde directamente ante su cliente de los bienes y de los servicios adicionales acordados en relación con éstos y es su interlocutor directo”. Consultora *Deloitte*

Un operador logístico es la organización que coordina todas las actividades de dirección del flujo de los materiales y productos que necesita una empresa, desde la fuente de suministro de los materiales hasta su utilización por el consumidor final.

Son funciones de un operador logístico las siguientes:

- Procesado de pedidos: Actividades relativas a la recogida, comprobación y transmisión de órdenes de compra.
- Manejo de materiales: Determina que medios materiales y procedimientos se han de utilizar para mover los productos dentro de los almacenes y entre estos y los locales de venta.
- Embalaje: Decidir que sistemas y formas de protección va a utilizar para sus productos.
- Transporte de los productos: Decidir medios de transporte a utilizar y elaboración de los planes de ruta.
- Almacenamiento: Encargado de seleccionar el emplazamiento, la dimensión y las características de los almacenes.
- Control de inventarios: Determinación de la cantidad de productos que se deben tener disponibles para entregar a un posible comprador. También ha de establecer la periodicidad de los pedidos.

- Servicio al cliente: Determina donde van a estar los puntos de servicio y que medios materiales y que personas hay que tener en cada punto para atender correctamente al cliente.

Todas estas funciones deben realizarse con el mínimo coste posible y teniendo en cuenta todas las funciones.

2. Operador a analizar

Para realizar el estudio de mejoras de los operadores logísticos se va a partir de uno en concreto que servirá para ir presentando las propuestas de innovación tecnológica en automatización y gestión de procesos, integración de los servicios o posicionamiento y control de flotas. Se va a detallar su estructura para encontrar sus puntos débiles y así poder hacer un proyecto de innovación tecnológica.

2.1. Estructura tecnológica actual del operador a analizar

El operador a estudiar es una empresa dedicada a la producción y distribución diaria de producto variado a través de toda la Península Ibérica. Dispone de una sede principal en Barcelona y 2 nodos logísticos en Almería y Salamanca además de 6 almacenes con oficina de atención al cliente, en ciudades grandes y 24 almacenes con oficinas más pequeñas distribuidos a lo largo del territorio peninsular.

La empresa reparte producto variado, entre ellos producto caduco o fresco, cuya vida es corta. Esto obliga a que los plazos de distribución y entrega se ajusten al máximo. La logística en este tipo de productos es igual sino más importante que la propia producción del producto.

Actualmente el operador cuenta con aproximadamente mil camiones distribuidores desde 2 nodos logísticos y los 30 almacenes repartidos por toda la geografía española y desde allí a todos los negocios que lo soliciten/contraten. Además tiene un edificio corporativo en Barcelona donde se centralizan los departamentos comerciales y la dirección de la empresa.

El operador dispone de una red tecnológica heterogénea, debido al crecimiento ad-hoc de la red de datos que no es resultado de unos pasos lógicos como son el análisis de las necesidades, elaboración de un diseño que dé respuesta a estos requisitos y una implementación. Se han ido creando de forma paulatina en base

a demandas de ancho de banda y necesidades de conectividad interna dentro de cada sede, y externa entre sedes

A nivel interno, cada sede ha solucionado sus necesidades de forma independiente al resto

Sólo las sedes más grandes disponen de departamento técnico propio que se encarga de gestión, creación y mantenimiento de sus redes. Por el contrario, las sedes pequeñas (menos de 10 trabajadores) tienen externalizado el servicio de gestión y mantenimiento de las redes de voz y datos. Sin embargo, este servicio no lo reciben de manera integrada, cada sede tiene un contrato individual con su proveedor de soluciones de Tecnologías de la Información TI, concretamente con empresas geográficamente ubicadas en las adyacencias de las mismas. En ambos casos, tanto en sedes pequeñas como en medianas y grandes, el mantenimiento, la gestión y operación de los sistemas de telecomunicaciones e informáticos conlleva a un gasto muy grande que se acentúa a medida que la empresa crece.

La red corporativa está a día de hoy en la sede central. Cada almacén tiene una LAN de capacidad reducida. Los tres nodos logísticos situados en Almería, Barcelona y Salamanca se encuentran conectados en estrella Frame Relay mediante circuitos virtuales permanentes (PVC) mientras que los almacenes pequeños tienen contratadas conexiones ADSL o RDSI. El intercambio de información se realiza por medio de Internet (email, ftp…). La generación y el manejo de albaranes se realiza de manera manual y carece de servicios multimedia.

2.2. Deficiencias de la estructura actual

La topología actual mediante Frame Relay para la interconexión de las sedes principales ofrece un mínimo de calidad de servicio ya que se basa en circuitos virtuales. No obstante, los anchos de banda que garantizan se están quedando cada vez más cortos dificultando la implantación de nuevos servicios de red; además el precio de estas interconexiones es muy elevado en relación con el ancho de banda ofrecido lo que lo convierte en una opción poco rentable. Al tener accesos diferentes para la red de empresa que para el acceso a internet, existe un control para internet que reduce el uso de ancho de banda para las conexiones a la red corporativa. El operador está conectado a la red pública de telefonía a través de enlaces primarios RDSI (PRI). Estos enlaces garantizan la accesibilidad de cada sede desde la red pública, siendo además el único camino existente para realizar llamadas entre la mayoría de sedes.

Inexistencia de mecanismos fiables de redundancia para su conexión a la red pública a caída del nodo central supondría una caída global de la red en estrella, que sólo se sustentaría con enlaces RDSI (BRI) de back up.

Por otro lado la previsión del incremento del volumen de tráfico entre las oficinas superará la capacidad de los enlaces debido a los nuevos servicios de videoconferencia o video vigilancia además de no dejar margen de crecimiento. La tecnología Frame Relay es poco flexible ante la posibilidad de interconexión de nuevas sedes.

Cada una de las sedes pequeñas maneja líneas RDSI básicas (BRI) para interconexión telefónica interna de manera que ante una caída en el enlace, la sede afectada pierde conectividad con el exterior.

La sede central y los 2 nodos logísticos no están interconectados con los almacenes, cada uno de ellos maneja entornos informáticos y bases de datos no unificados. La gestión y generación de albaranes de recepción de pedidos se realiza de forma manual lo cual obliga a dedicar un tiempo al envío de éstos a final del día.

Retrasos en la recepción de la información en la central a causa de:

- Plazos prolongados entre la emisión del albarán y la recepción del mismo en la central.
- Empleo de gran cantidad de tiempo en las tareas de introducción de los albaranes en el sistema informático y la corrección de errores.

- Ausencia de algún sistema que permita controlar y gestionar las rutas que siguen los camiones.

Pérdida de tiempo en la gestión (solicitud, acopio y distribución) de la documentación exigida por los clientes y la Administración Central; Además de la dificultad que existe para la gestión de red al existir tanta diversidad de tecnologías.

. El haber crecido de una manera tan desordenada y dificulta enormemente las tareas de gestión y mantenimiento de las sedes debido a su poca homogeneidad.

Existe un control de seguridad externalizado. Carecen de un Plan de Contingencia y de uno de continuidad que asegura la continuidad del negocio en caso de caída de alguno de los elementos de red. Realizan copias de seguridad sin una política determinada y en el mismo PC/servidor de manera que un accidente/incidencia en aquel equipo puede provocar una pérdida importante de datos.

Para llevar a cabo la gestión explotación y el mantenimiento de los servicios e infraestructura del operador logístico no se sigue ningún procedimiento y el servicio de atención al usuario se realiza siempre de manera telefónica al personal de IT. Tampoco disponen de ningún historial de incidencias al que poder consultar.

2.3. Necesidades actuales del operador logístico (gestión de flotas, infraestructura de red…)

A partir de la estructura actual analizada se han detectado lagunas tecnológicas en el operador, el cual debe dotarse de una infraestructura que además de situarlo en una posición competitiva le permita estar preparado para las soluciones del futuro.

Trazabilidad y calidad de servicio son los términos que se imponen en el sector logístico de gran consumo y particularmente en el de alimentación; (producto más crítico del operador).

El primer término, apoyado por la normativa comunitaria que implica a los operadores en el control y seguimiento de la cadena de suministro desde primeros del año 2005. La calidad de servicio es consecuencia de ello, puesto que la trazabilidad, es decir, el seguimiento del producto desde el origen hasta el consumidor, es responsabilidad de fabricantes y distribuidores, aunque el operador logístico se sitúa

como factor fundamental en dicha cadena de suministro. Este Control total de la flota permitirá asegurar todos los pedidos, acelerar las gestiones, es decir ser más eficiente.

Otro punto importante es la de automatización y por tanto mejora del proceso logístico de las empresas. Esta mejora de los procesos se consigue mediante la aplicación de los “Sistemas móviles”, que se basan en nuevas tecnologías como telefonía móvil, redes inalámbricas o wifi. Estos sistemas permiten introducir en los canales de distribución mejoras sustanciales en la calidad y costo del servicio y en los procesos administrativos. Por ejemplo disponer en tiempo real información sobre el estado de los pedidos o localización de la flota de reparto y estado de las entregas; permite incrementar la eficacia en la toma de decisiones y hace posible la entrega del producto en el momento justo y adecuado.

Por último se debe actualizar sus redes corporativas para estar al día con las recomendaciones europeas actuales. Se deben integrar sus redes de voz y datos y así permitir nuevas aplicaciones relacionadas con el mundo multimedia, eso además de tener la ventaja de compartir infraestructura de acceso y transporte.

Esta integración de voz y datos debe sentar la base para actualizar la vigilancia del operador en sus edificios.

Por otro lado la implantación y por tanto dependencia tan grande de tecnología debe ir acompañada de un Plan de Contingencia del negocio que permita la prevención y continuidad en caso de que alguno de los activos de la red falle.

2.4. Previsión de nuevas aplicaciones y necesidades

A partir de las necesidades analizadas anteriormente, se van a exponer las soluciones tecnológicas que se han previsto con el objetivo de modernizar la infraestructura del operador. Estas soluciones se centran en la aplicación de las nuevas tecnologías que permitan la automatización y mejora de su proceso logístico. Para ello requieren:

- ✓ Realizar el diseño de una red corporativa a partir de la actual, que interconecte todas las sedes entre sí teniendo en cuenta parámetros como l las capacidades de tráfico de datos (BW) entre todas las sedes y con Internet, redundancia, QoS, disponibilidad, que se ajusten con las

necesidades actuales y futuras del operador. Integrar voz y datos en una infraestructura de electrónica de comunicaciones común y que contemple la implementación futura de soluciones multimedia (videoconferencia en PCs, Imágenes, tráfico de fotografías o e-learning y video vigilancia). Además uno de los factores clave en esta implementación será la priorización de datos en las horas punta de descarga de material en los almacenes, pues en ciertas horas estas descargas des de los dispositivos de datos (p.ej. PDA) deberán ser posibles y sobre todo priorizadas sobre cualquier otro tipo de dato.

- ✓ Solución para el control y localización de los camiones en todo momento durante el reparto, mediante dispositivos capaces de sincronizarse con los sistemas de información de la empresa, optimizando el funcionamiento de la misma. Proponer una solución GPS de seguimiento de flota, que brinde la ubicación de camiones de reparto en las rutas planificadas en tiempo real.
- ✓ Una solución que permita asignar a cada repartidor lo que está listo para ser distribuido cada día, y recibir de estos los documentos (albaranes) de lo que han repartido al final del día.
- ✓ Solución en almacenes y camiones que permita la eliminación del papel, es decir la digitalización de las bases de datos de los clientes además del registro de los albaranes mediante dispositivos móviles.
- ✓ Estandarización del sistema de atención al usuario, definición de un Service Desk centralizado que canalice todas las incidencias que aparezcan. Para llevar a cabo la explotación y el mantenimiento de los servicios e infraestructura del operador logístico se seguirán las mejores prácticas de ITIL para la definición de procesos de Gestión de TI.
- ✓ Realizar un plan de contingencia (Back-up, soluciones de indisponibilidad…).
- ✓ Implantación de un servicio de video vigilancia centralizado en una de las sedes principales.
- ✓ Implantación de un servicio de alarmas centralizado.

Es esencial que este plan de automatización del proceso logístico se realice con herramientas, plataformas y terminales que permitan compatibilizarse con las tecnologías actuales a la vez que permitan una línea de migración frente a nuevas tecnologías.

3. Solución para la red corporativa

Después de un análisis tanto tecnológico como de infraestructuras del operador, se ha realizado una propuesta de solución tecnológica que abarcará des del dimensionado de anchos de banda para voz y datos que se solicitará al operador de Telecomunicaciones hasta la estructura que tendrá cada uno de los puestos de trabajo de cada sede. Posteriormente se definirán las políticas de contingencia y estructura tanto del Centro de Procesamiento de Datos (a partir de aquí CPD); que es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización, es decir, el centro de datos; como del Disaster Recovery System (DRS), que es el centro de respaldo del CPD normalmente situado en otra localización.

El objetivo es interconectar todas las sedes mediante un Red Privada Virtual con ancho de banda garantizado basado en tecnología MPLS.

3.1. Solución sobre tecnología VPN/MPLS

La Red Privada Virtual (RPV), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, en este caso Internet.

La VPN nos permite interconectar las sucursales del operador logístico utilizando como vínculo la infraestructura de Internet. Se salvan las distancias físicas existentes entre las distintas sedes de la empresa y evita problemas derivados de no poder tener las BBDD centralizadas o replicar documentos tantas veces como sedes hay.

La tecnología MPLS se despliega en el núcleo de la red del proveedor de servicios, lo que le proporciona a este un mayor control sobre la calidad del servicio, la ingeniería de tráfico y la utilización del ancho de banda a la vez que reduce los requisitos a los equipos de comunicación de los clientes que se conectan a un servicio sobre MPLS. Como el tráfico VPN/IP no necesita de tunelización ni cifrado en los enlaces de usuario no tiene ningún requisito especial para los equipos de comunicaciones del cliente y no consume recursos caros adicionales como son la CPU de los routers o el ancho de banda en los enlaces.

De esta forma, MPLS para VPN/IP reduce considerablemente la complejidad y los problemas técnicos que se producen al aumentar o reducir el número de sedes

corporativas que participen en una VPN/IP, reduciendo los costes asociados y los plazos de puesta en marcha.

Los datos son codificados o cifrados e inmediatamente enviados a través de la conexión, para de esa manera asegurar la información y la contraseña que se esté enviando. Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

En cuanto a la utilización del protocolo MPLS (Multi Protocol Label Switching) es un método para enviar paquetes a través de la red usando información contenida en etiquetas añadidas a los paquetes IP.

Factores positivos de MPLS:

- ✓ El alto coste del equipamiento que supondría adoptar una nueva solución sobre ATM o WDM.
- ✓ Permite crear redes flexibles y escalables con un incremento en el desempeño y estabilidad.
- ✓ MPLS es similar a tener circuitos privados virtuales con QoS sobre una red IP con lo que ofrece retardos contratados extremo a extremo similares a los protocolos ATM orientados a conexión eso habilita la transferencia de la voz.
- ✓ Configuraciones de QoS diferenciadas según las necesidades de cada sede de la VPN. Mediante el etiquetado, MPLS ofrece priorización de paquetes y calidad de servicio según tipo de tráfico y la modalidad contratada al operador.;
- ✓ IP/MPLS permite además reserva de recursos y garantía de tráfico transportado.
- ✓ MPLS permitirá diferenciar entre las redes de voz, datos e Internet de la plantilla, centralizado en la sede de Barcelona.
- ✓ Permitiría integrar en una misma red servicios tanto de datos como de voz, telefonía IP con lo que significaría un ahorro de costes en cuanto al uso de RTB en cada centro para comunicaciones entre sedes.
- ✓ Direccionamiento IP privado, permitiendo nombrar cuantos dispositivos quiera implementar la empresa sin gastar recursos escasos como el direccionamiento IP público.
- ✓ Políticas centralizadas de seguridad mediante compartición de firewalls y servidores Internet en un único punto de la red privada

Debido a que el operador tiene sedes dispersas geográficamente por todo el territorio nacional, es necesario un diseño que diferencie claramente dos partes: la red de acceso y la red de transporte.

La red de transporte es la encargada de interconectar las sedes entre sí, la tecnología seleccionada es MPLS por sus capacidades de calidad de servicio y de creación de redes virtuales. Con esta red es posible crear una red virtual que conecta todas las sedes de forma transparente a los usuarios. Esto es necesario para que las comunicaciones de voz y datos entre sedes viajen de forma directa sin tener que pasar por Internet.

La red de acceso depende del ancho de banda utilizado por cada sede. Las sedes con necesidades reducidas accederán mediante ADSL con unos SLAs (Service Level Agreement) garantizados y las sedes con requisitos mayores utilizarán enlaces de fibra que permiten anchos de banda superiores y con SLAs concretos.

A nivel LAN cada sede tiene un diseño particular pero en general todas tienen una arquitectura con mecanismos en común. Se garantiza QoS mediante el uso de VLANs, 802.1p y políticas de priorización de colas.

3.2. Clasificación de las sedes

Para poder dimensionar todas las sedes dentro de la VPN, se ha diferenciado según necesidades de cara a determinar la tecnología de acceso que deberá instalarse,

Después de analizar las necesidades de cada sede se ha tomado varias decisiones. Para facilitar el dimensionado de éstas se ha definido 4 estándares en los que se pueden clasificar las necesidades de todas las sedes.

Se definen cuatro tipos de sedes:

- **TIPO “D”:** Sede central (Barcelona), la más grande. Se trata de un edificio entero con diversos departamentos como son marketing, I+D secretaría,

administración, contabilidad y Exportaciones. Está constituida por 120 puestos de trabajo distribuidos en diferentes departamentos.

- **TIPO "C":** 2 nodos logísticos situados en Almería y Salamanca, con oficinas importantes y Departamentos de Calidad y Control de Procesos. Está constituido por 60 puestos de trabajo.

- **TIPO "B":** 6 almacenes con oficina de atención al cliente, situados en grandes ciudades, constan de 30 puestos de trabajo.

- **TIPO "A":** Resto de almacenes (24 sedes), con oficinas pequeñas, estas "microsedes" constan de 4 puestos de trabajo.

3.3. Situación actual de la red

Actualmente las dos sedes C y la sede principal D están comunicadas mediante conexiones en estrella Frame Relay con sus respectivos circuitos virtuales permanentes (PVC) mientras que las sedes tipo A y B no están interconectadas ni entre ellas ni a las sedes C Y D. En este cuadro están las infraestructuras actuales de las sedes:

Tipo de Sede	A	B	C	D
Router ADSL	1	1	-	-
Router Frame Relay	-	-	1	1
Bri RDSI (2 canales de voz)	1	3	-	-
Switch 24 puertos	-	1	3	5
PRI	-	-	1	2
PBX	1			
Cableado UTP CaT 5	Si	Si	Si	Si
Servidor Correo Electrónico	-	-	1	1
Servidor BB.DD.	-	-	1	1

Tabla 1. Elementos de red en cada tipo de sede

Cada sede tiene 3 líneas ISDN básicas, de las cuales 2 se utilizan en las comunicaciones internas y otra sirve de respaldo en caso de caída de la red Frame Relay.

El gran inconveniente de la infraestructura actual es la falta de redundancia pues existe un solo enlace entre cada una de las 3 sedes remotas, lo cual le resta fiabilidad. La caída de uno de los nodos supondría una caída global de la red en estrella y depender de los enlaces ISDN de backup, actualmente insuficientes.

El objetivo de este proyecto es dotar a todas las sedes de una sólida infraestructura de comunicaciones redundada y que conecte todas y cada una de las sedes. Ésta tendrá además la capacidad de crecer tanto añadiendo nuevas sedes a la red cómo ampliando las ya existentes simplemente añadiendo un nuevo nodo a la red (gran ventaja de MPLS) o contratando más ancho de banda sin alterar la infraestructura actual (fácil escalabilidad).

3.4. Dimensionado y distribución del caudal telefónico

En este capítulo se describirá la estructura de la telefonía del operador y su dimensionado a partir de los consumos por departamento de las sedes de la VPN; tanto del tráfico dentro de la VPN (on net- on net) y el que debe salir a la red de telefonía conmutada (on net-off net).

3.4.1. Modelo de telefonía IP centralizado

La telefonía IP permite el uso de la línea personal desde cualquier punto en el que exista un punto de conexión de red. El número o extensión no está asociado al teléfono sino a la posibilidad de acceder a la red y registrarse con un Call manager a esto se le llama ubicuidad. Esto permite la movilidad de un trabajador a cualquier ámbito ó lugar de la organización sin perder comunicación y su perfil de usuario correspondiente.

Se usará un modelo centralizado en el CDP para la telefonía basado en un Call Manager redundado en modo clúster, es decir compartiendo base de datos y recursos, que hace las funciones de Gate Keeper. Éste enlaza la red VoiP con la RTC además de realizar la gestión de sesiones. Las ventajas de esta tecnología de clústeres, es que provee a nuestro sistema una mayor escalabilidad y capacidad de expansión en el procesamiento de llamadas. Con el uso de tecnología de clústeres el operador logístico podrá agregar nuevas sucursales y superar las necesidades futuras de telefonía con mucha facilidad. Esta tecnología también nos aporta redundancia y mayor disponibilidad, ya que si un call manager falla, uno secundario inmediatamente lo substituye hasta que sea necesario.

Una de los equipos más usados hoy en día es el Cisco Unified Communication Manager 5.0, éste permite una mayor flexibilidad y proporcionar la calidad y garantía de tráfico que se necesita.

A nivel LAN se tendrá una segmentación o clasificación del tráfico utilizando una VPN exclusivamente para el tráfico de voz. Esta VPN de voz estará configurada en los Switches Cisco serie Catalyst que implementan o incluyen el 802.1q. Esto normalmente permite el encolamiento de los paquetes de voz en colas con mayor prioridad que los paquetes de datos pero en el caso del operador se priorizarán las descargas de los albaranes desde los dispositivos móviles (PDASs) en los almacenes sobre el resto de paquetes de datos y las llamadas en caso de que se supere el tráfico multimedia contratado, que será el encargado de priorizar las llamadas de voz y video conferencias.

Este encolamiento permite darle a los paquetes de voz una circulación rápida y de baja latencia. Y en casos de congestión o fallas en la red, se realiza un descarte de los paquetes de datos y no de paquetes de voz.

Por lo que todas las llamadas que se deseen cursar, tendrán que acceder a este servidor para que haga las funciones pertinentes que finalmente permitan comunicar emisor y receptor de forma directa. Las llamadas hacia la red telefónica conmutada saldrán utilizando enlaces RDSI que estarán centralizados en el CPD de la sede principal. Las llamadas provenientes de la RTC entrarán por también a través del CPD.

Se ha analizado el uso telefónico de los usuarios y se ha optado por concentrar los primarios en la sede principal (Barcelona), de esta manera todas las llamadas desde la RTC serán recibidas por un Call Manager situado en el CPD en la misma ciudad (misma MAN) que la sede principal (Barcelona) que las redirigirá donde toque. Centralizar la salida a la RTC tiene el peligro de que todos los almacenes dependan de la sede central, pero en caso de caída del CPD de ésta se redirigirán las llamadas al DRS y por último en caso de algún otro fallo existe el teléfono móvil que es el último back up.

3.4.2. Llamadas

Aquí está la distribución según las necesidades de cada departamento tanto de las llamadas internas como de las externas.

4.3.2.1. Distribución de llamadas en la Sede D:

Recordemos que este es el edificio corporativo de la empresa situado en Barcelona. Destaca el volumen de tráfico a la RTC de los comerciales y de administración hacia otras sedes.

					Total	On-net	Off-net	
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	12h-13h	13h-14h
Comerciales	35				158	50	108	
Administración	20				120	72	48	
Dpto IT	20				20	16	4	
Gerentes	15				60	46	14	
At cliente	10				45	10	35	
Dirección	5				30	22	8	
Dpto.Marketing	10				30	22	8	
Mantenimiento	5				20	4	1	
Total líneas	120							
					483	242	226	

Tabla2. Distribución de llamadas y ocupación por departamentos en la sede D

Aquí se observa el total de llamadas que realizaba la sede D hasta el momento desglosadas por departamentos. Se debe diferenciar aquí las llamadas on-net de las off-net, en general el número de llamadas internas será mayor excepto en el caso del departamento comercial y atención al cliente, los cuales obviamente se comunican a través de la red telefónica conmutada (RTC).

Tenemos un total de 242 llamadas internas y 226 a la red conmutada, eso considerando la duración media por llamada en 2 minutos

Según el cuadro el número de llamadas en **hora cargada** en el caso On-net es de 242 al día, por lo tanto el número de Erlangs necesario es:

1/60=x/2 ->x=0.03333 →Erlangs por llamada. (Que es lo mismo que multiplicar por 120seg / 3600seg).

242 llamadas *(120 seg/3600 seg)= 8,06 -> 9 E

Para el caso Offnet es:

226 llamadas *(120 seg/3600 seg)=7,53 -> 8 E

Si consideramos unos 30 k por línea, nos da un caudal de 0.270 megas en el caso On-net dado que la contratación mínima de caudal multimedia que es el que utilizaremos para priorizar este tipo de tráfico es de 1 mega nos quedará margen. De cara al futuro no supone ningún problema ampliar esta cuota, sólo que se deberá tener en cuenta que el escalado se realiza mega a mega.

4.3.2.2. Distribución de llamadas en la Sede C:

					Total	On-net	off-net	
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	12h-13h	13h-14h
Control de procesos	30				90	85	15	
Administración	5				40	29	11	
Dpto Calidad	10				30	22	8	
Dpto IT	5				10	6	4	
Almacen	10				20	14	6	
Mantenimiento	5				20	16	4	
Total líneas	60							
Total					210	172	48	

Tabla3. Distribución de llamadas y ocupación por departamentos en la sede C

Tenemos un total de 166 llamadas internas y 44 a la red conmutada, eso considerando la duración media por llamada en 2 minutos

El número de llamadas en hora cargada en el caso On-net es de 166 al día, por lo tanto el número de Erlangs necesario es:

1/60=x/2 ->x=0.03333 →Erlangs por llamada.

166 llamadas *(120 seg/3600 seg)= 5.5333 E =>6 E

Para el caso Offnet es:

44 llamadas *(120 seg/3600 seg)=1,44 -> 2 E

Si consideramos unos 30 k por línea, nos da un caudal de 0.180 megas en el caso On-net dado que la contratación mínima de caudal multimedia que es el que utilizaremos para priorizar este tipo de tráfico es de 1 mega mucho margen. De cara al futuro no supone ningún problema ampliar esta cuota, sólo que se deberá tener en cuenta que el escalado se realiza mega a mega.

4.3.2.3. Distribución de llamadas en la Sede B:

					Total	On-net	Off-net	
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	12h-13h	13h-14h
Administración	5				30	22	8	
At cliente	5				35	12	23	
almacen	10				20	14	6	
Mantenimiento	5				20	15	5	
Total líneas	30							
Total					105	63	42	

Tabla 4. Distribución de llamadas y ocupación por departamentos en la sede B

Tenemos un total de 63 llamadas internas y 42 a la red conmutada, eso considerando la duración media por llamada en 2 minutos

El número de llamadas en hora cargada en el caso On-net es de 63 al día, por lo tanto el número de Erlangs necesario es:

1/60=x/2 ->x=0.03333 →Erlangs por llamada.

63 llamadas *(120 seg/3600 seg)= 2,1 E =>3 E

Para el caso Offnet es:

42 llamadas *(120 seg/3600 seg)=1,4 -> 2 E

Si se consideran unos 30 k por línea, nos da un caudal de 0.090 megas en el caso On-net dado que la contratación mínima de caudal multimedia que es el que se utilizará para priorizar este tipo de tráfico es de 1 mega mucho margen. De cara al futuro no supone ningún problema ampliar esta cuota, sólo que se deberá tener en cuenta que el escalado se realiza mega a mega.

4.3.2.4. Distribución de llamadas en la Sede A

					total	On-net	Off-net	
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	12h-13h	13h-14h
Administración	2				12	8	4	
mozos de carga	2				8	7	1	
Mantenimiento	1				5	3	2	
Total líneas	4							
Total Líneas					25	18	7	

Tabla5. Distribución de llamadas y ocupación por departamentos en la sede A

Tenemos un total de 18 llamadas internas y 7 a la red conmutada, eso considerando la duración media por llamada en 2 minutos

El número de llamadas en hora cargada en el caso On-net es de 18 al día, por lo tanto el número de Erlangs necesario es:

1/60=x/2 ->x=0.03333 →Erlangs por llamada.

18 llamadas *(120 seg/3600 seg)= 0,6 E => 1 E

Para el caso Offnet es:

7 llamadas *(120 seg/3600 seg)=0,233 -> 1 E

Si consideramos unos 30 k por línea, nos da un caudal de 0.030 megas en el caso On-net dado que la contratación mínima de caudal multimedia que es el que utilizaremos para priorizar este tipo de tráfico es de 1 mega mucho margen. De cara al futuro no supone ningún problema ampliar esta cuota, sólo que se deberá tener en cuenta que el escalado se realiza mega a mega.

4.3.2.5. Resumen:

Aquí se detalla el número de enlaces necesarios según los cálculos anteriores y el número calculado mediante las tablas earlang que nos detallan el número de enlaces necesarios para asegurar una probabilidad de bloqueo máxima determinada.

Con probabilidad de bloqueo de 0,4% se necesita:

Número de enlaces	On net- on net		On net - Off net	
		P. bloqueo<= 0,4%		P. bloqueo<= 0,4%
Sede A	9	14	8	13
Sede B	6	10	3	7
Sede C	3	7	2	5
Sede D	1	4	1	4

Tabla 6. Número total de enlaces necesarios

Se debe tener en cuento que para el caso de RTC, en las sedes A deberán poder llamar 2 líneas a la vez como mínimo entonces eso hará que el número de líneas que deben salir a la RTC serán:

24(sedes A) *4 + 6 (sedes B)*5 + 2(sedes C)*7 +1(sede D)*13 =96+30+14+13 = 153 líneas

Esto implica la necesidad de instalar 6 E1s.

Respecto a las llamadas On-net-On-net en todas las sedes B y C bastará con el mínimo caudal contratable multimedia que es un mega para priorizar la voz. En la sede D me sale que 1 pero considero que es poco y en las sedes A entiendo que también pido 1 mega.

4.3.2.6. Llamadas desde las sedes a móviles

Las llamadas que se realizan desde cualquier sede hacia un terminal móvil, es decir las llamadas con destino a la red GSM, accederán a ésta mediante un Gateway GSM conectado a la PBX.

El Gateway GSM realiza la función de un teléfono móvil con una sim integrada que comparte para los dos enlaces analógicos, de este modo el coste de las llamadas se factura como una llamada de móvil a móvil.

El problema con este sistema es la ocupación que se genera cuando el personal utiliza los dos canales disponibles para móviles que están conectados a la centralita,

Figura 1. Esquema de salida de las llamadas a través de GSM Gateway

3.5. Dimensionado de los datos

La plantilla de la compañía se ha clasificado en estas categorías:

- Comerciales que necesitarán usar aplicaciones como Outlook, PowerPoint, Word, Excel y acceder a las bases de datos de los clientes. Consumen un promedio de 30k
- Administración necesitarán acceder a las mismas aplicaciones que los comerciales pero además acceden a aplicaciones bancarias.
- Departamento de IT necesitarán acceder a las aplicaciones estándar y además suelen acceder a aplicaciones pesadas relacionadas con la administración de la red.30k
- Gerentes se les debe dimensionar para que puedan usar toda clase de aplicaciones.60k
- At. Al cliente usarán Outlook, Word y acceso a bases de datos de clientes.20k
- Dirección 50k
- Departamento de Marketing Outlook, Word, Power Point, bases de datos de clientes.30k
- Mantenimiento solo accederán a Outlook y Word.5k
- Control de procesos
- Mozos de carga

A partir de aquí determinaremos a partir de la hora más cargada de tráfico cuales serán las necesidades de ancho de banda de la red por usuario y las de videoconferencia dado que son aplicaciones usadas muy frecuentemente en horario de trabajo, se le ha puesto un factor de concurrencia elevado, 50%:

(Todos los datos de tráfico por WAN son en Kbps)

Sede A

					WAN	Videoconferencia		
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	13h-14h	14h-16h
Administración	2				40			
mozos de carga	2				20			
Mantenimiento	1				5			
Total líneas	4							
Total					65	0		

Tabla 7. Ocupación de la red WAN por departamentos de la sede A

Sede B

					WAN	Videoconferencia		
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	13h-14h	14h-16h
Administración	5				100			
At cliente	5				50			
almacen	10				50			
Mantenimiento	5				25			
Total líneas	30							
Total					225	0		

Tabla8. Ocupación de la red WAN por departamentos de la sede B

Sede C

					WAN	Videoconferencia		
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	13h-14h	14h-16h
Control de procesos	30				600			
Administración	5				200			
Dpto Calidad	10				150			
Dpto IT	5				75			
Almacen	10				50			
Mantenimiento	5				25			
Total líneas	60							
Total					1100	4 megas / sede		

Tabla9. Ocupación de la red WAN por departamentos de la sede C

Sede D

					WAN	Videoconferencia		
Secciones	num. Empleados	9h-10h	10h-11h	11h-12h	12h-13h	12h-13h	13h-14h	14h-16h
Comerciales	35				525			
Administración	20				400			
Dpto IT	20				300			
Gerentes	15				450			
At cliente	10				100			
Dirección	5				125			
Dpto.Marketing	10				150			
Mantenimiento	5				25			
Total líneas	120							
					2075	4 megas		

Tabla 10. Ocupación de la red WAN por departamentos de la sede D

3.5.1.1. Dimensionado de los datos que accederán al CPD

Se ha tenido en cuenta que al centro de procesado de datos accederán todas las sedes en el momento de descargar los datos de los albaranes.

Teniendo en cuenta el volumen de la empresa, se tiene que de los 1000 camiones se tiene en marcha una media de 940, dado que cada albarán tiene una media de 30 kbytes, y que cada camión entrega una media de 20 entregas:

940 (camiones) * 20(entregas) * 30 kb (cada albarán) = 564000000 bytes

Esto son 537,87 Megabytes por día de datos. Por las dimensiones de la empresa no es un flujo muy elevado.

Tenemos dos opciones de traspaso de datos entre BBDD del CPD al DRS:

- ✓ Traspasar los datos a partir de las 22:00 h, hora en la que en general la red estará libre pues las oficinas están vacías y los camiones deberían haber acabado los repartos.

- ✓ Usar software replicador tipo MIMIX

Si se usa la propia red fuera de horas de trabajo para replicar las BBDD, contando con que la conexión rinda a un 25 % (mínimo asumible) y teniendo en cuenta que el cuello de botella lo encontraremos en la conexión entre la nube MPLS y la sede del DRS; se tiene que:

537,87 Megabytes / 12,5 Megas= 43.05 segundos

Observando que el traspaso diario se puede realizar en menos de un minuto se decide no instalar ningún software replicador de pago, pues el traspaso de datos entre las sedes a través de la propia red corporativa es más que suficiente.

Por otro lado, el sistema implantado de Video Vigilancia se activará normalmente fuera del horario laboral, por tanto se trata de una reutilización de la infraestructura, pero se ha tenido en cuenta en el dimensionado por si surge la necesidad de activarlo en horario laboral también.

Modalidad	FPS	RESOLUCIÓN	TIPO DE COMPRESIÓN	% Compresión	BW(Kbps)	Capacidad HDD(MB)
Respaldo Online	6	640x360	H264	90	52	255.9
Grabación Local en DVR	30	640x480	H264	90	283	1,300
Acceso Remoto	12	320x240	H264	90	31	0

Tabla 11. Configuración general de las cámaras

Cantidad de cámaras	Almacenamiento DIARIO HDD (MB)	TOTAL (MB)	Almacenamiento DIARIO TOTAL (GB)
1-5 CAMARAS	255.9	1.280	1.2
6-10 CAMARAS	255.9	2.559	2.5
10-15 CAMARAS	255.9	3.839	3.7
16-20 CAMARAS	255.9	5.118	5

Tabla 12. Detalle de la capacidad y del video emitido para el CPD

Enlace Sede Principal (Barcelona)

SEDE PRINCIPAL					
SISTEMA	Q	BW Unitario (Kbps)	BW (Kbps)	Relación	BW Total (Mbps)
CCTV Cat. A	10	768	7680	1:1	7.5
CCTV Cat. B	12	320	3840	1:1	3.75
CCTV Cat. C	12	0	0	0	0
ALARMAS	22	16	352	1:1	0.3438

Tabla 12. Detalle de la ocupación del video emitido según el tipo de instalación

La siguiente tabla detalla los anchos de banda necesarios por servicio:

(Megas)	Videoconferencia	Video Vigilancia	Alarmas	Datos	Voz
Sede A	4	3.75	0.3	0.065	1
Sede B	4	3.75	0.3	1.025	1
Sede C	4	3.75	0.3	0.225	1
Sede D	4	7.5	0.3438	2.125	1

Tabla 13. Detalle de anchos de banda según tipo de sede

Analizando estos datos se concluye que:

- La sede D (edificio de 5 plantas y CPD) tendrá 100 megas redundados mediante acceso en dos fibras separadas. Tráfico multimedia contratado 1 Mega.
- La sede C (edificio de 2 plantas y DRS) tendrá una conexión de 50 megas con un back up de 10 megas. Tráfico multimedia contratado 1 Mega.
- La sede C (edificio de 2 plantas) tendrá una conexión de 20 megas con un back up de 10 megas. Tráfico multimedia contratado 1 Mega.
- Las sedes B (única planta) tendrá una conexión de 10 megas con un back up ADSL Premium que nos proporciona 8 megas de conexión y nos asegura 6 líneas de voz con un CIR del 10%. Tráfico multimedia contratado 400 k.
- Las sedes A tendrán conexión ADSL Premium que proporciona una conexión de 8 megas con hasta 6 canales de voz con un 10% de tráfico garantizado. Tiene un backup RDSI. Tráfico multimedia contratado 400 k.

En este esquema se observa la propuesta de VPN del operador logístico:

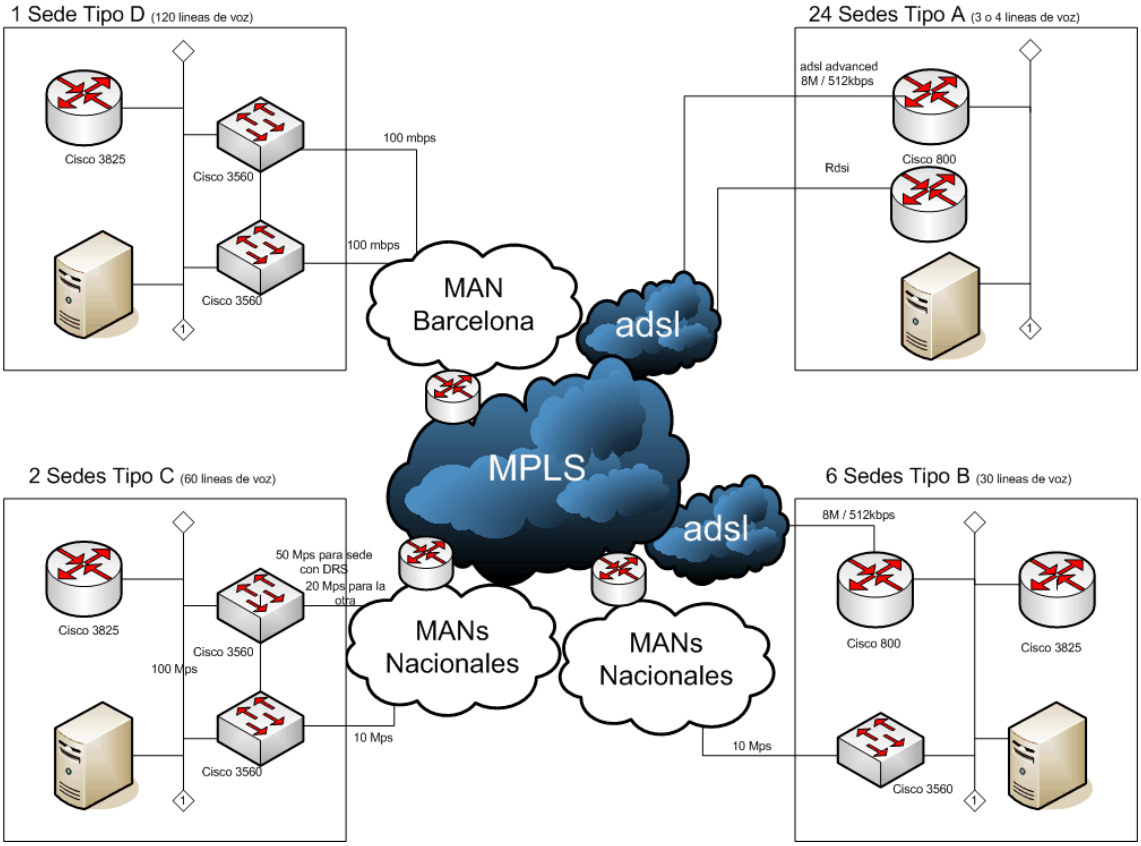


Figura 2. Esquema de la VPN del operador logístico

3.6. Arquitectura de cada sede

Las redes actuales de las sedes del cliente se basan en tecnología Ethernet. Esta tecnología es utilizada en la mayoría de redes de área local del mundo porque ofrece unas prestaciones muy buenas a un precio reducido.

El cableado instalado en las sedes soporta velocidades de hasta 1 Gbps, en el caso de las sedes C y D es de tipo cat6 lo que permite utilizar todos los servicios que están previstos.

Se ha optado por utilizar switches para concentrar el tráfico de cada una de las sedes pues la utilización de hubs es muy poco eficiente al crear muchos dominios de colisión.

Al tener que soportar la red voz sobre IP, se aplican medidas de QoS a la red que son soportadas por los switches utilizados en todas las sedes, esto se hará mediante políticas de marcación y priorización de tráfico según el tipo. Así se evitarán problemas en caso de que se colapse la red y afecte al tráfico de voz. Se va a utilizar el estándar 802.1q referido a VLAN para separar el tráfico de voz y datos, y reducir así los dominios de broadcast. Por otro lado con el objetivo de aplicar políticas de priorización se utiliza la tecnología definida en el estándar 802.1p.

Se utilizarán teléfonos y switches que se alimentarán mediante PoE, es decir a través del cableado eléctrico. Casi todos los teléfonos IP están diseñados para funcionar así hoy en día.

3.6.1. Configuración de los puestos de trabajo

3.6.1.1. Equipos en sedes A

Estas sedes constarán de un switch de 12 puertos y un router ADSL . Dado que sólo hay 4 equipos en esta sede y sabiendo que voz y datos de cada puesto de trabajo solo ocupan un puerto, los 12 puertos serán suficientes en caso de una ampliación de este tipo de sedes.

3.6.1.2. Equipos en sedes B

Estas sedes, con 30 equipos voz y 30 de datos, constarán de 2 switches de 12 puertos cada uno. En caso de ampliar el número de equipos, bastará con poner otro switch de 12 puertos

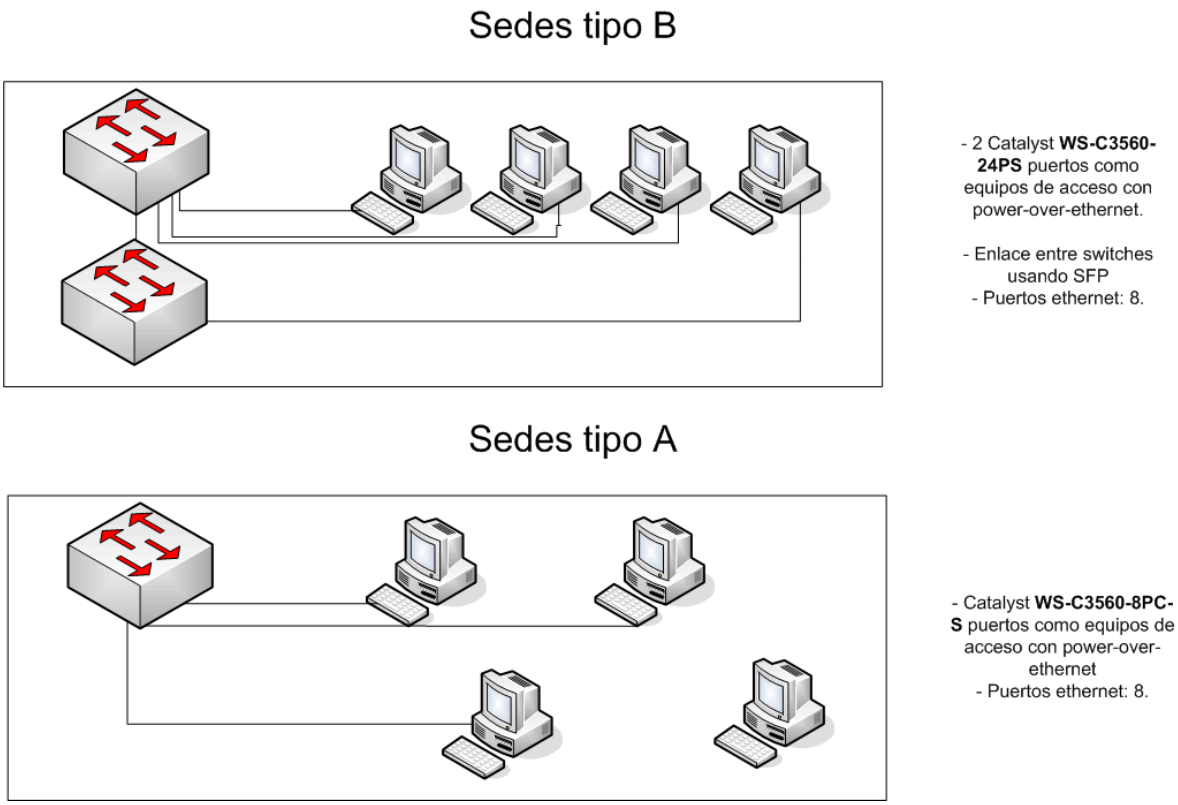


Figura 3. Propuesta de configuración de la electrónica de red de las sedes A y B

3.6.1.3. Equipos en sedes C

Las dos sedes C constan de 2 y tres plantas (el que contiene el DRS), Aquí a continuación se observa la sede simple.

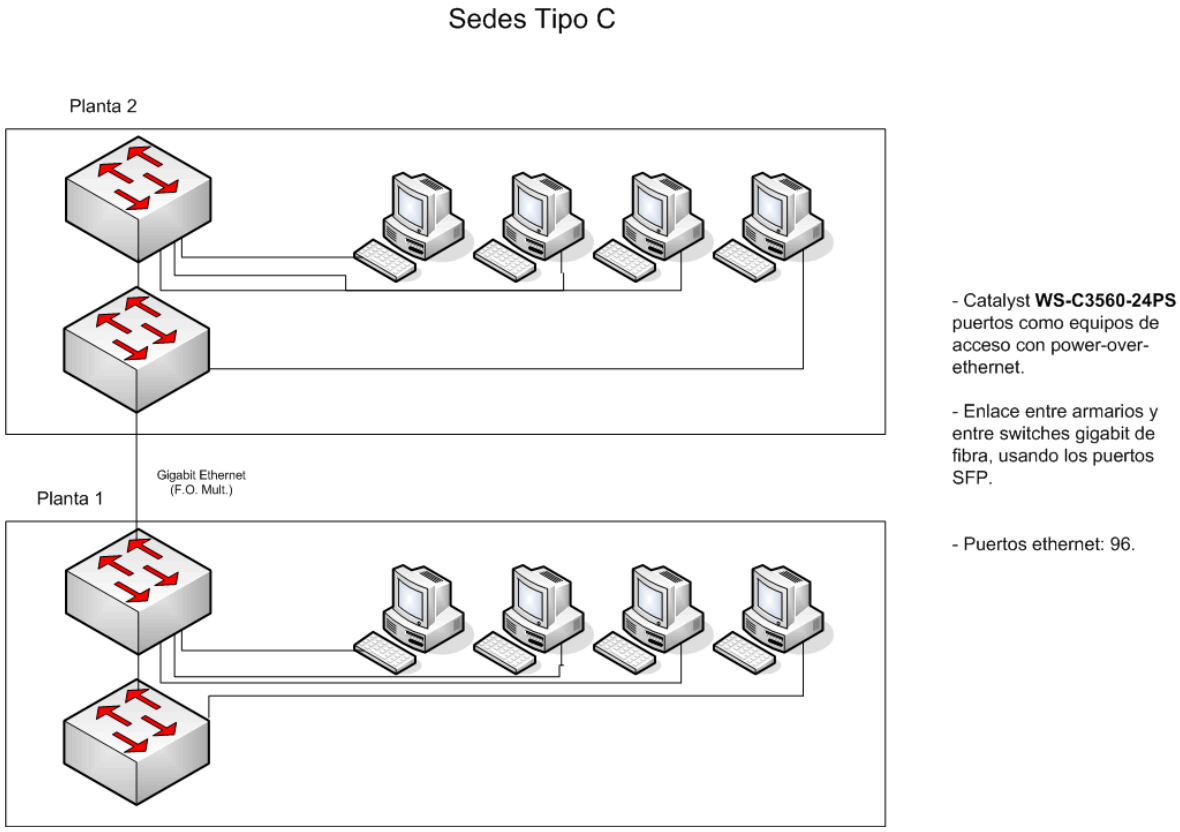


Figura 4. Propuesta de configuración de la electrónica de red de las sedes C

3.6.1.4. Equipos en sede D

Como se puede observar en el esquema la sede principal de Barcelona consta de cinco plantas y tiene el CPD en el primer piso.

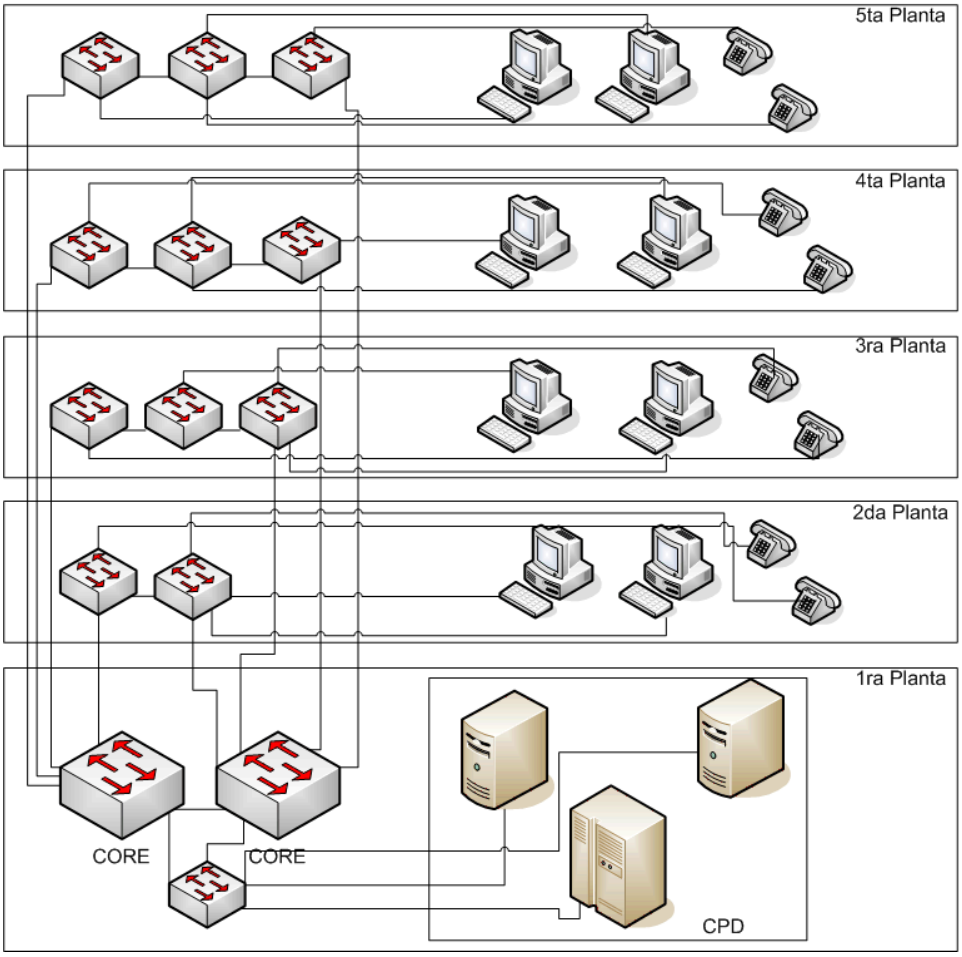


Figura 5. Propuesta de configuración de la electrónica de red de la sede D

3.6.2. Configuración CPD y DRS

El Centro de Procesado de Datos situado en la sede central constará de el siguiente equipamiento: CPD constará de:

- Servidores de BBDD
- Servidores de Aplicaciones
- Proxy

- NAS
- Radius
- GSM Gateway
- Call Manager x2
- Firewall con DMZ
- Servidor Web
- Servidor de correo SMTP/POP3
- Los servidores actuales en el CPD de Barcelona son:

- Servidor NAS: es el servidor de almacenamiento dedicado que compartirá su capacidad de almacenamiento de ficheros con los PCs del personal a través de la red TCP/IP.

- Servidor PROXY: sirve para permitir el acceso a Internet de todos los equipos del operador cuando solo se puede disponer de un único equipo conectado, esto es, una dirección IP pública.

- Servidor SNMP: servidor que se encarga de ejecutar aplicaciones que monitorizan y controlan los dispositivos de gestión de la red del operador, tales como switches, routers, servidores de acceso, hubs, teléfonos IP, computadoras y impresoras.

- Servidor WEB: responde a las peticiones http de los navegadores Web del personal interno.

- Servidor DNS: servidor que traduce los nombres de dominio a direcciones IP. También localiza los servidores de correo electrónico de cada dominio.

- Servidor de BBDD: integra los datos provenientes de las bases de datos distribuidas del operador para favorecer posteriormente el análisis y la divulgación eficiente de esta información, en las tomas de decisiones de la organización. Separa en dos bases de datos, los datos de uso diario (información transaccional u operacional) y los datos para el análisis y operaciones de control.

- Servidor de Aplicaciones: Servidor para los programas que utiliza el personal interno.

- Servidor RADIUS: son los servidores a los que se conecta el servidor web para autenticar a los usuarios que quieran acceder a su cuenta desde otras sedes, servicio de ubicuidad. Podrán acceder a su información confidencial, mediante protocolos SSL, certificados de seguridad, etc.

En cuanto al sistema de Firewall, si diferenciarán dos subredes aisladas una se encontrará en la DMZ, es decir la zona “desmilitarizada” que posee equipos disponibles tanto para la red interna de la compañía como para la red externa estas son servidores web, de correo y los FTP. La DMZ actúa como una zona de búfer entre la red que necesita protección y la red hostil.

Los servidores en la DMZ son habitualmente denominados “anfitriones bastión” ya que actúan como un puesto de avanzada en la red de la compañía. La política de seguridad que seguirá la DMZ será la siguiente:

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**
- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**
- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles del operador.

En la DMZ se encuentran los servidores WEB, correo y FTP, porqué son servidores que deben ser accesibles desde la red exterior. El resto de servidores estarán detrás del firewall protegidos.

Por último resaltar que tanto en CPD como en el DRS Se dispone de 2 Call Manager (CM), modelo en cluster modo activo-pasivo, es decir si falla uno se activa el otro.

En el primer esquema se detalla la estructura que se ha propuesto para el CPD y para el centro de respaldo DRS.

Estructura del Centro de Procesado de Datos

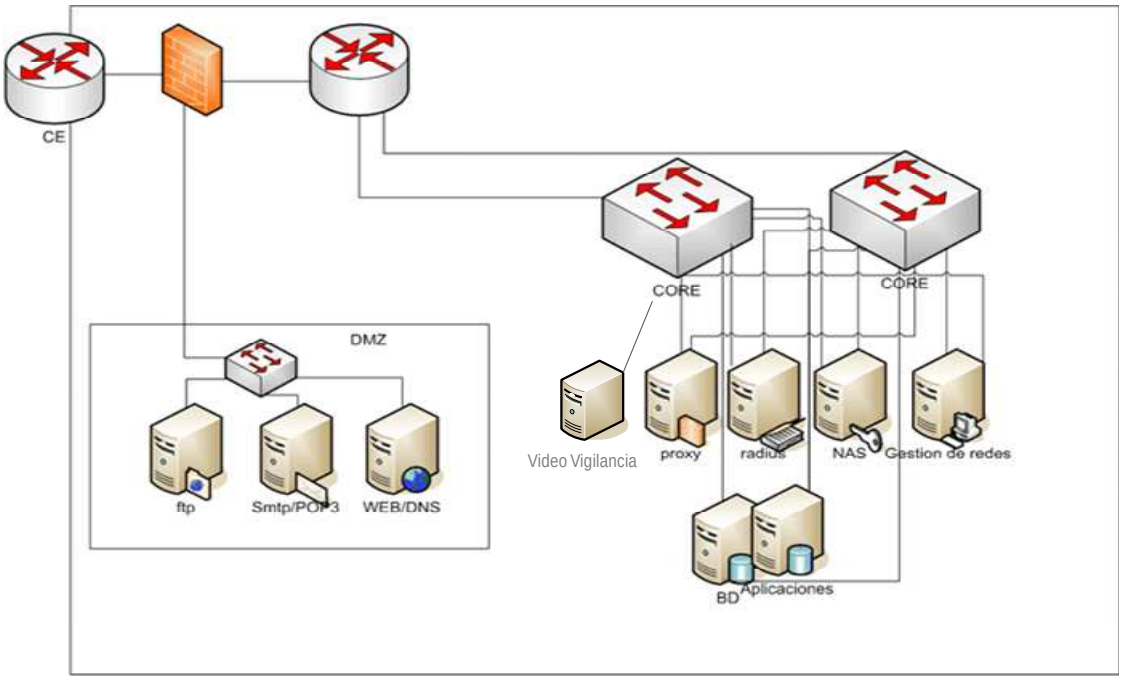


Figura 6. Propuesta de configuración del Centro de Procesado de Datos

Estructura del Centro de Recuperación de Desastres

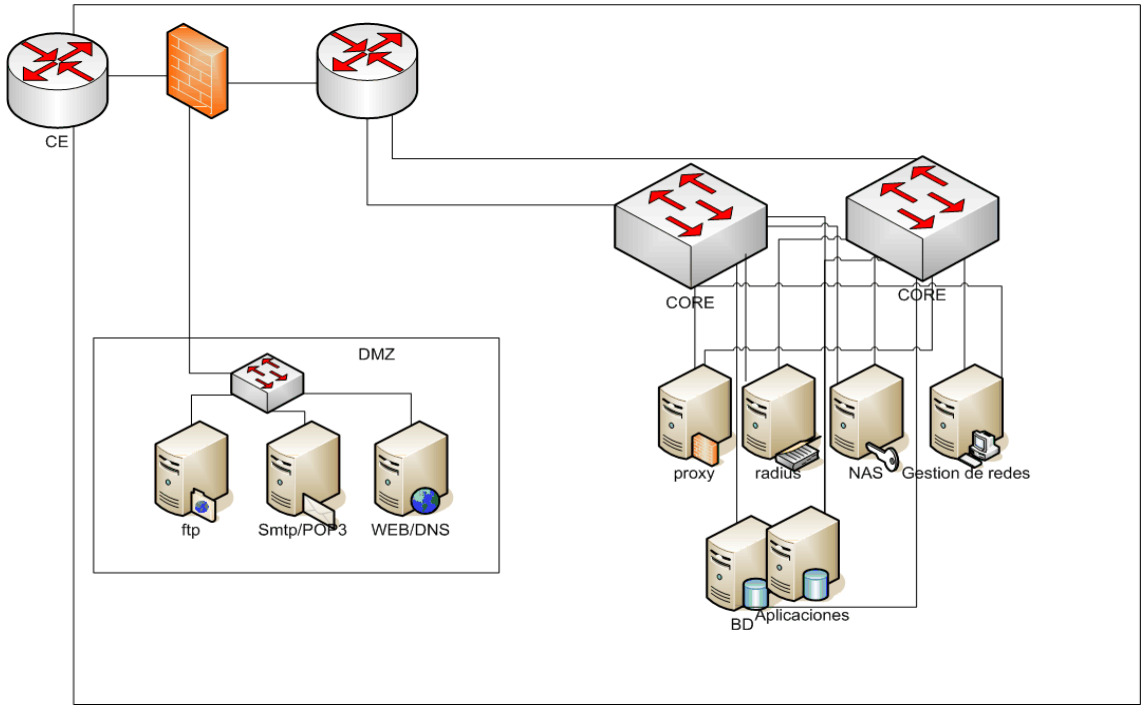


Figura 7. Propuesta de configuración del Disaster Recovery System

4. Solución propuesta para el sistema de posicionamiento y control de la flota

4.1. Arquitectura de la solución propuesta

La solución elegida es el producto **MOVILOC,** firma que está especializada en sistemas de localización de vehículos**.** Permite configurar y parametrizar el sistema a la medida del cliente. Además, el sistema tiene altas prestaciones y elevada eficiencia en la transmisión y codificación del tráfico de gestión de vehículos, lo cual permite un uso eficiente de los recursos de comunicaciones móviles. Se trata de una solución completa, que incluye hardware y software embarcado y aplicaciones de gestión y control para PC. Todos los elementos se comunican entre sí por medio de protocolos específicos de comunicaciones, sobre la red GPRS/3G/GSM, como se explica a continuación.

El sistema de localización de los vehículos propuesto se basa en el sistema GPS, efectuándose las comunicaciones sobre la red móvil, que se conecta a través de un acceso dedicado a la red de área local de la sede central. Las conexiones para acceder a la información sobre la situación de la flota, recibir información sobre eventos y enviar comandos de gestión a los vehículos desde cualquiera de las 33 sedes de la empresa se establecen sobre los túneles de la VPN corporativa. La conexión de la red interna de la empresa a la red móvil del operador se efectúa a través de un acceso dedicado a la red de área local de la sede central (Barcelona).

Las aplicaciones de gestión de la flota siguen un modelo cliente/servidor (el servidor se encuentra ubicado en la sede central). Es posible acceder a la información sobre la situación de la flota, recibir información sobre eventos y enviar comandos de gestión a los vehículos desde cualquier puesto de supervisión instalado en cualquiera de las 33 sedes a través de la VPN.

A continuación se muestra el esquema general de la arquitectura:

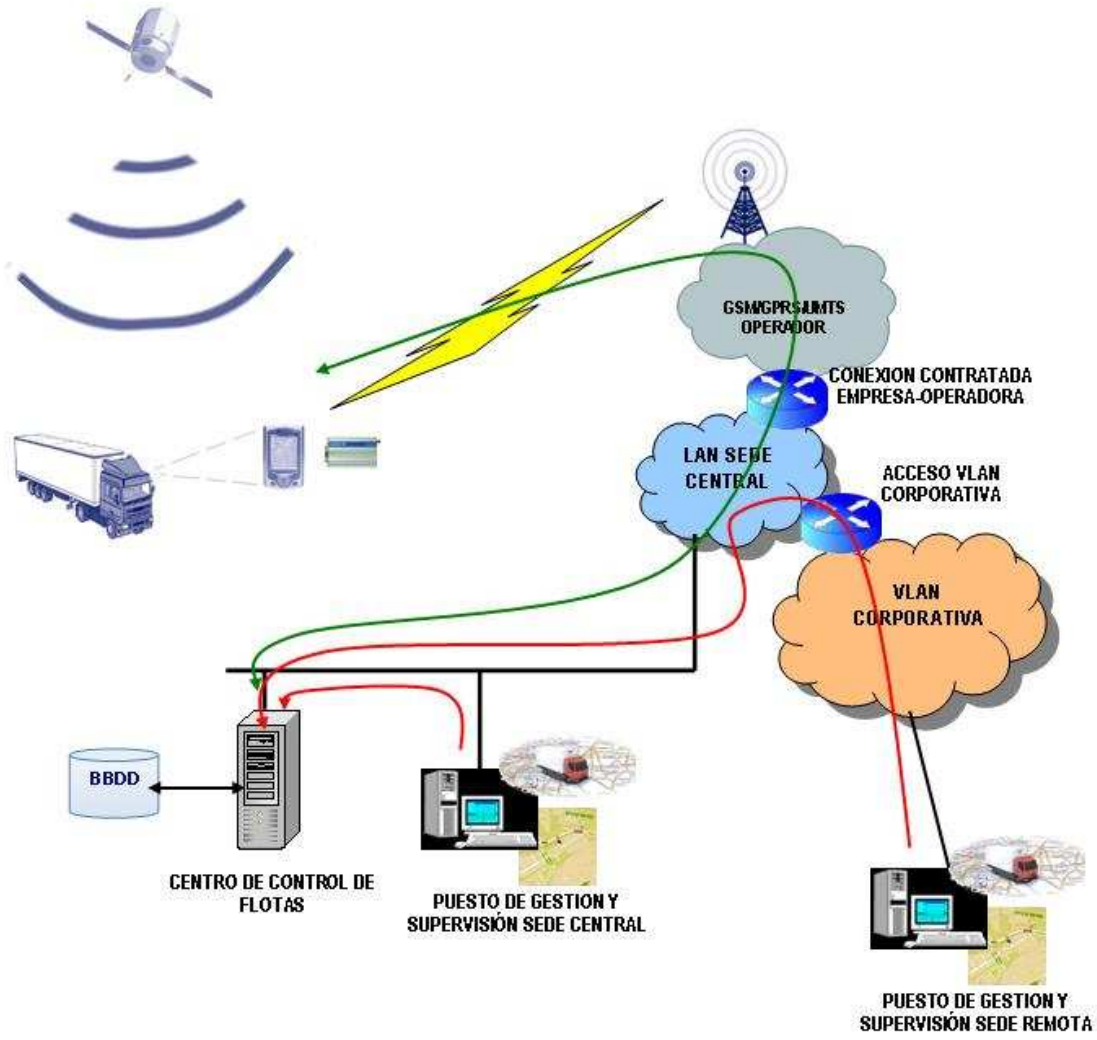


Figura 8. Propuesta Esquema del sistema de posicionamiento y control de flota

4.1.1. Hardware/software embarcado

Los vehículos disponen del siguiente equipamiento:

- Navegador GPS con cartografía actualizada.
- Sistema de control embebido, gestionado desde los puestos supervisión. Permite el envío de mensajes ante eventos, así como el envío periódico de la posición actualizada del vehículo.

- Las comunicaciones se efectúan a través de un terminal GPRS preferentemente, como se explica en el punto siguiente, pudiendo enviarse mediante la red GSM (vía SMS) en zonas sin cobertura GPRS.

  El terminal de comunicaciones está integrado con el sistema de control embebido. Para seguir con la propuesta se ha elegido un dispositivo que responde a las necesidades del operador a modo de ejemplo, sin ánimo de entrar en un análisis de mercado. Se ha elegido el dispositivo A-30 de GMV Sistemas, de bajo coste, que proporciona todas las funcionalidades requeridas. Sus características básicas son las siguientes:

  - Receptor GPS de 12 canales
  - Unidad de control con funciones avanzadas
  - Modem GSM/GPRS integrado
  - Control de las comunicaciones con Central
  - Conectores de entrada y salida de señales y datos
  - Posibilidad de antena dual GPS/GSM

Figura 9. Dispositivo A-30

La principal ventaja de la plataforma de GMV es que ofrece una solución completa y totalmente integrada que cubre las necesidades del cliente (sistema MOVILOC). El dispositivo A-30 se comunica con el centro de control de la flota mediante un protocolo de comunicaciones específico que asegura la fiabilidad, la confidencialidad y la privacidad de la información (ello además de la seguridad que

ya de por sí ofrecen los túneles de la VPN corporativa). Más adelante se describe con mayor detalle la plataforma software.

Existen varias posibilidades de navegador a instalar en el vehículo. El navegador está conectado al dispositivo A-30 y, además de las funciones de posicionamiento, cálculo y planificación de rutas, contendrá el software de gestión y envió de albaranes, que se detalla en el apartado correspondiente:

a. Ordenadores portátiles

b. PDAs o similares (está será la opción más habitual, salvo necesidades específicas)

- El navegador calcula por defecto la ruta más corta o más rápida. Para el cálculo de la ruta, se tienen en cuenta las características del vehículo (camión pesado, ligero, furgoneta, etc.) Asimismo recalcula la ruta en caso de no seguir la indicada. Indica el itinerario por voz, lo que supone conectarlo a los altavoces del vehículo.

4.1.2. Comunicaciones

El modelo de conexión de los terminales móviles embarcados se basa en conmutación de paquetes, utilizando APNs (Access Point Name) específicos, según se describe a continuación:

- Se utiliza un APN específico proporcionado por la operadora para la empresa (Ej. “miempresa”)
- Se configura el terminal y su definición de conexión en el sistema operativo para que dicha conexión se realice a través de éste APN.

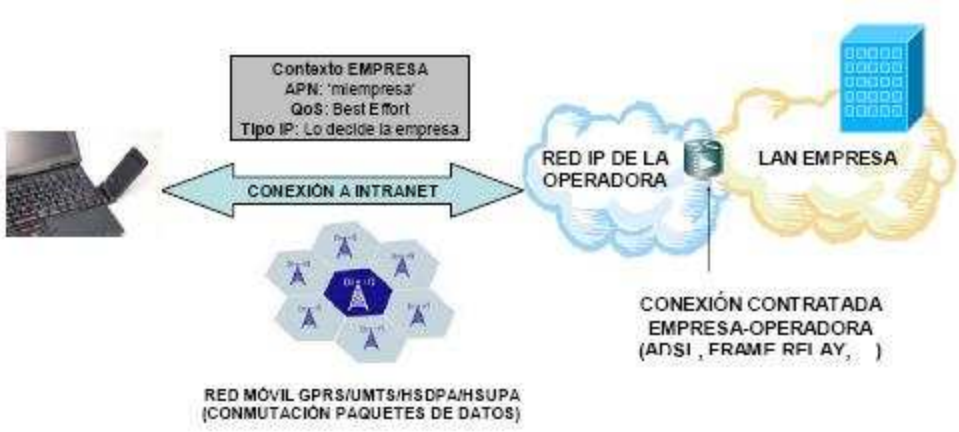


Figura 10. Detalle del modelo de conexión a la red corporativa

Las comunicaciones en GPRS se facturan por cantidad de bytes transmitidos:

• La solución de GMV Sistemas optimiza el tráfico mediante empleo de protocolos UDP y algoritmos de compresión de tramas

• Los mensajes de localización son periódicos (se pueden programar por tiempo o distancia) o a petición desde el puesto de supervisión.

• Se pueden configurar también mensajes asociados a eventos: paso por puntos concretos, alarmas, etc.

Como back-up, de forma alternativa, los vehículos enviaran la posición mediante SMS a través de la red GSM, cuando ello no sea posible mediante GPRS (por ejemplo, en zonas de sombra de cobertura). De este modo, se proporciona redundancia en las comunicaciones ante eventuales fallos de la conexión de acceso contratada con el operador móvil.

El envío de la información de posicionamiento resulta mucho más económico mediante conexiones de datos GPRS que mediante SMS, teniendo en cuenta que actualmente los operadores ofrecen una gran diversidad de tarifas planas. A modo de ejemplo, para corroborar lo económico de este sistema, se pone como ejemplo la siguiente tabla que contiene el abanico de ofertas de tarifa plana estándar de Movistar:

Módulo de datos - Tarifas planas estándar:

Módulo datos	Compromiso mínimo mensual	Datos Zona ADSL Wi-Fi	Datos GPRS/UMTS	Precio GPRS/UMTS fuera del compromiso
Internet en el Móvil	10 euros (11,6 euros)	No	100 MB	Sin sobreprecio. Una vez superado los 100MB de tráfico se reducirá la velocidad de acceso en bajada a 64kbps y la velocidad de acceso en subida a 16kbps.
Internet en el Móvil Plus	15 euros (17,4 euros)	Ilimitado	200 MB	Sin sobreprecio. Una vez superado los 200MB de tráfico se reducirá la velocidad de acceso en bajada a 128kbps y la velocidad de acceso en subida a 64kbps.
Tarifa Plana Internet	30 euros (34,8 euros)*	No	1 GB	Exceso por bloques de 15 euros/0,5GB hasta un máx. de 90 euros, después Tarifa Plana real.
Tarifa Plana Internet Plus	39 euros (45,24 euros)*	Ilimitado	3 GB	Al sobrepasar 3GB de tráfico, se limitará la velocidad a 128kbps en bajada y a 64kbps en subida
Tarifa Plana Internet Premium	59 euros (68,44 euros)*	Ilimitado	10 GB	Al sobrepasar los 10GB de tráfico, se limitará la velocidad a 128kbps en bajada y a 64kbps en subida

Tabla 14. Detalle de tarifas de un operador según servicio

M2M movistar (Máquina a Máquina ó Machine to Machine) permite automatizar los procesos de recogida de datos, la monitorización, vigilancia y el control remoto de los sistemas mediante la incorporación de la telefonía móvil movistar. M2M movistar produce la mejora de los procesos operativos, reduce los costes asociados a la empresa y abre nuevas oportunidades de desarrollo de servicios en el negocio y para terceros. M2M movistar es una solución específica y diferenciadora que ofrece tarifas planas específicas para cada entorno:

- M2M Básico: para proyectos con bajo volumen de tráfico, como vending o alarmas.
- M2M Médium: para proyectos con mayor número de transacciones, como TPVs o transporte.
- M2M Plus: si la necesidad es de mayor ancho de banda o recurrencia, como cajeros o terminales de información.
- M2M nocturna: para enviar los datos beneficiándose de tarifas muy ajustadas, como el caso de contadores de agua, luz, gas ...

- M2M roaming: para el envío de datos en itinerancia, como es el caso de gestión de flotas.

Las características principales de esta solución M2M son las siguientes:

- Control total de las comunicaciones mediante acceso seguro y restringido
- Líneas específicas para su instalación en máquinas remotas
- Comunicación siempre disponible
- Disminución de la complejidad de desarrollo
- Operativa de alta y resolución de incidencias específica con personal cualificado y formado para resolver cualquier duda

Se ha efectuado un estudio para verificar la adecuación del tráfico de localización al modelo M2M. Una de las ventajas de la solución escogida, es su elevado nivel de compresión y optimización de la información enviada (cada posición supone 1 kbit), lo cual es un aspecto crítico en términos de coste en comunicaciones, como se verá seguidamente a través del cálculo incluido. La carga de tráfico de posicionamiento provendrá fundamentalmente del envío periódico de posiciones de los camiones, que se programa por defecto con un intervalo de 5 minutos. Seguidamente se muestra el cálculo que se ha realizado para obtener el tráfico mensual por vehículo, así como el volumen de tráfico mensual procedente del conjunto de la flota que tendrá que asumir el enlace dedicado a la red móvil ubicado en la sede central de Barcelona:

	Número de envíos diarios por vehículo	Tamaño del mensaje (kbit)	Tráfico mensual cursado por vehículo (MB)	Tráfico mensual cursado por la flota de 1.000 vehículos (MB)
Información de posición actualizada (1 kbit/5 min)	288,00	1,00	1,08	1.080,00
Alarmas y eventos	50,00	5,00	0,94	937,50
Comandos de gestión	75,00	5,00	1,41	1.406,25
Descargas de información logística (residual, habitualmente se hará vía bluetooth/wifi)	0,14	1.000,00	0,54	535,71
TOTAL			**3,96**	**3.959,46**

Tabla 15. Dimensionado de los accesos móviles (vehículos y centro de control)

Accesos móviles para los vehículos

Para los cálculos se ha considerado para cada vehículo:

- Actualización de posición cada 5 minutos
- Envío de unas 50 alarmas diarias (muy conservador, casi nunca se dará este caso)
- Recepción de unos 75 comandos de gestión desde los puestos de gestión
- Descargas puntuales de información logística al final del reparto (1 a la semana). Se trata de una estimación muy conservadora, pues casi siempre se optará por descargar los datos una vez en almacén, a través de la red inalámbrica local (vía WiFi/Bluetooth).

Como puede comprobarse en la tabla anterior, se espera que cada vehículo (en promedio) envíe/reciba alrededor de **4 Mbytes mensuales,** y la mayor parte del tráfico corresponderá a la actualización de los datos de localización al centro de control (envío de posiciones cada 5 minutos). Por tanto, es adecuada la elección de la tarifa M2M Medium, que permite hasta un máximo de 50 Mbytes de tráfico cursado al mes. Por tanto, existe margen más que suficiente para asumir el tráfico generado por la flota de vehículos. En cualquier caso, se hará un seguimiento durante los 6 primeros meses de funcionamiento del sistema, para obtener datos empíricos y, según el uso que el personal del operador haga del sistema de localización, se valorará la posibilidad de migrar a una tarifa inferior, si bien se considera más conveniente contar con un margen amplio de seguridad que permitiría mayor flexibilidad a la hora de **aprovechar la capacidad sobrante para** gestionar **un mayor número de descargas de tráfico logístico a través de la red móvil**, o **para aumentar la frecuencia de actualización de posiciones**.

De los cálculos anteriores, se concluye que la tarifa que mejor se adapta al tráfico de posicionamiento (incluyendo los picos puntuales de tráfico logístico) previsto es la **M2M Médium**, cuya tarifa es **de 3€/mes** por terminal.

- Accesos dedicados de la sede central

Como se ve en la tabla presentada, el enlace dedicado de la sede central que sirve de conexión del centro de control de flotas a la red móvil de Movistar soportará en total alrededor de **4 GB** de datos de localización/logística al mes (en promedio, resultan **unos 13 kbps**). Por tanto, se ha escogido un enlace **dedicado a la red móvil de 512 kbps** (40 veces mayor al promedio del tráfico total cursado) y envío/descarga de datos ilimitado (el exceso se facturaría aparte). La velocidad contratada es más que suficiente para asumir potenciales picos de tráfico, porque además se contratará un enlace redundante para hacer frente a fallos o contingencias del enlace principal. Este

enlace se configurará para que funcione en modo balanceado con el acceso principal y pueda asumir picos de tráfico hasta un límite de 10 GB mensuales, sin coste adicional.

Debe tenerse en cuenta además que el mayor volumen de tráfico procede del envío periódico de posiciones, que se distribuye uniformemente a lo largo del día, por tanto no se esperan grandes picos puntuales de tráfico, a excepción del tráfico de descargas de datos logísticos. Pero este tráfico, aunque prioritario, no es sensible al retardo. Por tanto, con este dimensionado las necesidades de envío de datos a través de la red móvil se cubren satisfactoriamente y optimizando al máximo los costes.

En conclusión, los accesos móviles que se contratarán a Movistar son los siguientes:

	Modalidad (kbps)	Capacidad datos GPRS/UMTS
Vehículos	M2M Médium	50 MB
Centro de control de flotas (sede central Barcelona)	Línea dedicada 512 kbps (con enlace redundante)	Ilimitada

Tabla 16. Accesos móviles seleccionados

Revisión de la facturación

No obstante, durante la duración total del contrato con el operador, se deberá analizar periódicamente la facturación mensual en concepto de comunicaciones móviles y se estudiará la idoneidad de migrar a una tarifa superior de las M2M, o incluso de las estándar (en caso de que el tráfico efectivamente cursado desborde el límite permitido, lo cual penalizaría en términos de costes pues se facturaría con un precio superior) o a la categoría inferior M2M básico (en caso de que el tráfico sea muy inferior al estimado), para así optimizar los costes al máximo. También se analizará el tráfico cursado por el enlace dedicado, para comprobar que se ha dimensionado correctamente.

4.1.3. Software de control y gestión de la flota

El software de control y gestión de la flota sigue una arquitectura cliente/servidor:

- Un servidor o centro de control de flotas, ubicado en la sede central de la empresa. Los datos actualizados de los vehículos se almacenan en una BBDD. Servidor y BBDD están configurados en redundancia.
- Aplicaciones cliente que acceden a la información de posicionamiento de los vehículos a través de la red corporativa, estableciendo conexiones con el servidor. Las conexiones remotas se establecen a través de los correspondientes túneles de la VPN corporativa. Las aplicaciones cliente se pueden instalar en cualquier puesto de trabajo y permiten gestionar y visualizar la situación actual de la flota de vehículos.
- Existen diferentes perfiles, para otorgar distintos niveles de privilegio a cada usuario.
- El sistema es modular, parametrizable y configurable, de forma que pueda adaptarse fácilmente a requerimientos futuros. La inversión y los gastos de mantenimiento del entorno técnico son compartidos con el resto de los sistemas corporativos de la empresa.

El centro de control consta de los siguientes módulos:

1. Gestor de Comunicaciones: Control del intercambio de datos entre equipos móviles y Servidor.
2. Servidor de Aplicación y base de datos. Gestión del interfaz con el operador y la comunicación con la base de datos.
3. Módulo de Fonía: Comunicaciones de voz (opcional, para el caso de que se requieran comunicaciones de voz con el conductor a través del sistema).
4. Módulo mensajería y localización: Intercambio de mensajes vehículos – central. Localización GPS.
5. Módulos Configuración. Horarios, servicios, cartografía, …

Figura 11. Interfaz de cartografía en el centro de control

La aplicación se suministra en dos formatos posibles: software instalable en los PC de supervisión (disponible para S.O. Windows y Linux) o plataforma web, con funcionalidades más limitadas. Las ventajas de este último formato son:

- Clientes usan su navegador, no instalación de SW
- Programación modular
- Se podrían agregar funcionalidades de terceros basadas en Web Services.

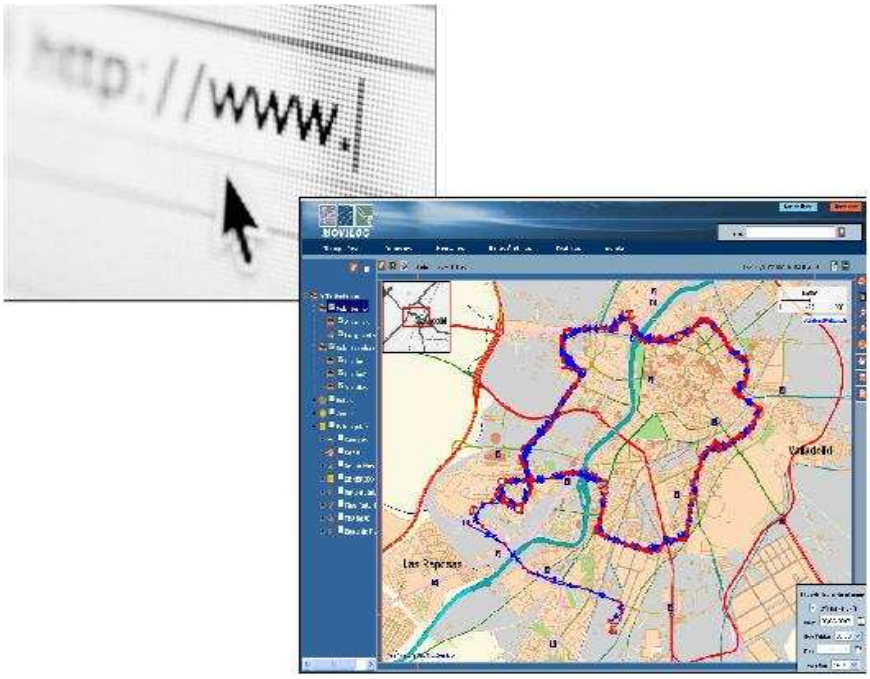


Figura 12. Interfaz de sistema Moviloc

4.2. Automatización del proceso logístico

La automatización del proceso logístico presenta un flujo bidireccional de información entre la sede central de la empresa ubicada en Barcelona y los 30 almacenes repartidos por toda la península. Este intercambio de información se basa en un modelo cliente servidor, y se efectúa de forma segura utilizando la red privada virtual corporativa.

En la red corporativa estos datos tienen marcada relevancia, por ser prioritarios para la compañía, La gestión de la red tendrá sus horas criticas por las mañanas al ser enviados los pedidos y por las tardes al cierre de la jornada.

4.2.1. Plataforma Cliente –Servidor

En nuestro modelo cliente servidor, se contemplan dos áreas diferenciadas:

1. Área 1: conexión entre los almacenes y la Sede Central donde se generan los pedidos (Servidor Central).
2. Área 2: conexión de los camiones con su respectivo almacén. Cada almacén tiene asignado un grupo de camiones.

En la Sede central de la empresa, se ubica la BD Central, donde se van asignando entregas por cada almacén (por ejemplo una tabla por cada almacén). Por las mañanas, al inicio de la jornada de trabajo la parte cliente del Área 1; conformada por '30' terminales (pc's) pertenecientes cada uno de ellos a un almacén, recogen todas las entregas a realizar en el día y las asignan a la parte cliente del Área 2: un dispositivo PDA que recoge cada mañana las expediciones correspondientes a cada repartidor.

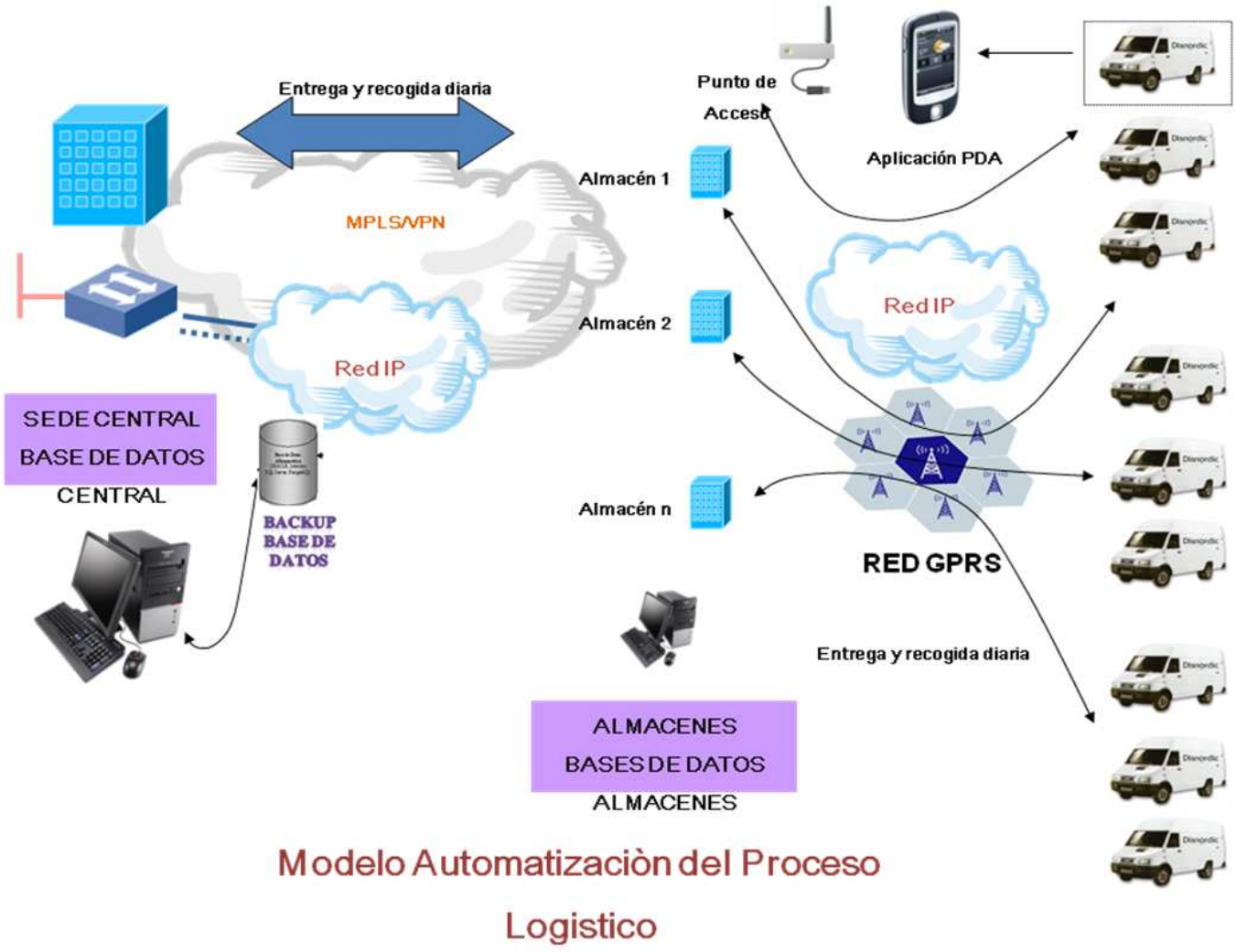


Figura 13. Modelo de automatización del proceso logístico

Durante el día la aplicación que reside en las PDA de los camiones va almacenando los datos de todas las entregas realizadas y al final del día (a una hora prefijada) volcaría dichos datos a su almacén. Éste, a su vez, cuando tuviera los datos de todos sus camiones, volcaría la información a la base de datos central.

4.2.2. Aplicación Software

El software/aplicación de automatización del proceso logístico se caracteriza por:

- Plataforma de movilidad a medida, que permite la sincronización con los sistemas centralizados de gestión ERP's, a través de la red vpn corporativa, BD de los sistemas desarrollados en redundancia

- Cada terminal es reconocido con su propio ID univoco para la creación de CUG (grupo cerrado de usuarios) en casos de acceso a la red corporativa vía GPRS, cada autista se identifica para recibir la actividad que le ha sido asignada.

- Sincronización remota de datos: Clientes, Artículos, Tarifas, incidencias.... wireless o GPRS/SMS.

- A carga completa se muestra una síntesis del total de entregas a realizar, siempre disponible indicador de batería, iconos para envío de mensajes sms/emails.

- Al inicio del reparto son elencadas (según secuencia de entrega) las paradas previstas, el repartidor puede seguir la primera la ruta listada o seguir una ruta alternativa a aquella sugerida seleccionando otra.

- En cada entrega prevista se reporta información básica del cliente, nombre teléfono, dirección, en presencia de navegador GPS en ese momento las coordenadas geográficas del destino estarán disponibles.

Figura 14. Interfaz del software de automatización

- Posibilidad de llamada integrada solo al pulsar un icono, también de inserir notas para gestión de ocurrencias.

- Si está indicado el nombre de la persona o razón social, esta viene propuesta y debe ser recogida la firma que certifica la entrega del producto, prevé la posibilidad de registro de productos rechazados (razón, gestión de retorno al almacén).

Equipos Terminales PDA

Figura 15. Interfaz del software de automatización

- Al final del día el repartidor firma en una opción de la aplicación confirmando los datos que ha recogido en el reparto.
- A este punto los datos y albaranes vienen retransmitidos al software de gestión de los almacenes para su actualización.
- Posibilidad de impresión de documentos.

4.2.3. Plataforma Hardware

En la fase inicial de elección de los terminales se tomo en cuenta la posibilidad de optar por equipos robustos para uso industrial, la idea luego fue desestimada por tratarse de equipos demasiado costosos, no era factible para el proyecto. Axial se Eligio el PDAphone HTC touch cruise II cuyas principales características son:

- Versión nueva de HTC Cruise, una PDAPhone especialmente diseñado para uso como GPS. Combina perfectamente **el GPS, el teléfono y la agenda** en un único terminal completo y ligero.
- **Interfaz de usuario**: Pantalla táctil, Lector de código de barras.Dispone de un procesador de **528 MHz**, **512Mb de ROM y 256Mb de RAM** y el sistema operativo **Windows Mobile 6.1 Professional** con la tecnología **TouchFLO**.
- Incorpora conectividad inalámbrica **PAN Bluetooth 2.0** (Red Inalámbrica de Área Personal) que permite comunicaciones inalámbricas con periféricos tales como impresoras en un radio de 10 metros de distancia por ejemplo **y Wi-Fi IEEE 802.11 b/g** que permite altas tasas de transmisión, además de ranura para tarjetas **microSD**.
- El teléfono permite conexiones **HSDPA/WCDMA/UMTS/GSM/GPRS**.
- M**ultifuncional** independiente del tipo de aplicación: modelo autónomo, cliente-servidor, basado en navegador o emulación de terminal.
- **Accesorios:** Impresoras portátiles y de vehículo, Cuna de vehículo, Cuna de sobremesa, Cargador de baterías, Empuñadora para escáner. **Almacenamiento Persistente,** memoria no volátil en tarjeta incorporada para proteger las aplicaciones y las DB incluso cuando se agotan las baterías.

Figura 16. Dispositivo GPS

4.2.4. Proceso de comunicaciones

Las actividades se dan inicio utilizando distintos tipo de comunicaciones, la entrega y recogida diaria de la información logística, en toda la red corporativa se hace utilizando los túneles securizados de la VPN:

- Sistema Wireless: mediante un punto de acceso a la Lan inalámbrica, el cual permite cargar toda la información necesaria en la PDA desde la DB de cada almacén, de igual manera al final del día de trabajo se realiza el proceso inverso, se traspasa la información referente a entregas y albaranes electrónicos generados a la DB de cada almacén, posteriormente a la sede central.

- Sistema Radio WAN, GPRS, GSM/3G: el uso de estos sistemas permitirán realizar operaciones móviles desde lo vehículos de reparto, los camiones volcarían de forma remota los albaranes electrónicos generados después de cada entrega (actualización y gestión de la información en tiempo real), otra facilidad seria el poder enviar por ejemplo mensajes cortos como que el NºPEDIDO XXX, ha sido entregado.

Por razones de seguridad, el uso de de la red móvil GPRS/3G, conlleva adoptar un Modelo Intranet utilizando la red IP de nuestro socio Telefónica, la cual utiliza APN's específicos, para el establecimiento de un contexto.

4.2.5. Firma Digital

Validación de la firma digital

- Firma 'digitalizada' en una pantalla táctil, en donde la persona que recibe la mercancía 'firma' sobre la pantalla de la PDA.
- Uso de certificados digitales, en cuyo caso se deberá tener tarjetas inteligentes que puedan 'leerse' desde la PDA. Estas tarjetas serian propiedad de los clientes finales. Aun es una tecnología bastante en desuso y con el DNI electrónico puede que algún día pueda ser mucho más extendida

5. Video Vigilancia y centralización de alarmas

La Video Vigilancia es hoy en día una opción viable de una manera remota en cualquier empresa y en concreto en el operador estudiado. Esta cualidad permite el resguardo de lugares donde no se requiere la presencia física de un guardia, en este caso al operador vigilar todos los almacenes y las tres sedes principales des de un solo puesto de trabajo. Se va a realizar la instalación de cámaras IP de video vigilancia en todas las sedes del operador, existirá un centro de monitorización centralizado en la sede principal.

A través del equipo de gestión centralizada de alarmas se pueden configurar adecuadamente para filtrar los avisos.

5.1. Sistema centralizado de alarmas

El operador instalará un sistema de alarmas instaladas en cada uno de los almacenes, este sistema, que es gestionado por un centro de control situado en la sede central, posee una consola, equipo que procesa las comunicaciones de los terminales que están instalados en los almacenes.

Este sistema se estructurará en 4 secciones: Recolección de datos, Terminal de abonado, Transmisión y Central Receptora de Alarmas (CRA).

Recolección de Datos: Está conformado por variedad de sensores de contacto, movimiento, humo, contactos magnéticos, rotura de cristal e interruptores de pánico. Esta sección está ubicada en el extremo del almacén que debe ser vigilado.

Terminal de Abonado: Está constituido por un panel donde llegan las señales provenientes de la sección de recolección de datos, este sistema procesa estas señales y en caso de ser necesario activa el sistema de transmisión de alarmas hacia el CRA, usando la interfaz RJ11 de la PTSN. Esta sección está ubicada en el extremo del almacén.

Transmisión: Esta sección constituye el medio de transporte del sistema que es básicamente la PTSN. Esta sección está ubicada entre los dos extremos (Sede central-Almacén)

Central Receptora de Alarmas: Esta sección está constituida por una consola que recibe las comunicaciones que son generadas por todas las terminales de los clientes. Y es la encargada de gestionar las diferentes alarmas que llegan

provenientes de los terminales, El operador utiliza el código proporcionado por el sistema para buscar en una aplicación propietaria los datos del cliente al que corresponde dicha terminal. Esta sección está ubicada en el extremo de la sede central.

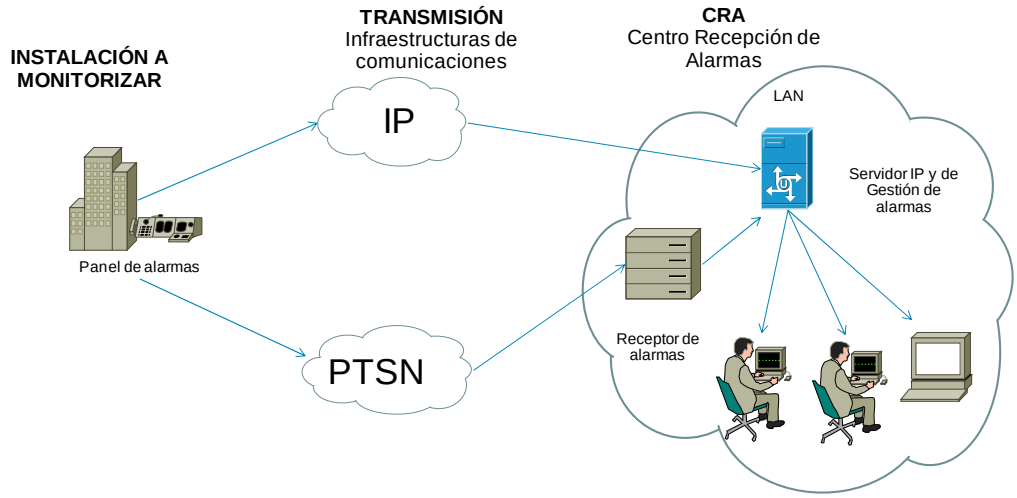


Figura 17. Sistema de alarmas centralizado

El terminal de abonado tendrá un sistema de escalamiento con prioridad teniendo la opción de utilizar al menos dos medios de comunicación, el sistema de escalamiento tendría como primer nivel la interfaz RJ45 para acceder a la red IP, como segunda opción el interfaz RJ11 con conexión a la PSTN.

En la sección de la Central receptora de Alarmas se adicionará el módulo IP para la interconexión con la red IP y la incorporación de un Servidor de Gestión de Alarmas.

Este esquema funcionaría de la manera siguiente, al activarse una alarma en el Terminal de abonado éste establecería una conexión con el CRA usando cualquiera de las tres salidas que posee y utilizando el sistema de escalamiento antes mencionado, el terminal podrá establecer la conexión usando la nube IP,PTSN, respectivamente.

Estos serán los caminos que seguirán las dos opciones del sistema de escalamiento: En el caso de utilizar la interfaz IP la Terminal se comunicara con el Servidor Receptor IP / Gestión de Alarmas mediante la VPN. En el caso de utilizar las interfaces RJ11 (Telefonía Fija) la Terminal se comunicará con la Receptora de alarmas mediante la PSTN, misma que está conectada al Servidor de Gestión de Alarmas.

Al establecerse la comunicación con el Receptor de Alarmas, éste pasará la información al servidor de Gestión de Alarmas, el cual mostrará en el monitor la alerta, pero una de las mejoras de este sistema de Gestión de Alarmas es que brindará mucha más información del cliente, por ejemplo su dirección, que zona y sensor se activó, que hacer en caso de una incidencia, tipo de servicio contratado, imprimir o guardar dicha incidencia y muchas más, todo esto mediante la interfaz gráfica que posee.

Los terminales están enviando información al CRA cada vez que sucede un incidente, la configuración de estos equipos permite cambiar el orden del sistema de escalado así como clasificar que tipo de incidencias debe transmitir y cuáles no, brinda servicios de envío SMS, canal de voz, envío de correo electrónico, alertas a equipos remotos y mucho más.

Es de suma importancia el registrar en el servidor de gestión de alarmas todos los incidentes de cara a poder realizar análisis históricos de incidencias.

Puntos favorables:

- ✓ Fácil instalación
- ✓ Bajo costo operacional
- ✓ Sistema versátil al utilizar tecnología punta
- ✓ No se depende de un solo medio de transporte, cumpliendo así con la normativa legal correspondiente. (UNE-CLC/TS 50136-4:2005 EX UNE-CLC/TS 50136-7:2005 V2 Sistemas de alarma. Sistemas y equipos de transmisión de alarma).
- ✓ Fácil monitorización y reprogramación remota.
- ✓ Modular.

5.2. Sistemas de Video Vigilancia

Se propone implementar equipos modernos que puedan interactuar con sistemas IP y que nos brinden las opciones de mayor velocidad de transmisión, menor tamaño en los datos a almacenar y por ende a transmitir.

En este esquema se detalla la topología totalmente IP que se instalará en los almacenes.

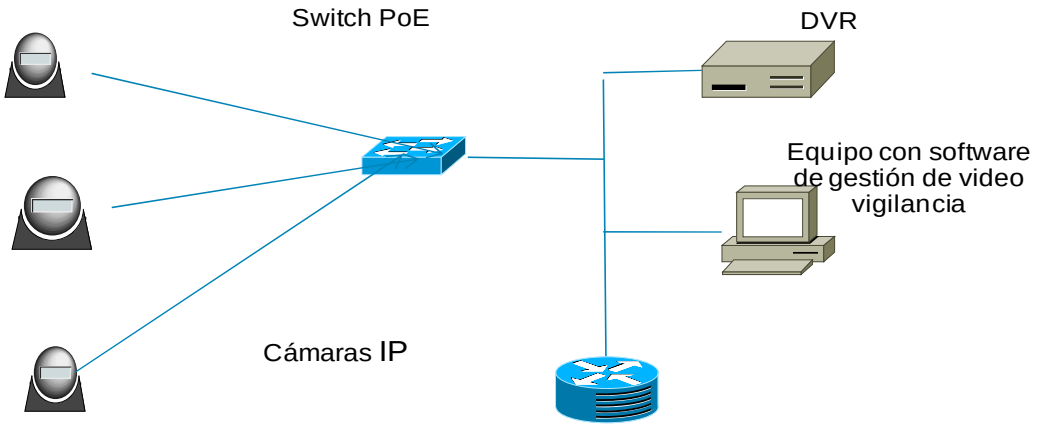


Figura 18. Sistema de Video Vigilancia centralizado

Descripción de la solución

La propuesta cuenta con la incorporación de un sistema que permitirá realizar las grabaciones en formato digital, permitiendo almacenar y monitorear el sistema con diferentes tecnologías.

Siguiendo la estructura antes mencionada podemos describir los cambios en el sistema de la siguiente manera:

Sección Captura

Esta sección está conformada por cámaras IP con tecnología de video H264, la cual nos permitirá tener conexiones multiusuario, visualización, grabación y reproducción de imágenes en tiempo real. Estas imágenes son compatibles con Apple Quick Time, Windows Media Player, VLC Placer entre otros. Estas cámaras poseen tecnología para captura de imágenes en baja luminosidad, así como ampliación de imágenes en directo o en grabaciones HD, PTZ digital. Estos equipos permiten la alimentación por vía Ethernet (PoE), con transmisión de datos desde 12 Kbps hasta 55 Mbps con control de Bit Rate, según la configuración empleada.

El vídeo IP permite el control de la velocidad de imagen a diferencia del vídeo analógico donde todo el vídeo se transmite desde la cámara de forma permanente. El control de la velocidad de imagen en los sistemas de vídeo IP significa que la cámara IP únicamente envía imágenes a la velocidad de imagen especificada, sin tener que transferir vídeo innecesario a través de la red. La cámara IP puede configurarse para transmitir imágenes si por ejemplo se detecta actividad en una zona, por una alarma y/o sensor o por una configuración horaria previa.

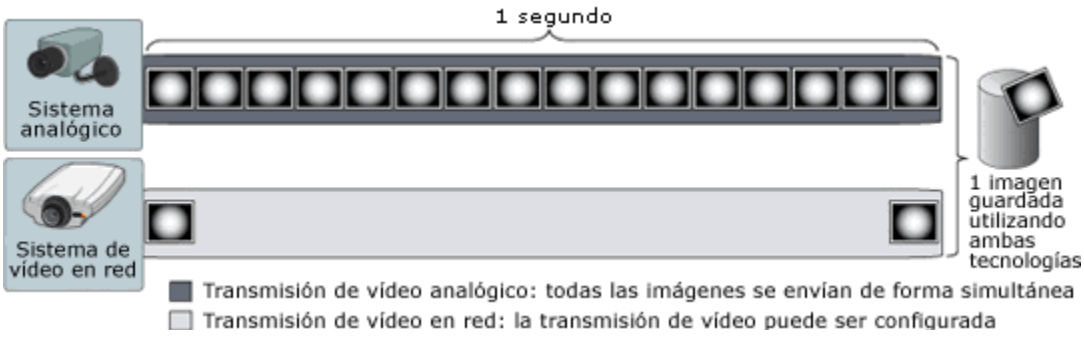


Figura 19. Transmisión de video analógico y en red

También es posible enviar vídeo con velocidades de imagen distintas a destinatarios diferentes, lo que supone una ventaja especialmente en aquellos casos en que se utilizan enlaces de ancho de banda mínimos para ubicaciones remotas.

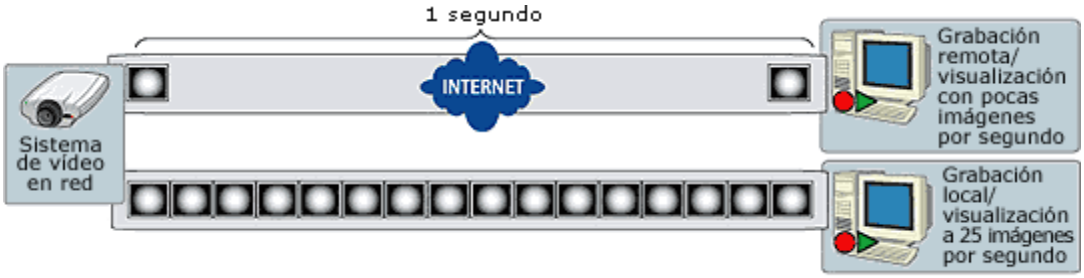


Figura 20. Ejemplos de calidad de video

Al hacer uso de estas características podemos tener la opción de hacer respaldos remotos bajo la modalidad de grabación “En tiempo real” lo cual da una gran ventaja respecto a la antigua tecnología analógica, que solo nos brindaba la opción de hacer respaldos de manera local.

Sección Transmisión.

Esta sección se puede dividir en sección de LAN y WAN

En esta sección LAN los cambios a implementar serán la incorporación de un nuevo cableado y equipos intermedios, contando con cableado UTP Categoría 6e y conmutadores con alimentación vía Ethernet (PoE) de 8 o 16 puertos.

En la sección WAN se utilizara tecnología MPLS como medio de transporte para realizar los respaldos de las grabaciones en Tiempo Real, estas grabaciones se

realizaran en un servidor ubicado en la sede central con alta capacidad de almacenamiento con arreglos RAID5 HOT SWAP y un servicio FTP instalado.

Sección Grabación

Esta sección consta de un equipo de grabación de video digital (DVR) que se encargará de realizar las grabaciones de todas las cámaras IP con la "configuración global" de grabación la cual es de 30 fps (cuadros por segundo), 640x480 de resolución con un 90% de compresión H264, generando hasta 2.9 GB diarios por cámara para su almacenamiento con un ancho de banda de 283 Kbps por cámara. La configuración de "Respaldo Remoto" será de 6 fps (cuadros por segundo), 640x480 de resolución con un 90% de compresión H264, con un ancho de banda de 69 Kbps por cámara.

El sistema de grabación se hará de manera local en el DVR, mediante métodos de grabación específicos según la necesidad del cliente en función de tiempo o alarmas que activen el sistema, con una longevidad de 31 días el día 32 se comienza el ciclo nuevamente reescribiendo sobre el primer día del ciclo anterior. Las copias de respaldo se realizaran vía FTP a un servidor remoto ubicado en la sede central del operador, mismas que serán gestionadas por el DVR. Esta capacidad estará limitada por un máximo de 8 cámaras bajo la configuración de "Respaldo Remoto". En la sede central estas grabaciones serán almacenadas en formato DVD, clasificadas y etiquetadas por fecha y cliente, para luego ser resguardas asegurando su integridad física.

Monitorización

Este sistema está constituido por una versátil interfaz grafica proporcionada por un software de gestión integrado al DVR. Este Software de gestión es una herramienta muy potente a la hora de monitorear y administrar el sistema de vigilancia, brindando facilidades como la grabación por horario, zonas críticas o por sensores de movimiento, control de tramas por segundo (fps), edición de videos, captura de imágenes fijas, acercamientos y demás.

Centro de Control y Monitorización en sede Central.

En el Centro de control y monitorización situado en la sede principal del operador se instalaran servidores de almacenaje de video como respaldo "Online" y como sistema central de control se implementara un servidor CMS que comprueba la

conexión, estado de los discos duros, eventos, detección de movimiento, pérdida de vídeo, grabación, copias de seguridad, etc de todos los equipos.

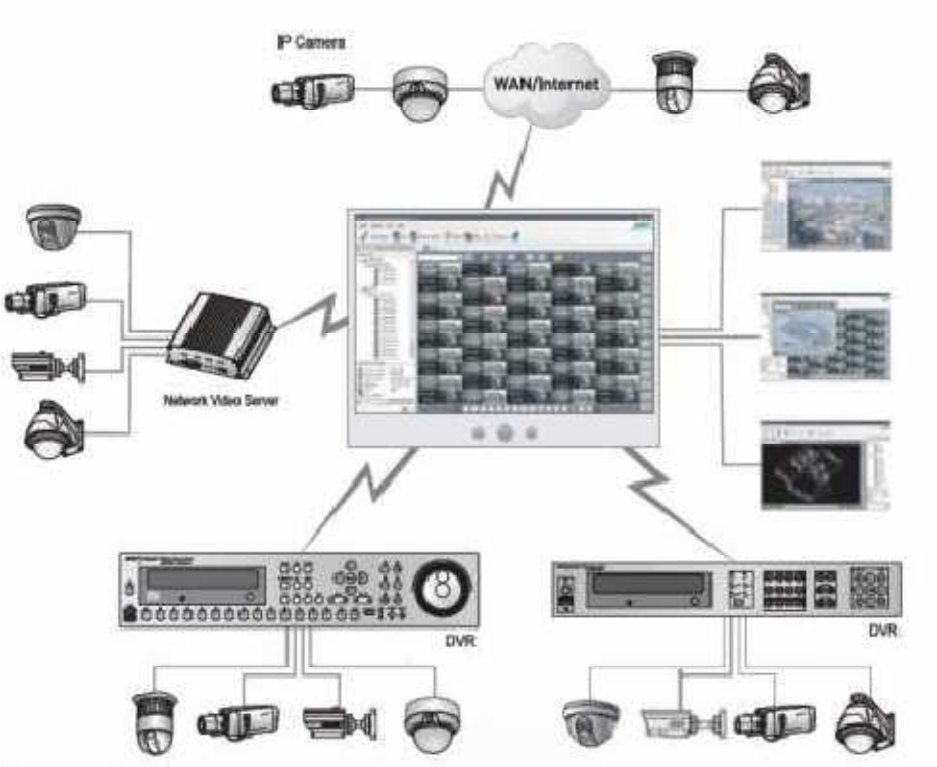


Figura 21. Esquema del centro de control y monitorización

Ventajas de este sistema:

- Acceso local y remoto a las imágenes y videos, usando la red informática, lo que además elimina la necesidad de monitores de seguridad dedicados en la oficina central.
- Seguridad en el acceso al DVR mediante autenticación por medio de un Usuario y Contraseña.
- Mayor flexibilidad pues el programa de gestión de video vigilancia permite realizar un sin número de tareas y modificaciones en las acciones de grabación y monitoreo.
- Permite el respaldo de las grabaciones de manera remota, mediante La grabación en tiempo Real de los videos en un servidor de almacenamiento de datos.
- Centraliza la gestión de estos sistemas mediante la conexión desde un centro de control remoto del operador hasta las estaciones de los clientes para el monitoreo de las cámaras.
- Fácil integración con otros sistemas y aplicaciones.

Categorías	CARACTERÍSTICAS	Ancho de Banda de Subida		Cantidad de usuarios
		DSL (Kbps)	ADSL (Kbps)	
A	1.Clientes con Cámaras IP y DVR 2. Con Respaldo “on line” con un máximo de 8 cámaras y un mínimo de 4, permitiendo entre 2 y 6 conexiones remotas simultaneas. 3. Con Servicio DSL, Modalidad Y (1.5Mbps/1.5Mbps, 50% SCR Subida 768 Kbps). 4.DVR con capacidad de almacenar información diaria de 48 Gb. Con capacidad total de 1,5 TB en HHDD. 5.Configuración de las cámaras de acuerdo a la “Configuración General” 6. Un máximo de 16 cámaras instaladas.	768	0	10
B	1.Clientes con Cámaras IP y DVR 2. Con Respaldo “on line” con un máximo de 3 cámaras y un mínimo de 4, permitiendo entre 1 y 3 conexiones remotas simultaneas. 3. Con Servicio DSL, Modalidad L (2Mbps/640Kbps, 50% SCR Subida 320 Kbps). 4. DVR con capacidad de almacenar información diaria de 48 Gb. Con capacidad total de 1,5 TB en HHDD. 5. Configuración de las cámaras de acuerdo a la “Configuración General”. 6. Un máximo de 16 cámaras instaladas.	0	320	12

Tabla 17. 2 ejemplos de configuración en los que se indican caudales necesarios según el número de dispositivos instalados

6. Plan de implantación y calendario

Esta sección detalla la forma en que se llevará a cabo la implementación de cada una de las soluciones pero como una solución global. Se detallarán aspectos como el plan de actuación, cronograma de instalación, las jornadas de capacitación del personal clave, entrega y adaptación del proyecto.

6.1. Plan de actuación

Como primera fase se ha contemplado una etapa de análisis de requerimientos, cambios, actualizaciones y ampliaciones en los sistemas que posee el operador.

Como segunda fase se procederá a realizar los estudios, cálculos e investigaciones necesarias para brindar las mejores soluciones a los requerimientos del operador, se debe analizar tecnología actual, problemas, deficiencias, modelos, ubicación geográfica de las sedes, cobertura de los servicios, cantidades de usuarios, cantidades exactas de equipos instalados, detalle de la infraestructura en cada sede y en las oficinas de las sedes.

En la tercera fase se procederá a la preparación de las soluciones propuestas siguiendo los aspectos antes mencionados.

Como cuarta fase se entregará un documento que encerrará todas las mejoras como una solución definitiva, la cual deberá ser aceptada por el operador (etapa de negociación de SLA, SLO, precios, modo de implantación…etc.) previo a la puesta en marcha del proyecto; una vez recibido el visto bueno del cliente se procederá al inicio de cada una de las tareas del proyecto.

La quinta y última fase corresponde a la entrega del proyecto.

Fase	Descripción
Primera	Análisis , requerimientos y Contrato
Segunda	Estudios, cálculos e investigaciones
Tercera	Elaboración de Propuesta
Cuarta	Aceptación y puesta en marcha
Quinta	Cierre

Tabla 18. Fases de la implantación

"Networking" término inglés que significa trabajar en una red o trabajar en colaboración con otros. Tomando este concepto se ha denominado Networking a este apartado, ya que sin la colaboración del personal del operador, no se podrían satisfacer las necesidades y requerimientos planteados.

6.2. Plan de implantación

El plan de implantación será de forma lineal y con fases simultáneas, siguiendo un orden de planificación. A su vez el método de implantación será metodológico y seguro. Se realizarán implementaciones de la solución en paralelo tanto en sedes grandes como en sedes pequeñas. Como última parte del proyecto, después de una fase previa de control de posibles errores, se desconectará la antigua red para dar paso al funcionamiento de la nueva red diseñada.

El plan incluirá los detalles de fechas y recursos asignados. Esta planificación tendrá en cuenta los siguientes condicionantes:

- Dependencias con otros proyectos de adecuación de infraestructuras (instalación y/o renovación de electrónica de red, enlaces de comunicaciones, etc…).
- Mínimo impacto en el servicio. En todo momento se perseguirá este objetivo, lo que implicará un cuidadoso diseño de la coexistencia entre los nuevos sistemas y los de partida.

El despliegue del equipamiento de los nodos ubicados en los edificios del cliente incluirá las siguientes tareas:

- Notificación a los responsables y usuarios (si fuese necesario) de las fechas y naturaleza de las intervenciones que se realizarán, así como el impacto que tendrán en los servicios del cliente.
- Instalación, migración y puesta en marcha del nuevo sistema. La puesta en servicio incluirá la conexión entre los equipos instalados a los enlaces de la red de telefonía pública existente y los dispositivos de red del cliente.
- Batería de pruebas para comprobar el correcto funcionamiento del nuevo sistema.
- Traspaso de información a soporte. Actualización de la documentación.
- El despliegue de los equipos requerirá que se cumplan unas condiciones mínimas sin las cuales no es posible garantizar la correcta implantación y el funcionamiento del sistema. Para ello, deben estar aprobadas las condiciones para la Ejecución de las Instalaciones, que verifican que la adecuación del entorno cumple los requerimientos.

Además, el operador deberá de aportar la dirección exacta de cada una de las sedes donde se llevaran a cabo las actividades de instalación, indicando explícitamente el piso o la plata donde se encuentre ubicado la sala de equipos, así como la identificación de dicha sala dentro del piso o planta, mediante un nombre o numero claramente visible.

6.3. Fase de Ingeniería de detalle

Después de que el cliente aceptó esa solución y sus condiciones económicas, (este proceso conlleva varias reuniones) se pasó a definir un contexto temporal en el que el proyecto deberá estar finalizado. Se deberán determinar cuáles son los términos exactos de entrega y definir con exactitud dónde empiezan y dónde acaban las responsabilidades tanto del fabricante o proveedor como la del cliente pasando por nosotros como consultora.

A partir de estas “obligaciones” se establecerán con exactitud unos SLAs que determinaran el servicio que prestará cada uno de los actores en de esta implantación. No debemos olvidar que deberemos negociar también otros SLAs con el propio operador para asegurarnos el buen funcionamiento de esta instalación.

Posteriormente se determinarán las penalizaciones correspondientes en caso de no cumplir estos acuerdos de servicio y por último se diseñará el servicio de atención al cliente que se adapte al escenario diseñado donde también se determinará o contratará a quién se contacta en caso de fallo o mal rendimiento de la infraestructura.

6.4. Calendario de implantación

Se ha realizado un cronograma de trabajo, el cual detalla cada uno de los Hitos, tareas y fechas concernientes al proyecto; herramienta que facilitará el control análisis, evaluación y cambios del proyecto.

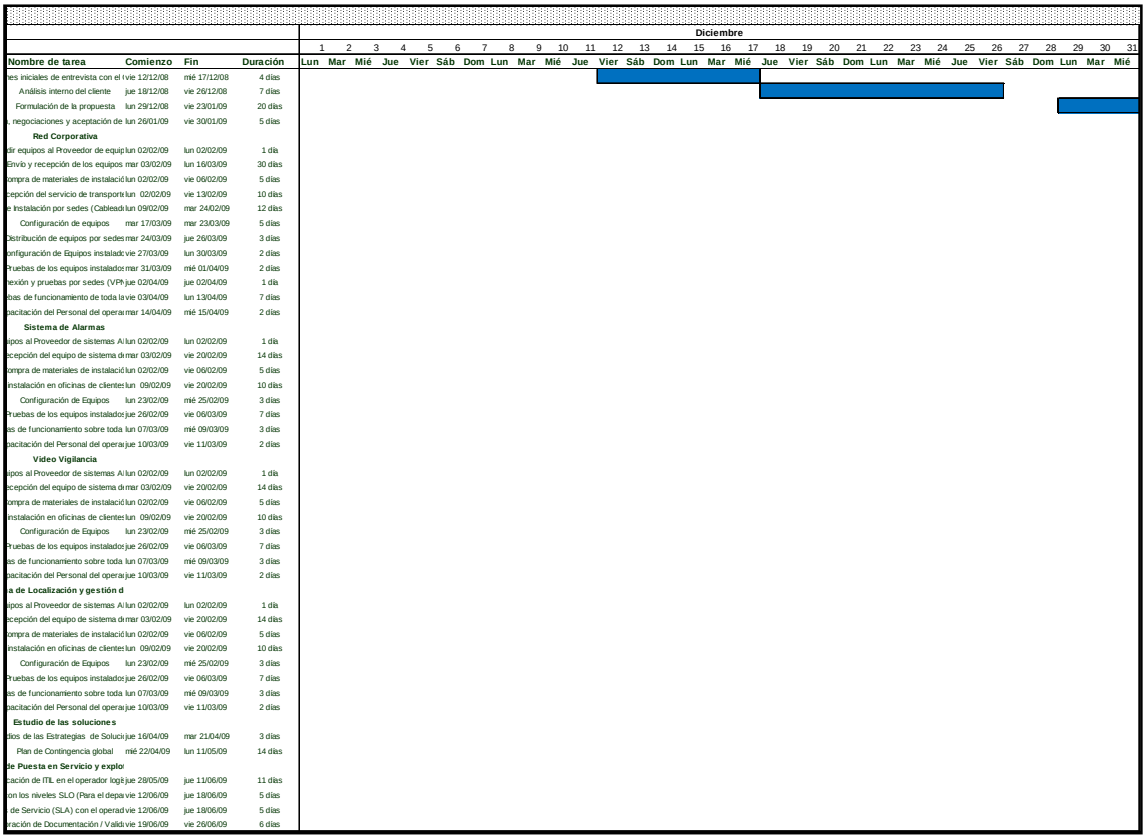


Figura 22. Cronograma (al completo en los anejos)

Para realizar la entrega del servicio exitosamente, y en el tiempo acordado, Se debe coordinar los equipos técnicos necesarios para la instalación de todo el equipamiento en cada sede del cliente.

A efectos del despliegue del sistema, existirán varias empresas involucradas, cada una con ciertas funciones claramente definidas. Dichas empresas son las siguientes:

- Fabricante: Encargado de entregar los equipos a cada sede del cliente y comprobar que los equipos entregados sean los correctos.

- Operadora de Telecomunicaciones: Proporcionara el acceso requerido en cada una de las sedes. Permitirá la conectividad entre sedes mediante la tecnología mpls y comprobara el correcto funcionamiento de la tecnología gprs sobre los dispositivos portátiles.

- Instaladora de Telecomunicaciones: Encargada de realizar la instalación del cableado estructurado en las sedes donde sea necesario, incluyendo el

conexionado y etiquetado de la red, el montaje del rack, la instalación de los equipos de red y la certificación final del cableado.

- Empresa de Servicios Informáticos: Encargada de realizar la configuración técnica de los equipos de red, siguiendo los lineamientos descritos previamente y será responsable de tomar acciones en caso de que algún problema se presentara una vez finalizado el despliegue.

6.5. Instalación y pruebas

Después de la aceptación por parte del operador se da por finalizada la fase de instalación. Se habrán realizado previamente las comprobaciones necesarias según los planteamientos del escenario inicial para poder asegurar las condiciones necesarias para la correcta implantación de la solución propuesta.

Una vez finaliza esta fase de instalación, se realizan las pertinentes pruebas (anexo pruebas) y controles de errores por parte del responsable técnico sobre la instalación realizada, con el propósito de comprobar que se cumplen las condiciones acordadas previamente.

6.6. Entrega y visto bueno del sistema

Una vez culminada la fase de instalación, se informara al cliente de la puesta en marcha del sistema y con esto se da por culminada la fase de instalación.

Es importante recalcar que las demoras causadas por condiciones inapropiadas de la sala de equipos de clientes, no serán tomadas en cuenta en el tiempo de entrega del servicio, que está contemplado entre la entrada de los equipos a cada sede hasta la disponibilidad completa del mismo.

En caso de ser necesario, se implantaran cursos de capacitación al personal de la empresa para el correcto manejo de los equipos involucrados en el nuevo sistema.

7. Plan de explotación, mantenimiento y monitorización

7.1. Mejores prácticas ITIL

Para llevar a cabo la explotación y el mantenimiento de los servicios e infraestructura del operador logístico se seguirán las mejores prácticas de ITIL para la definición de procesos de Gestión de TI.

La implantación de estos procesos facilitará de forma considerable la medición y observación de todas las actividades de Gestión de Servicios de TI, de modo que se proporcionará un aumento del control por parte del operador y de la optimización de los servicios prestados.

Establecer un entorno de gestión basado en ITIL no es un proceso inmediato pues supone un cambio cultural en la empresa, sobre todo en lo que se refiere a la organización de los recursos de TI. Brindar una vía para que los procesos del negocio del cliente mejoren con una gestión de soporte al usuario basado en ITIL, proporciona un plus que incrementará la calidad de sus servicios.

La versión 3 de ITIL enfoca la gestión de los servicios a partir del Ciclo de Vida del Servicio. Este ciclo está formado por cinco fases:

- Estrategia del Servicio
- Diseño del Servicio
- Transición del Servicio
- Operación del Servicio
- Mejora Continua del Servicio

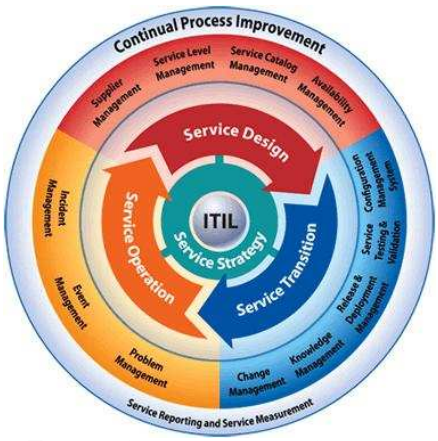


Figura 23. Fases del ciclo de vida del servicio

Cada una de estas fases consta de varios procesos, y la de Operación del Servicio también de varias funciones.

- Estrategia del Servicio:
    - Gestión de la Demanda
    - Gestión de la Cartera de Servicios
    - Gestión Financiera

- Diseño del Servicio:
    - Gestión de Proveedores
    - Gestión del Catálogo de Servicios
    - Gestión de la Seguridad
    - Gestión de la Continuidad
    - Gestión de la Capacidad
    - Gestión de la Disponibilidad
    - Gestión de Nivel de Servicio

- Transición del Servicio:
    - Planificación y Soporte de la Transición
    - Gestión de la Configuración y Activos del Servicio
    - Gestión de Cambios
    - Gestión de Versiones y Despliegues
    - Validación y Pruebas del Servicio
    - Evaluación
    - Gestión del Conocimiento

- Operación del Servicio:
    - Gestión de Eventos
    - Gestión de Accesos
    - Gestión de Peticiones
    - Gestión de Incidencias
    - Gestión de Problemas
    - Centro de Servicio al Usuario (Función)
    - Gestión de Operaciones de TI (Función)

- Gestión de Aplicaciones (Función)
- Gestión Técnica (Función)

- Mejora Continua del Servicio:
  - Proceso de Mejora en 7 Pasos

7.2. Herramientas

Para que la implantación de ITIL sea realmente factible se utilizará la herramienta software Remedy ITSM de BMC, que cuenta con un módulo para cada uno de los procesos. Actualmente es una de las herramientas de este tipo más utilizadas.

Con la ayuda de este software y los procesos comentados se gestionará mucho más eficientemente los servicios y la infraestructura de TI.

A continuación se especifica el módulo asociado a cada uno de los procesos que se van a adoptar:

Proceso	Módulo Remedy ITSM
G. Continuidad ---	---
G. Capacidad	---
G. Disponibilidad	---
G. Nivel de Servicio	BMC Service Level Management
G. Configuración	BMC Atrium CMDB + BMC Remedy Asset Management
G. Cambios	BMC Remedy Change Management
G. Versiones	BMC Remedy Change Management
G. Incidencias	BMC Remedy Service Desk
G. Problemas	BMC Remedy Service Desk
G. Peticiones	BMC Remedy Service Desk
Service Desk	BMC Remedy Service Desk

Tabla 19. Módulo seleccionado para cada proceso

Para gestionar el proceso de Gestión de la Continuidad no hace falta ninguna herramienta específica.

Para gestionar los procesos de Gestión de Capacidad y Disponibilidad se hará mediante una herramienta de monitorización de red, concretamente IBM Tivoli Netcool/OMNIbus/HP Openview/Nagios. Con ella se establecerán se podrán monitorizar los niveles de disponibilidad de los diferentes componentes, su rendimiento, su correcto funcionamiento, etc. Se establecerán alarmas para evitar llegar a niveles que puedan comprometer el cumplimiento de los SLAs, SLOs y OLAs.

7.3. Procesos y funciones adoptadas

Para el caso del operador logístico, se adoptarán algunos de estos procesos y funciones. Hay que destacar que las mejores prácticas ITIL son unas recomendaciones para gestionar los servicios de TI y no es necesario implantar cada uno de los procesos y funciones.

Los procesos que se han decidido adoptar para el caso del operador son los siguientes:

7.3.1. Diseño del servicio

- **Gestión de la Continuidad**

  Tiene por objetivo garantizar la continuidad de los servicios asegurando que las capacidades técnicas y de servicio requeridas son recuperadas en los tiempos acordados y demandados por el negocio. Para ello se definen Planes de Contingencia mediante las siguientes actividades.

  - Actividades:
    - Asignación de responsabilidades
    - Análisis de impacto sobre el negocio identificando procesos de negocio críticos y daños o pérdidas potenciales, recurso necesario para dar continuidad al negocio a un nivel aceptable, y los tiempos de recuperación parcial y total de los procesos caídos
    - Análisis de riesgos identificando el nivel de vulnerabilidad de la organización y las posible amenazas
    - Definición e implantación de medidas para reducir riesgos (estrategia de back up, eliminación de puntos únicos de fallo, controles de seguridad…)
    - Definición y análisis de opciones de recuperación

- Elaboración del plan de continuidad y de los procedimientos de recuperación
- Prueba del plan
- Gestión del plan (formación, revisiones, pruebas)
- Definición del procedimientos de invocación del plan de recuperación

Se definirá un **Comité de Crisis** que será el responsable de declarar la situación de emergencia e invocar el **Plan de Contingencia** que haga falta. Básicamente este proceso de encarga de diseñar los Planes de Contingencia, probarlos y mantenerlos operativos. En el Capítulo 8.4 se especifican los Planes de Contingencia definidos.

A continuación de define el procedimiento seguido para activar un Plan de Contingencia:

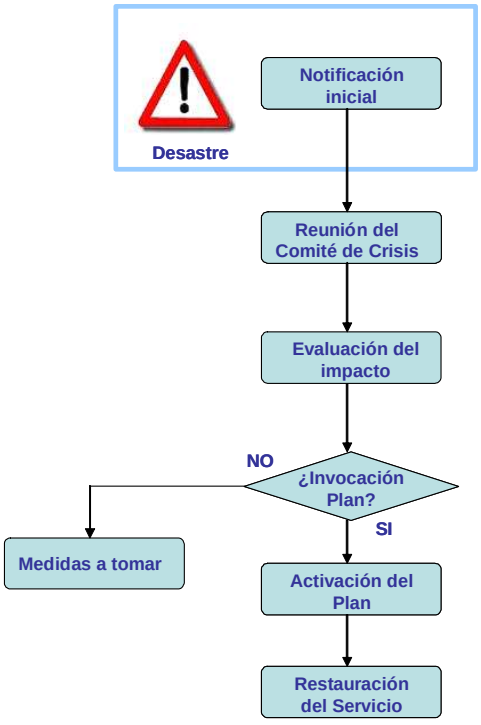


Figura 24. Diagrama de flujo del procedimiento a seguir para invocar un Plan de Contingencia

En caso de que no se invoque el Plan de Contingencia porque el Comité de Crisis no lo considera adecuado, éste decidirá qué medidas tomar para solucionar la situación.

Herramienta:

Este proceso no requiere una herramienta específica para gestionarlo.

Gestor de Continuidad:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Comité de Crisis:

Este comité será el responsable de invocar los Planes de Contingencia, y estará formado por el Director de TI y por los diferentes gestores de cada proceso.

Personal dedicado:

A parte del gestor, se designará a 2 personas del equipo de TI de la sede principal de Barcelona, como se indica en la tabla del punto 8.4 Definición de Roles.

Gestión de la Capacidad

Se responsabiliza de asegurar que la capacidad de la infraestructura tecnológica se ajusta de manera eficiente a las necesidades del operador logístico mediante la monitorización del rendimiento de los componentes de la infraestructura y de los servicios de TI, la definición de actividades de ajuste para garantizar un uso eficiente de los recursos, y la elaboración de un Plan de Capacidad que permita al proveedor de servicios ofrecer estos con la calidad definida en el ANS.

- Actividades:
  - Monitorización de la utilización de cada recurso
  - Análisis de datos para identificar tendencias, establecer niveles de servicio y de utilización, predecir crecimientos en el uso de componentes, y prevenir incumplimientos de los SLAs
  - Identificación de áreas que pueden ser ajustadas para mejorar su utilización o rendimiento y recomendación de medidas de ajuste
  - Ejecución de medidas de ajuste
  - Generación de informes de gestión de capacidad

- Estimación de los recursos necesarios para soportar la incorporación de nuevas aplicaciones o la modificación de aplicaciones existentes asegurando los niveles de servicio acordados
- Elaboración del Plan de Capacidad que documente los niveles actuales de utilización de recursos y rendimiento de los servicios, y estime los futuros requerimientos.

Se monitorizarán lodos los elementos fundamentales para mantener la capacidad de los servicios:

- LAN: el equipo conformado para continuidad enmarcados (*7.4 Definición de Roles) tendrá a disposición el sistema de de control de grafica(SCG), que permite generar la utilización del los recurso (Llámese recurso a uso de procesamiento /Memoria / ancho de banda así como también formularios de registros para aquellos elementos no soportados por la automatización pero que* requieren ser monitorizados para definir su nivel de utilización y capacidades con el objeto de identificar las tendencias de posibles crecimientos, Los informes de gestión de Capacidad estarán programados semanalmente,
- WAN: los niveles de capacidad en términos de ancho de banda, priorización, retardos teóricos y entre otros parámetros de Q&S, el SCG dispone de un modulo (GUI) con una serie de funciones para verificar el estado de la línea de transmisión así como su nivel de Q&S, variables como perdidas de paquetes / congestión /retardos, con lo cual será indicadores primordiales para registrar y alerta sobre los SLA de **Retardos de transito / Perdida de paquetes / Jitter de la red Ip**

La **herramienta Remedy** analizará la información que reporten las herramientas de monitorización, y a partir de los niveles de rendimiento de los recursos, se evaluará si se deben realizar mejoras en la infraestructura para poder soportar nuevas aplicaciones o servicios. En ese caso se deberán realizar Peticiones de Cambio (RFC) a Gestión de Cambios para realizar dichas mejoras.

Mensualmente el quipo de Gestión de la Disponibilidad deberá realizar **informes** con información sobre la capacidad de los recursos comentados anteriormente.

El **Plan de Capacidad** se realizará anualmente con revisiones trimestrales y tendrá la siguiente estructura:

- Introducción: alcance, suposiciones realizadas y resumen ejecutivo.
- Resumen del servicio: actual, reciente y previsto.
- Resumen de recursos.
- Opciones de mejora.
- Recomendaciones sobre que opciones tomar, valorando sus beneficios, su impacto, riesgos, recursos necesarios y coste.

Un ejemplo sería el caso en que se quiere implantar una nueva aplicación interna. Gestión de la Capacidad debería estudiar si la infraestructura actual sería capaz de soportarla y en caso de no poder, estudiar qué se debe hacer para solucionarlo.

Herramienta:

Como se ha comentado en el punto de Herramientas, se utilizará la herramienta de monitorización IBM Tivoli Netcool/Ómnibus para controlar los niveles de capacidad de los diferentes componentes de la infraestructura TI y definir alarmas.

Gestor de Capacidad:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 2 personas del equipo de TI de Barcelona, como se indica en la tabla del punto 7.4 Definición de Roles.

Gestión de la Disponibilidad

Tiene como objetivo diseñar, implantar, gestionar y optimizar la disponibilidad y el uso de los servicios y de la infraestructura en base a lo establecido en los SLAS, siempre que esos niveles de disponibilidad sean rentables de forma que el operador logístico pueda cumplir sus objetivos.

- Actividades:

- Monitorizar los elementos claves de la disponibilidad
- Determinar los requisitos de disponibilidad
- Diseñar y pronosticar los niveles de disponibilidad necesarios
- Producir el Plan de Disponibilidad
- Recopilar información y medidas sobre la disponibilidad
- Asegurar que se cumplen los SLAs en cuanto a disponibilidad
- Revisión y mejora continua de la disponibilidad.

Se monitorizarán lodos los elementos fundamentales para mantener la disponibilidad de los servicios:

- LAN: para definir el nivel de disponibilidad y cumplir con el SLO (Gestión de la Red -**Disponibilidad de la LAN**), el sistema SCG generara los valores porcentuales de no disposición de equipo, con lo cual le será información necesaria para la herramienta Remedy y saltar la respectiva alarma de gestión de disponibilidad.
- WAN: del igual forma el equipo IT en cuestión, tendrá acceso a los snmp de los equipos pertenecientes a la operadora (CE = 4 * cisco 1841), estarán bajo la monitorización de (SCG), el sistema SCG generara los valores porcentuales de no disposición de los CE, la data generada será información necesaria para la herramienta Remedy y saltar la respectiva alarma de gestión de disponibilidad, asegurando el SLA de **Disponibilidad Almacén o Sede**.

La **herramienta Remedy** analizará la información que reporten las herramientas de monitorización, y a partir los niveles de disponibilidad acordados se establecerán unos umbrales, que si son superados harán saltar una **alarmas** para avisar al personal de Gestión de Disponibilidad.

El personal deberá estudiar el motivo por el que la disponibilidad está disminuyendo y tomar las medidas necesarias para solucionarlo.

El **Plan de Disponibilidad** se realizará anualmente con revisiones trimestrales y tendrá la siguiente estructura:

- Introducción: alcance, suposiciones realizadas y resumen ejecutivo.

- Resumen del servicio: actual, reciente y previsto.
- Resumen de la disponibilidad actual comparada con la acordada en los SLAs.
- Opciones de mejora para reducir los problemas de disponibilidad.
- Recomendaciones sobre qué opciones tomar, valorando sus beneficios, su impacto, riesgos, recursos necesarios y coste.

Herramienta:

Como se ha comentado en el punto de Herramientas, se utilizará la herramienta de monitorización IBM Tivoli Netcool/Ómnibus para controlar los niveles de disponibilidad de los diferentes componentes de la infraestructura TI y definir alarmas.

Gestor de Nivel de Disponibilidad:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 3 personas del equipo de TI de Barcelona, como se indica en la tabla del punto 7.4 Definición de Roles.

- **Gestión de Nivel de Servicio**

Pretende mantener y mejorar la calidad de los servicios de TI mediante un ciclo continuo de negociación, monitorización y generación de informes sobre los logros de los servicios de TI y la propuesta de acciones para realizar mejoras en los servicios.

- Actividades
  - Planificación de la estructura de los SLAs
  - Establecimiento de los requerimientos de nivel de servicio (SLR)
  - Negociación de los SLAs
  - Monitorización del rendimiento de los servicios con respecto a los SLAs y comunicación de los resultados.

- Revisión de contratos con proveedores externos e internos cuya actividad afecte al servicio y a los objetivos de los SLAs.
- Elaboración de informes del servicio.
- Mantenimiento y actualización de los SLAs.

Este proceso es clave para la gestión de los servicios de TI. Esencialmente las actividades más importantes de este proceso será la **modificación**, si es necesario, de SLAs existentes, la **incorporación** de nuevos SLAs si es requerido, la **monitorización** de los SLAs actuales. En caso de incumplimiento, el gestor de este proceso deberá ponerse en contacto con el proveedor responsable de ese SLA.

Se realizarán **informes** mensualmente en los que se presentarán por una parte, los SLAs más significativos y se comentarán las tenencias de éstos, como por ejemplo, si se observa una aproximación progresiva al umbral acordado que puede hacer peligrar su cumplimiento. Y por otro lado, se detallarán todos los SLAs clasificados por servicio (ToIP, LAN, WAN, etc.)

Herramienta:

El seguimiento de los SLAs se realizará mediante el módulo de Gestión de Nivel de Servicio, BMC Service Level Management, con el que se monitorizarán os diferentes SLAs.

Gestor de Nivel de Servicio:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 2 personas del equipo de TI, como se indica en la tabla del punto 7.4 Definición de Roles.

7.3.2. TRANSICIÓN DEL SERVICIO

- **Gestión de la Configuración y Activos del Servicio**

Proporciona un modelo lógico de la infraestructura tecnológica y un modo de identificar, controlar, mantener y verificar las versiones de los distintos elementos de configuración, sus configuraciones y la documentación necesaria para su soporte. Es fundamental para contar con una base sólida para la gestión de incidencias, problemas, cambios y versiones, y para poder verificar que los registros de configuración son correctos.

Este modelo lógico se obtiene implementando y manteniendo actualizada una CMDB (Configuration Management Data Base,) que es una base de datos en la que se registra cada elemento de configuración (CI) que sea relevante y la relación que hay entre ellos. Estos CIs pueden ser tanto un Servicio TI, hardware, software, personal, documentación formal (SLAs, etc.), etc.

A la hora de **construir la CMDB** se debe definir su alcance y su profundidad. Con **alcance** nos referimos a los componentes de *qué servicios* vamos a incluir en este modelo lógico. Y con **profundidad**, nos referimos a *hasta qué nivel de detalle* vamos a descomponer los componentes de cada servicio.

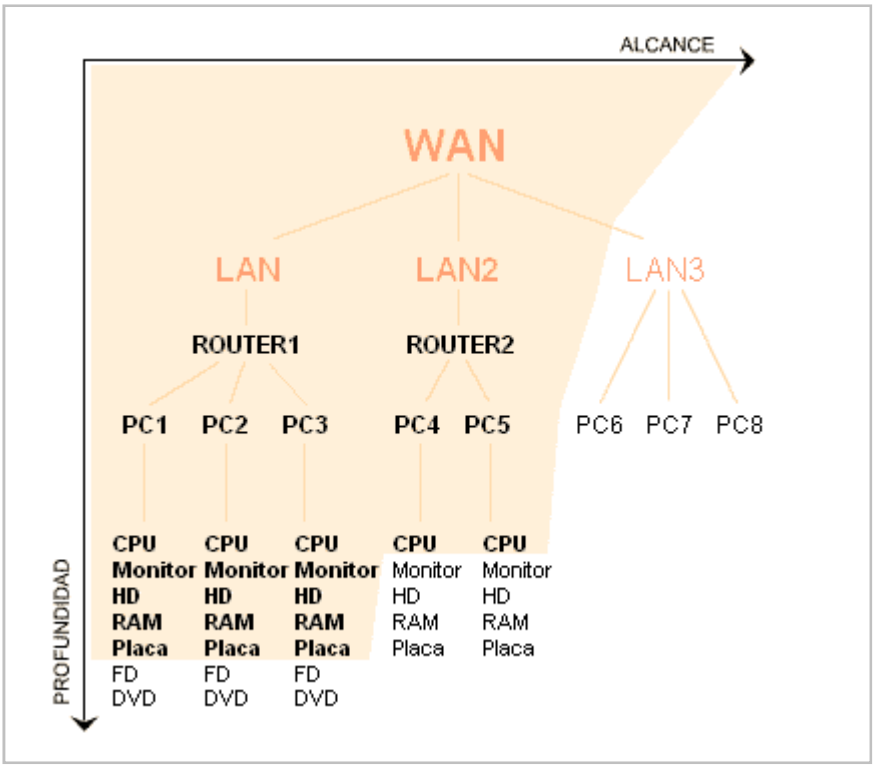


Figura 25. Ejemplo del esquema del alcance y profundidad de la CMDB

Para el caso del operador logístico, se abarcarán los servicios de ToIP, LAN, WAN, Video Vigilancia, alarmas, CPD, Telepresencia y PCs. Y se desglosará cada servicio hasta llegar a unidades HW independientes (Router, Switch, PC, Servidor, etc.), unidades SW (sistema operativo, aplicaciones, etc.), SLAs asociados, licencias y documentación relacionada.

Herramienta:

Se utilizará el módulo BMC Atrium CMDB para crear la CMDB. Y mediante el módulo de Gestión de Configuración BMC Remedy Asset Management, se realizará la gestión de la configuración.

Gestor de Configuración:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Actualizador de la CMDB:

A parte del gestor, se designará al un miembro del personal de TI como encargado de realizar la actualización de la CMDB añadiendo nuevos CIs o eliminándolos. Esta será la única personada con autorización para realizar modificaciones en esta base de datos.

- **Gestión de Cambios**

Proceso que gestiona todas las peticiones que suponen una modificación de la infraestructura de configuración (hardware, software y equipos de comunicación), permitiendo minimizar el impacto de estos cambios, reduciendo las posibles incidencias producidas por los mismos, mejorando la calidad final de los servicios.

- Actividades:
  - Solicitud de cambio (RFC - Request For Change)
  - Registro y Clasificación
  - Convocatoria del CAB
  - Autorización del Cambio
  - Planificación de actualizaciones
  - Coordinación de la implementación del cambio
  - Revisión del cambio
  - Cierre

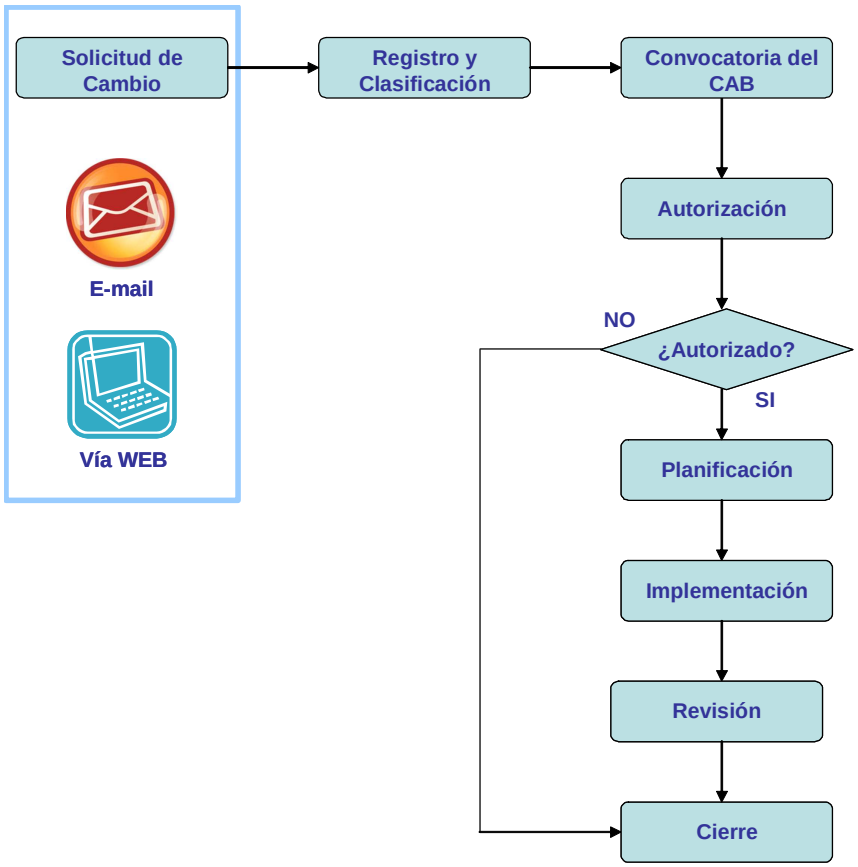


Figura 26. Diagrama de flujo de de las actividades de Gestión de Cambios

Las solicitudes de cambio pueden ser originadas por un usuario que realiza una petición de cambio, por el servicio técnico a la hora de resolver una incidencia o un problema, etc. Las peticiones de cambio se realizarán mediante los siguientes canales de comunicación:

- Correo electrónico

El Gestor de Cambios realizará el **registro** y la **clasificación** de la petición de cambio. La clasificación se realizará de idéntica forma a la de Gestión de Incidencias que se comenta más adelante.

Es importante destacar la figura del **Comité de Asesor del Cambio** o **CAB**, formado por representantes de las diferentes áreas de la gestión de servicios TI, y que es la encargada de asesorar al Gestor de Cambios en la valoración, priorización y planificación de los Cambios. Los miembros de este comité dependerán del servicio al que afecte el cambio, a excepción del Gestor de Cambios que será siempre un miembro fijo del CAB. El siguiente paso es que una vez el Gestor del Cambio ha sido

asesorado por el CAB, decida **autorizar** o no la solicitud. Si la deniega, se pasará directamente al cierre. En caso de que se haya autorizado, el gestor pasará a realizar la **planificación** del cambio indicando las tareas a realizar para llevarlo a cabo.

A continuación se pasa a realizar la **implantación** por parte del personal técnico del banco, y es el gestor de cambios el responsable de su coordinación. A la hora de realizar un cambio siempre se realizará un **Plan de Marcha Atrás** que permita restaurar el servicio al estado anterior a la realización del cambio. Este plan es útil para restaurar el estado original en caso de surgir problemas graves debido a la realización del cambio. La realización de este cambio es responsabilidad de Gestión de Versiones, pero lo supervisa el gestor de Cambios.

Para acabar, una vez se ha finalizado la implantación, se **revisa** que todo funcione correctamente, y si es así, se procede al **cierre** de la petición de cambio.

A continuación se especifican los posibles motivos para realizar una petición de cambio:

- **Correctivo:** Cambio propuesto para la resolución de una incidencia, de un error conocido o de un problema.
- **Mantenimiento:** Cambio propuesto para asegurar el correcto funcionamiento de un servicio (por ejemplo, reemplazar un hardware próximo al fin de su vida útil.)
- **Mejora de Servicio:** Cambio propuesto para optimizar un servicio que está en funcionamiento (por ejemplo, ampliar la memoria RAM de un servidor para mejorar su rendimiento.)
- **Solicitud de usuario asociada a un servicio:** Cambio derivado de una petición de un usuario (por ejemplo, la actualización de un software.)
- **Nueva Funcionalidad:** Cambio propuesto por la introducción de una nueva funcionalidad en un servicio existente
- **Nuevos Servicios:** Cambio propuesto por la introducción de nuevos servicios.

Herramienta:

El registro y seguimiento de las peticiones de cambio (RFC) se realizará mediante el módulo de Gestión de Cambios BMC Remedy Change Management.

Gestor de Cambios:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de **autorizar** los cambios y de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Gestión de Versiones y Despliegues

Tiene como objeto planificar y dirigir el éxito (desde su construcción a la realización de las pruebas) del despliegue de software y de hardware nuevo o de implantar nuevas versiones de ellos.

- Actividades:
  - Planificación de las tareas necesarias para el despliegue
  - Preparación de construcción, pruebas y despliegue (el Gestor de Cambios será quién dé el visto bueno para proceder a la siguiente actividad)
  - Construcción y pruebas de la nueva versión
  - Despliegue de la nueva versión
  - Verificación de que el despliegue ha sido correcto
  - Cierre

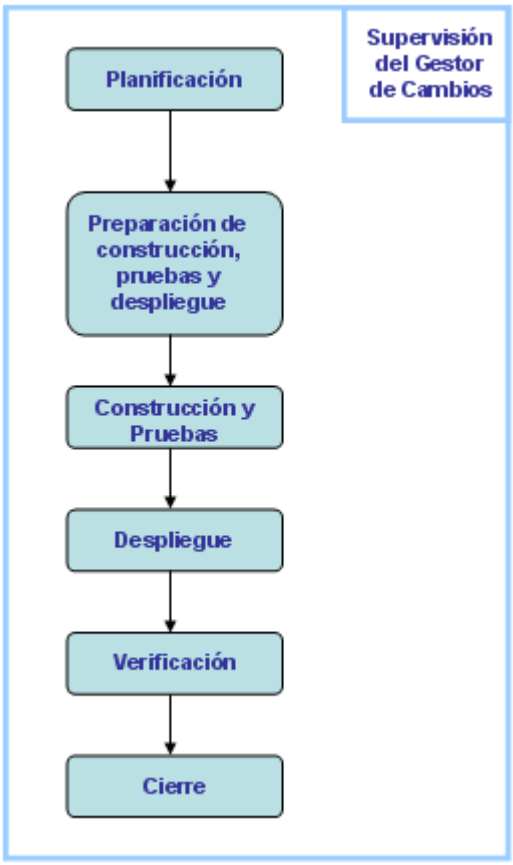


Figura 27. Diagrama de flujo de de las actividades de Gestión de Versiones

Herramienta:

El seguimiento de los despliegues de nuevas versiones se realizará mediante el módulo de Gestión de Cambios BMC Remedy Change Management.

Gestor de Versiones:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 6 personas del equipo de TI de Barcelona y dos por cada una de las demás sedes, como se indica en la tabla del punto 7.4 Definición de Roles.

OPERACIÓN DEL SERVICIO

- **Gestión de Incidencias**

  Según el libro de Soporte del Servicio de ITIL un incidente es:

  "*Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo*".

Esta gestión tiene como objeto restaurar el funcionamiento normal (de acuerdo a lo estipulado en los acuerdos de nivel de servicio) de los servicios lo más rápidamente posible y minimizar su posible impacto negativo, de manera que se aseguren que los mejores niveles de calidad y disponibilidad se mantienen.

- Actividades:
  - Identificación
  - Registro
  - Categorización
  - Priorización
  - Diagnóstico inicial
  - Escalado
  - Investigación y diagnóstico
  - Resolución y recuperación
  - Cierre

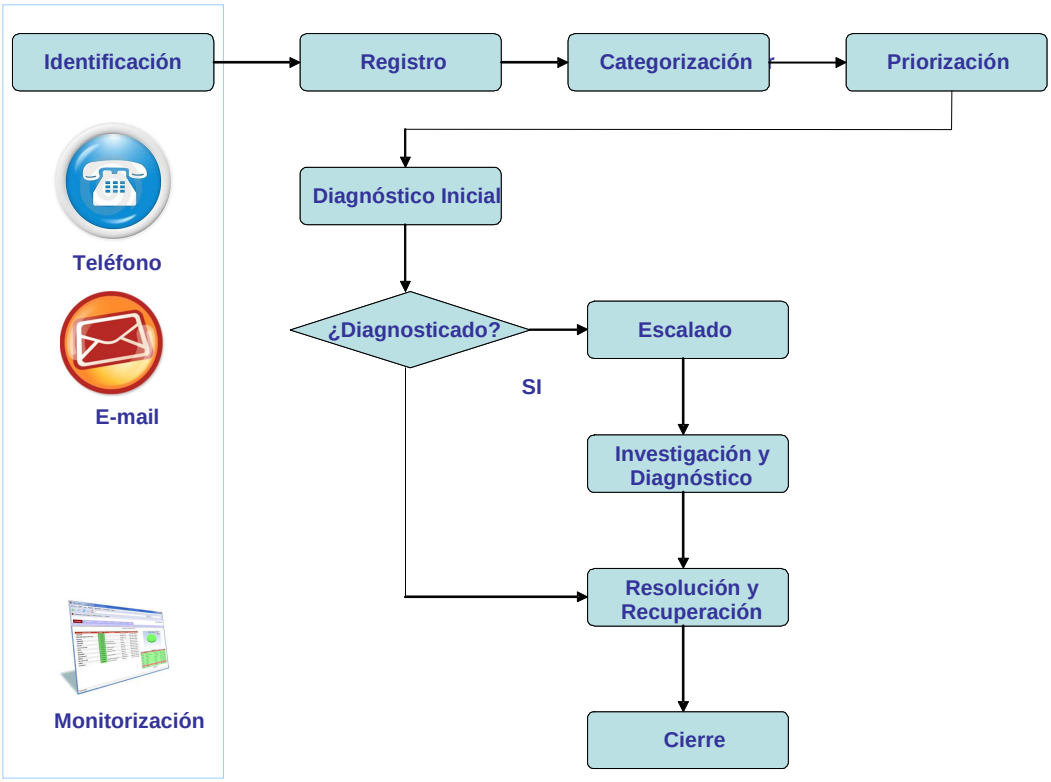


Figura 28. Diagrama de flujo de las actividades de Gestión de Incidencias

El reporte de incidencias comenzará por el registro de las mismas en el single Point of Contact (SPOC) que es el Service Desk. Se trata de un punto de entrada para múltiples procesos, no solamente para la gestión de incidencia. Por lo tanto evita cualquier intento de contacto directo con los especialistas. (más información anexo 1)

Las incidencias podrán ser **identificadas** y comunicadas por personal del operador logístico al detectar una pérdida o degradación del servicio, o por las herramientas de monitorización. Los canales por lo que se comunicarán incidencias serán:

- Teléfono: llamando al Service Desk
- Correo electrónico: dirección de correo del Service Desk
- Herramientas de monitorización

El personal del Service Desk realizará el **registro** (incluir anexo sobre service desk) de las incidencias iniciadas por el personal mediante el módulo de Gestión de

Incidencias de la aplicación Remedy. Las iniciadas por herramientas de monitorización se registrarán automáticamente.

La **categorización** se hará en función de los componentes de infraestructura a los que afecta la incidencia:

- ToIP
- Video Vigilancia
- CPD
- LAN
- WAN
- Alarmas
- Telepresencia
- Otros

Dentro de cada una de estas clasificaciones se distinguirá entre:

- Software
- Hardware
- Otros

La **prioridad** de una incidencia se calcula en función de su impacto y de su urgencia.

El **impacto** se calculará a partir de la siguiente tabla, en la que se evalúa en función de las siguientes variables:

- **Afectación del servicio**: Servicios a los que afecta.
- **Disponibilidad del servicio**: Si supone una degradación o una indisponibilidad del servicio.

Afectación	Disponibilidad	Impacto
ToIP	Degradado	**Medio**
	Indisponible	**Alto**
LAN	Degradado	**Medio**
	Indisponible	**Alto**
WAN	Degradado	**Alto**

	Indisponible	**Alto**
Video Vigilancia	Degradado	**Bajo**
	Indisponible	**Medio**
Alarmas	Degradado	**Medio**
	Indisponible	**Alto**
Telepresencia	Degradado	**Bajo**
	Indisponible	**Medio**
CPD	Degradado	**Alto**
	Indisponible	**Alto**
SW Monitorización	Degradado	**Medio**
	Indisponible	**Alto**
Otro SW	Degradado	**Bajo**
	Indisponible	**Medio**

Tabla 20. Disponibilidad e impacto en cada servicio

La **urgencia** de una incidencia se calculará a partir de las siguientes variables:

- **Repetitiva**: Si el usuario vuelve a contactar con el Service Desk porque una incidencia que se le había resuelto anteriormente no se había hecho correctamente, y el incidente ha vuelto a aparecer.
- **Crítica**: Si la incidencia impide el acceso a los servicios del Banco por parte de los clientes.

Repetitiva	Crítica	Urgencia
No	No	**Baja**
Si	No	**Media**
-	Si	**Alta**

Tabla 21. Clasificación de urgencia según criticidad y repetición

Finalmente la **prioridad** se calcula con la siguiente tabla:

Impacto / Urgencia	Alto	Medio	Bajo
Alta	Máxima	Alta	Media
Media	Alta	Media	Baja
Baja	Media	Baja	Baja

Tabla 22. Cálculo de Priorización

El agente del Service Desk realizará un **diagnóstico inicial** e intentará dar una solución. Si pasado unos minutos (no más de 5 minutos) no lo consigue porque no dispone de los conocimientos necesarios **escalará** la incidencia al segundo nivel de resolución.

Este segundo nivel de resolución está formado por personal de TI más cualificado y será el encargado de realizar la **investigación y el diagnóstico**. En el caso de no dar con una solución escalará la incidencia al tercer nivel de resolución, que corresponde al Servicio Técnico del proveedor del CI que produce la incidencia (router, servidor, aplicación, sistema de comunicación, etc).

Como se ha comentado, se dispone de tres niveles de resolución:

- *Primer nivel de resolución*: formado por lo propios agentes del Service Desk.
- *Segundo nivel de resolución*: formado por el personal de TI especialista.
- *Tercer nivel de resolución*: formado por el servicio técnico de los proveedores.

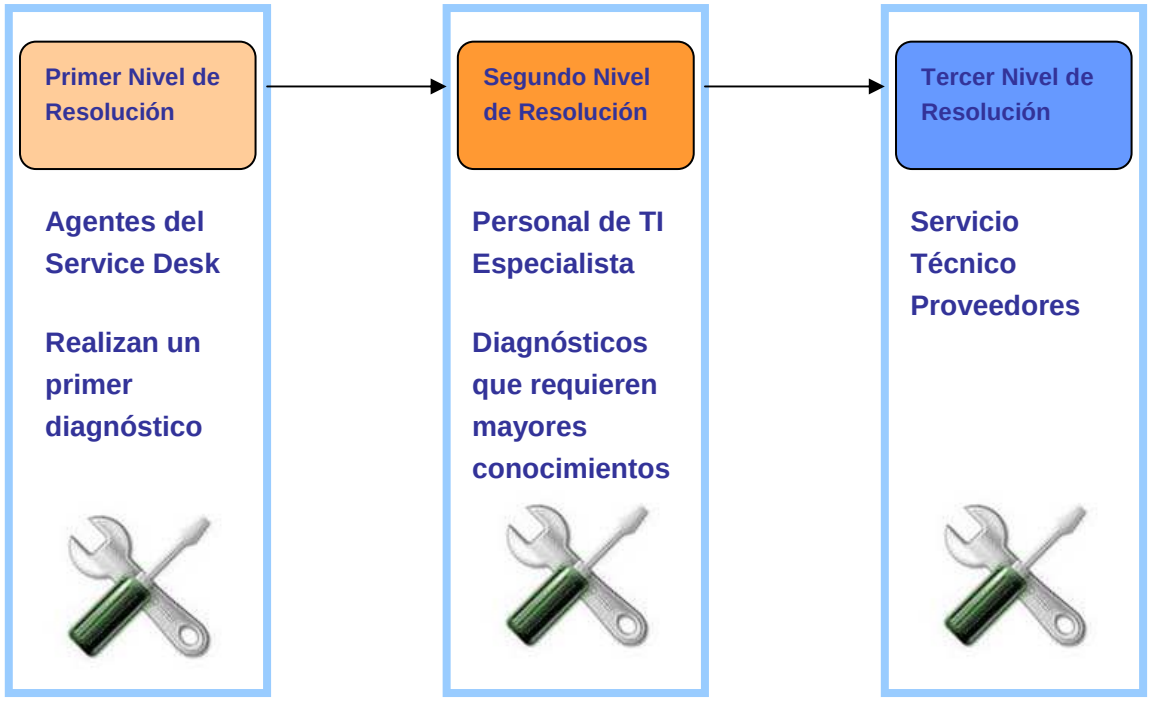


Figura 29. Niveles de Resolución de las Incidencias

El servicio técnico de los proveedores serán los siguientes:

Servicio	Proveedor
ToIP	Cisco
Telepresencia	Cisco
LAN	Cisco
WAN	Telefónica

Tabla 23. Proveedor de cada servicio

Una vez se ha dado con la **solución** se resuelve la incidencia y se **recupera** el servicio que se había visto degradado o indispuesto. Seguidamente el personal de TI valida que la solución funciona correctamente. A continuación se le **comunica** al usuario que la ha iniciado (en el caso de haber sido abierta por un usuario) mediante un correo electrónico, y seguidamente se **cierra** la incidencia.

Los **estados** por lo que puede pasar una **incidencia** son los siguientes:

- **Nuevo:** estado en el que la incidencia acaba de ser registrada pero aun no asignada.
- **Asignado:** estado en el que la incidencia ha sido asignada a un grupo de trabajo técnico, pero todavía no ha sido aceptada por éste.
- **En progreso:** estado en el que el grupo de trabajo asignado ha aceptado la incidencia y empieza a trabajar en ella.
- **Pendiente:** estado en el que la incidencia se ha paralizado por la falta de algún dato importante para su resolución. En el momento es que se disponga de ese dato, se pasará al estado “En Progreso” o “Asignado”.
- **Resuelto:** estado en el que la incidencia ha sido resuelta y se espera a que se compruebe que la solución funciona correctamente.
- **Cerrada:** estado en el que se da por finalizado el ciclo de vida de la incidencia.

Al final de cada mes se publicarán **informes** sobre las incidencias registradas para evaluar el comportamiento del proceso. En ellos se clasificarán las incidencias

por servicio al que afectan (ToIP, LAN, WAN, etc.) y se mostrarán los tiempos de resolución para cada una indicando si se cumplen los tiempos de resolución acordados.

Herramienta:

Todo el flujo de actividades explicado para la gestión de incidencias, se gestionará mediante el módulo de BMC Remedy Service Desk, con la que se llevará el registro de incidencias y su seguimiento hasta el cierre de ésta.

Gestor de Incidencias:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 6 personas del equipo de TI de Barcelona y dos por cada una de las demás sedes, como se indica en la tabla del punto 7.4 Definición de Roles.

Gestión de Problemas

Se entiende como problema aquella causa desconocida de una o más incidencias. El objetivo de este proceso es minimizar el impacto de incidencias y problemas causados por errores en la infraestructura tecnológica, y prevenir que las incidencias asociadas a estos errores vuelvan a ocurrir. Para ello se analiza la causa origen de incidencias y se toman medidas para resolverla.

- Actividades:
  - Identificación de Problemas
  - Registro, categorización y priorización de Problemas
  - Asignación del Problema
  - Investigación y diagnóstico
  - Control de errores
  - Revisión técnica (Post Implementation Review o PIR)
  - Cierre del registro del problema
  - Gestión proactiva de problemas

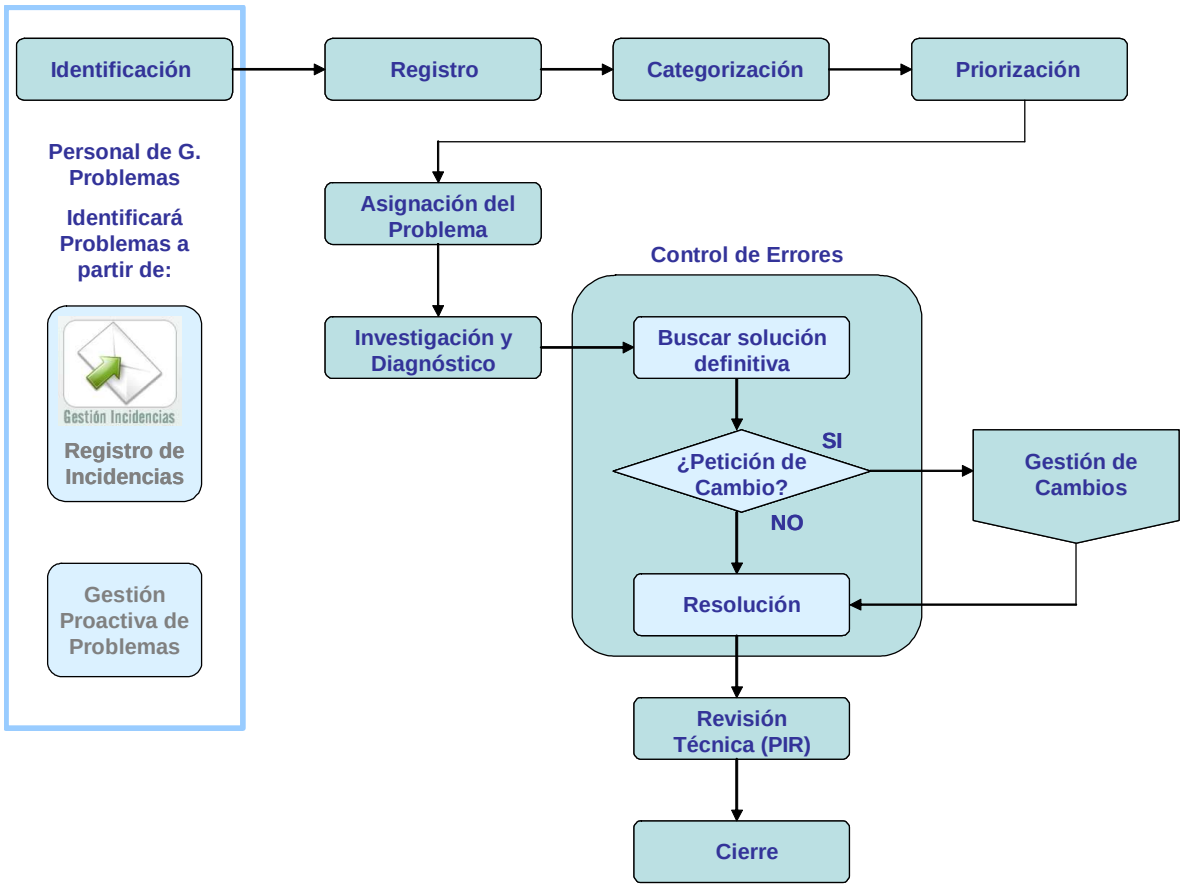


Figura 30. Diagrama de flujo de las actividades de Gestión de Problemas

El personal de Gestión de Problemas se encargará de la **identificación** de problemas. Lo harán a partir de los registros de incidencias, identificando las que son repetitivas o las que están relacionadas entre ellas, por ejemplo a través de uno o varios CIs. También podrá haber problemas detectados mediante la actividad de "Gestión proactiva de problemas".

Una vez detectado un problema de **registra** y se acepta.

A continuación de realizar la **categorización.** Se hará de la misma forma que con las Incidencias. Esto se hace para facilitar la relación entre un problema y las incidencias que éste genera. Como se ha indicado en el punto de Gestión de Incidencias, la asignación de categorías se hace en función de los componentes de infraestructura a los que afecta el problema:

- ToIP

- Video Vigilancia
- CPD
- LAN
- WAN
- Alarmas
- Telepresencia
- Otros

Dentro de cada una de estas clasificaciones se distinguirá entre:

- Software
- Hardware
- Otros

La **priorización** seguirá un esquema muy parecido al del proceso de Gestión de Incidencias. Para empezar se asignará el **impacto** del problema en función de dos variables:

- **Afectación del servicio**: Servicios a los que afecta.
- **Disponibilidad del servicio**: Si supone una degradación o una indisponibilidad del servicio.

Afectación	Disponibilidad	Impacto
ToIP	Degradado	**Medio**
	Indisponible	**Alto**
LAN	Degradado	**Medio**
	Indisponible	**Alto**
WAN	Degradado	**Alto**
	Indisponible	**Alto**
Video Vigilancia	Degradado	**Bajo**
	Indisponible	**Medio**
Alarmas	Degradado	**Medio**
	Indisponible	**Alto**
Telepresencia	Degradado	**Bajo**
	Indisponible	**Medio**
CPD	Degradado	**Alto**
	Indisponible	**Alto**
SW Monitorización	Degradado	**Medio**
	Indisponible	**Alto**

Otro SW	Degradado	**Bajo**
	Indisponible	**Medio**

Tabla 24. Disponibilidad e impacto según servicio

La **urgencia** se determinará en función de los dos siguientes parámetros:

1. Existe una **solución temporal** al problema.
2. Existen **alternativas para dar el servicio** que se ha visto degradado o indispuesto.

Se propone el siguiente esquema para la valoración de la urgencia:

Solución Temporal	Alternativas para el servicio	Urgencia
No	No	**Alta**
No	Si	**Media**
Si	No	**Media**
Si	Si	**Baja**

Tabla 25. Valoración de urgencia según alternativas y urgencia

Finalmente la **prioridad** se calcula con la siguiente tabla:

Impacto / Urgencia	Alto	Medio	Bajo
Alta	Máxima	Alta	Media
Media	Alta	Media	Baja
Baja	Media	Baja	Baja

Tabla 26. Cálculo de Priorización

Llegado a este punto se procede a la **asignación** del problema al personal de TI encargado de la **investigación y diagnóstico** del problema. Deberá buscar una *solución temporal* para reducir o eliminar el impacto del problema y de los incidentes que causa, hasta que no se disponga de una resolución definitiva. Esta solución temporal será utilizada por la Gestión de Incidencias. Se determinará la *causa raíz del problema* y en caso de no tener capacidad suficiente se escalará al segundo nivel de resolución.

Una vez descubierta la causa raíz y se dispone de una solución temporal, el Problema se pasa a considerar como un *Error Conocido*. En este punto es donde entra el **Control de Errores,** que se encarga de buscar una solución definitiva y aplicarla, y enviar la Petición de Cambio (RFC) requerida para aplicar dicha solución en el caso de que sea necesario.

La siguiente actividad a realizar será la **revisión técnica (PIR)** que se encargará comprobar que la solución definitiva aplicada funciona correctamente.

A continuación se procede al **cierre del problema.**

Una actividad importante en el proceso de Gestión de Problemas es la **Gestión Proactiva de Problemas**, que se encarga de realizar estudios para detectar posibles problemas y así evitar posibles incidencias. Como por ejemplo realizando estudios de los históricos de Incidencias y Problemas, de datos sobre la capacidad y rendimiento de sistemas y aplicaciones, de la información de fabricantes. Este último es interesante, dado que con información que nos puedan suministrar los proveedores como el tiempo medio entre fallos de sus productos (MTBF), podemos prever posibles problemas y tomar medidas antes de que aparezcan.

Los *grupos de soporte* que se encargan de las actividades de este proceso, son los mismos que dan soporte a la Gestión de Incidencias. En este caso existien dos niveles de resolución:

- *Primer nivel de resolución*: formado por el personal de TI especialista.
- *Segundo nivel de resolución*: formado por el servicio técnico de los proveedores.

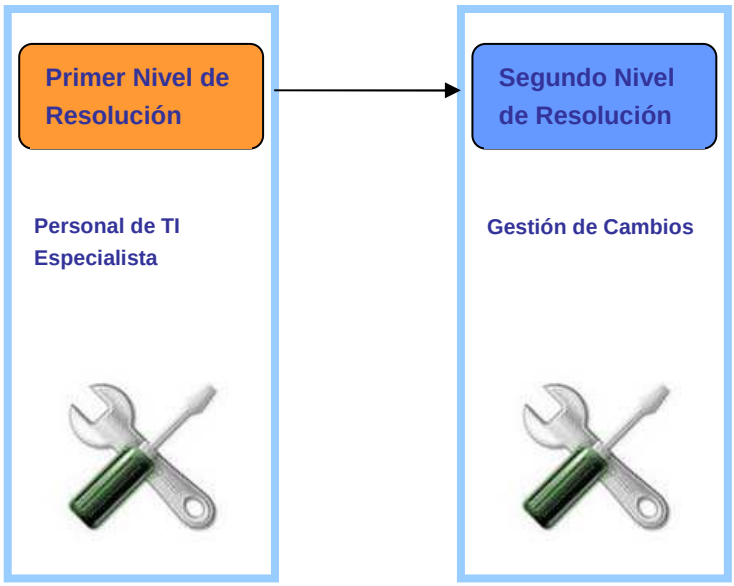


Figura 31. Niveles de Resolución de los Problemas

Al igual que en el caso de la Incidencias, el servicio técnico de los proveedores serán los siguientes:

Servicio	Proveedor
ToIP	Cisco
Telepresencia	Cisco
LAN	Cisco
WAN	Telefónica

Tabla 27. Proveedor de cada servicio

Al igual que en el caso de las incidencias, los problemas pueden pasar por varios **estados**:

- **Nuevo:** estado en el que el problema acaba de ser registrado pero aun no asignado.
- **Asignado:** estado en el que el problema ha sido asignada a un grupo de trabajo técnico.
- **En progreso:** estado en el que el grupo de trabajo asignado empieza a trabajar en el problema.
- **Pendiente:** estado en el que la solución del problema se ha paralizado por la falta de algún dato importante para su resolución. En el momento

es que se disponga de ese dato, se pasará al estado “En Progreso” o “Asignado”.

- **En Revisión:** estado en el que la solución definitiva al problema está siendo revisada.
- **Cerrada:** estado en el que se da por finalizado el ciclo de vida del problema.

Al final de cada mes se publicarán **informes** sobre los problemas registrados para evaluar el comportamiento del proceso. En ellos se clasificarán los problemas por servicio al que afectan (ToIP, LAN, WAN, etc.) y se mostrarán los tiempos de resolución para cada una indicando si se cumplen los tiempos de resolución acordados.

Herramienta:

Todo el flujo de actividades explicado para la gestión de problemas, se gestionará mediante elmódulo de BMC Remedy Service Desk, con la que se llevará el registro de problemas y su seguimiento hasta el cierre de éstos.

Gestor de Problemas:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 2 personas del equipo de TI por sede para dedicarse a las tareas de Gestión de Problemas, como se indica en la tabla del punto 7.4 Definición de Roles.

Gestión de Peticiones

Se encarga de la gestión de solicitudes de servicio por parte de los usuarios. Estas peticiones pueden ser de información, de cambios estándar como por ejemplo un cambio de contraseña, etc.

- Actividades:
  - Contacto del iniciador de la petición: el usuario de pone en contacto con el Service Desk por los canales de comunicación especificados para ello:
    - Teléfono
    - Correo electrónico
  - Aceptación de la petición: el agente del Service Desk debe aceptar la petición.
  - Registro de la petición, clasificación: el agente mediante la aplicación de gestión de peticiones la registrará y clasificará. Si le es posible intentará resolverla al momento.
  - Investigación: si no se ha podido resolver al momento, se escala al grupo de soporte que corresponda para su resolución.
  - Respuesta al iniciador: El agente del Service Desk se pondrá en contacto con el usuario que ha iniciado la petición a través del teléfono o por correo electrónico, para indicarle la resolución.

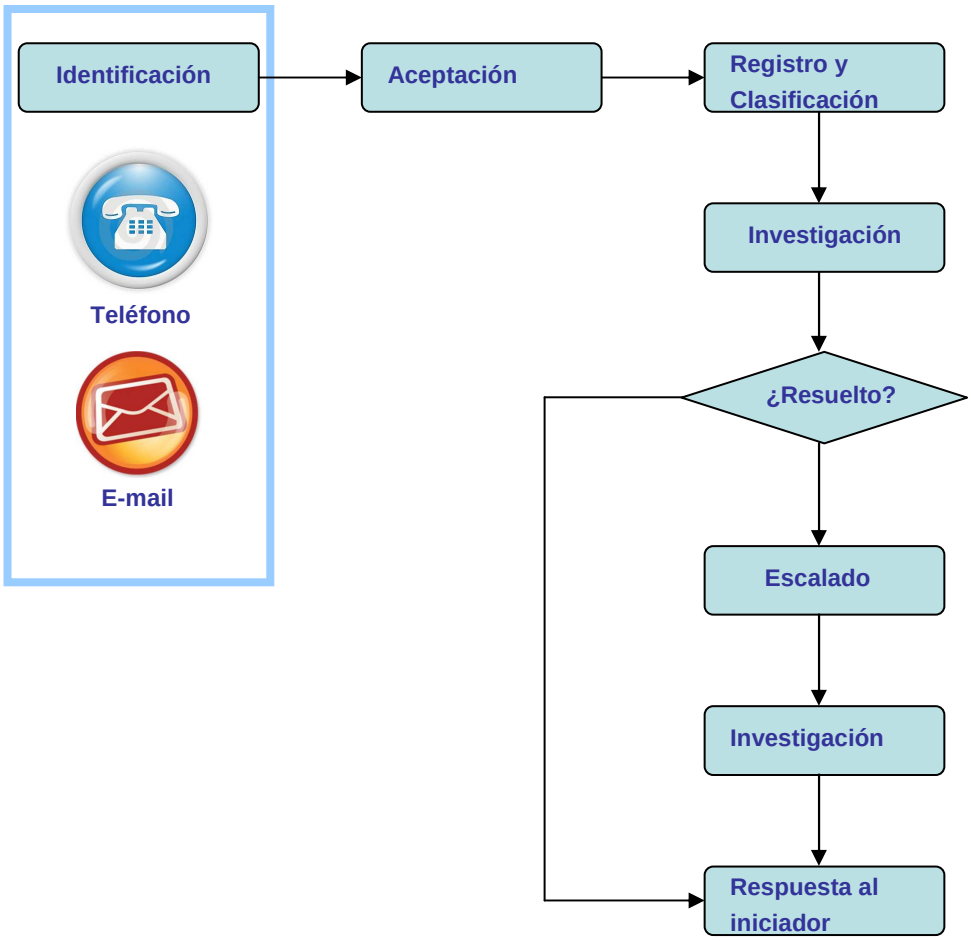


Figura 32. Diagrama de flujo de las actividades de Gestión de Peticiones

La categorización de las peticiones se realizará de la misma forma que en las incidencias y en los problemas:

- ToIP
- CPD
- LAN
- WAN
- Video Vigilancia
- Alarmas
- Telepresencia

Dentro de cada una de estas clasificaciones se distinguirá entre:

- Software
- Hardware
- Otros

Herramienta:

Todo el flujo de actividades explicado para este proceso, se gestionará mediante el módulo de BMC Remedy Service Desk, con la que se llevará el registro de peticiones y su seguimiento hasta el cierre de éstas.

Gestor de Peticiones:

Se asignará este rol a un miembro del personal de TI, como se indica en la tabla del punto *7.4 Definición de Roles*. Será el responsable de controlar que todas las actividades de este proceso se lleven a cabo correctamente.

Personal dedicado:

A parte del gestor, se designará a 2 personas del equipo de TI para dedicarse a las tareas de Gestión de Peticiones, como se indica en la tabla del punto 7.4 Definición de Roles.

- **Centro de Servicio al Usuario *(Service Desk)***

Es una función que tiene como objetivos:

- Ser el punto único de contacto entre los usuarios internos del operador y el servicio de TI, permitiendo la comunicación y escalado de incidencias y peticiones de servicio entre ellos, la comunicación de su estado y evolución.
- Analizar la satisfacción del cliente con los servicios ofrecidos

Estructura

El Service Desk dispondrá de un Centro Primario en la sede central de Barcelona y un Centro Secundario en la sede C que tiene el DRS.

El Centro Primario tiene una estructura centralizada, dado que es el único punto de contacto para todos los usuarios. Esto supone un uso más eficiente y rentable de los recursos, y permite un menor número de personal comparado con una estructura en la que hubiese un centro en cada una de las cuatro sedes, por ejemplo, evitando la necesidad de tener cuatro responsables de Service Desk, uno para cada sede.

El Centro Secundario de define como un centro de apoyo que entrará en funcionamiento en caso de contingencia.

Accesibilidad

La accesibilidad al Service Desk es un punto muy importante dada su función como único punto de contacto. Se han definido los siguientes canales de comunicación:

- Teléfono
- Correo electrónico

Cobertura horaria

La cobertura horaria es 24x7.

El personal que da soporte al Service Desk se organiza en tres turnos de 8 horas para dar dicha cobertura horaria (de 6-14, de 14-22 y de 22-6)

Lenguaje

El personal de soporte utilizará el idioma castellano para atender a los usuarios.

Responsable del Service Desk:

Se designará una personal de TI como responsable del Service Desk, como se indica en la tabla del punto *7.4 Definición de Roles*.

Personal dedicado:

El personal dedicado al Service Desk será parte de los dedicados para el proceso de Gestión de Incidencias y de Peticiones como se indica en la tabla del punto *7.4 Definición de Roles*.

Herramienta:

Los agentes dedicados a realizar las actividades del Service Desk emplearán el módulo de BMC Remedy Service Desk.

7.3.3. MEJORA CONTINUA DEL SERVICIO

Para esta fase del Ciclo de Vida del Servicio no adoptaremos ningún proceso. En vez de contar con un proceso exclusivo para realizar la mejora continua, cada uno de los procesos implantados se encargará de su mejora.

7.4. DEFINICIÓN DE ROLES

Como se ha comentado en el punto anterior, para llevar a cabo las tareas que cada proceso implica, se nombrará a un gestor para cada uno de ellos, que será el responsable de su cumplimiento. Estos roles se distribuirán entre el personal de TI de las diferentes sedes, siendo solo una persona la responsable de cada proceso.

Teniendo en cuenta que en cada sede secundaria el personal de TI está formado por 5 personas y en Barcelona por 10, el resto de personal dedicado a cada proceso se indica a continuación:

Proceso	Personal de TI																														
	Sede D																				Sede C					Sede C				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Continuidad	X																		X	X										
Capacidad	x																							X	X				x	x
Disponibilidad	x														X															
Nivel Servicio		X											X	X																
Configuración			X												X															
Cambios				X																										
Versiones			X										X	X						X					X					X
Incidencias					X		X	X	X	X	X	X				X	X				X	X				X	X			
Problemas						X					X	X					X	X				X	X				X	X		
Peticiones					X		X	X																						
Service Desk					X		X	X	X	X	X	X																		

Tabla 28. Reparto de responsabilidades entre el Personal de TI

Las casillas sombreadas en verde indican los roles de gestor de proceso.

Hay que decir que excepto el personal dedicado a Incidencias, Problemas y Service Desk, la carga de trabajo del resto de personal no es muy grande, por lo que les quedará tiempo para dedicar a otras tareas.

5.5 SLAs / SLOs

Los **SLAs** o **Acuerdos de Nivel de Servicio** servirán para definir el compromiso entre el operador logístico y los proveedores de servicios que contrate. En caso de incumplimiento suponen una penalización. El Proceso de Gestión de Nivel de Servicio será el encargado de controlar su cumplimiento. Los **SLOs** son parámetros que el proveedor se compromete a cumplir pero sin posibilidad de penalización si se incumplen.

A continuación se detallan los SLAs y SLOs que se deberán acordar con el proveedor, que será Telefónica.

- **Plazos de entrega (SLA)**

Se define como el número de días naturales transcurridos desde la recepción del pedido en Telefónica hasta el RFS de la Oficina correspondiente.

	Tipo de Acceso Principal	SLA
MacroLAN	Oficina dedicado red	100 días
VPNIP	Oficina dedicado red	50 días
VPNIP	Oficina ADSL	50 días

Tabla 29. SLA's de entrega

Penalización

Desviación del Plazo de Entrega	Compensación económica
Por cada día natural de retraso completo respecto al valor comprometido	2% de la cuota de alta

Tabla 30. Tabla de penalización

- **Disponibilidad Oficina (SLA)**

Se define la Disponibilidad de Oficina como el porcentaje de tiempo al mes que la comunicación de la oficina del cliente está operativa dentro de la RPV.

Tipo de Oficina	SLA Disponibilidad por Oficina Con Redundancia	
	Diversificado Fibra	Otros accesos de Cobre
Oficina con Accesos Fibra		99,70%
Oficina dedicado red		99,45%
Oficina ADSL		98,95%

Tabla 31. SLA de disponibilidad

Penalización

Desviación de la Disponibilidad		Compensación económica
Hasta 0,1%	1,5% +100%	De la cuota mensual de la Oficina afectada + Cuota Mensual de la Facilidad del SLA Mejorado
Entre 0,1% y 0,3%	3% +100%	
Más de 0,3%	4,5% +100%	

Tabla 32. Penalización sobre disponibilidad

- **Disponibilidad Global (SLA)**

Cálculo del tiempo de indisponibilidad

El tiempo de indisponibilidad se calcula sumando los tiempos de incomunicación de las averías del cliente. Con los datos de averías entregados por el Sistema de Atención a Clientes o Trouble Ticketing (SAC), se mide la disponibilidad mensual de la sede de un cliente de la siguiente forma:

$$\textit{Disponibilidad de Oficina (mensual)} = (T_{tot} - T_{nodisponibilidad\_oficina})/ T_{tot} * 100\ (\%)$$

donde :

T_{tot} = tiempo total del período considerado expresado en minutos/mes, considerando número de días/mes, 24 horas/día y 60 minutos/hora.

$T_{nodisponibilidad}$ = tiempo de no disponibilidad de la comunicación entre la oficina y a RPV dentro del intervalo T_{tot} considerado (minutos). El tiempo de no disponibilidad se contabilizará como la suma de los tiempos de no disponibilidad de todas las averías del cliente, en las condiciones expuestas en el anterior apartado de condiciones.

Se define como la media ponderada de las disponibilidades de todas las oficinas del cliente.

Tipo de Oficina	SLA Disponibilidad Global		
	Sin respaldo	Con respaldo	
		Diversificado Fibra	Otros accesos de Cobre
Oficina con Accesos Fibra	99,95		99,97
Oficina dedicado red	99,50		99,80
Oficina ADSL	-		99,25

Tabla 33. SLA disponibilidad

Penalización

Desviación de la Disponibilidad		Compensación económica
Hasta 0,1%	1,5%	De la cuota mensual de toda la Red del Cliente
Entre 0,1% y 0,3%	3%	
Más de 0,3%	4,5%	

Tabla 34. SLA de penalización sobre disponibilidad

- **Pérdida de Paquetes (SLA)**

Se asegura que el valor de pérdida de paquetes se encuentra por debajo de un valor máximo para cada una de las Clases de Servicio.

Pérdida Diaria de Paquetes	SLA
Clase Plata	< o igual 0.9 %
Clase Oro	< o igual 0.8%
Clase Multimedia	< o igual 0.7%

Tabla 35. SLA de Pérdida de paquetes

Penalización

Desviación Pérdida de Paquetes		Compensación económica
Hasta 0,1 %	1%	De la cuota mensual del Caudal (Caudales Nacionales para el caso de MacroLAN)
Entre 0,1 % y 1%	5%	
Entre 1 % y 5%	10%	
Más de 5%	20%	

Tabla 36. SLA penalización sobre pérdida de paquetes

- **Retardo de Tránsito en la Red IP (SLA)**

Es el tiempo de transmisión medio en milisegundos entre los nodos de la red. Se considera como tiempo de transmisión, el tiempo de ida y vuelta de un paquete de prueba.

Retardo Medio Diario de Tránsito	SLA
Clase Plata	45 msg
Clase Oro	35 msg
Clase Multimedia	25 msg

Tabla 37. SLA retardo de tránsito

Penalización

	Compensación económica
Retardo de Tránsito	6% de la cuota mensual del Caudal de toda la red del cliente (Caudal Nacional para el caso de MacroLAN).

Tabla 38. SLA penalización sobre retardo de tránsito

- **Jitter en Red IP (SLA)**

El Jitter es un parámetro que tan solo se mide en la clase Multimedia. Se define como la diferencia de retardo entre un paquete y el siguiente en la transmisión de la comunicación.

Jitter Diario	SLA
Clase Multimedia	2 msg

Tabla 39. SLA de Jitter

Penalización

	Compensación económica
Jitter en Red	6% de la cuota mensual del Caudal de toda la red del cliente (Caudal Nacional para el caso de MacroLAN).

Tabla 40. SLA penalización sobre Jitter

- **Tiempo medio de respuesta ante averías (SLO)**

Se define como el plazo transcurrido desde la notificación realizada por el cliente hasta que se le da una respuesta indicando el primer diagnóstico.

	SLO
Tiempo medio de respuesta averías	1 hora

Tabla 41. SLO de tiempo de respuesta en averías

- **Tiempo de Resolución de Incomunicaciones (SLA)**

Se define incomunicación como el periodo en el que no existe comunicación entre una Oficina del Cliente con el resto de la RPV, por ninguna de sus conexiones, principal o de backup.

Tipo de Oficina	Tiempo de Resolución de Incomunicaciones (SLA)	
	Oficinas de cliente ubicadas en capitales de provincia	Oficinas de cliente ubicadas en el resto del territorio
Oficina dedicado red (FR, ATM) y Accesos MacroLAN	5 horas	6.5 horas
Oficina ADSL con respaldo	6.5 horas	7 horas

Tabla 42. SLA sobre tiempo de resolución de incomunicaciones

Penalización

	Compensación económica
Tiempo de Resolución de Incomunicaciones	5% de la cuota mensual de la oficina correspondiente por cada hora de desviación respecto al SLA.

Tabla 43. SLA de penalización sobre el tiempo de resolución de incomunicaciones

- **Proactividad (SLO)**

El ratio de proactividad se define como el porcentaje de incidencias abiertas directamente por Telefónica frente al número total de incidencias del cliente-servicio.

	Valor Objetivo (SLO)
Proactividad	60%

Tabla 44. SLO de proactividad

5.6 OLAs

Se entiende como **OLA o Acuerdo de Nivel de Operación**, un documento interno de la organización donde se especifican las responsabilidades y compromisos de los diferentes departamentos de la organización TI en la prestación de un determinado servicio.

Para realizar la explotación y mantenimiento de la infraestructura y de los servicios de TI, se establecerán los siguientes OLAs con el Departamento de IT del operador.

Service Desk		
Indicador	**Medida**	**Objetivo**
Porcentaje de Llamadas abandonadas	Porcentaje de Llamadas abandonadas	7%
Respuesta ante incidencias	Porcentaje de incidencias correctamente diagnosticadas	90%
Tiempo de respuesta vía telefónica	Tiempo transcurrido desde que el operador descuelga el teléfono	90% de las llamadas en menos de 45"
Tiempos de Respuesta vía e-mail		Cada 15 minutos debe ser chequeado el buzón de e-mail

Tabla 45. OLA sobre Service Desk

Resolución de Incidencias		
Indicador	**Medida**	**Objetivo**
Resolución de incidencias de prioridad Máxima	Tiempo máximo	4 horas
Resolución de incidencias de prioridad Alta	Tiempo máximo	8 horas
Resolución de incidencias de prioridad Media	Tiempo máximo	24 horas
Resolución de incidencias de prioridad Baja	Tiempo máximo	48 horas

Tabla 46. OLA de resolución de incidencias

Resolución de Peticiones

Indicador	Medida	Objetivo
Resolución de peticiones de prioridad Máxima	Tiempo máximo	4 horas
Resolución de peticiones de prioridad Alta	Tiempo máximo	8 horas
Resolución de peticiones de prioridad Media	Tiempo máximo	24 horas
Resolución de peticiones de prioridad Baja	Tiempo máximo	48 horas

Tabla 47. OLA de resolución de peticiones

Gestión de Problemas		
Indicador	**Medida**	**Objetivo**
Problemas abiertos después de un nombre incidentes correlados de cómo mínimo: **- 2 de Prioridad Máxima** **- 4 de Prioridad Alta** **- 6 de Prioridad Media** **- 10 de Prioridad Baja**	Porcentaje mínimo	98 %

Tabla 48. OLA de gestión de problemas

Equipamiento CPD		
Indicador	**Medida**	**Objetivo**
Disponibilidad de los equipos del CPD	Porcentaje mínimo	99,90%
Disponibilidad de los sistemas que soporta el CPD	Porcentaje mínimo	99,90%
Disponibilidad del backup	Porcentaje mínimo	99,95%

Tabla 49. OLA de disponibilidad de equipos en el CPD

8. Plan de contingencia

La introducción de las tecnologías no solo en operadores logísticos sino en muchos tipos de empresas crea una dependencia muy grande del negocio sobre ellas. Es por eso que cada día se hace más necesario un plan B, es decir un protocolo que mantenga la continuidad del negocio en caso de fallo de alguno de los sistemas tecnológicos.

Algunas incidencias pueden llegar a tener un impacto altamente perjudicial para el correcto funcionamiento de las operaciones del operador. Conocer de forma precisa los puntos de operación críticos del mismo permite crear procedimientos que mitiguen el efecto adverso de ellas. Esto se realiza mediante un *Business Impact Analysis (BIA).* Hay que tener bien claro el negocio del operador para estudiar cómo posibles fallos en los servicios de TI puedan afectarlo.

Se deben definir una serie de parámetros que servirán para realizar el BIA:

- Consecuencias de la interrupción del servicio en el negocio:
  - Pérdida de rentabilidad.
  - Pérdida de cuota de mercado.
  - Mala imagen de la marca.
- Otros efectos secundarios.
- Cuánto se puede esperar a restaurar el servicio sin que tenga un alto impacto en los procesos de negocio.
- Compromisos adquiridos a través de los SLAs.

	Probabilidad (1 a 5)	Impacto (1 a 9)	Total	RTO (horas)	RPO (horas)	Coste de pérdidas (€/hora)	Probabilidad (mes)	Coste total (€)
Causas Tecnológicas								
Fallo Servidores								
Servidores CPD/Backbone	2	9	11	3	6	5000	1	15000
Fallo Network								0
MacroLan CPD	2	9	11	0,5		15000	1	7500
MacroLan Sedes	4	7	11	0,5		7000	1	3500
ADSL sedes	3	5	8	1		1000	4	4000
Error Hardware								
Servidores Centralizados	2	9	11	0,2		120000	0,5	12000

Routers Backbone	2	9	11	0,2		10000	0,2	400
Routers Sedes	2	6	8	0,5		3000	0,5	750
Switches Distribución	2	8	10	0,2		5000	0,5	500
Switches Sedes	2	6	8	0,5		1000	1	500
Call Manager	1	9	10	0,3		6000	0,2	360
PCs								
Teléfonos	2	2	4	1	N/A	200	0,5	100
Corte de suministro Eléctrico								
CPD/Backbone	1	9	10	0,1	N/A	coste indirecto		
Fallo en SAIS-UPS CPD						coste indirecto		
Causas Naturales:								
Inundación								
Sedes en Planta Baja	4	8	12	N/A	N/A	coste indirecto		
Sedes en Planta 1ª y superior	1	8	9	N/A	N/A	coste indirecto		
Terremoto	1	6	7	N/A	N/A	coste indirecto		
Tormentas Severas/ Eléctricas	2	6	8	N/A	N/A	coste indirecto		
Huracanes	1	5	6	N/A	N/A	coste indirecto		
Causas Circumstanciales								
Riesgo de Bomba	1	9	10	N/A	N/A	coste indirecto		
Vertido de sustancias químicas	1	5	6	N/A	N/A	coste indirecto		
Disturbios Civiles	1	4	5	N/A	N/A	coste indirecto		
Fallo Eléctrico	3	9	12	N/A	N/A	coste indirecto		
Fuego	3	9	12	N/A	N/A	coste indirecto		
Detención de la producción/huelga	1	4	5	N/A	N/A	coste indirecto		
Total								44610

Tabla 50. BIA

Toda empresa que desee asegurar todos sus sistemas informáticos deberá crear un plan de contingencia. Se trata de determinar cuáles son los procesos, datos o aplicaciones mínimos necesarios para el funcionamiento de la empresa.

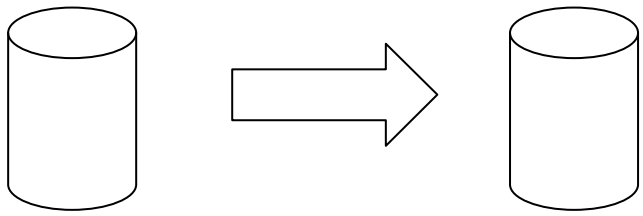
8.1. Metodología de replicación de datos entre CPD y DRS en caso de incidencia

La infraestructura de comunicaciones del operador logístico debe estar disponible 24x7. Para que exista ese nivel de disponibilidad garantizada incluso en caso de fallo del CPD, es necesario que toda la información de las bases de datos que almacenan transacciones replique de manera síncrona en un nuevo DRS (Disaster Recovery System) que como se ha comentado anteriormente estará situado en una sede C la de Almería.

Dado que una replicación síncrona supone un gasto elevado y además en distancias tan largas no es posible implementar este tipo de sistemas sin poner algún punto de copias intermedio; hay que analizar cuáles son las necesidades de disponibilidad de datos de la empresa.

Mediante la implementación del DRS en la Sede de Almería, completamente equipado y listo para entrar en funcionamiento en caso de contingencia, se consigue que el nivel de actualización de los datos recuperados dependa exclusivamente de la frecuencia con la que se replican los datos entre el CPD y el DRS.

Se ha establecido que los camiones descargarán desde las PDAs los datos de todas las entregas realizadas al final de la jornada, de manera que si el CPD sufre alguna incidencia en el DRS se dispone de la copia del día anterior.



En caso de incidencia del CPD El gestor de incidencias comunicará al encargado correspondiente que se desvíen enviar las descargas de datos de los almacenes directamente al DRS. Por otro lado y para evitar que se pierdan datos que ya se han pasado al CPD durante el día y todavía no han sido traspasados al DRS se guardarán los de la jornada anterior en el dispositivo PDA. Además se guardarán en espacios separados las copias antiguas y nuevas, pues el encargado de IT en el DRS deberá determinar hasta qué fecha está actualizada esa base de datos. Esto se sabrá mediante la hora de llegada del último documento, esa será la última hora válida.

.

La empresa necesita por encima de todo tener disponibles los datos de los albaranes de las entregas de cara a la gestión de los pedidos, pues en caso de no tenerlos o tener datos no actualizados puede repetir pedidos o tener problemas de facturación de los pedidos.

El resto de datos y aplicaciones están replicados a diario fuera de horas de trabajo, estos datos tienen un criticidad menor de manera que no supone un problema para el negocio perder algún dato aportado durante el día pues son datos que no son tan urgentes y pueden ser recuperados por otras vías como pueden ser teléfono o e-mail.

Por otro lado debe priorizarse la actividad del departamento de IT en cada sede en caso de caída del enlace y entrada del back up mientras dure la reparación del operador; esto se debe a que el enlace de respaldo excepto en la Sede principal es de menor ancho de banda. En caso de necesitar priorizar algún proceso urgente se permitirá al usuario contactar al departamento IT/Service Desk. Hay excepciones:

- Sede tipo A: en estas sedes dado que no tienen departamento técnico, pues en caso de necesitar asistencia lo hacen remotamente con la sede principal. Dado que manejan muy poco tráfico la conexión RDSI de backup debe ser suficiente. RDSI reduce el número de líneas disponibles a 2 y estas se distribuirán una a administración y otra al almacén.

8.2. Sistema de Alarmas:

Debido a la naturaleza de este sistema que ya presenta una diversidad en la transmisión de las alertas, el plan de contingencia es intrínseco en vista del sistema de escalamiento que el mismo posee. Por lo que no se considera crítico y se asume las consecuencias en caso de fallas de algunos de sus sistemas.

Solo se considera el restablecimiento de los enlaces troncales cargo del responsable adecuado.

1. El responsable activará la recuperación del sistema con el responsable del operador contratado

2. Una vez finalizada la contingencia, el responsable informará al personal de monitorización culminación de contingencia.
3. El responsable debe documentar la incidencia.

8.3. Sistema de Video Vigilancia

Debido a la alta fiabilidad del sistema y a la ausencia de agentes externos influyendo dentro del sistema, consideramos que el factor principal para la falla del sistema sería el corte del suministro eléctrico, pero el sistema cuenta con sistemas UPS que suministran energía por un periodo de 12 horas.

Solo se considera el restablecimiento de los enlaces troncales a cargo del responsable.

1. El responsable activará la recuperación del sistema con el responsable del operador contratado.
2. Una vez finalizada la contingencia, el responsable informará al personal de monitorización culminación de contingencia.
3. El responsable debe documentar la incidencia.

8.4. Transporte y Sede Principal.

En vista de que la mayor contingencia sería la caída del enlace de fibra óptica que llega tanto a la sede principal en Barcelona (tipo D, contiene CPD) como a la sede de Almería (tipo C, contiene DRS), ha sido conveniente contratar back ups.

En caso de contingencia donde la conectividad de algunas de las sedes (Barcelona o Almería) se pierda, se seguirá el plan de Disaster Recovery a cargo del Departamento IT. El plan contempla estos pasos:

1. Una vez identificada la contingencia, el responsable activará la recuperación del sistema con el responsable adecuado del operador contratado, reportando la pérdida de una de las sedes.
2. Se desviará el tráfico de la sede siniestrada a la sede operativa.
3. Activación de equipos de respaldo en la sede de Barcelona o Almería, según sea el caso.
4. Se realizarán las pruebas de verificación de tráfico consiste en:

4.1. Conexión Remota al sistema de administración de Alarmas y verificar el status de los terminales.

5. Hacer seguimiento para el restablecimiento de la sede siniestrada.
6. Se debe documentar la incidencia.

8.5. Pruebas funcionales:

Se ha planificado que en cada uno de los sistemas a implementar se dedicará un periodo de tiempo para la parte de pruebas.

Pruebas periódicas:

Estas pruebas abarcan la parte de conectividad entre las sedes, alcance de la cobertura, configuración, gestión, plan de contingencia y demás. El tiempo de pruebas será monitorizado por personal calificado del operador, de esta manera se asegura el correcto funcionamiento del sistema en general.

Las pruebas a realizar se detallan a continuación:

Sistema de alarmas:

Frecuencia: 1 cada 4 meses

1. Comportamiento del módulo adicionado al terminal de usuario.
2. Envío de alarmas
3. Envío y recepción de la configuración
4. Funcionamiento del sistema de escalamiento
5. Funcionamiento del sistema en caso de fallo del servicio de energía eléctrica
6. Funcionamiento del sistema de escalamiento en caso de fallo del servicio de energía eléctrica.
7. Envío y recepción de la configuración de los terminales desde el CRA.
8. Recepción de las alarmas en el CRA.
9. Gestión del sistema de seguimiento de eventos en el CRA
10. Recepción de alarmas de los módulos IP
11. Caída de servicio del enlace de transporte del CRA
12. Funcionamiento general del sistema con la sede secundaria.

Video Vigilancia (CCTV)

Frecuencia: 1 cada 4 meses

1. Envío de video para la grabación remota (Respaldo Online).
2. Funcionamiento del acceso remoto
3. Capacidad de grabación de los equipos y servidores
4. Funcionamiento de los sistemas CCTV IP
5. Recepción del video remoto en el servidor de almacenamiento en sede central
6. Almacenamiento de las copias de respaldo de los videos.
7. Caída de servicio del enlace de transporte en almacenes
8. Caída de servicio del enlace de transporte en la sede central
9. Cambios de configuración en los equipos por acceso remoto
10. Caída de servicio del sistema de grabación o almacenamiento en sede central
11. Caída de servicio del sistema de grabación en oficinas del cliente
12. Caída de servicio de una o varias cámaras y/o digitales.

Todas estas pruebas se realizarán antes de la puesta en marcha de los sistemas, luego de la implementación se deberán realizar con la frecuencia que se determine en cada uno de los sistemas, las pruebas serán realizadas por el personal IT del operador.

8.6. Mantenimiento y pruebas del plan de contingencia

Realizar periódicamente un informe sobre el plan de contingencia, teniendo en cuenta las posibles modificaciones que se pudieran hacer. No sirve de nada montar todo un plan de contingencia y que luego fallen las copias de discos o el propio software de traspaso de datos así que se realizará lo siguiente:

a. Verificar los procedimientos que se emplearan para almacenar y recuperar los datos (backup).

b. Comprobar el correcto funcionamiento del disco extraíble, y del software encargado de realizar dicho backup.

c. Realizar simulacros de incendio, capacitando al personal en el uso de los extinguidores; caída de sistemas o fallas de servidores, para la medición de efectividad del plan de contingencia.

9. Impacto económico

No es el objetivo del proyecto realizar un estudio de mercado de la tecnología utilizada y por tanto no se realizará un cálculo exacto de la implantación tecnológica realizada. Pero por otro lado se pretende dar alguna pincelada de los beneficios que la implantación de estos sistemas tiene en término económicos.

Es difícil hacer una estimación exacta del impacto económico que puede tener esta evolución de la tecnología en el operador logístico. Por un lado tenemos el ROI (Return of Investment) que es el beneficio directo que resulta de esta innovación tecnológica adaptada; por otro lado tenemos la mejora de imagen que es consecuencia de esa mayor eficiencia en el transporte del operador y que por lo tanto se traduce en mayor fidelidad del cliente.

Se tratará de establecer un escenario realista para cuantificar económicamente el ahorro económico en alguna de las mejoras:

El simple cambio de usar dispositivos móviles (PDAs) en vez de albaranes en la entrega de los pedidos le podrí permitir a cada camión ahorrar media hora al día. Esto se ha calculado estimando que cada camión descarga 20 veces de media al día. Teniendo en cuenta que la flota es de mil camiones y siguiendo con el mismo razonamiento, podría aportar **500 horas de ahorro al día**.

0.5 horas/día/camión* 1000 camiones = 500 horas

Estimando un sueldo medio razonable mensual de camionero de 2000 euros mensuales nos queda que cada profesional cobra 2000 euros al mes / 20dias laborales al mes * 8 horas x día = 12,5 euros/hora

Entonces a partir de estos datos tenemos un ahorro diario de 12,5 * 500= 6250 euros/día.

Extrapolando los datos a un año y nos queda un ahorro anual de 6250 * 220 días laborables y nos queda

6250*220 = **1.375.000 euros de ahorro al año**

Se trata de sólo una estimación pero refleja la cantidad de dinero que puede ahorrarse mediante esta migración tecnológica.

Por otro lado el poner GPS en cada camión nos permite monitorizar la posición exacta de cada vehículo lo que permite reaccionar más rápido a la empresa en caso

de avería y por tanto resolver esa entrega; o por otro lado realizar servicios de urgencia con los que se puede incrementar las ganancias. Este hecho no solo aporta valor económico a la empresa sino que consolida a la empresa como una organización segura y fiable.

La implantación de un sistema de Video Vigilancia centralizado permitirá que se controle la seguridad de todas las sedes desde un solo centro de control y el ahorro que ello implica en cuanto a personal de vigilancia en los almacenes.

A pesar de que a corto plazo adoptar las mejores prácticas ITIL puede parecer un gasto más que un beneficio, a medio y largo plazo supone una importante mejora en la eficiencia de la gestión de servicios TI, lo que conlleva una reducción en costes.

10. Conclusiones

Como se ha explicado el negocio de los operadores logísticos exige tener a su disposición las tecnologías más punteras en cuanto a la localización, trazabilidad de la flota. Al ser organizaciones formadas por muchas sedes es necesaria una interconexión completa entre ellas. Esto permite a la empresa alinearse con las recomendaciones europeas y además tener una infraestructura preparada para la aparición de nuevas tecnologías y aplicaciones.

El hecho de automatizar y por lo tanto dejar en manos de la tecnología el negocio de todo un operador logístico requiere un plan de contingencia, y deben gestionarse los procesos y funcionalidades adquiridas adecuadamente.

Se puede decir a partir de las soluciones adoptadas que:

- ✓ Las propuestas planteadas, solucionan mejorablemente las deficiencias en los sistemas actuales.
- ✓ El buen control, mantenimiento y capacitación del personal, hará posible alcanzar el máximo rendimiento del sistema. La adopción de las directivas ITIL permitirá procedimentar estas actividades.
- ✓ La red del operador será escalable y ofrecerá servicios convergentes a IP, hecho que garantizará la escalabilidad y adaptabilidad de la red a futuros servicios.

- ✓ El sistema de supervisión del que dispondrá el operador logístico junto con el mantenimiento suministrado, los sistemas de back up y redundancia, posibilitaran a la empresa disponer de una red fiable y de alta disponibilidad.
- ✓ En caso de incidencia, la empresa tiene procedimientos y plan de contingencia para no tener que para su actividad de negocio.

Por otro lado el aumento de la rendibilidad en los procesos de la infraestructura logística como consecuencia de la integración de voz y datos o la gestión de flota permite al operador ser más respetuoso con el medio ambiente. El avance tecnológico debe enfocarse hacia un desarrollo sostenible.

Este estudio tecnológico debería realizarse periódicamente con el propósito de sacar provecho de las innovaciones tecnológicas.

11. Bibliografía

- *Juan Gaspar Martínez,* ***Planes de contingencia****. Díaz de Santos*
- *Gonzalo Álvarez y Pedro Pérez,* ***Seguridad Informática para empresas***
- ***MPLS: Technology and Applications****, Bruce S.Davie, Yakov Rekhter*
- ***MPLS and VPN Architectures, Volume I****, Ivan Pepelnjak, Jim Guichard*
- ***Fundamentos de la Gestión de Servicios de TI Basada en ITIL V3****, itSMF International, The IT Service Management Forum*

Enlaces:

- http://www.disasterrecoveryworld.com
- Http://standards.ieee.org
- http://www.securityforum.org/index.htm
- www.**metroethernetforum**.org/

Anejo 1 service desk

Service Desk

El service Desk es uno de los elementos más importantes dentro de las buenas prácticas que recomienda ITIL. Así que aquí se detalla más a fondo sus características

Se trata de una función y por lo tanto de una unidad organizativa especializada. La especialización consiste en atender las llamadas, correos u otros eventos provenientes de usuarios y atenderlas de manera adecuada en función de su naturaleza y de los niveles acordados en los SLAs.

Es punto de entrada para múltiples procesos, no solamente para la gestión de incidencias. Se hace especial mención al grado de especialización del Service Desk, y destacando la posibilidad de acudir a bases de datos de conocimiento para ser más autosuficientes. Según ITIL puede identificarse con el primer nivel de soporte, en este caso lo es.

Un aspecto relevante para ITIL es que el Service Desk actúe como Único Punto de Contacto con el usuario, por lo tanto evitando cualquier intento de contacto directo con los especialistas. Las razones por las que se sugiere esto son:

- Los especialistas no son interrumpidos de manera aleatoria y arbitraria y pueden gestionar mejor su tiempo.
- Los usuarios no siempre acuden al especialista adecuado.
- Los usuarios pueden tender a identificar servicio con personas.
- Cuando los especialistas están ocupados, Service Desk puede ofrecer alternativas que de otro modo los usuarios no conocerán.
- No se “matan moscas a cañonazos”, el Service Desk puede resolver muchas cuestiones sin necesidad de un especialista.

Un buen Service Desk será aquel que des del punto de vista de los usuarios no es un elemento de poco valor.

Este servicio servirá para canalizar todas las incidencias detectadas y que afecten a los usuarios del servicio de red.

La relación con procesos de este servicio:

Con el proceso	Papel del Service Desk
Incidencias	Registra, clasifica y monitoriza las

	incidencias. Incluye la coordinación de actividades de terceros relacionados con la gestión de incidencias. Excepto la investigación y resolución, es el responsable de ejecutar el resto de actividades de la gestión de incidencias.
Entregas	Puede tener asignada la capacidad para software y hardware de manera controlada
Configuración	En su continua consulta de la CMDB es el más indicado para la verificar detalles y reportar discrepancias cuando se detecten.
Cambios	Siendo una de las partes que más contactan con los usuarios, pueden contribuir a la evaluación de la necesidad de los cambios. La atenta observación diaria puede también sugerir cambios proactivos.
Nivel de Servicio	Informa a los usuarios sobre los productos que tienen soporte y sobre los servicios a los que tienen derecho. Notifica reclamaciones o peticiones a la Gestión de Nivel de Servicio.
Otros	Mantiene contacto con los clientes a través de promociones y de provisión de información sobre los servicios Constituye una herramienta excelente para el seguimiento de la satisfacción

Tabla 51. La relación con procesos de el Service Desk

Las funciones del centro son de gestión de incidencias, Centro de información y de Relación con los proveedores.

Tareas a cumplir:

- Registro y monitorización de incidentes. (descrito en el apartado correspondiente)

- Como centro de información, informando a los usuarios de nuevos servicios, canalización de las **Peticiones de Servicio** de los clientes. El cumplimiento de los **SLAs**. El Service Desk juega un papel importante identificando nuevas oportunidades de negocio, y valorando el grado de satisfacción de clientes y usuarios con el servicio prestado.
- Como punto de relación con proveedores, es responsable de la relación con proveedores de servicios externos.

- Aplicación de soluciones temporales a errores conocidos en colaboración con otros centros de gestión.
- Centralización de todos los procesos asociados a la Gestión TI.

Horario de Atención:

- Tipo I: El horario de trabajo será 24x7 (24 horas al día, 7 días a la semana sin excepciones)

- Tipo II: El horario de trabajo será de lunes a viernes en horario laboral de 8:00 a 20:00 horas para lo que no se encuentra incluido en el Tipo I.

En el caso de verificarse un problema de mal funcionamiento de software y/o hardware el personal del Centro Asistencia estará en grado de poder guiar al cliente o usuario a la solución de problemas de 1°nivel.

Si el problema no está en grado de resolverse, se procede con la solicitud de intervención, donde un técnico será enviado a la sede del cliente en un tiempo previsto para la solución del problema.

Con respecto al problema de gestión de telecomunicaciones y de red, se procederá a Informar al proveedor del servicio de red.

Tipo de Problema	Tiempo de Envío de Personal Técnico
Problema software	Dentro de las 2 horas de solicitud
Problema hardware	Dentro de las 2 horas de solicitud
Problema en la Red del Operador de Telecomunicaciones	Dentro de las 2 horas de solicitud

Tabla 52. Tiempos de respuesta del Service Desk

Entre las ventajas que caracterizan a este tipo de Service Desk se tienen las siguientes:

- El “conocimiento” está centralizado.
- Se evitan duplicidades innecesarias con el consiguiente ahorro de costes.
- Se puede ofrecer un “servicio local” sin incurrir en costes adicionales.
- La calidad del servicio es homogénea y consistente.
- Los especialistas no son interrumpidos de manera aleatoria y arbitraria y pueden gestionar mejor su tiempo.
- Los usuarios no siempre acuden al especialista adecuado.
- Los usuarios pueden tender a identificar servicio con personas.
- Cuando los especialistas están ocupados, Service Desk puede ofrecer alternativas que de otro modo los usuarios no conocerán.
- No se “matan moscas a cañonazos”, el Service Desk puede resolver muchas cuestiones sin necesidad de un especialista.

Un buen Service Desk será aquel que desde el punto de vista de los usuarios no es un elemento de poco valor.

Tiene como principal función la de resolver a la brevedad posible, cualquier incidente que cause la interrupción del servicio, el mismo que puede provenir del mismo centro de asistencia, del servicio técnico, de una alarma provocada por nuestros sistemas de supervisión de red instalados en el cliente o de los usuarios, toda alteración e incidencia en el servicio será registrada y clasificada por El centro de Asistencia de consultores IT, siendo necesario para la gestión del mismo, cumplir ciertos parámetros como:

- Estar descrito como un SLA del cliente, de lo contrario reorientarlo a la dependencia correspondiente.
- Que el incidente no haya sido registrado con anterioridad, normalmente como consecuencia de un malfuncionamiento o avería más de un usuario notifica el mismo problema.(evitar duplicaciones innecesarias)
- La prioridad de un incidente esta dado por: el impacto que este tenga en el proceso del negocio y por la urgencia con el que debe ser atendido previo acuerdo en un SLA.

- A cada incidente registrado se le asociara una referencia:

N°Referencia	XXX
Hora y Fecha:	Hora de inicio incidente
Sede:	Lugar de la Sede donde se origino el incidente
Estado:	Registrado, En curso, Resuelto
Tiempo de respuesta esperado:	Tiempo de resolución en base a la prioridad
Nombre Usuario:	Datos persona que informa la avería
Descripción/Síntomas	Detalle de los síntomas de la avería y el equipo involucrado.

Tabla 53. Ejemplo de referencia de un incidente

Se procede a investigar la causa de la incidencia con la ayuda de la KDB (Knowledge data Base) para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento adecuado., documentar la solución, actualizar la información del estado del incidente en la DB, y cerrar la incidencia. Informar a usuarios de su solución, ingresar la información a la base del conocimiento. Se comunica automáticamente al usuario a través de email el estado de su solicitud. Si dicho incidente persiste se eleva a una instancia superior para su oportuna resolución.

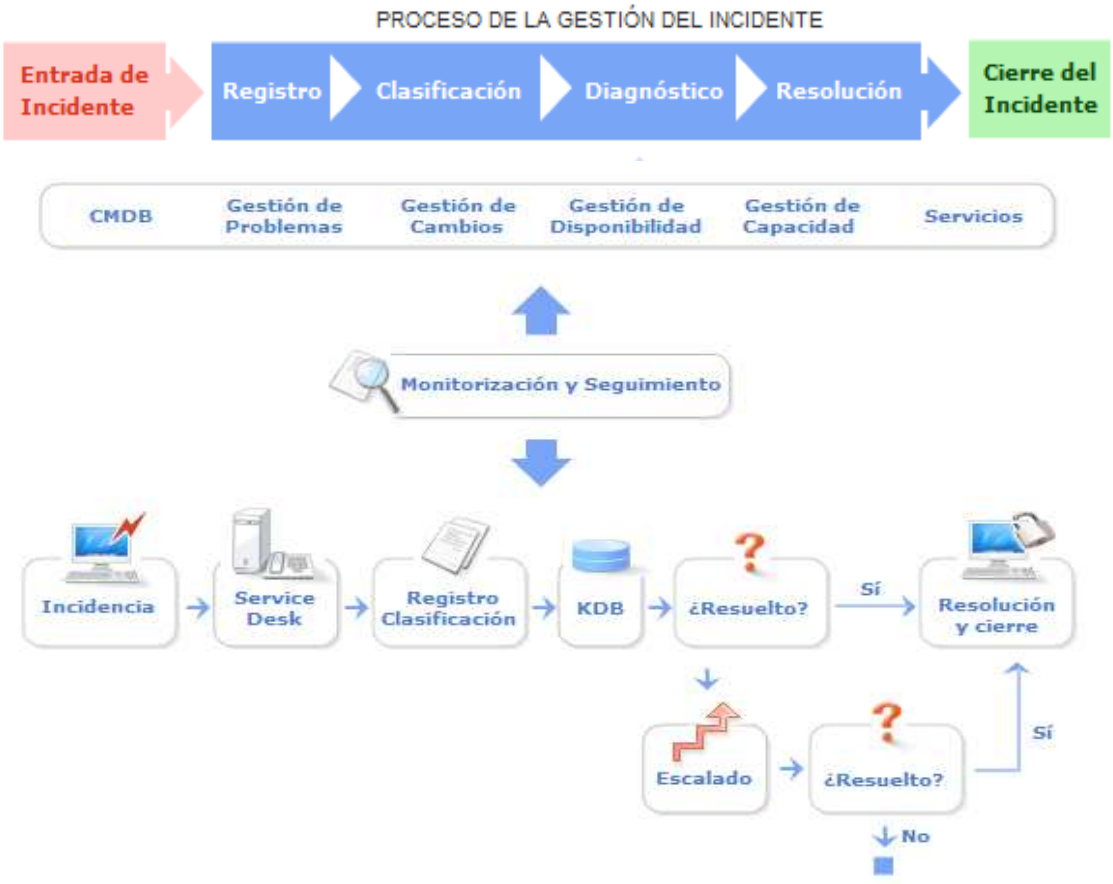


Figura 33. Proceso de la gestión del incidente

Anexo 2 Video Conferencia

Propuesta de equipos para la implementación de las dos salas de video conferencia

Existirán dos salas de videoconferencia en cada sede: una para reuniones del personal directivo y otra para el ofrecimiento de charlas de capacitación para clientes de PYMES.

Para dar el servicio de Telepresencia se han valorado los productos de dos proveedores, Cisco y Polycom. Existen varias alternativas en función del número de participantes en las videoconferencias.

Algunas de las opciones de Cisco se mencionan a continuación:

Cisco Telepresence System 500. Para un participante en cada extremo.

Figura 34. Equipo Cisco Telepresence System 500

Cisco Telepresence System 1000. Para dos participantes en cada extremo.

Figura 35. Equipo Cisco Telepresence System 1000

Cisco Telepresence System 3000. Para seis participantes en cada extremo.

Figura 36. Equipo Cisco Telepresence System 3000

Cisco Telepresence System 3200. Para dieciocho participantes en cada extremo.

Figura 37. Equipo Cisco Telepresence System 3200

Algunas de las opciones de Polycom se mencionan a continuación:

Polycom® HDX 9000™ Series.

Figura 38. Equipo Polycom HDX 9000

Polycom® HDX 8000® Series.

Figura 39. Equipo Polycom HDX 8000

Polycom® HDX 7000 Series.

Figura 40. Equipo Polycom HDX 7000

Una vez valorado el precio de cada uno de los equipos, que se muestra en el siguiente punto,se ha decidido optar por Polycom para dar el servicio de Telepresencia. De entre los equipos estudiados de este proveedor optamos por Polycom® HDX 8000® Series, dado que tiene una buena relación entre las características técnicas y el precio.

El modelo escogido permite una resolución de 1280x720, mediante una pantalla secundaria permite compartir contenido gráficos y presentaciones, y permite realizar hasta 4 video llamadas en una misma conferencia. Estos sistemas suministran

con su códec, micrófonos, cámara control remoto.

Se habilitarán dos salas en cada sede, una para reuniones del personal directivo y otra para el ofrecimiento de charlas de capacitación para clientes de PYMES.

Este servicio requerirá de un ancho de banda de entre 1 y 4 Mbps en función de la calidad deseada para la videoconferencia.

Anejo 3. Planes Pilotos.

Estos Planes son considerados de mucha importancia pues su buena implementación brindara información valiosa sobre la cobertura, funcionalidad, mejoras y dificultades técnicas u operativas que cada sistema pueda tener. Al tener esta información se podrán hacer los cambios necesarios antes de la completa implantación de los sistemas y redes, evitando así complicaciones o gastos innecesarios, al igual que ayudara a tener una retroalimentación de los usuarios sobre las mejoras concretas que estos sistemas brindan en los diferentes departamentos.

Los planes pilotos que se planean desarrollar son los siguientes:

Sistema de Video Vigilancia (CCTV).

En este sistema se ha previsto implementar primero un plan piloto y luego dos fases más, los cuales detallaremos a continuación.

Plan Piloto: Se instalaran sistemas CCTV-IP en 10 clientes ubicados en la ciudad de Barcelona, los cuales tendrán el equipamiento y la configuración necesaria para realizar respaldos locales y remotos, para llevar acabo esto se utilizaran:

6 DVR D1-2408 de 8 canales

4 DVR D1-4816 de 16 canales

6 Switch PoE de 8 puertos

4 Switch PoE de 16 puertos

80 cámaras IP P1311

10 cámaras IP de domo M3011

10 cámaras IP de domo P3301

6 Accesos con ADSL Tipo L (respaldo remoto)

4 Accesos con ADSL Tipo Y (respaldo remoto)

Fase I: Esta fase contempla realizar el Plan Piloto y la implementación de sistemas CCTV MIXTOS en el resto de clientes. La implementación de los sistemas CCTV MIXTOS se hará mediante el uso de la actual infraestructura de CCTV

(Cámaras, cableado coaxial y cableado de alimentación eléctrica) más la incorporación de un DVR como equipo para la digitalización y almacenamiento de las imágenes y los accesos ADSL correspondientes como medio de transporte para los clientes que tengan el servicio de Respaldo Remoto. Para implementar los sistemas CCTV Mixtos se utilizaran:

15 DVR D1-2408 de 8 canales
9 DVR D1-4816 de 16 canales
6 Accesos con ADSL Tipo L (respaldo remoto)
6 Accesos con ADSL Tipo Y (respaldo remoto)

Fase II: Para esta fase hemos considerado que ya se habrá completado la migración de los sistemas CCTV análogos y/o Mixtos por los CCTV-IP, lo que significaría la utilización de los siguientes equipos:

19 Switch PoE de 8 puertos
5 Switch PoE de 16 puertos
173 cámaras IP P1311
28 cámaras IP de domo M3011
24 cámaras IP de domo P3301

GLOSARIO DE ACRÓNIMOS DEL PROYECTO

Acrónimo	Término	Página de aparición
GPS	Global Position System	**2**
PDA	Personal Digital Assistant	**2**
QoS	Quality of Service	**2**
LAN	Local Area Network	**3**
PVC	Virtual Circuit Path	**3**
ADSL	Asymmetric Digital Subscriber Line	**3**
RDSI	Red Digital de Servicios Integrados	**3**
FTP	File Transfer Protocol	**3**
ISDN	Integrated Services Digital Network	**3**
PC	Personal Computer	**4**
IT	Informatio Tecnology	**4**
BW	Bandwith	**5**
ITIL	Information Technology Infrastructure Library	**5**
CPD	Centro de Procesado de Datos	**7**
DRS	Disaster Recovery System	**7**
MPLS	Multiprotocol Label Switching	**8**
VPN	Virtual Private Network	**8**
ATM	Asysnchronous Transfer Mode	**8**
WDM	Wavelenght Division Multiplexing	**8**
RTB	Red Telefonía Básica	**8**
SLA	Service Level Agreement	**9**
VLAN	Virtual Local Area Network	**9**
PRI	Acceso Primario (RDSI)	**10**
BRI	Acceso Básico (RDSI)	**10**
PBX	Private Branch Exchange	**10**
UTP	Unshielded Twisted Pair	**10**
BB.DD	Bases de Datos	**10**
VoIP	Voice over IP	**11**
On-net	On net	**11**

Off-net	Off net	**11**
MAN	Metropolitan Area Network	**12**
WAN	Wide Area Network	**18**
GSM	Groupe Special Mobile	**17**
FPS	Frames Per Second	**20**
HDD	Hard Disk Drive	**20**
DVR	Digital Video Recorder	**20**
Kbps	Kilo bytes per second	**20**
Gbps	Gyga bytes per second	**23**
MB	Mega Byte	**21**
GB	Gyga Byte	**21**
PoE	Power over Ethernet	**24**
CORE	Elemento Central	**27**
NAS	Network Attached Storage	**27**
DMZ	Desmilitarized Zone	**29**
SMTP	Simple Mail Transfer Protocol	**29**
POP	Post Office Protocol	**29**
TCP	Transmission Control Protocol	**29**
GPRS	General Packet Radio Service	**29**
3G	Tercera Generación	**30**
APN	Acces Point Name	**31**
SMS	Short Message Service	**33**
SW	Software	**38**
SO	Sistema Operativo	**38**
ERP	Enterprise Resource Planning	**42**
ID	Identidad	**42**
MHZ	Megahercio	**43**
PAN	Personal Area Network	**44**
SD	Secure Digital	**44**
HDSPA	High-Speed Downlink Packet Access	**44**
WCDMA	Wideband Code Division Multiple Access	**44**
UMTS	Universal Mobile Telecommunications System	**44**
RAM	Random Access Memory	**44**

CRA	Centro Recepción de Alarmas	**47**
PTSN	Public Switched Telephone Network	**47**
RJ	Registrered Jack	**47**
CCTV	Circuito Cerrado Televisión	**50**
TB	Tera Byte	**50**
DVD	Digital Versatil Disc	**52**
CMS	Content Management System	**53**
SLO	Service Level Objectives	**62**
OLA	Operation Level Agreement	**62**
RFC	Request For Change	**65**
CE	Costumer Edge	**67**
ToIP	Todo sobre IP	**70**
CMDB	Configuration Management Database	**70**
CI	Item of Configuration	**69**
PIR	Post Implementation Review	**83**
BIA	Business Impact Analysis	**104**
RTO	Recovery Time Objective	**104**
RPO	Recovery Point Objective	**104**

LISTA DE FIGURAS DEL PROYECTO

LISTA DE TABLAS DEL PROYECTO