Proyecto Fin de Carrera
Ingeniería de Telecomunicación

Gestión y mantenimiento de los puntos de información de un edificio basado en ITIL

Autor: Miguel Rodríguez Iglesias
Tutor: Jesús Iván Maza Alcañiz

Dpto. Ingeniería de Sistemas y Automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2018

Proyecto Fin de Carrera
Ingeniería de Telecomunicación

Gestión y mantenimiento de los puntos de información de un edificio basado en ITIL

Autor:
Miguel Rodríguez Iglesias

Tutor:
Jesús Iván Maza Alcañiz
Profesor titular

Dpto. de Ingeniería de sistemas y automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2018

Proyecto Fin de Carrera: Gestión y mantenimiento de los puntos de información de un edificio basado en ITIL

Autor: Miguel Rodríguez Iglesias

Tutor: Jesús Iván Maza Alcañiz

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2018

El Secretario del Tribunal

A mi familia

A mis maestros

Agradecimientos

A mi tutor Iván Maza, por su eterna paciencia y no perder la esperanza conmigo. A mis padres, por apoyarme en todo lo que pudieron durante este largo camino. A mis suegros, por cuidar de los niños y permitirme tener tiempo para finalizar este proyecto. A mi pareja, Carolina, por ayudarme a levantarme en los momentos de bloqueo y por su infinita comprensión. A mis hijos, Alicia y Héctor, vosotros me habéis dado la motivación necesaria para terminar este proyecto.

Miguel Rodríguez Iglesias

Alumno de Ingeniería de Telecomunicación y autor de este Proyecto Fin de Carrera

Sevilla, 2018

Resumen

En este proyecto se describe la metodología ITIL (Information Technology Infrastructure Library) una guía de buenas prácticas para la gestión y prestación de los servicios de TI (Tecnología de la Información). Se ha realizado un extenso resumen de las fases que componen esta metodología, centrándose más en aquellas que tienen menos orientación comercial.

Se ha definido también un servicio de gestión y mantenimiento de los puntos de información, donde se muestra cómo se trasladaría esta metodología a la práctica.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

La continua evolución de la tecnología de la información ha permitido el desarrollo de nuevos servicios basados en esas tecnologías. Los primeros servicios de TI eran tan novedosos que no existía ningún marco adecuado para estructurarlos. Cada empresa que prestaba estos servicios intentaba organizarlos de acuerdos a modelos que no se adaptaban correctamente a la demanda de cambio y evolución de este tipo de servicios, provocando que la calidad ofrecida fuese muy desigual.

En el escenario anteriormente descrito, surge ITIL, una guía de buenas prácticas para los servicios TI, cuyo objetivo es ofrecer un marco en el que se puedan apoyar las organizaciones que prestan estos servicios para mejorar la calidad ofrecida.

ITIL se ha establecido cómo el estándar de facto para la gestión de servicios de TI, hoy en día prácticamente todas las organizaciones que prestan servicios de TI siguen esta metodología, por lo que es importante conocerla para entender mejor cómo funcionan estos servicios.

En los siguientes apartados se ofrecerá un amplio resumen de la metodología ITIL y su aplicación práctica a un servicio de Gestión y Mantenimiento de Puntos de Información de la Escuela Técnica Superior de Ingenieros.

2 DESCRIPCIÓN DE ITIL

Se puede definir **ITIL** como un conjunto de buenas prácticas cuyo objetivo es mejorar la gestión y provisión de servicios de las Tecnologías de la Información (de ahora en adelante TI). Su fin último es mejorar la calidad de los servicios TI ofrecidos, tratar de evitar los problemas asociados a los mismos y en caso de que estos surjan ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible.

El origen de ITIL data de la década de los 80 cuando el gobierno del Reino Unido, preocupado por la calidad de los servicios TI de los que dependía su administración, solicitó a una de sus agencias, la CCTA (Central Computer and Telecommunications Agency), que desarrollase un estándar para la provisión eficiente de servicios TI.

Actualmente AXELOS es el organismo encargado de velar por este estándar y la responsable de la última versión de ITIL (v3) que data del año 2011.

AXELOS cuenta con la colaboración de varias organizaciones para el mantenimiento de ITIL:

- **itSMF (Information Technology Management Forum):** se trata de una organización independiente y reconocida que tiene como principal misión impulsar la adopción de las buenas prácticas definidas en ITIL para la gestión de servicios TI a nivel internacional.
- **APMG:** se trata de una organización comercial que se encarga de definir, publicar y gestionar las certificaciones ITIL, así como de acreditar a los organismos examinadores.
- **Organismos examinadores:** Organismos acreditados por AXELOS para realizar exámenes para la obtención de las certificaciones de ITIL.

2.1 Gestión de servicios TI

Todos ponemos tener una idea más o menos clara del concepto de servicio, por lo que no es sencillo proponer una única y concisa definición del mismo.

ITIL nos ofrece la siguiente definición:

"Un servicio es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados."

Es decir, el objetivo de un servicio es satisfacer una necesidad sin asumir directamente las capacidades y recursos necesarios para ello.

Por ejemplo, si tenemos una empresa que desea poder ofrecer a sus clientes la posibilidad de que reciban en sus domicilios los productos que adquieren, disponemos de dos opciones:

- Contratar a todo el personal y recursos necesarios (transportistas, vehículos, etcétera) asumiendo todos los costes y riesgos directos de su gestión.

- Contratar los servicios de una empresa especializada.

Si nos decantamos por la segunda opción, los valores que nos aportarán la empresa contratada para prestar el servicio serán los siguientes:

- Utilidad: los productos se enviarán a los domicilios de los clientes.
- Garantía: la empresa contratada será responsable de que los envíos se realicen de acuerdo con lo acordado con el cliente y según unos estándares de calidad predeterminados.

Naturalmente, optar por una opción u otra dependerá de las circunstancias de cada empresa: su tamaño, estructura, etcétera. Actualmente lo habitual es subcontratar todos aquellos servicios que tengan poca relación con la actividad principal de la empresa.

Una correcta gestión de este servicio requerirá:

- Conocer las necesidades del cliente
- Estimar la capacidad y recursos necesarios para la prestación del servicio
- Establecer los niveles de calidad del servicio
- Supervisar la prestación del servicio
- Establecer mecanismos de mejora y evolución del servicio

El objetivo de ITIL es ofrecer, tanto a los proveedores como receptores de servicios TI, un marco que facilite todas estas tareas y procesos.

ITIL define la Gestión de Servicios como un conjunto de capacidades organizativas especializadas para aportar valor a los clientes en forma de servicios.

Los principios básicos para la gestión de servicios se resumen en:

- **Coordinación y especialización**: el proveedor debe especializarse en la gestión del servicio y garantizar la coordinación entre los recursos y capacidades propios y de cliente. El cliente debe especializarse en la gestión de su negocio.
- **El principio de Agencia**: los agentes son los responsables de la correcta prestación de los servicios, actúan como intermediarios entre el cliente o usuario y el proveedor de servicios. Los agentes deben actuar de acuerdo con las indicaciones del cliente y protegiendo los intereses tanto del cliente, cómo de los usuarios y los suyos propios. Los agentes pueden ser trabajadores del proveedor de servicios o también interfaces electrónicas de interacción con el usuario, cómo por ejemplo una herramienta de ticketing.
- **Encapsulación:** los clientes y usuarios solo están interesados en la utilidad y garantía del servicio y no en los detalles precisos para su correcta prestación. Para conseguir la encapsulación es necesario:
    - División de conceptos complejos en distintas partes que pueden ser abordadas independientemente.
    - Modularidad que permite agrupar funcionalidades similares en forma de módulos autocontenidos.
    - Acoplamiento flexible entre recursos y usuarios, mediante, por ejemplo, sistemas redundantes, que evita que cambios o alteraciones en los recursos tengan un impacto negativo en la experiencia de usuario.
- **Sistemas:** ITIL define los sistemas cómo conjuntos de componentes qué se relacionan y colaboran entre sí, constituyendo una unidad con un objetivo común. Los puntos clave para el correcto rendimiento de un sistema son:

- Procesos de control
- *Feedback* y aprendizaje

2.2 Gobierno TI

No existe una única y universal definición de Gobierno TI. Aunque en general podríamos definirlo así:

"Conjunto de acciones que realiza el área de TI en coordinación con la alta dirección de la empresa para movilizar los recursos de forma eficiente."

El Gobierno TI forma parte del Gobierno Corporativo y debe centrarse en considerar las implicaciones que la infraestructura y servicios TI tienen en el futuro y la sostenibilidad de la empresa asegurando su alineación con los objetivos estratégicos.

Aunque a veces se considera a ITIL como un marco para el Gobierno TI sus objetivos son más modestos pues se limitan exclusivamente a aspectos de gestión.

Las diferencias entre estos conceptos son similares a las que hay entre los conceptos de gobierno y administración pública:

El gobierno es el responsable de establecer políticas y directrices de actuación que recojan las inquietudes y cubran las necesidades de los ciudadanos. Las administraciones públicas son las que se ocupan de garantizar en la medida de lo posible que esas políticas se ejecuten, ofreciendo los servicios correspondientes, asegurando el cumplimiento de las normas establecidas, prestando apoyo, recogiendo reclamaciones y propuestas, etcétera.

Siguiendo con este paralelismo, ITIL equivaldría a un conjunto de buenas prácticas para la administración del estado, pero no para su gobierno (aunque a veces las líneas que separan a ambos no estén claramente definidas). Por ejemplo, la Declaración Universal de Derechos Humanos sí sería un conjunto de buenas prácticas para el gobierno.

2.3 Funciones, procesos y roles

2.3.1 Funciones

Una **función** es una unidad especializada en realizar una cierta actividad y es la responsable de su resultado. Las funciones incorporan todas las capacidades y recursos necesarios para el correcto desarrollo de dicha actividad.

El principal objetivo de las funciones es dotar a las organizaciones de una estructura acorde con el principio de especialización. Sin embargo, si se produce una descoordinación entre las diferentes funciones, el rendimiento global de la organización se puede ver afectado negativamente. En caso de que se produzca esa descoordinación un modelo organizativo basado en procesos puede ayudar a mejorar la productividad de la organización en su conjunto.

2.3.2 Procesos

Un **proceso** es un conjunto de actividades relacionadas entre sí para cumplir un objetivo específico.

Los procesos comparten las siguientes características:

- Son cuantificables y se basan en el rendimiento.

- Tienen un cliente final.
- Tienen resultados específicos, cuyo receptor es el cliente final.
- Se inician como respuesta a un evento.

El Centro de Servicios y la Gestión de Incidencias son dos ejemplos de función y proceso respectivamente.

Sin embargo, en la práctica la división entre funciones y procesos no siempre es tan evidente pues puede depender de la estructura organizativa de la empresa u organismo en cuestión.

2.3.3 Rol

Un **rol** es un conjunto de actividades y responsabilidades asignada a una persona o grupo. Un grupo o persona puede desempeñar varios roles de forma simultánea.

Los cuatro roles más importantes en la gestión de servicios TI son:

- **Gestor del Servicio:** responsable de la gestión de un servicio durante todo su ciclo de vida.
- **Propietario del Servicio:** es el responsable último de cara al cliente y a la organización TI de la prestación de un servicio específico.
- **Gestor del Proceso:** responsable de la gestión de todas las tareas asociadas a un proceso en particular.
- **Propietario del Proceso:** es el último responsable frente a la organización TI de que el proceso cumple sus objetivos. Debe estar involucrado en su fase de diseño, implementación y cambio asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora

2.4 El ciclo de vida de los servicios TI

ITIL estructura la gestión de los servicios TI sobre el concepto de Ciclo de Vida de los Servicios.

Con este enfoque se persigue ofrecer una visión global de la vida de un servicio desde su diseño hasta su posible abandono sin por ello ignorar los detalles de todas las funciones y procesos involucradas en la eficiente prestación del mismo.

El Ciclo de Vida del Servicio consta de cinco fases:

1. **Estrategia del Servicio**: Trata la gestión de servicios no sólo como una capacidad sino como un activo estratégico.
2. **Diseño del Servicio**: cubre los métodos y principios necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
3. **Transición del Servicio**: cubre el proceso de transición para la implementación de nuevos servicios o su mejora.
4. **Operación del Servicio**: abarca las mejores prácticas para la gestión del día a día durante la operación del servicio.
5. **Mejora Continua del Servicio**: proporciona una guía para la creación y mantenimiento del valor ofrecido a los clientes a traces de un diseño, transición y operación del servicio optimizado.

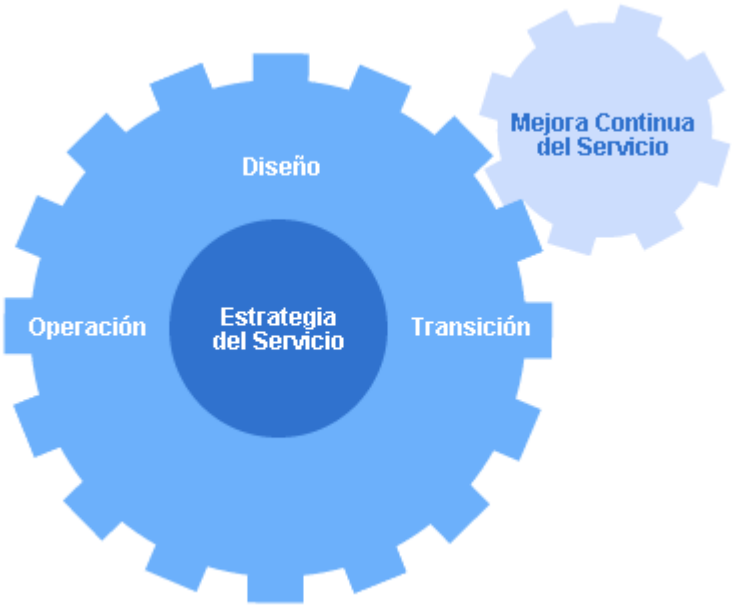


Ilustración 2-1 Fases de un servicio

ITIL no trata estas fases como aisladas e independientes, sino que tiene en cuenta las múltiples relaciones entre ellas y como estas afectan a los aspectos globales de todo el ciclo de vida del servicio.

En los siguientes apartados describiremos las 5 fases que componen el ciclo de vida de los servicios TI, haciendo hincapié en las fases de Diseño, Transición, Operación y Mejora Continua del Servicio.

3 ESTRATEGIA DEL SERVICIO

La fase de **Estrategia del Servicio** es central al concepto de **Ciclo de vida del servicio** y tiene como principal misión convertir la **Gestión del Servicio** en un activo estratégico.

Para conseguir este objetivo es imprescindible determinar en primera instancia qué servicios deben ser prestados y por qué han de ser prestados desde la perspectiva del cliente y el mercado.

Una correcta Estrategia del Servicio debe:

- Ser la guía para establecer y priorizar objetivos y oportunidades.
- Tener el conocimiento del mercado y los servicios que ofrece la competencia.
- Armonizar la oferta con la demanda de servicios.
- Proponer servicios diferenciados que aporten valor añadido al cliente.
- Gestionar las capacidades y recursos necesarias para la prestación de los servicios ofrecidos teniendo en cuenta los costes y riesgos asociados.
- Alinear los servicios ofrecidos con la estrategia de negocio.
- Elaborar planes que permitan un crecimiento sostenible.
- Crear casos de negocio para justificar inversiones estratégicas.

La fase de Estrategia del Servicio es la base que permite que las fases de **Diseño**, **Transición** y **Operación** del servicio se ajusten a las políticas y visión estratégica del negocio.

Para realizar una correcta implementación de la estrategia del servicio debemos intentar dar respuesta a las siguientes preguntas:

- ¿Qué servicios debemos ofrecer?
- ¿Cuál es su valor?
- ¿Cuáles son nuestros clientes potenciales?
- ¿Cuáles son los resultados esperados?
- ¿Qué servicios son prioritarios?
- ¿Qué inversiones son necesarias?
- ¿Cuál es el retorno a la inversión o ROI?
- ¿Qué servicios existen ya en el mercado que puedan representar una competencia directa?
- ¿Cómo podemos diferenciarnos de la competencia?

Para dar una adecuada respuesta, debemos abordar estas cuestiones desde un enfoque que va más allá del ámbito puramente TI, abarcando campos como el márketing o la gestión financiera.

3.1 Creación de valor

Los servicios son definidos en ITIL como un medio de aportar valor al cliente sin que éste deba asumir los riesgos y costes específicos de su prestación.

El valor al que nos referimos no depende exclusivamente del rédito económico asociado al resultado específico de cada servicio, sino que incluye algunos otros indicadores intangibles como por ejemplo la percepción que el cliente puede llegar a tener del servicio.

Para que nuestro servicio aporte valor al cliente tenemos que priorizar los siguientes aspectos:

- La **funcionalidad** ofrecida debe adaptarse lo máximo posible a las necesidades reales del cliente,
- La **garantía** del proveedor debe ser la adecuada para asegurar que el servicio se preste de forma continuada preservando los niveles de calidad acordados,

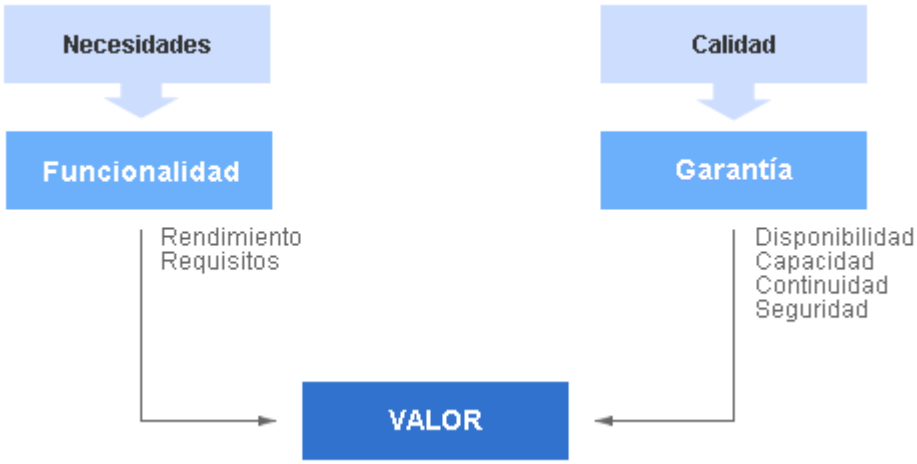


Ilustración 3-1 Creación de valor

Siempre se debe tener en cuenta que el valor para el cliente está en el impacto que éste tiene en su negocio y no en el servicio en sí mismo.

Cuando se concibe un nuevo servicio hay que tener en cuenta que la funcionalidad y garantía de un servicio frecuentemente son interdependientes, por lo que se debe buscar un equilibrio entre ambas características, minimizando a su vez los aspectos que los potenciales clientes puedan percibir negativamente.

La funcionalidad debe reportar un beneficio para el cliente, bien disminuyendo directamente los costes o contribuyendo a aumentar los ingresos. Para ello, es necesario que el servicio cumpla con los requisitos del cliente y aumente lo máximo posible el rendimiento.

La garantía presupone que el servicio:

- Estará disponible cuando se le necesite
- Estará correctamente dimensionado para cumplir sus objetivos
- Sea seguro
- Dispondrá de los mecanismos de respaldo necesarios para asegurar su continuidad.

Un servicio, por ejemplo, puede ofrecer a priori una interesante utilidad a buen precio, pero si la percepción del cliente es que tiene un riesgo elevado, no lo contratará.

3.2 Activos del servicio

Para que una organización TI pueda aportar valor mediante servicios debe asegurarse de hacer buen uso de sus **recursos y capacidades.**

Los **recursos** son la "materia prima" necesaria para la prestación del servicio e incluyen el capital, las infraestructuras, aplicaciones e información.

Las **capacidades** representan las habilidades desarrolladas a lo largo del tiempo para transformar los recursos en valor a través de la gestión, la organización, los procesos y el conocimiento.

El personal forma la base de los recursos y capacidades, siendo es en sí mismo un recurso que aporta entre otras capacidades su profesionalidad, creatividad y capacidad de liderazgo.

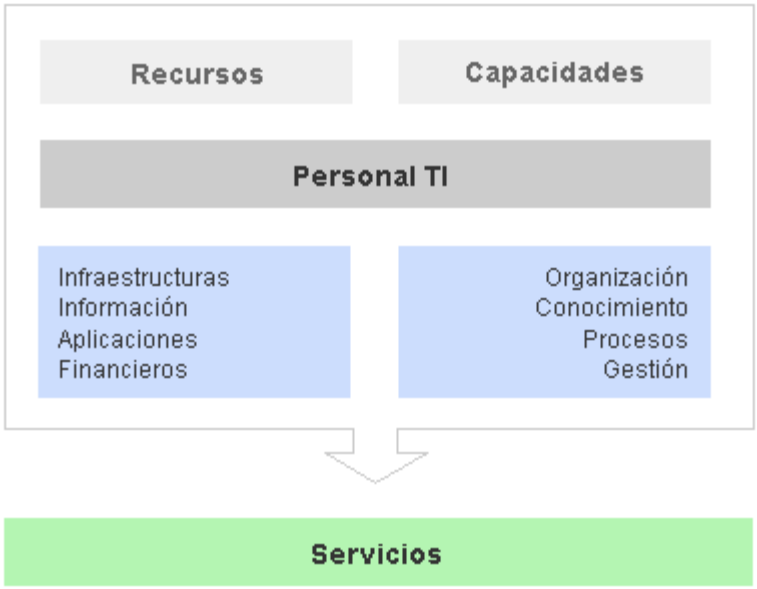


Ilustración 3-2 Activos del servicio

Las capacidades y los recursos son interdependientes a la hora de crear valor. Si tenemos muy buenas capacidades, pero insuficientes recursos no será imposible crear valor, al igual que en el caso contrario, si tenemos muchos recursos, pero no tenemos las capacidades suficientes para gestionarlos, seremos incapaces de crear valor. Teniendo en cuenta esto, la organización TI debe buscar siempre el adecuado equilibrio entre ambos aspectos para aportar el máximo valor al cliente en forma de servicios.

3.3 Proveedores de servicios

ITIL distingue entre tres tipos diferentes de proveedores de servicios:

- **Tipo I**: proveedor interno
- **Tipo II**: unidad de servicios compartidos
- **Tipo III:** proveedores externos

Aunque los aspectos generales de la gestión del servicio son comunes a todos ellos existen evidentes diferencias en los aspectos organizativos en cada caso.
Cada tipo de proveedor de servicios tiene sus ventajas e inconvenientes que pasamos a analizar.

3.3.1 Proveedores de Servicios Interno (Tipo I)

Sólo se recomienda esta opción cuando los servicios prestados forman parte esencial en el posicionamiento estratégico de la organización.
Las ventajas de esta opción se resumen en:

- Mayor control sobre los servicios prestados.
- Mayores niveles de personalización.
- Comunicación directa.

Lo inconvenientes se resumen en:

- Posibilidad de falta de optimización en los recursos.
- Mayor dificultad a la hora de incrementar las capacidades.
- Organizaciones más endogámicas y menos flexibles.
- Concentración de costes y riesgos

3.3.2 Unidades de Servicio Compartidas (Tipo II)

Estos proveedores prestan servicio a diferentes unidades de negocio que operan bajo una estructura común. Las ventajas de esta opción se resumen en:

- Menores costes y riesgos al compartirse entre diferentes unidades.
- Posicionamiento más competitivo frente a proveedores externos.
- Procedimientos estandarizados
- Opciones mayores de crecimiento

Y entre las desventajas se incluyen:

- Asumir actividades que no aportan ventajas competitivas a la organización.
- Posibles conflictos de intereses entre diferentes unidades de negocio.

3.3.3 Proveedores de Servicios Externo (Tipo III)

Estos proveedores ofrecen sus servicios a diferentes clientes que habitualmente son competidores entre sí.

Las ventajas de la contratación externa de los servicios son evidentes, mientras que estos no formen parte del núcleo del negocio del cliente, las resumimos en:

- Mayor flexibilidad y oferta.
- Minimización de riesgos, ya que estos son compartidos entre una amplia red de clientes.
- Procedimientos estandarizados.

Entre las desventajas se cuentan:

- El coste aumenta según el nivel de personalización de los servicios.
- Se puede tener demasiada dependencia del proveedor, haciendo que el cliente sea cautivo del mismo.

3.4 Redes de valor

ITIL utiliza el concepto de **red de valor** en vez de el de **cadena de valor**, ya que se adapta mucho mejor al caso de los servicios TI.

El concepto de cadena de valor se asocia a un proceso lineal en el cual cada uno de los eslabones va añadiendo valor al servicio final.

Sin embargo, los modelos lineales no son capaces de modelar los procesos y actividades necesarias para la correcta gestión de un servicio TI. Por ello, ITIL usa el concepto **redes de valor** que se definen como redes de relaciones que generan valor a través de complejas interdependencias que pueden implicar a múltiples organizaciones.

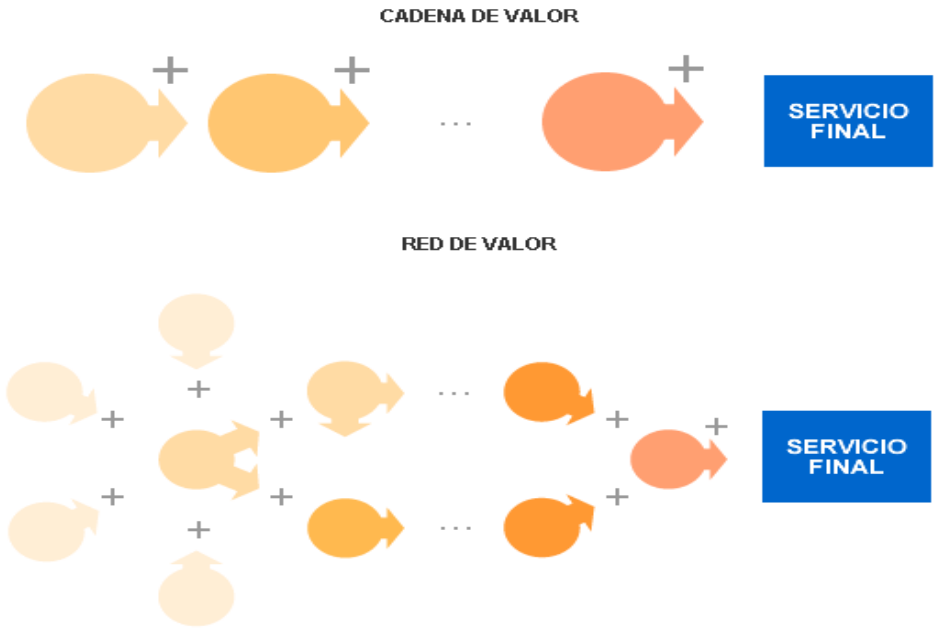


Ilustración 3-3 Cadena y Red de Valor

Es necesario conocer esas redes de valor para desarrollar una estrategia del servicio:

- ¿Cuáles son los nodos de esa red de valor?
- ¿Cuáles son sus interrelaciones?
- ¿Cuáles son los mecanismos de generación de valor?
- ¿Cómo optimizar sus flujos de trabajo?

Estos planes han de realizarse para el medio largo plazo centrándose en evoluciones del Porfolio de Servicios, inversiones estratégicas, nuevos desarrollos y planes de mejora.

El **Patrón** garantiza la coherencia en las actividades realizadas y establece reglas que aseguran que las actividades necesarias sean realizadas en forma y plazo.

Los patrones trazan las líneas que definen el perfil de la organización TI frente al cliente y facilitan la priorización de actividades y la asignación de recursos.

3.5 Las 4 P de la estrategia

Las 4 Pes de Mintzberg nos dan un buen punto de partida para definir la Estrategia del Servicio:

- **Perspectiva**: hay que tener objetivos y valores bien definidos y asumibles. Debe establecer las normas generales tanto dentro de la organización TI como en la relación con sus clientes.

- **Posición**: se definirán qué servicios se prestarán, cómo se prestarán y a quién irán dirigidos, buscando diferenciarlos de los de la competencia. Existen varias posibilidades para posicionarse en el mercado. Se puede optar por ser un proveedor con un alto grado de especialización que sirva a un pequeño nicho de mercado o por el contrario ofrecer un amplio catálogo de servicios.
- **Planificación**: establecer criterios claros de desarrollo futuro. Se deben realizar planes que establezcan una hoja de ruta para alcanzar los objetivos generales fijados. Estos planes han de realizarse para el medio largo plaza, centrándose en evoluciones del Porfolio de Servicios, inversiones estratégicas, nuevos desarrollos y planes de mejora.
- **Patrón**: mantener una coherencia en la toma de decisiones y acciones adoptadas. Asegurando que las actividades necesarias sean realizadas en forma y plazo.

3.6 Procesos

Como se ha comentado anteriormente, cada fase tiene una serie de procesos asociados. Para la fase de Estrategia solo los nombraremos y resumiremos muy brevemente.

Los procesos que forman parte a la fase de Estrategia son:

- **Gestión Financiera**: responsable de asegurar la prestación de servicios con una correcta relación calidad-precio y costes controlados.
- **Gestión del Porfolio de Servicios:** El porfolio de servicios proporciona una referencia estratégica y técnica clave dentro de la organización TI, dando una descripción detallada de todos los servicios que se prestan y los recursos asignados para ello. Este proceso es el responsable de la inversión en servicios nuevos y actualizados que ofrezcan el máximo valor al cliente minimizando a su vez los riesgos y costes asociados.
- **Gestión de la Demanda:** responsable de la armonización de la oferta de los servicios ofrecidos con las demandas del mercado.

3.7 Relación con otras fases

Ninguna de las fases de los servicios debe ser considerado como un compartimento estanco pues sus interrelaciones con las otras fases son de vital importancia para la correcta Gestión del Servicio.

Esto es algo que es particularmente cierto para la Estrategia del Servicio pues ésta debe de servir de guía al diseño, transición, operación y mejora continua del servicio.

A continuación, resumimos las principales interdependencias.

3.7.1 Estrategia y Diseño

La fase de Estrategia de Servicio aporta principalmente a la fase de Diseño del Servicio un Porfolio de Servicios orientado a cada segmento del mercado.

La estrategia debe aportar al diseño del servicio:

- Modelos de servicio que ofrezcan una guía sobre como aportar valor a los servicios propuestos.
- Información sobre políticas de precios, restricciones indicadas por los clientes, etc.

3.7.2 Estrategia y Transición

A la hora de establecer una correcta Estrategia del Servicio es necesario conocer en profundidad sus implicaciones en la fase de Transición del Servicio. Cada cambio y evolución conlleva costes y tiene impacto en clientes y usuarios.

Es indispensable sopesar los riesgos y potenciales beneficios asociados para establecer una estrategia que

minimice los primeros maximizando a su vez los segundos.

Por otro lado, la Transición del Servicio debe dar soporte a la perspectiva y posicionamiento del servicio establecidos en la fase de estrategia.

3.7.3 Estrategia y Operación

La fase de operación es la más importante desde el punto de vista del cliente, los servicios pueden ser adecuados y estar bien diseñados, pero si el eslabón de la operación falla los resultados no serán los buscados y la percepción del cliente será negativa.

Por lo tanto, un factor esencial en el enfoque estratégico de los servicios es asegurar que son operacionalmente viables.

Recíprocamente, la Operación del Servicio debe de resultar en la fuente más fiable sobre las demandas y restricciones de los clientes que servirán de guía para dar forma a la estrategia más adecuada.

3.7.4 Estrategia y Mejora Continua

La tecnología evoluciona continuamente, por lo que las estrategias no deben ser inamovibles. La estrategia debe ser continuamente rediseñada atendiendo a múltiples factores.

La Mejora del Servicio debe ofrecer información a la fase de Estrategia sobre aspectos que pueden ser optimizados, tales como calidad y rendimiento, pero esto siempre debe hacerse partiendo de la perspectiva de negocio establecida durante la fase de estrategia.

4 DISEÑO DEL SERVICIO

El principal objetivo de la fase de **Diseño del Servicio** es diseñar nuevos servicios o modificar los que ya existen para incluirlos en el catálogo de servicios y realizar su paso al entorno de producción.

El Diseño del Servicio debe seguir las directrices establecidas en la Fase de Estrategia y debe a su vez colaborar con ella para que los servicios diseñados:

- Se adapten a las necesidades del mercado.
- Sean eficientes en costes y rentables.
- Cumplan los estándares de calidad adoptados.
- Aporten valor a clientes y usuarios.

El Diseño del Servicio debe tener en cuenta tanto los requisitos del servicio como los recursos y capacidades disponibles en la organización TI. Tal y como se comentó en la fase de estrategia, un desequilibrio entre recursos y capacidades puede dar como resultado servicios donde la funcionalidad o la garantía se vean comprometidas.

El proceso de diseño del servicio no es independiente y debe tener en cuenta que los procesos y actividades involucrados afectan y se ven afectados por el resto de fases del ciclo de vida.

Una adecuada implementación de la fase de Diseño del Servicio debe ayudar a responder cuestiones tales como:

- ¿Cuáles son las necesidades y requisitos de los clientes?
- ¿Cuáles son las capacidades y recursos necesarios para prestar los servicios propuestos?
- ¿La disponibilidad ofrecida por el servicio es la necesaria?
- ¿Se garantiza la continuidad del servicio?
- ¿Son necesarias nuevas inversiones para prestar los servicios con los niveles de calidad propuestos?
- ¿Están todos los agentes involucrados correctamente informados sobre el alcance y los objetivos de los nuevos servicios o de las modificaciones a realizar en los ya existentes?
- ¿Se necesita la colaboración de proveedores externos?

4.1 Principios del Diseño de Servicios

ITIL contempla cinco aspectos esenciales en el **Diseño del Servicio**:

- Diseño de soluciones de servicio
- Diseño del Porfolio de Servicios
- Diseño de la arquitectura del servicio
- Diseño de procesos
- Diseño de métricas y sistemas de monitorización

4.1.1 Diseño de soluciones de servicio

Debe incluir de forma estructurada todos los elementos clave del nuevo o modificado servicio:

- Requisitos de negocio.
- Requisitos de servicio (SLR en inglés).
- Adecuación a la estrategia del servicio.
- Análisis funcional.
- Estudios de los servicios prestados para ver si es posible reutilizar módulos de otros servicios en cartera.
- Análisis de costes (TCO) y retorno a la inversión (ROI).
- Estudio de las capacidades y recursos necesarios.
- Estrategias de contratación con los proveedores externos (si estos se consideraran necesarios)

4.1.2 Diseño del Porfolio de Servicios

El Porfolio de Servicios es una de las principales herramientas para la gestión del servicio a través de todas las fases del ciclo de vida. Debe incluir información sobre todos los servicios ofrecidos, los servicios en fase de desarrollo y los servicios retirados en términos de valor para el negocio.

La fase de Diseño del Servicio es responsable de determinar su contenido específico, así como sus permisos de acceso.

El Porfolio de Servicios debe contener información sobre:

- Los objetivos del servicio
- Su valor: funcionalidad y garantía
- Su estado
- Los acuerdos de nivel de servicios (ANS o SLA en inglés) asociados
- Capacidades y recursos utilizados
- Sus costes y retorno esperado
- Los controles o métricas de calidad asociados
- Los responsables del mismo
- Servicios relacionados
- Proveedores externos involucrados (OLAs y UCs)

Y toda aquella otra información que se pueda considerar de interés referente a la prestación del servicio.

4.1.3 Diseño de la arquitectura del servicio

La arquitectura debe tener en cuanto todos los elementos necesarios para la Gestión del Servicio, así como la interrelación entre ellos y el mercado. Debe ofrecer una guía para el diseño y evolución del servicio teniendo en cuenta:

- La alineación entre la tecnología y el negocio.
- La infraestructura TI necesaria.
- La Gestión de las aplicaciones.
- La Gestión de los datos y la información.

- La Documentación y Gestión del Conocimiento.
- Los Planes de Despliegue del servicio.

4.1.4 Diseño de procesos

En la fase de diseño del servicio se han de definir los procesos involucrados con una descripción detallada de sus actividades, funciones, organización, entradas y salidas.

En particular deben establecerse los procesos de control para asegurar que los procesos se realizan de forma eficiente y cumplen los objetivos establecidos.

Los procesos no deben ser un fin en sí mismo, sino que deben tener como principal objetivo que la organización TI ofrezca servicios de valor al cliente de forma eficiente.

4.1.5 Diseño de métricas y sistemas de monitorización

Es imprescindible diseñar sistemas de medición y seguimiento que permitan evaluar tanto la calidad de los servicios prestados como la eficiencia de los procesos involucrados. Los resultados obtenidos de estos sistemas deben ser la principal fuente de información para la fase de Mejora del Servicio.

Existen cuatro tipos principales de métricas a considerar:

- Progreso: cumplimiento de los calendarios previstos
- Cumplimiento: adecuación a las políticas y requisitos predefinidos.
- Eficacia: calidad de los resultados obtenidos.
- Rendimiento: productividad de los procesos y gestión de los recursos utilizados.

4.2 Modelos de diseño

La elección del modelo de desarrollo del servicio puede ser clave para el éxito o fracaso del mismo.

Se pueden distinguir tres tipos de modelos:

- Tradicional
- Ágil
- Empaquetado

La elección de uno u otro modelo de desarrollo para cada servicio es una de las principales decisiones del Diseño del Servicio y se optará por una u otra dependiendo de múltiples factores tales como:

- Decisiones estratégicas basadas en la criticidad del servicio.
- Cuestiones financieras.
- Requisitos del cliente.
- Generación de valor.
- Condiciones del mercado.
- Perspectivas de negocio.

A continuación, se describen brevemente cada uno de los tres modelos.

4.2.1 Modelo tradicional

En este modelo se busca que el servicio sea muy estable, es decir, que no haya que hacer modificaciones en el mismo una vez implantado.

Para conseguir está estabilidad es necesario realizar un arduo estudio previo de los aspectos técnicos y de negocio que evite, en la medida de lo posible, la necesidad de cambios ya sea por errores o por una funcionalidad incompleta.

El principal problema de este modelo es que el tiempo empleado en el diseño del servicio, puede ser demasiado elevado para lo que demanda el mercado, pudiéndose dar situaciones en las que el servicio se quede obsoleto incluso antes de su entrada en producción.

4.2.2 Modelo ágil o RAD

El modelo Rápido de Desarrollo (RAD) es un modelo incremental e iterativo que se basa en la creación de prototipos.

La funcionalidad tiende a ser modular de forma que ésta se pueda ir integrando incrementalmente aportando las siguientes ventajas:

- Los módulos pueden ser reutilizables.
- El cliente tiene un acceso más anticipado a la funcionalidad (*early-access*), aunque ésta pueda ser reducida lo que facilita su feedback desde las primeras fases de desarrollo.
- Permite un desarrollo distribuido que facilite la incorporación de proveedores externos en el proceso.

El concepto de prototipo supone que el proceso será por naturaleza iterativo e irán generando múltiples versiones que irán introduciendo progresivamente los requisitos del cliente.

Su principal problema es que al no estar completamente cerrada desde un principio su arquitectura se puede entrar en un proceso inacabable de prototipos que no culmine en un servicio adecuado para su paso a producción.

4.2.3 Soluciones empaquetadas

Este modelo implica la existencia de módulos predefinidos con una funcionalidad general. Existen en la actualidad muchas soluciones TI empaquetadas que simplifican el proceso de diseño del servicio.

Sus ventajas se resumen en:

- Disponible rápidamente.
- Configurable.
- Costes (iniciales) reducidos.
- Actualizaciones periódicas.

Sus principales inconvenientes suelen residir en:

- Dificultades de integración con otros servicios/plataformas.
- Insuficiente funcionalidad debida a necesidades muy específicas.
- Potenciales altos costes de personalización y posibles incompatibilidades con las actualizaciones.

4.3 Procesos de la fase de Diseño

Las funciones y procesos asociados directamente a la **fase de Diseño** son:

- **Gestión del Catálogo de Servicios**: responsable de crear y mantener un catálogo de servicios de la organización TI que incluya toda la información relevante: gestores, estatus, proveedores, etcétera.
- **Gestión de Niveles de Servicio**: responsable de acordar y garantizar los niveles de calidad de los servicios TI que son prestados.
- **Gestión de la Capacidad:** responsable de asegurar que la organización TI dispone de la capacidad

suficiente para prestar los servicios acordados.

- **Gestión de la Disponibilidad:** responsable de garantizar que se cumplen los niveles de disponibilidad recogidos en los SLA.
- **Gestión de la Continuidad de los Servicios TI:** responsable de establecer planes de contingencia que aseguren la continuidad del servicio en un tiempo predeterminado con el menor impacto posible en los servicios de carácter crítico.
- **Gestión de la Seguridad de la Información:** responsable de establecer las políticas de integridad, confidencialidad y disponibilidad de la información.
- **Gestión de Proveedores:** responsable de la relación con los proveedores y el cumplimiento de los UCs.

4.3.1 Gestión del Catálogo de Servicios

4.3.1.1 Introducción y objetivos

El Porfolio de Servicios, tal y como hemos visto, proporciona una referencia estratégica y técnica clave dentro de la organización TI, ofreciendo una descripción detallada de todos los servicios que se prestan y los recursos asignados para ello. El **Catálogo de Servicios** cumple exactamente la misma función, pero de cara al exterior.

La existencia de dos documentos tan similares se explica porque el Porfolio de Servicios, al ser de carácter interno, no sólo contiene información sobre el funcionamiento de la organización que no interesa a los clientes, sino que está además escrito en un lenguaje demasiado técnico que no es adecuado ni eficaz para la comunicación externa.

Además, el Porfolio de Servicios incluye información sobre todos los servicios que alguna vez ha prestado, presta o prestará la organización, mientras que el Catálogo prescinde de aquellos retirados o inactivos y se centra en los que pueden interesar a los clientes.

La creación del Catálogo de Servicios puede ser una tarea compleja, ya que es necesario alinear cuestiones técnicas con políticas de negocio. Sin embargo, es un documento imprescindible puesto que:

- Sirve de guía a los clientes a la hora de elegir un servicio que se adapte a sus necesidades.
- Delimita las funciones y compromisos de la organización TI.
- Se puede usar como herramienta de venta.
- Evita que se genere confusión entre los distintos actores implicados en la prestación de servicios.

El objetivo principal del **Catálogo de Servicios** es compendiar toda la información referente a los servicios que los clientes deben conocer para asegurar un buen entendimiento entre éstos y la organización TI.

Para cumplir esa tarea, el Catálogo de Servicios debe:

- Ofrecer una descripción de los servicios ofrecidos que sea comprensible para personal no especializado, poniendo especial cuidado en evitar el lenguaje técnico.
- Ser utilizado como guía para orientar y dirigir a los clientes.
- Incluir, en líneas generales, los Acuerdos de Niveles de Servicio (ANS o SLA) y los precios en vigor. Debe recoger también otras condiciones y políticas de prestación de los servicios, así como las responsabilidades asociadas a cada uno de éstos.
- Registrar los clientes actuales de cada servicio.
- Encontrarse a disposición del Centro de Servicios y de todo el personal que se halle en contacto directo con los clientes.

Los principales beneficios de crear, mantener y utilizar un Catálogo de Servicios se pueden resumir en que la relación entre la organización y el cliente gana en fluidez y solidez porque:

- Al poner por escrito de forma detallada los acuerdos alcanzados (características, plazos e hitos y

entregables contratados para el servicio), se evitan abusos y malentendidos por ambas partes.

- Al estar mejor informado sobre las capacidades y recursos asociados a la prestación del servicio, el cliente puede entender de manera más precisa los costes asociados al mismo. Esto ayuda a generar más confianza en el cliente hacia la organización, algo vital a la hora de renovar o ampliar el contrato de prestación servicios.
- Al poner por escrito los responsables de cada servicio, se evitan situaciones en las que el cliente no sabe a quién acudir para por ejemplo reclamar la resolución de una incidencia.

Por otro lado, las principales dificultades que pueden surgir con relación al Catálogo de Servicios son:

- No está claro, bien dentro de la organización, bien en el Porfolio, qué servicios están en activo y cuáles han sido retirados definitivamente.
- No se interiorizado en el personal la costumbre de consultar el Catálogo a la hora de buscar información sobre un servicio. Esto es especialmente crítico si es el Centro de Servicios el que no lo utiliza, ya que es el principal interlocutor con los clientes.
- El Catálogo de Servicios, pese a los esfuerzos iniciales, contiene muchas expresiones y palabras técnicas o alude a conceptos demasiado especializados.
- El Catálogo de Servicios muestra aspectos internos sobre el funcionamiento de la organización que no es recomendable que los clientes conozcan.
- El Catálogo de Servicios se actualiza con muy poca frecuencia, por lo que en la práctica resulta ineficaz.

4.3.1.2 Conceptos básicos

A continuación, definimos los conceptos básicos del proceso Gestión del Catálogo de Servicios:

- **Sistema de Gestión de la Configuración**: Muchas organizaciones integran el Catálogo de servicios y el Porfolio en una única herramienta que recibe el nombre de **Sistema de Gestión de la Configuración** (CMS). De este modo, la información contenida en ellos puede ser utilizada por otras herramientas de gestión.
- **El Catálogo de Servicios de Negocio:** Se denomina **Catálogo de Servicios de Negocio** a la información contenida en el Catálogo de Servicios que se refiere a los procesos de negocio, las relaciones entre unidades de negocio, etc.
- **El Catálogo de Servicios Técnico:** Se denomina Catálogo de Servicios Técnico a aquellos aspectos del Catálogo de Servicios que abordan los propios servicios TI: distinción entre servicios de apoyo, servicios compartidos, componentes, elementos de configuración, etc.

Esta parte del catálogo tan sólo está disponible para la organización: los clientes no pueden consultarla.

4.3.1.3 Definición de servicios

El primer paso a la hora de definir el **Catálogo de Servicios** consiste en tomar los servicios recogidos en el Porfolio de Servicios y discriminar la parte "histórica", es decir, los registros que se refieren a servicios que ya no están en activo.

El siguiente punto consiste en trazar las líneas de servicio o familias principales en las que éstos se van a agrupar. Generalmente, las familias de servicios están relacionadas con las áreas funcionales en las que se desarrollan éstos.

Esto aporta una visión de conjunto sobre los servicios que presta la organización, lo cual es un arma de doble filo. Si la estrategia es clara y se ha puesto en práctica con rigor a la hora de definir los servicios, de un solo vistazo al Catálogo quedarán patentes los fines de la organización. En cambio, si ha habido improvisación también quedará patente al no haber denominadores comunes claros entre unos servicios y otros.

Una vez constituido el primer nivel, el de las familias, se van detallando los servicios existentes en cada una de ellas, así como los clientes que los han contratado y la previsión de demanda para cada servicio.

A continuación, ofrecemos un listado resumido de los datos que debe contener el Catálogo para cada servicio:

- Nombre y descripción.
- Propietario del servicio.
- Cliente.
- Otras partes implicadas (proveedores, instituciones, etc.)
- Fechas de versión y revisión.
- Niveles de servicio acordados (tiempos de respuesta, disponibilidad, continuidad, horarios, etc.) en los OLAs y SLAs.
- Condiciones de prestación del servicio. Precios.
- Cambios y excepciones.

Es importante reiterar en que el lenguaje empleado debe ser comprensible para aquellos que no están familiarizados con el lenguaje técnico.

Sin embargo, en la mayoría de los casos, por muy detallado y completo que sea el Catálogo de Servicios, la complejidad de los servicios ofrecidos requiere un largo y extenso periodo de negociación con el cliente.

4.3.1.4 Mantenimiento y actualización del Catálogo de Servicios

Al margen de la confección del propio **Catálogo de Servicios**, la gestión del mismo conlleva la realización de otras tareas relacionadas con su aprovechamiento y utilización que no deben pasarse por alto.

En primer lugar, es necesario definir en detalle los destinatarios y el objetivo de la información detallada en el Catálogo. Estos planteamientos deben transmitirse después a la Gestión del Conocimiento con el propósito de que organice sesiones formativas: contenido del catálogo, casos en los que puede resultar de utilidad, etc.

Por otro lado, la Gestión del Catálogo de Servicios debe planificar las tareas de actualización de la información consignada en él. Junto a revisiones periódicas, deben determinase previamente los casos que pueden requerir una "actualización extraordinaria" y los protocolos para la aprobación de estos cambios.

Entre los puntos que pueden precisar actualizaciones al margen de las revisiones, destacan aquellos que o bien son críticos, o bien suelen cambiar con mucha frecuencia:

- Estado de los servicios ("aprobado", "en preparación", etc.).
- Responsables de los servicios.
- Precios.
- Proveedores.

4.3.1.5 Control y medición del proceso

El rendimiento de la creación y mantenimiento del **Catálogo de Servicios** puede medirse a través de los siguientes indicadores:

- N.º de actualizaciones enviadas al Porfolio de Servicios.
- N.º de modificaciones efectuadas en el Catálogo de Servicios en un periodo determinado.
- N.º de accesos o solicitudes de consulta del Catálogo dentro de la organización TI.

4.3.2 Gestión de Niveles de Servicio

4.3.2.1 Introducción y Objetivos

La **Gestión de Niveles de Servicio** es el proceso en el que se define, negocia y supervisa la calidad de los

servicios TI ofrecidos.

Ilustración 4-1 Gestión de Niveles de Servicio

La Gestión de Niveles de Servicio es responsable de buscar un compromiso realista entre las expectativas y necesidades del cliente y los costes de los servicios asociados, de tal manera que estos sean asumibles tanto por el cliente como por la organización TI.

Para cumplir sus objetivos es imprescindible que la Gestión de Niveles de Servicio:

- Conozca las necesidades de sus clientes.
- Defina correctamente los servicios ofrecidos.
- Monitorice la calidad del servicio respecto a los objetivos establecidos en los SLAs.

La Gestión de Niveles de Servicio debe:

- Documentar todos los servicios ofrecidos.
- Presentar los servicios de forma comprensible para el cliente.
- Poner foco en el cliente y su negocio y no en la tecnología.
- Colaborar estrechamente con el cliente para proponer servicios realistas y que se ajusten a sus necesidades.
- Alcanzar los acuerdos necesarios con clientes y proveedores para ofrecer los servicios demandados. (SLAs)
- Establecer los indicadores claves de rendimiento del servicio.
- Monitorizar la calidad de los servicios que se prestan, con el objetivo último de implementar mejoras con un coste aceptable por el cliente.
- Realizar informes de calidad del servicio y Planes de Mejora del Servicio (SIP).

Los principales beneficios de una correcta Gestión de Niveles de Servicio son:

- Los servicios son diseñados para cumplir sus auténticos objetivos: cubrir las necesidades del cliente.
- Se facilita la comunicación con los clientes, haciendo que no surjan malentendidos sobre la características y calidad de los servicios ofrecidos.
- Se establecen objetivos claros y cuantificables.
- Se establecen claramente las responsabilidades tanto de los clientes como de los proveedores del servicio.
- Los clientes son conscientes de los niveles de calidad ofrecidos. Se establecen claros protocolos de actuación en caso de degradación del servicio.
- La constante monitorización del servicio permite detectar los aspectos en los que el servicio flojea y priorizar su mejora.
- La Gestión TI comprende los servicios ofrecidos, facilitando los acuerdos con proveedores.
- El personal del Centro de Servicios tiene disponible la documentación necesaria (SLAs, OLAs, etc.) para poder tener una relación fluida con clientes y proveedores.
- Los SLAs ayudan a la Gestión TI tanto al cálculo de los costes del servicio como a justificar el precio

ante los clientes.

Estos beneficios repercuten, a largo plazo, en una mejora del servicio con la correspondiente satisfacción de clientes y usuarios.

Las principales dificultades para llevar a cabo la implementación de la Gestión de Niveles de Servicio son:

- No hay una buena comunicación con clientes y usuarios, lo cual puede hacer que los SLAs acordados no recojan sus necesidades reales.
- Por complacer los deseos y expectativas del cliente se establecen unos SLAs poco realistas en relación con el nivel de calidad de servicio que la infraestructura TI puede ofrecer.
- No se alinean adecuadamente los procesos de negocio del cliente con los servicios.
- Los SLAs son excesivamente largos y técnicos, incumpliendo así sus objetivos primordiales.
- Los recursos dedicados son insuficientes, debido a que la dirección los considera como un gasto añadido y no como parte integral del servicio ofrecido.
- Problemas de comunicación: una parte de los usuarios desconocen las características del servicio y los niveles de calidad acordados.
- No se monitoriza correctamente el cumplimiento de los SLAs, dificultando así la mejora de la calidad del servicio.
- No existe en la organización un verdadero compromiso con la calidad del servicio TI ofrecido.

4.3.2.2 **Conceptos básicos**

A continuación, definimos los conceptos básicos del proceso **Gestión del Catálogo de Servicios:**

- **Requisitos de Nivel de Servicio (SLR):** Recogen información detallada sobre las necesidades del cliente y sus expectativas de rendimiento y nivel de servicios. El documento de SLR constituye el elemento base para desarrollar los SLA y posibles OLAs correspondientes.
- **Hojas de Especificación:** se tratan de documentos técnicos de carácter interno que delimitan y precisan los servicios ofrecidos al cliente. Las Hojas de Especificación deben evaluar los recursos necesarios para ofrecer el servicio requerido con un nivel de calidad suficiente y determinar si es necesario el outsourcing de determinados procesos, sirviendo de documento de base para la confección de los OLAs y UCs correspondientes.
- **Plan de Calidad del Servicio (SQP):** documento que contiene la información necesaria para que la organización TI conozca los procesos y procedimientos que se aplican en la provisión de los servicios, garantizando que estos se alineen con los procesos de negocio y mantengan unos niveles de calidad adecuados. En el SQP se debe recoger la siguiente información:
    - Objetivos de cada servicio.
    - Estimación de recursos.
    - Indicadores clave de rendimiento.
    - Procedimientos de monitorización de proveedores.
- **Acuerdo de Nivel de Servicio (SLA):** documento que recoge en un lenguaje no técnico, o cuando menos comprensible para el cliente, todos los detalles del servicio ofrecido. Tras su firma, el SLA se considerará el documento de referencia para la relación con el cliente en todo lo relacionado con la provisión del servicio, por tanto, es indispensable que contenga claramente definidos los aspectos esenciales del servicio tales como su cobertura, descripción, disponibilidad, niveles de calidad, etc.
- **El Acuerdo de Nivel de Operación (OLA):** 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.
- **Contrato de Soporte (UC):** se trata de un acuerdo con un proveedor externo a la organización TI, para la prestación de servicios qué ésta no soporta.
- **Plan de Mejora del Servicio (SIP):** documento que recoge tanto las medidas correctivas a adoptar ante errores

detectados en los niveles de servicio, como las propuestas de mejora basadas en los avances tecnológicos. El SIP debe ser parte integrante de la documentación de base para la renovación de los SLAs y deben tenerlo a su disposición de los gestores de los otros procesos TI.

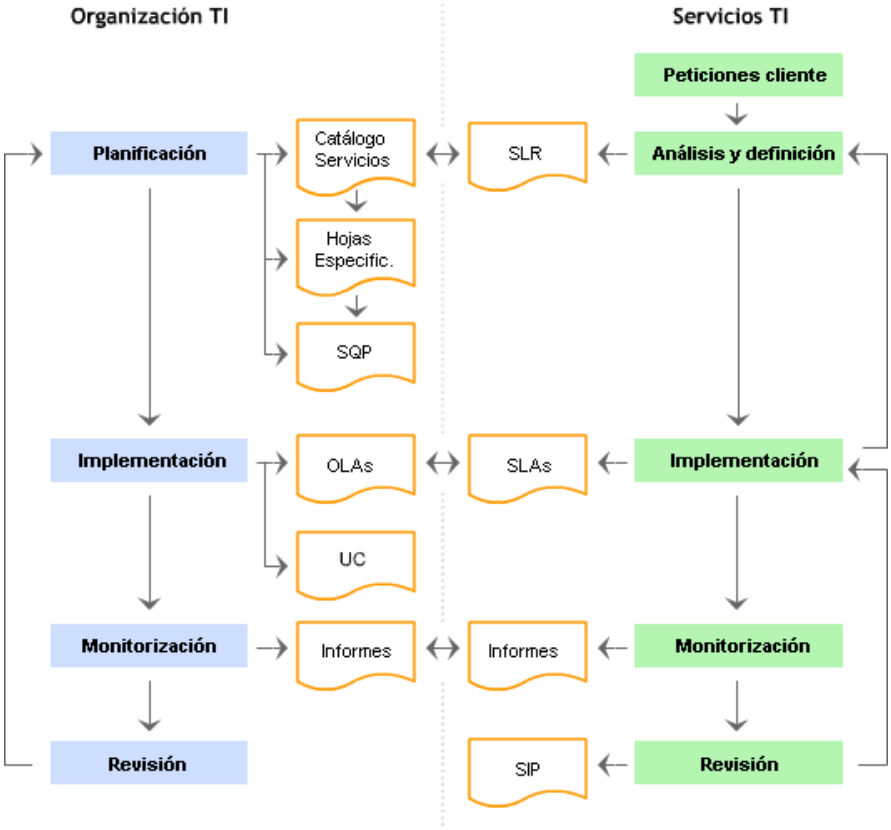


Ilustración 4-2 Conceptos Gestión de Niveles de Servicio

4.3.2.3 Planificación de la Gestión

La correcta planificación de la **Gestión de Niveles de Servicio** requiere la implicación de prácticamente todos los estamentos de la organización TI. Y, si esto no fuera ya de por sí una labor lo suficientemente compleja, resulta imprescindible la colaboración activa de los clientes y usuarios de los servicios TI.

El objetivo primordial de la Gestión de Niveles de Servicio es definir, negociar y monitorizar la calidad de los servicios TI ofrecidos. Si los servicios no se adaptan a las necesidades del cliente, o bien la calidad de los mismos será insuficiente o los costes serán desproporcionados, tendremos entonces clientes insatisfechos y la organización TI será responsable de las consecuencias que puedan derivar de ello.

Todo el proceso de planificación previo debe estar orientado a dar respuesta a las siguientes preguntas:

- ¿Qué servicios debemos ofrecer a nuestros clientes?
- ¿Cuáles son las necesidades de nuestros clientes?
- ¿Cuál es el nivel adecuado de calidad de servicio?
- ¿Quiénes y cómo se van a suministrar esos servicios?
- ¿Cuáles serán los indicadores clave de rendimiento para los servicios prestados?
- ¿Disponemos de los recursos necesarios para proveer los servicios propuestos con los niveles de calidad acordados?

La respuesta a cada una de estas preguntas debe darse en forma de documentos, algunos de carácter interno y otros accesibles a los clientes, que pasamos a describir sucintamente a continuación.

Los resultados de esta interacción/negociación deben ser incorporados al documento de Requisitos de Nivel de Servicio (SLR), que debe reflejar las necesidades del cliente y sus expectativas respecto a:

- La funcionalidad y características del servicio.
- La disponibilidad del servicio.
- La interacción del servicio con su infraestructura TI o de otro tipo.
- La continuidad del servicio.
- Los niveles de calidad del servicio.
- Tiempo y procedimientos de implantación del servicio.
- La escalabilidad del servicio ofrecido.

La información contenida en el SLR debe servir de base para elaborar la documentación interna que permita determinar "cómo" se prestara el servicio y "quién o quiénes" serán responsables del mismo.

Las Hojas de Especificación del Servicio deben contener:

- Una descripción detallada, con todos los detalles técnicos necesarios, sobre cómo se prestará el servicio.
- Cuáles serán los indicadores internos de rendimiento y calidad del servicio.
- Cómo se implementará el servicio.

Si la prestación del servicio requiere la interacción con los servicios TI del cliente o presentas exigencias técnicas a su infraestructura, esta información deberá reflejarse en una Hoja de Especificaciones "externa" que habrá de acordarse con el cliente y sus responsables técnicos.

El Plan de Calidad del Servicio (SQP) debe ser el documento maestro para la gestión interna de los servicios prestados y contener información detallada sobre todos los procesos TI involucrados en la prestación de los servicios.

En función de los requisitos plasmados en las Hojas de Especificación del Servicio, se elabora un plan global que permita asignar los recursos a la organización TI, establecer metas claras basadas en los indicadores de rendimiento elegidos y asegurar que los niveles de calidad ofrecidos se adaptan a las necesidades de los clientes y a los compromisos asumidos por la organización.

En caso de que se estimen insuficientes los recursos internos o sencillamente se considere oportuno externalizar parte de los servicios, el SQP servirá de documento guía para el establecimiento de los contratos con los proveedores externos.

4.3.2.4 **Implementación**

La fase de planificación debe concluir con la elaboración y aceptación de los acuerdos necesarios para la prestación del servicio.

Estos acuerdos incluyen los ANS o SLAs, OLAs y UCs.

4.3.2.4.1 Acuerdos de Nivel de Servicio

Los Acuerdos de Nivel de Servicio (ANS o SLAs en inglés) deben contener una descripción del servicio que abarque desde los aspectos más generales hasta los detalles más específicos del servicio.

Es conveniente estructurar los SLAs más complejos en diversos documentos, de forma que cada grupo involucrado reciba exclusivamente la información correspondiente al nivel en que se integra, ya sea en el lado del cliente o en el del proveedor.

La elaboración de un SLA requiere tomar en cuenta aspectos no tecnológicos entre los que se encuentran:

- La naturaleza del negocio del cliente.
- Aspectos organizativos del proveedor y cliente.
- Aspectos culturales locales.

4.3.2.4.2 Acuerdos de Nivel de Operación

Los Acuerdos de Nivel de Operación (OLAs) son documentos de carácter interno de la propia organización TI que determinan los procesos y procedimiento necesarios para ofrecer los niveles de servicio acordados con los clientes.

El OLA, por su naturaleza, involucra detalles sobre la prestación del servicio que deben ser opacos para el cliente pero que resultan imprescindibles a la organización TI para desarrollar y coordinar su labor.

4.3.2.4.3 Contratos de Soporte

Los Contratos de Soporte (UCs) definen las responsabilidades de los proveedores externos en el proceso de prestación de servicios.

Mientras que los OLAs son documentos internos que pueden irse modificando con cierta frecuencia, los Contratos de Soporte deben representar compromisos claros y perfectamente delimitados. A pesar de esta diferencia crucial, los UCs pueden considerarse como una extensión "externa" de los OLAs, en el sentido de que persiguen el mismo fin: organizar los procesos y procedimientos necesarios para la correcta provisión del servicio.

4.3.2.5 Monitorización de Niveles de Servicio

El proceso de **monitorización** de Niveles de Servicio es imprescindible si queremos mejorar progresivamente la calidad del servicio ofrecido, su rentabilidad y la satisfacción de los clientes y usuarios.

La monitorización de la calidad del servicio requiere el seguimiento tanto de procedimientos y parámetros internos de la organización como los relacionados con la percepción de los usuarios.

Para llevar a cabo esta tarea de manera eficiente es necesario haber establecido con anterioridad unos baremos de calidad del servicio que han de servir de guía en la elaboración de los informes correspondientes.

Las principales fuentes de información las constituyen:

- La documentación disponible: SLAs, SLRs, OLAs, SQP, SIP, UCs, etc.
- La Gestión de Incidencias y la Gestión de Problemas, que deben informar de las incidencias en el servicio y los tiempos de recuperación.
- La Gestión de la Continuidad y la Gestión de la Disponibilidad, que deben proporcionar la información sobre la infraestructura utilizada para satisfacer la calidad de servicios acordada.
- El Centro de Servicios (*Service Desk*), que mediante su trato diario con los clientes, usuarios y organización TI supervisa la calidad de los servicios y conoce la percepción del cliente respecto a los mismos.

Los informes de rendimiento elaborados deben cubrir factores clave tales como:

- Cumplimiento de los SLAs, con información sobre la frecuencia y el impacto de las incidencias responsables de la degradación del servicio.
- Quejas, justificadas o no, de los clientes y usuarios.
- Utilización de la capacidad predefinida.
- Disponibilidad del servicio.
- Tiempos de respuesta.
- Costes reales del servicio ofrecido.
- Problemas detectados y cambios realizados para restaurar la calidad del servicio.
- Calidad del servicio de los proveedores externos: nivel de cumplimiento de los OLAs.

4.3.2.6 Revisión de la calidad de los servicios

La correcta **Gestión de Niveles de Servicio** es un proceso continuo que requiere la continua revisión de la calidad de los servicios ofrecidos.

En este último tramo del proceso se trata de revisar aquellos SLAs que se han incumplido buscando las razones para, a partir de este análisis, elaborar un Plan de Mejora del Servicio (SIP). Esta función enlaza directamente, con la fase de Mejora Continua del Servicio.

4.3.2.7 Control y medición del proceso

El objetivo de la **Gestión de Niveles de Servicio** no es otro que el de mejorar la calidad del servicio y la satisfacción del cliente, pero esto no se puede llevar a cabo sin una buena gestión de los procesos involucrados.

Es esencial disponer de:

- Unos objetivos claros y contrastables.
- Un equipo con experiencia liderado por un Gestor del Nivel de Servicio con la cualificación y experiencia necesarios.
- Una asignación clara de tareas y responsabilidades.
- Indicadores específicos de rendimiento tales como:
    - Porcentaje de servicios amparados bajo SLAs.
    - Porcentaje de incumplimiento de los SLAs clasificados por su impacto en la calidad del servicio.
    - SIPs elaborados e impacto de los mismos en la calidad del servicio.
    - Encuestas de satisfacción del cliente.

La correcta elaboración de informes internos de gestión permite evaluar el rendimiento de la Gestión de Niveles de Servicio y aporta información de vital importancia a otras áreas involucradas en el soporte y la provisión de los servicios TI.

Entre la documentación generada cabría destacar:

- Informes Estadísticos de Rendimiento: donde se detallen los SLAs, OLAs y UCs elaborados y el nivel de cumplimiento de los mismos, costes promedio asociados al proceso, etc.
- Informes de Seguimiento: donde se especifiquen las acciones de monitorización realizadas, sus resultados y el grado de satisfacción de los clientes con el servicio prestado.
- Planes de Mejora (SIP): donde se especifiquen las acciones propuestas para la mejora del servicio TI y el impacto que estas han tenido en la calidad del servicio.

4.3.3 Gestión de la Capacidad

4.3.3.1 Introducción y Objetivos

El objetivo principal de la **Gestión de la Capacidad** es poner a disposición de clientes, usuarios y del propio departamento de TI los recursos técnicos necesarios para desempeñar de una manera eficiente sus tareas y todo ello sin incurrir en costes desproporcionados.

Para ello, la Gestión de la Capacidad debe:

- Conocer el estado actual de la tecnología y previsibles futuros desarrollos.
- Conocer los planes de negocio y acuerdos de nivel de servicio para prever la capacidad necesaria.
- Analizar el rendimiento de la infraestructura para monitorizar el uso de la capacidad existente.
- Realizar modelos y simulaciones de capacidad para diferentes escenarios futuros previsibles.

- Dimensionar correctamente las aplicaciones y servicios, alineándolas a los procesos de negocio y necesidades reales del cliente.
- Gestionar la demanda de servicios tecnológicos racionalizando su uso.

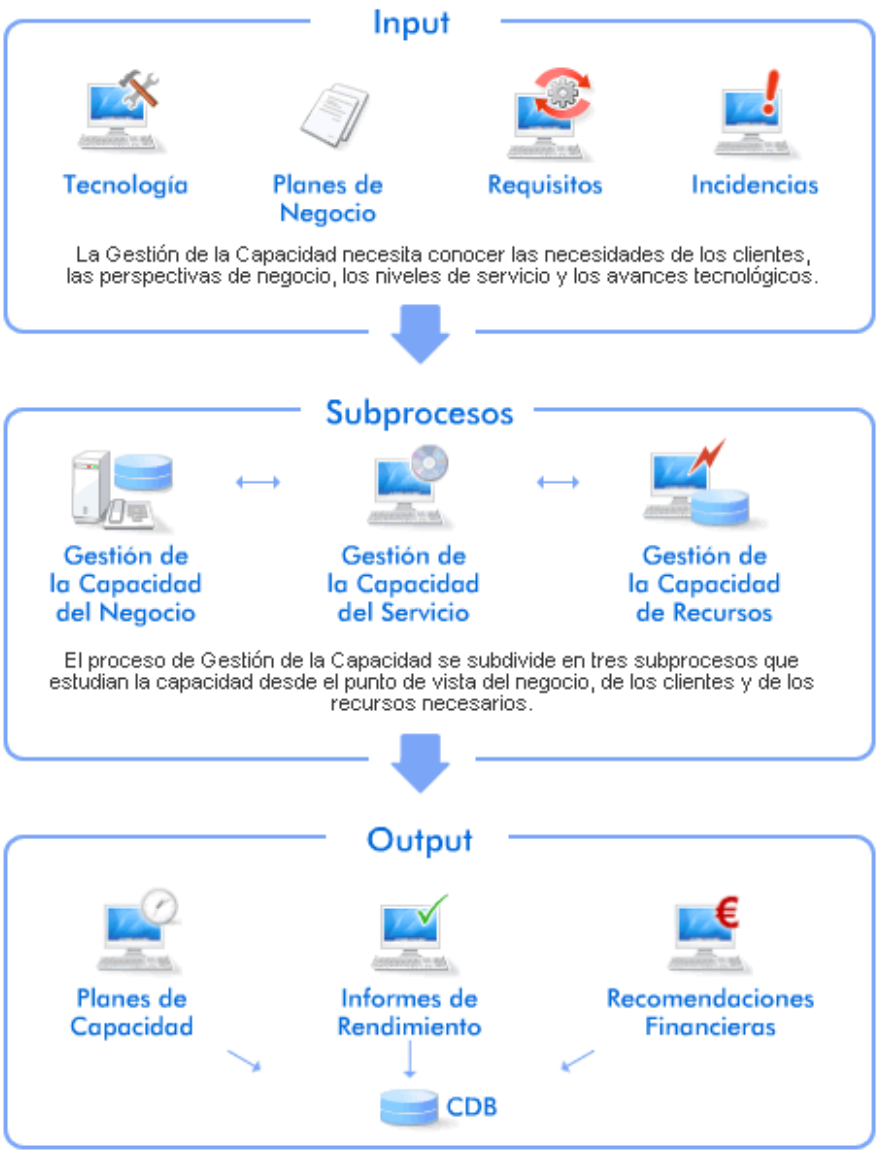


Ilustración 4-3 Gestión de la Capacidad

La **Gestión de la Capacidad** intenta evitar situaciones en las que se realizan inversiones innecesarias en tecnologías que no se adaptan a las necesidades reales del negocio o están sobredimensionadas, o, por el contrario, evitar situaciones en las que la productividad se ve mermada por un insuficiente o deficiente uso de las tecnologías existentes.

Ambos escenarios son habituales y a menudo se pueden encontrar conviviendo en una misma organización: directivos, clientes y otros profesionales informáticos deslumbrados por tecnologías que realmente no necesitan y adquieren pero que ignoran hardware, software y servicios que realmente aumentarían la productividad en sus respectivos entornos de trabajo.

Una de las principales tareas de la Gestión de la Capacidad es la de matizar la percepción de que la "capacidad es barata". Aunque el aumento de la capacidad puede requerir, en primera instancia, de modestos desembolsos, debido a la reducción de costes en los equipos de hardware y aplicaciones informáticas, la administración y mantenimiento de infraestructuras desproporcionadas puede resultar, a la larga, muy cara.

Los principales beneficios derivados de una correcta Gestión de la Capacidad son:

- Se optimiza el rendimiento de los recursos tecnológicos.
- Se dispone de la capacidad necesaria en el momento oportuno, evitando así que se pueda resentir la calidad del servicio.
- Se evitan gastos innecesarios producidos por compras de "última hora".
- Se planifica el crecimiento de la infraestructura adecuándolo a las necesidades reales de negocio.
- Se reducen de los gastos de mantenimiento y administración asociados a equipos y aplicaciones que han quedado obsoletos o son innecesarios.
- Se reducen posibles incompatibilidades y fallos en la infraestructura informática.

Resumiendo, se racionaliza la gestión de las compras y mantenimiento de los servicios TI con la consiguiente reducción de costes e incremento en el rendimiento.

La implementación de una adecuada política de Gestión de la Capacidad también se encuentra con algunas serias dificultades:

- Información insuficiente para una planificación realista de la capacidad.
- Expectativas injustificadas sobre las mejoras del rendimiento y el ahorro de costes.
- Insuficiencia de recursos para monitorizar adecuadamente el rendimiento.
- Infraestructuras técnicas distribuidas y excesivamente complejas en las que es difícil un correcto acceso a los datos.
- La dirección de la organización TI no tiene el nivel de compromiso suficiente para implementar rigurosamente los procesos asociados.
- La rápida evolución de las tecnologías puede obligar a una revisión permanente de los planes y escenarios contemplados.
- Un correcto establecimiento de las dimensiones de la propia Gestión de la Capacidad: un excesivo celo puede provocar costosos análisis de capacidad que podrían haber sido innecesarios con la compra de nuevo hardware o software.

Las principales actividades de la **Gestión de la Capacidad** se resumen en:

- Desarrollo del Plan de Capacidad y modelado de diferentes escenarios de capacidad.
- Monitorización de los recursos de la infraestructura TI.
- Supervisión de la capacidad y administración de la Base de Datos de la Capacidad (CDB) contenida en el Sistema de Información de Gestión de la Capacidad (CMIS).

El proceso de Gestión de la Capacidad puede segmentarse en subprocesos que analizan las necesidades de capacidad TI desde diferentes puntos de vista:

- Gestión de la Capacidad del Negocio (BCM, del inglés *Business Capacity Management*): que centra su objeto de atención en las necesidades futuras de usuarios y clientes.
- Gestión de la Capacidad del Servicio (SCM, del inglés *Service Capacity Management*): que analiza el rendimiento de los servicios TI con el objetivo de garantizar los niveles de servicio acordados.
- Gestión de la Capacidad de Recursos (CCM, del inglés *Component Capacity Management*): que estudia tanto el uso de la infraestructura TI como sus tendencias para asegurar que se dispone de los recursos suficientes y que estos se utilizan eficazmente.

4.3.3.2 **Planificación de la Capacidad**

4.3.3.2.1 Plan de Capacidad

La elaboración del Plan de Capacidad es la tarea principal de la Gestión de Capacidad.

El Plan de Capacidad recoge:

- Toda la información relativa a la capacidad de la infraestructura TI.

- Las previsiones sobre necesidades futuras basadas en tendencias, previsiones de negocio y SLAs existentes.
- Los cambios necesarios para adaptar la capacidad TI a las novedades tecnológicas y las necesidades emergentes de usuarios y clientes.

El Plan de Capacidad debe incluir información sobre los costes de la capacidad actual y prevista. Esta información es indispensable para que la Gestión Financiera pueda elaborar los presupuestos y previsiones financieras de manera realista.

Aunque, en principio, el Plan de Capacidad puede tener una vigencia anual o bianual es importante que se monitorice su cumplimiento para adoptar medidas correctivas en cuanto se detecten desviaciones importantes del mismo.

4.3.3.2.2 Modelado y Benchmarking

Cuanto más compleja sea una infraestructura técnica más difícil es prever las necesidades de capacidad futura. En esos casos, es imprescindible realizar modelos y simulaciones sobre posibles escenarios de desarrollo futuro que aseguren la correcta escalabilidad de las aplicaciones y hardware.

El nivel de detalle al que se lleve este modelado dependerá de varios factores:

- Costes asociados al incremento de la capacidad.
- Costes del propio proceso de modelado y simulación.
- Alcance de los aumentos de capacidad previstos.
- La "criticalidad" de los sistemas implicados.

Teniendo en cuenta los anteriores factores podemos optar por:

- Un simple análisis de tendencias que permita evaluar la carga de proceso esperada en la infraestructura de TI y escalar consecuentemente su capacidad actual.
- Realizar modelos y simulaciones sobre diferentes escenarios para llevar a cabo previsiones de carga y repuesta de la infraestructura técnica.
- Realizar *benchmarks* (pruebas de rendimiento comparativas) con prototipos reales para asegurar la capacidad y el rendimiento de la futura infraestructura.

4.3.3.3 Recursos de gestión de la Capacidad

Un aspecto esencial de la **Gestión de la Capacidad** es el de asignar recursos adecuados de hardware, software y personal a cada servicio y aplicación.

El correcto dimensionamiento requiere que la Gestión de la Capacidad disponga de información fiable sobre:

- Los niveles de servicio acordados y/o previstos (SLAs).
- Niveles de rendimiento esperados.
- Impacto de la aplicación o servicio en los procesos de negocio del cliente.
- Márgenes de seguridad y disponibilidad.
- Informes de monitorización de los niveles de servicio.
- Costes asociados a los equipos de hardware y otros recursos TI necesarios.

En la fase de diseño de un servicio, la Gestión de la Capacidad asegura que se dispondrá de la capacidad necesaria para llevar el proyecto a buen término. Una vez se ha puesto en marcha el servicio, también es la encargada de analizar las tendencias de uso y prever las necesidades futuras.

Es relativamente frecuente no tener en cuenta aspectos relativos al adecuado dimensionamiento de una aplicación a causa de expectativas injustificadas sobre la tecnología. Se puede pensar erróneamente que los

costes asociados a la capacidad se limitan a la compra de más equipos, más memoria, más espacio de almacenamiento, etcétera, olvidando que sistemas más complejos conllevan unos mayores gastos de administración y mantenimiento, o ignorando los problemas que pueden conllevar dichos cambios.

4.3.3.4 Supervisión de la Capacidad

La **Gestión de la Capacidad** es un proceso continuo e iterativo que monitoriza, analiza y evalúa la capacidad y rendimiento de la infraestructura TI y que, con los datos obtenidos, optimiza los servicios o envía una RFC a la Gestión de Cambios.

Tanto la información obtenida cómo resultado de estas actividades, como la generada a partir de ella por la Gestión de la Capacidad se almacenan y registran en la Base de Datos de la Capacidad (CDB).

Ilustración 4-4 Supervisión de la Capacidad

4.3.3.4.1 Monitorización

Su objetivo principal es asegurar que el rendimiento de la infraestructura de TI se adecua a los requisitos de los SLAs.

La monitorización debe incluir, además de aspectos técnicos, todos aquellos relativos a licencias y otras cuestiones de carácter administrativo.

4.3.3.4.2 Análisis y Evaluación

Los datos recogidos deben ser analizados para evaluar la conveniencia de adoptar acciones correctivas tales como petición de aumento de la capacidad o una mejor Gestión de la Demanda.

4.3.3.4.3 Optimización y cambios

Si se ha optado por solicitar un aumento de la capacidad, se elevará una petición de cambio (RFC) a la Gestión de Cambios para que se desencadene todo el proceso necesario para la implementación del cambio. La Gestión de la Capacidad prestará su apoyo en todo el proceso y será corresponsable, junto a la Gestión de Cambios y Versiones, de asegurar que el cambio solicitado cumpla los objetivos previstos.

En el caso de que una simple racionalización de la demanda sea suficiente para solventar las posibles deficiencias o incumplimientos de los SLAs, será la propia Gestión de la Capacidad la responsable de gestionar ese subproceso.

4.3.3.4.4 Base de Datos de la Capacidad

La Base de Datos de la Capacidad (CDB) debe cubrir toda la información de negocio, financiera, técnica y de servicio que reciba y genere la Gestión de la Capacidad relativas a la capacidad de la infraestructura y sus elementos.

Idealmente la CDB debe estar interrelacionada con la CMDB para que esta última ofrezca una imagen integral de los sistemas y aplicaciones con información relativa a su capacidad. Esto no es óbice para que ambas bases de datos puedan ser "físicamente independientes".

4.3.3.5 Control y medición del proceso

Es indispensable elaborar informes que permitan evaluar el rendimiento de la **Gestión de la Capacidad**.

La documentación elaborada debe incluir información sobre:

- El uso de recursos.
- Desviaciones de la capacidad real sobre la planificada.
- Análisis de tendencias en el uso de la capacidad.
- Métricas establecidas para el análisis de la capacidad y monitorización del rendimiento.
- Impacto en la calidad del servicio, disponibilidad y otros procesos TI.

El éxito de la Gestión de la Capacidad depende de algunos indicadores clave, entre los que se encuentran:

- Correcta previsión de las necesidades de capacidad.
- Reducción de los costes asociados a la capacidad.
- Más altos niveles de disponibilidad y seguridad.
- Mayor satisfacción de los usuarios y clientes.
- Cumplimiento de los SLAs.

4.3.4 Gestión de la Disponibilidad

4.3.4.1 Introducción y Objetivos

El objetivo primordial de la **Gestión de la Disponibilidad** es asegurar que los servicios TI estén disponibles y funcionen correctamente siempre que los clientes y usuarios deseen hacer uso de ellos en el marco de los SLAs en vigor.

Las responsabilidades de la Gestión de la Disponibilidad incluyen:

- Determinar los requisitos de disponibilidad en estrecha colaboración con los clientes.
- Garantizar el nivel de disponibilidad establecido para los servicios TI.
- Supervisar el cumplimiento de los OLAs y UCs acordados con proveedores internos y externos.
- Monitorizar la disponibilidad de los sistemas TI.
- Proponer mejoras en la infraestructura y servicios TI que aumenten los niveles de disponibilidad.

Los indicadores clave sobre los que se sustenta el proceso de Gestión de la Disponibilidad se resumen en:

- **Disponibilidad**: porcentaje de tiempo sobre el total acordado en el que el servicio ha sido accesible por el usuario y ha funcionado correctamente.
- **Fiabilidad**: tiempo durante el cual el servicio ha funcionado correctamente sin sufrir ninguna interrupción.
- **Capacidad de mantenimiento**: capacidad de recuperar el servicio en caso de interrupción.
- **Capacidad de Servicio**: determina la disponibilidad de los servicios internos y externos contratados y si se corresponde con los OLAs y UCs en vigor. Nótese que si un servicio es subcontratado en su totalidad la

disponibilidad y la capacidad de servicio pasan a ser términos equivalentes.

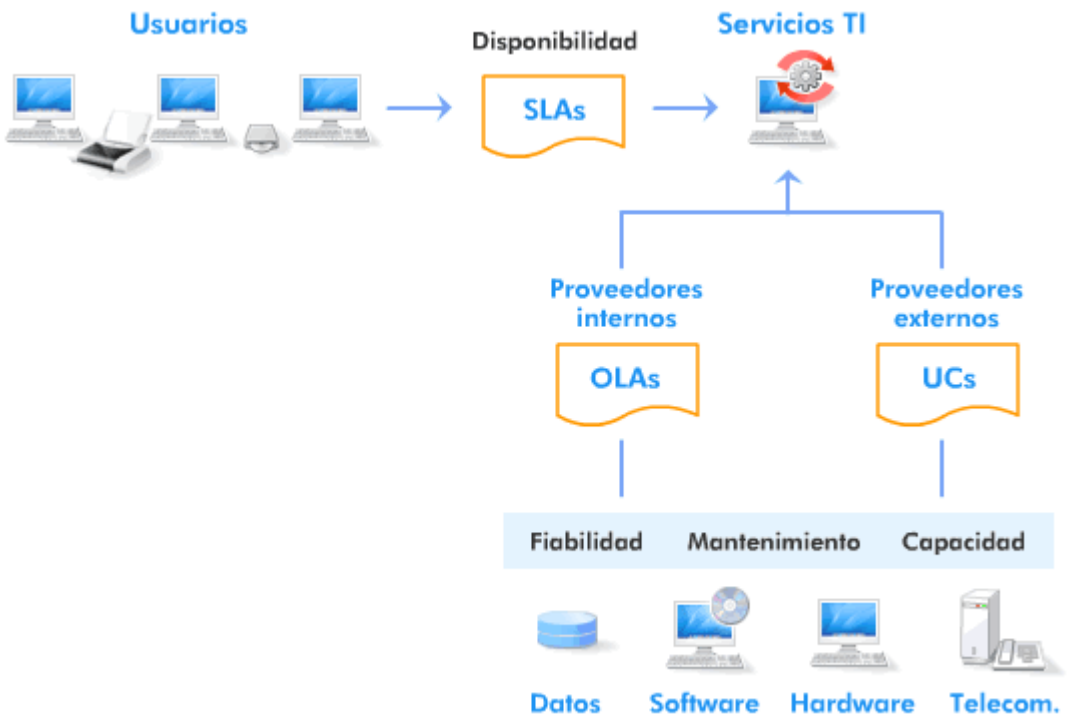


Ilustración 4-5 Indicadores Gestión de Disponibilidad

La disponibilidad depende del correcto diseño de los servicios TI, la fiabilidad de los CIs involucrados, su correcto mantenimiento y la calidad de los servicios internos y externos acordados.

Los principales beneficios de una adecuada Gestión de la Disponibilidad son:

- Se reduce el número de incidencias.
- Se aumentan progresivamente los niveles de disponibilidad.
- Cumplimiento de los niveles de disponibilidad acordados.
- Se reducen los costes asociados a un alto nivel de disponibilidad.
- El cliente percibe una mayor calidad de servicio.

Las principales dificultades con las que topa la Gestión de la Disponibilidad son:

- No se monitoriza correctamente la disponibilidad real del servicio.
- No se dispone de las herramientas de software y personal adecuado.
- Los objetivos de disponibilidad no están alineados con las necesidades del cliente.
- Falta de coordinación con los otros procesos.
- No existe compromiso con el proceso dentro de la organización TI.
- La falta de apoyo de la dirección provoca que los proveedores internos y externos no reconozcan la autoridad del Gestor de la Disponibilidad por falta de apoyo de la dirección.

4.3.4.2 Requisitos de disponibilidad

Es imprescindible cuantificar los requisitos de disponibilidad para la correcta elaboración de los SLAs.

La disponibilidad propuesta debe encontrase en línea tanto con las necesidades reales del negocio como con las posibilidades de la organización TI.

Aunque en principio todos los clientes estarán de acuerdo con unas elevadas cotas de disponibilidad es importante hacerles ver que una alta disponibilidad puede generar unos costes injustificados dadas sus necesidades reales. Quizá unas pocas horas sin un determinado servicio pueden representar poco más allá de una pequeña inconveniencia mientras que la certeza de un servicio prácticamente continuo y sin interrupciones puede requerir la replicación de sistemas u otras medidas igualmente costosas que no van a tener una repercusión real en la rentabilidad del negocio.

Para llevar a cabo eficientemente esta tarea es necesario que la **Gestión de la Disponibilidad**:

- Identifique las actividades clave del negocio.
- Cuantifique los intervalos razonables de interrupción de los diferentes servicios dependiendo de sus respectivos impactos.
- Establezca los protocolos de mantenimiento y revisión de los servicios.
- Determine las franjas horarias de disponibilidad de los servicios (24x7, 12x5, ...).

4.3.4.3 Planificación de la disponibilidad

La correcta planificación de la disponibilidad permite establecer unos niveles de disponibilidad adecuados tanto en lo que respecta a las necesidades reales del negocio como a las posibilidades de la organización TI.

El documento que debe recoger los objetivos de disponibilidad presentes y futuros y qué medidas son necesarias para su cumplimiento es el **Plan de Disponibilidad**.

Este plan debe recoger:

- La situación actual de disponibilidad de los servicios. Obviamente esta información debe ser actualizada periódicamente.
- Herramientas para la monitorización de la disponibilidad.
- Métodos y técnicas de análisis a utilizar.
- Definiciones relevantes y precisas de las métricas a utilizar.
- Planes de mejora de la disponibilidad.
- Expectativas de disponibilidad.

Es imprescindible que este plan proponga los cambios necesarios para que se cumplan los estándares previstos y colabore con la Gestión de Cambios y la Gestión de Entregas y Despliegues en su implementación (en caso de ser aprobados, claro está).

Para que este plan sea realista, debe contar con la colaboración de los otros procesos TI involucrados.

4.3.4.4 Diseño para la Disponibilidad

Es crucial para una correcta Gestión de la Disponibilidad participar desde el inicio en el desarrollo de los nuevos servicios de forma que éstos cumplan los estándares plasmados en el Plan de Disponibilidad.

Un diferente nivel de disponibilidad puede requerir cambios drásticos en los recursos utilizados o en las actividades necesarias para suministrar un determinado servicio. Si éste se diseña sin tener en cuenta futuras necesidades de disponibilidad puede ser necesario un completo rediseño al cabo de poco tiempo, incurriendo en costes adicionales innecesarios.

4.3.4.5 Mantenimiento y Seguridad

Aunque hayamos realizado un correcto diseño de los servicios según el Plan de Disponibilidad y se hayan tomado todas las medidas preventivas necesarias, tarde o temprano, nos habremos de enfrentar a interrupciones del servicio.

En esos casos es necesario recuperar el servicio lo antes posible para que no tenga un efecto indeseado sobre los niveles de disponibilidad acordados.

Aunque la responsabilidad de restaurar el servicio corresponde a la Gestión de Incidencias y las actividades de recuperación han de ser coordinadas por el Centro de Servicios, la Gestión de la Disponibilidad debe prestar su asesoramiento mediante planes de recuperación que tengan en cuenta:

- Las necesidades de disponibilidad del negocio.
- Las implicaciones de la incidencia en la infraestructura TI y los procesos necesarios para restaurar el servicio.

4.3.4.5.1 Gestión de las Interrupciones de Mantenimiento

Independientemente de las interrupciones del servicio causadas por incidencias, es habitualmente necesario interrumpir el servicio para realizar labores de mantenimiento y/o actualización.

Estas interrupciones programadas pueden afectar a la disponibilidad del servicio y por lo tanto han de ser cuidadosamente planificadas para minimizar su impacto.

En aquellos casos en que los servicios no son 24/7 es obvio que, siempre que ello sea posible, deben aprovecharse las franjas horarias de inactividad para realizar las tareas que implican una degradación o interrupción del servicio.

Si el servicio es 24x7 y la interrupción es necesaria se debe:

- Consultar con el cliente acerca de la franja horaria en la que la interrupción del servicio afectará menos a sus actividades de negocio.
- Informar con antelación suficiente a todos los agentes implicados.
- Incorporar dicha información a los SLAs.

4.3.4.5.2 Seguridad

Uno de los aspectos esenciales para obtener altos niveles de fiabilidad y disponibilidad es una correcta Gestión de la Seguridad.

Los aspectos relativos a la seguridad deben ser tomados en cuenta en todas las etapas del proceso.

Es tan importante determinar cuándo el servicio estará disponible como el "quién y cómo" va a utilizarlo. La disponibilidad y seguridad son interdependientes y cualquier fallo en una de ellas afectará gravemente a la otra.

4.3.4.6 **Monitorización de la disponibilidad**

La monitorización de la disponibilidad del servicio y la elaboración de los informes correspondientes son dos de las principales actividades de la Gestión de la Disponibilidad.

Desde el momento de la interrupción del servicio hasta su restitución o "tiempo de parada" la incidencia pasa por distintas fases que deben ser analizadas por separado:

- **Tiempo de detección**: es el tiempo que transcurre desde que ocurre el fallo hasta que la organización TI tiene constancia del mismo.
- **Tiempo de respuesta**: es el tiempo que transcurre desde la detección del problema hasta que se realiza un registro y diagnóstico de la incidencia.
- **Tiempo de reparación/recuperación**: periodo de tiempo utilizado para reparar el fallo o encontrar un workaround o solución temporal al mismo y devolver el sistema a la situación anterior a la interrupción del servicio.

Ilustración 4-6 Monitorización de la disponibilidad

Es importante determinar métricas que permitan medir con precisión las diferentes fases del ciclo de vida de la interrupción del servicio. El cliente debe conocer estas métricas y dar su conformidad a las mismas para evitar malentendidos. En algunos casos es difícil determinar si el sistema está "caído o en funcionamiento" y la interpretación puede diferir entre proveedores y clientes, por lo tanto, estás métricas deben poder expresarse en términos que el cliente pueda entender.

Algunos de los parámetros que suele utilizar la Gestión de la Disponibilidad y que debe poner a disposición del cliente en los informes de disponibilidad correspondientes incluyen:

- **Tiempo Medio de Parada** (*Downtime* o (MTTR): que es el tiempo promedio de duración de una interrupción del servicio, e incluye el tiempo de detección, respuesta y resolución.
- **Tiempo Medio entre Fallos** (*Uptime* o MTBF): es el tiempo medio durante el cual el servicio está disponible sin interrupciones.
- **Tiempo Medio entre Incidencias** (MTBSI): es el tiempo medio transcurrido entre incidencias, que es igual a la suma del Tiempo Medio de Parada y el Tiempo Medio entre Fallos. El Tiempo Medio entre Incidencias es una medida de la fiabilidad del sistema.

4.3.4.7 Métodos y Técnicas

Aunque llevamos hablando ya un buen rato de disponibilidad, aún no hemos aportado un método para cuantificarla.

Es frecuente definir la disponibilidad en tanto por ciento de la siguiente manera:

$$\%Disponibilidad = \frac{(AST - DT)}{AST} \times 100 \qquad (4\text{-}1)$$

donde:

AST es el tiempo acordado de servicio y DT es el tiempo de interrupción del servicio durante las franjas horarias de disponibilidad acordadas.

Por ejemplo, si el servicio es 24x7 y en el último mes el sistema ha estado caído durante 6 horas por tareas de mantenimiento la disponibilidad real del servicio fue:

$$\%Disponibilidad = \frac{(720 - 6)}{720} \times 100 = 99,2\% \qquad (4\text{-}2)$$

La Gestión de la Disponibilidad tiene a su disposición un buen número de métodos y técnicas que le permiten determinar qué factores intervienen en la disponibilidad del servicio y que le permiten consecuentemente prever qué tipo de recursos se deben asignar para las labores de prevención, mantenimiento y recuperación, así como elaborar planes de mejora a partir de dichos análisis.

Entre dichas técnicas se cuentan:

- **Análisis del Impacto de Fallo de Componentes (CFIA):** El CFIA (siglas de Component Failure Impact Analysis) es un método mediante el cual se identifica el impacto que tiene en la disponibilidad de los servicios TI el fallo de cada elemento de configuración involucrado. Es evidente que este método requiere una CMDB correctamente actualizada.
- **Análisis del Árbol de Fallos (FTA):** El FTA (siglas de Failure Tree Analysis) tiene como objetivo estudiar cómo se "propagan" los fallos a través de la infraestructura TI para comprender mejor su impacto en la disponibilidad del servicio.
- **Método de Gestión y Análisis de Riesgos de la CCTA (CRAMM):** El CRAMM (siglas de CCTA Risk Analysis and Management Method) tiene como objetivo identificar los riesgos y vulnerabilidades a los que está expuesta la infraestructura TI, con el objetivo de adoptar contramedidas que los reduzcan o que permitan recuperar rápidamente el servicio en caso de interrupción del mismo.
- **Análisis de Interrupción del Servicio (SOA):** El SOA (siglas de Service Outage Analysis) es una técnica cuyo objetivo consiste en analizar las causas de los fallos detectados y proponer soluciones a los mismos. Se diferencia de los anteriores métodos en que realiza el análisis desde el punto de vista del cliente, haciendo especial énfasis en aspectos no exclusivamente técnicos ligados directamente a la infraestructura TI.

4.3.4.8 Control y medición del proceso

La **Gestión de la Disponibilidad** debe realizar informes periódicos sobre su gestión que contengan información relevante tanto para los clientes como para el resto de la organización TI.

Estos informes deben incluir:

- Métodos y técnicas utilizadas para el análisis y prevención de fallos.
- Información estadística sobre:
  - Tiempos de detección y respuesta a los fallos.
  - Tiempos de reparación y recuperación del servicio.
  - Tiempo medio de servicio entre fallos.
- Disponibilidad real de los diferentes servicios.
- Cumplimiento de los SLAs en todo lo referente a la disponibilidad y fiabilidad del servicio.
- Cumplimiento de los OLAs y UCs en todo lo referente a la capacidad de servicio prestada por los proveedores internos y externos.

Para que toda esta información sea fácil y correctamente analizada es imprescindible el establecimiento de métricas precisas que permitan determinar de forma inequívoca parámetros tales como tiempos de parada y funcionamiento. Por ejemplo, en el caso de un servicio online de comercio electrónico, se puede considerar que tiempos de respuesta superiores a 10 segundos son equivalentes a que el sistema esta caído, aunque estrictamente hablando el sistema termine respondiendo.

4.3.5 Gestión de la Continuidad de Servicios TI

4.3.5.1 Introducción y Objetivos

Los objetivos principales de la **Gestión de la Continuidad de los Servicios TI** (ITSCM) se resumen en:

- Garantizar la pronta recuperación de los servicios (críticos) TI tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las perniciosas consecuencias de un desastre o causa de fuerza mayor.

Aunque, a priori, las políticas proactivas que prevean y limiten los efectos de un desastre sobre los servicios TI

son preferibles a las exclusivamente reactivas, es importante valorar los costes relativos y la incidencia real en la continuidad del negocio para decantarse por una de ellas o por una sabia combinación de ambas.

Una correcta ITSCM debe formar parte integrante de la Gestión de Continuidad del Negocio (BCM) y debe estar a su servicio. Los servicios TI no son sino una parte, aunque a menudo muy importante, del negocio en su conjunto y no tiene mayor sentido que, por ejemplo, un sistema de pedidos online siga funcionando a la perfección tras un desastre si nos resulta imposible suministrar la mercancía a nuestros clientes.

Es importante diferenciar entre desastres "de toda la vida", tales como incendios, inundaciones, etcétera, y desastres "puramente informáticos", tales como los producidos por ataques distribuidos de denegación de servicio (DDOS), virus informáticos, etcétera. Aunque es responsabilidad de la ITSCM prever los riesgos asociados en ambos casos y restaurar el servicio TI con prontitud, es evidente que recae sobre la ITSCM una responsabilidad especial en el último caso pues:

- Sólo afectan directamente a los servicios TI, pero paralizan a toda la organización.
- Son más previsibles y más habituales.
- La percepción del cliente es diferente: los desastres naturales son más asumibles y no se asocian a actitudes negligentes, aunque esto no sea siempre cierto.

Los principales beneficios de una correcta Gestión de la Continuidad del Servicio se resumen en:

- Se gestionan adecuadamente los riesgos.
- Se reduce el periodo de interrupción del servicio por causas de fuerza mayor.
- Se mejora la confianza en la calidad del servicio entre clientes y usuarios.
- Sirve de apoyo al proceso de Gestión de la Continuidad del Negocio (BCM).

Las principales dificultades a la hora de implementar la Gestión de la Continuidad del Servicio se resumen en:

- Puede haber resistencia a realizar inversiones cuya rentabilidad no es inmediata.
- No se presupuestan correctamente los costes asociados.
- No se asignan los recursos suficientes.
- No existe el compromiso suficiente con el proceso dentro de la organización y las tareas y actividades correspondientes se demoran perpetuamente para hacer frente a "actividades más urgentes".
- No se realiza un correcto análisis de riesgos y se obvian amenazas y vulnerabilidades reales.
- El personal no está familiarizado con las acciones y procedimientos a tomar en caso de interrupción grave de los servicios.
- Falta de coordinación con la BCM.

Las principales actividades de la **Gestión de la Continuidad de los Servicios TI** se resumen en:

- Establecer las políticas y alcance de la ITSCM.
- Evaluar el impacto en el negocio de una interrupción de los servicios.
- Analizar y prever los riesgos a los que está expuesto la infraestructura TI.
- Establecer las estrategias de continuidad del servicio TI.
- Adoptar medidas proactivas de prevención del riesgo.
- Desarrollar los planes de contingencia.
- Poner a prueba dichos planes.
- Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

4.3.5.2 Política y Alcance

El primer paso necesario para desarrollar una **Gestión de la Continuidad del Servicio** coherente es establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI: su política.

La gestión de la empresa debe demostrar su implicación con el proceso desde un primer momento pues la

implantación de la ITSCM puede resultar compleja y costosa sin la contrapartida de un retorno obvio a la inversión.

Es imprescindible establecer el alcance de la ITSCM en función de:

- Los planes generales de Continuidad del Negocio.
- Los servicios TI estratégicos.
- Los estándares de calidad adoptados.
- El histórico de interrupciones graves de los servicios TI.
- Las expectativas de negocio.
- La disponibilidad de recursos.

La Gestión de la Continuidad del Servicio está abocada al fracaso sino se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipamiento (software y hardware). Su dimensión depende de su alcance y sería absurdo y contraproducente instaurar una política demasiado ambiciosa que no dispusiera de los recursos correspondientes.

Una importante parte del esfuerzo debe destinarse a la formación del personal. Éste debe interiorizar su papel en momentos de crisis y conocer perfectamente las tareas que se espera desempeñe: una emergencia no es el mejor momento para estudiar documentación y manuales.

4.3.5.3 Análisis de Impacto

Una correcta **Gestión de la Continuidad del Servicio** requiere en primer lugar determinar el impacto que una interrupción de los servicios TI pueden tener en el negocio.

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que un "apagón" de los servicios TI afecte a prácticamente todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que "simplemente" aumentan la productividad de la fuerza comercial y de trabajo.

Cuanto mayor sea el impacto asociado a la interrupción de un determinado servicio mayor habrá de ser el esfuerzo realizado en actividades de prevención. En aquellos casos en que la "solución puede esperar" se puede optar exclusivamente por planes de recuperación.

Los servicios TI han de ser analizados por la ITSCM en función de diversos parámetros:

- Consecuencias de la interrupción del servicio en el negocio:
  - Pérdida de rentabilidad.
  - Pérdida de cuota de mercado.
  - Mala imagen de 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.

Dependiendo de estos factores se buscará un balance entre las actividades de prevención y recuperación teniendo en cuenta sus respectivos costes financieros.

4.3.5.4 Evaluación de Riesgos

Sin conocer cuáles son los riesgos reales a los que se enfrenta la infraestructura TI es imposible realizar una política de prevención y recuperación ante desastre mínimamente eficaz.

La Gestión de la Continuidad del Servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes riesgos factores de riesgo. Para ello la ITSCM debe:

- Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración (CIs) involucrados en la prestación de cada servicio, especialmente los servicios TI críticos y estratégicos.
- Analizar las posibles amenazas y estimar su probabilidad.
- Detectar los puntos más vulnerables de la infraestructura TI.

Ilustración 4-7 Evaluación de riesgos

Gracias a los resultados de este detallado análisis se dispondrá de información suficiente para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio.

La prevención frente a riesgos genéricos y poco probables puede ser muy cara y no estar siempre justificada, sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente baratas.

Por ejemplo, si el riesgo de pérdida de alimentación eléctrica es elevado debido, por ejemplo, a la localización geográfica se puede optar por deslocalizar ciertos servicios TI a través de ISPs que dispongan de sistemas de generadores redundantes o adquirir generadores que proporcionen la energía mínima necesaria para alimentar los CIs de los que dependen los servicios más críticos, etcétera.

4.3.5.5 Estrategias de Continuidad

La continuidad de los servicios puede obtenerse bien aplicando medidas preventivas, que eviten la interrupción de los servicios, o medidas reactivas, que permitan recuperar unos niveles aceptables de servicio en el menor tiempo posible.

Es responsabilidad de la Gestión de la Continuidad del Servicio diseñar actuaciones de prevención y recuperación que ofrezcan las garantías necesarias a unos costes razonables.

4.3.5.5.1 Actividades preventivas

Las medidas preventivas requieren un detallado análisis previo de riesgos y vulnerabilidades. Algunos de ellos serán de carácter general: incendios, desastres naturales, etcétera, mientras que otros tendrán un carácter estrictamente informático: fallo de sistemas de almacenamiento, ataques de hackers, virus informáticos, etcétera.

La adecuada prevención de los riesgos de carácter general depende de una estrecha colaboración con la Gestión de la Continuidad del Negocio (BCM) y requieren medidas que implican a la infraestructura "física" de la organización.

La prevención de riesgos y vulnerabilidades "lógicas" o de hardware requieren especial atención de la ITSCM. En este aspecto es esencial la estrecha colaboración con la Gestión de la Seguridad.

Los sistemas de protección habituales son los de "Fortaleza" que ofrecen protección perimetral a la

infraestructura TI. Aunque imprescindibles no se hallan exentos de sus propias dificultades pues aumentan la complejidad de la infraestructura TI y pueden ser a su vez fuente de nuevas vulnerabilidades.

4.3.5.5.2 Actividades de recuperación

Tarde o temprano, por muy eficientes que seamos en nuestras actividades de prevención, será necesario poner en marcha procedimientos de recuperación.

En líneas generales existen tres opciones de recuperación del servicio:

- *Cold standby*: que requiere un emplazamiento alternativo en el que podamos reproducir en pocos días nuestro entorno de producción y servicio. Esta opción es la adecuada si los planes de recuperación estiman que la organización puede mantener sus niveles de servicio durante este periodo sin el apoyo de la infraestructura TI.
- *Warm standby*: que requiere un emplazamiento alternativo con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas.
- *Hot standby*: que requiere un emplazamiento alternativo con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución de la estructura de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales.

4.3.5.6 **Organización y Planificación**

Una vez determinado el alcance de la ITSCM, analizados los riesgos y vulnerabilidades y definidas unas estrategias de prevención y recuperación es necesario asignar y organizar los recursos necesarios. Con ese objetivo la **Gestión de la Continuidad del Servicio** debe elaborar una serie de documentos entre los que se incluyen:

- Plan de prevención de riesgos.
- Plan de gestión de emergencias.
- Plan de recuperación.

4.3.5.6.1 Plan de prevención de riesgos

Su objetivo principal es el de evitar o minimizar el impacto de un desastre en la infraestructura TI.

Entre las medidas habituales se encuentran:

- Almacenamiento de datos distribuidos.
- Sistemas de alimentación eléctrica de soporte.
- Políticas de back-ups.
- Duplicación de sistemas críticos.
- Sistemas de seguridad pasivos.

4.3.5.6.2 Plan de gestión de emergencias

Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por la incidencia que las causó. Por ello es imprescindible que en caso de situación de emergencia estén claramente determinadas las responsabilidades y funciones del personal, así como los protocolos de acción correspondientes.

En principio los planes de gestión de emergencias deben tomar en cuenta aspectos tales como:

- Evaluación del impacto de la contingencia en la infraestructura TI.
- Asignación de funciones de emergencia al personal del servicio TI.
- Comunicación a los usuarios y clientes de una grave interrupción o degradación del servicio.
- Procedimientos de contacto y colaboración con los proveedores involucrados.
- Protocolos para la puesta en marcha del plan de recuperación correspondiente.

4.3.5.6.3 Plan de recuperación

Cuando la interrupción del servicio es inevitable, llega el momento de poner en marcha los procedimientos de recuperación.

El plan de recuperación debe incluir todo lo necesario para:

- Reorganizar al personal involucrado.
- Reestablecer los sistemas de hardware y software necesarios.
- Recuperar los datos y reiniciar el servicio TI.

Los procedimientos de recuperación pueden depender de la importancia de la contingencia y de la opción de recuperación asociada ("cold o hot stand-by"), pero en general involucran:

- Asignación de personal y recursos.
- Instalaciones y hardware alternativos.
- Planes de seguridad que garanticen la integridad de los datos.
- Procedimientos de recuperación de datos.
- Contratos de colaboración con otras organizaciones.
- Protocolos de comunicación con los clientes.

Cuando se pone en marcha un plan de recuperación no hay espacio para la improvisación, cualquier decisión puede tener graves consecuencias tanto en la percepción que de nosotros tengan nuestros clientes como en los costes asociados al proceso.

Aunque pueda resultar paradójico, un "desastre" puede ser una buena oportunidad para demostrar a nuestros clientes la solidez de nuestra organización TI y, por tanto, incrementar la confianza que tiene depositada en nosotros.

4.3.5.7 **Supervisión de la Continuidad**

Una vez establecidas las políticas, estrategias y planes de prevención y recuperación, es indispensable que éstos no queden en papel mojado y que la organización TI esté preparada para su correcta implementación.

Ello depende de dos factores clave: la correcta formación del personal involucrado y la continua monitorización y evaluación de los planes para su adecuación a las necesidades reales del negocio.

4.3.5.7.1 Formación

Es inútil disponer de unos completos planes de prevención y recuperación si las personas que eventualmente deben llevarlos a cabo no están familiarizadas con los mismos.

Es indispensable que la ITSCM:

- Dé a conocer al conjunto de la organización TI los planes de prevención y recuperación.
- Ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación.
- Realice periódicamente simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado.
- Facilite el acceso permanente a toda la información necesaria, por ejemplo, a través de la Intranet o portal B2E de la empresa.

4.3.5.7.2 Actualización y auditorías

Tanto las políticas, estrategias y planes han de ser actualizados periódicamente para asegurar que responden a los requisitos de la organización en su conjunto.

Cualquier cambio en la infraestructura TI o en los planes de negocio puede requerir de una profunda revisión de los planes en vigor y una consecuente auditoría que evalúe su adecuación a la nueva situación.

En ocasiones en que el dinamismo del negocio y los servicios TI lo haga recomendable, estos procesos de

actualización y auditoría pueden establecerse de forma periódica.

La Gestión de Cambios juega un papel esencial a la hora de asegurar que los planes de recuperación y prevención están actualizados, manteniendo informada a la ITSCM de los cambios realizados o previstos.

4.3.5.8 Control y medición del proceso

La **Gestión de la Continuidad del Servicio** debe elaborar periódicamente informes sobre su propia gestión que contengan información relevante para el resto de la organización TI.

Estos informes deben incluir:

- Evaluación de los simulacros de desastre realizados.
- Análisis sobre nuevos riesgos y evaluación de su impacto.
- Actividades de prevención y recuperación realizadas.
- Costes asociados a los planes de prevención y recuperación.
- Preparación y capacitación del personal TI respecto a los planes y procedimientos de prevención y recuperación.

Uno de los factores clave para el éxito de la Gestión de la Continuidad del Servicio es mantener la "concentración". Tras largos periodos en los que la prevención o, simple y llanamente, la suerte ha impedido la existencia de graves interrupciones del servicio, se puede caer en un relajamiento que puede acarrear graves consecuencias.

Por esto es imprescindible llevar controles rigurosos que impidan que la inversión y compromiso inicial se diluyan y la ITSCM no esté a la altura de la situación cuando sus servicios sean vitales para evitar que "un desastre se convierta en una catástrofe".

Pero si el control del proceso es importante en condiciones normales, éste se vuelve crítico durante las situaciones de crisis. La ITSCM debe garantizar:

- La puesta en marcha de los planes preestablecidos.
- La supervisión de los mismos.
- La coordinación con la Gestión de Continuidad del Negocio.
- La asignación de recursos necesarios.

4.3.6 Gestión de la Seguridad de la Información

4.3.6.1 Introducción y Objetivos

Los principales objetivos de la **Gestión de la Seguridad** se resumen en:

- Diseñar una política de seguridad, en colaboración con clientes y proveedores, correctamente alineada con las necesidades del negocio.
- Asegurar el cumplimiento de los parámetros de seguridad acordados en los SLAs.
- Minimizar los riesgos de seguridad que supongan una amenaza para la continuidad del servicio.

Una correcta Gestión de la Seguridad necesita de la colaboración de especialistas en seguridad de la información con otros recursos que tengan conocimiento de los otros procesos de negocio. Si caemos en la tentación de establecer la seguridad como una prioridad en sí misma, limitaremos las oportunidades de negocio que nos ofrece el flujo de información entre los diferentes agentes implicados y la apertura de nuevas redes y canales de comunicación.

La Gestión de la Seguridad debe conocer en profundidad el negocio y los servicios que presta la organización TI para establecer protocolos de seguridad que aseguren que la información esté accesible cuando es necesaria para aquellos que tengan autorización para utilizarla.

Una vez comprendidos cuáles son los requisitos de seguridad del negocio, la Gestión de la Seguridad debe supervisar que estos se hallen convenientemente plasmados en los SLAs correspondientes para, a renglón

seguido, garantizar su cumplimiento.

La Gestión de la Seguridad debe asimismo tener en cuenta los riesgos generales a los que está expuesta la infraestructura TI, y que no necesariamente tienen por qué figurar en un SLA, para asegurar, en la medida de lo posible, que no representan un peligro para la continuidad del servicio.

Es importante que la Gestión de la Seguridad sea proactiva y evalúe a priori los riesgos de seguridad que pueden suponer los cambios realizados en la infraestructura, nuevas líneas de negocio, etcétera.

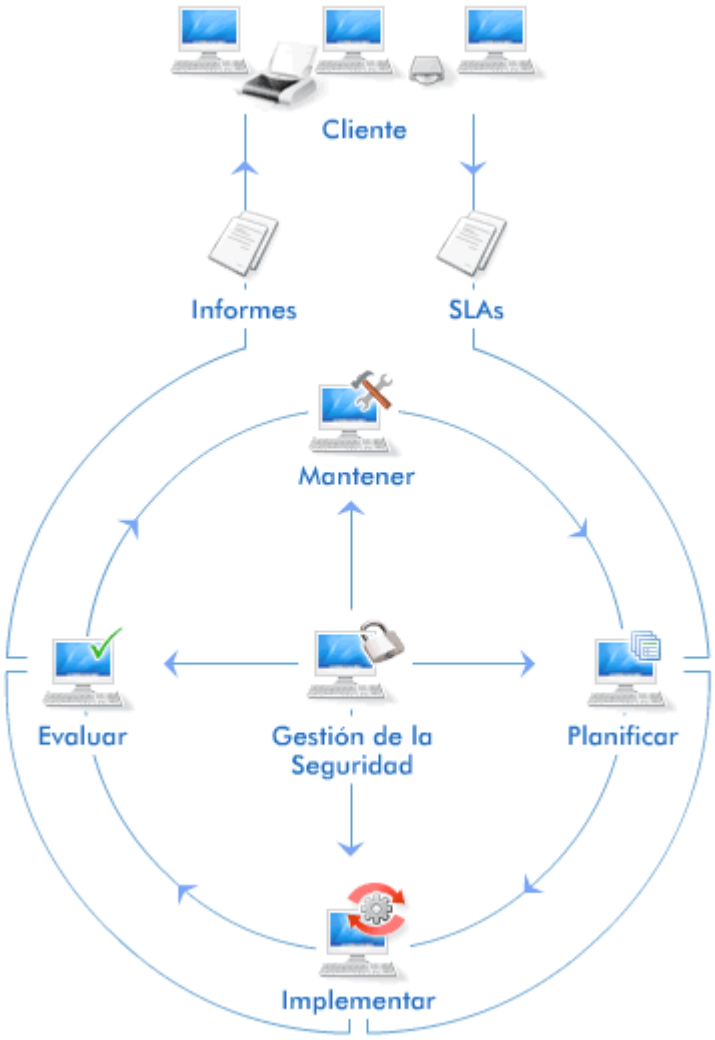


Ilustración 4-8 Gestión de la Seguridad

Los principales beneficios de una correcta Gestión de la Seguridad:

- Se evitan interrupciones del servicio causadas por virus, ataques informáticos, etcétera.
- Se minimiza el número de incidencias.
- Se tiene acceso a la información cuando se necesita y se preserva la integridad de los datos.
- Se preserva la confidencialidad de los datos y la privacidad de clientes y usuarios.
- Se cumplen los reglamentos sobre protección de datos.
- Mejora la percepción y confianza de clientes y usuarios en lo que respecta a la calidad del servicio.

Las principales dificultades a la hora de implementar la Gestión de la Seguridad se resumen en:

- No existe el suficiente compromiso de todos los miembros de la organización TI con el proceso.
- Se establecen políticas de seguridad excesivamente restrictivas que afectan negativamente al negocio.

- No se dispone de las herramientas necesarias para monitorizar y garantizar la seguridad del servicio (*firewalls*, antivirus, etc.).
- El personal no recibe una formación adecuada para la aplicación de los protocolos de seguridad.
- Falta de coordinación entre los diferentes procesos, lo que impide una correcta evaluación de los riesgos.

La **Gestión de la Seguridad** está estrechamente relacionada con prácticamente todos los otros procesos TI y necesita para su éxito la colaboración de toda la organización.

Para que esa colaboración sea eficaz, es necesario que la Gestión de la Seguridad:

- Establezca una clara y definida política de seguridad que sirva de guía a todos los otros procesos.
- Elabore un Plan de Seguridad que incluya los niveles de seguridad adecuados tanto en los servicios prestados a los clientes como en los acuerdos de servicio firmados con proveedores internos y externos.
- Implemente el Plan de Seguridad.
- Monitorice y evalúe el cumplimiento de dicho plan.
- Supervise proactivamente los niveles de seguridad analizando tendencias, nuevos riesgos y vulnerabilidades.
- Realice periódicamente auditorías de seguridad.

4.3.6.2 Política y Plan de Seguridad

Es indispensable disponer de un marco general en el que encuadrar todos los subprocesos asociados a la **Gestión de la Seguridad**. Su complejidad e intricadas interrelaciones necesitan de una política global clara en donde se determinen aspectos tales como los objetivos, recursos y responsabilidades.

En particular la Política de Seguridad debe determinar:

- Su relación con la política general del negocio.
- La coordinación con los otros procesos.
- Los protocolos de acceso a la información.
- Los procedimientos de análisis de riesgos.
- Los programas de formación.
- El nivel de monitorización de la seguridad.
- Qué informes deben ser emitidos periódicamente.
- El alcance del Plan de Seguridad.
- La estructura y responsables del proceso de Gestión de la Seguridad.
- Los procesos y procedimientos empleados.
- Los responsables de cada subproceso.
- Los auditores externos e internos de seguridad.
- Los recursos necesarios: software, hardware y personal.

4.3.6.2.1 Plan de Seguridad

El objetivo del **Plan de Seguridad** es fijar los niveles de seguridad que han de ser incluidos como parte de los SLAs, OLAs y UCs.

Este plan ha de ser desarrollado en colaboración con la Gestión del Nivel de Servicio, que es la responsable en última instancia tanto de la calidad del servicio prestado a los clientes como la del servicio recibido por la propia organización TI y los proveedores externos.

El Plan de Seguridad debe ser diseñado con el fin de ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio.

Siempre que sea posible, deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad acordados.

Un aspecto esencial a tener en cuenta es el establecimiento de unos protocolos de seguridad coherentes en

todas las fases del servicio y para todos los estamentos implicados. "Una cadena es tan resistente como el más débil de sus eslabones", por lo que carece de sentido, por ejemplo, establecer unas estrictas normas de acceso si una aplicación tiene vulnerabilidades frente a inyecciones de SQL. Quizá con ello podamos engañar a algún cliente durante algún tiempo ofreciendo la imagen de "fortaleza", pero esto valdrá de poco si alguien descubre que la "puerta de atrás está abierta".

4.3.6.3 Aplicación de las Medidas de Seguridad

Por muy buena que sea la planificación de la seguridad resultará inútil si las medidas previstas no se ponen en práctica.

Es responsabilidad de la **Gestión de Seguridad** coordinar la implementación de los protocolos y medidas de seguridad establecidas en la Política y el Plan de Seguridad.

En primer lugar, la Gestión de la Seguridad debe verificar que:

- El personal conoce y acepta las medidas de seguridad establecidas, así como sus responsabilidades al respecto.
- Los empleados firmen los acuerdos de confidencialidad correspondientes a su cargo y responsabilidad.
- Se imparte la formación pertinente.

Es también responsabilidad directa de la Gestión de la Seguridad:

- Asignar los recursos necesarios.
- Generar la documentación de referencia necesaria.
- Colaborar con el Centro de Servicios y la Gestión de Incidencias en el tratamiento y resolución de incidencias relacionados con la seguridad.
- Instalar y mantener las herramientas de hardware y software necesarias para garantizar la seguridad.
- Colaborar con la Gestión de Cambios y la de Entregas y Despliegues para asegurar que no se introducen nuevas vulnerabilidades en los sistemas en producción o entornos de pruebas.
- Proponer RFCs a la Gestión de Cambios que aumenten los niveles de seguridad.
- Colaborar con la Gestión de la Continuidad del Servicio para asegurar que no peligra la integridad y confidencialidad de los datos en caso de desastre.
- Establecer las políticas y protocolos de acceso a la información.
- Monitorizar las redes y servicios en red para detectar intrusiones y ataques.

Es necesario que la gestión de la empresa reconozca la autoridad de la Gestión de la Seguridad respecto a todas estas cuestiones y que incluso permita que ésta proponga medidas disciplinarias vinculantes cuando los empleados u otro personal relacionado con la seguridad de los servicios incumplan con sus responsabilidades.

4.3.6.4 Evaluación y mantenimiento

4.3.6.4.1 Evaluación

No es posible mejorar aquello que no se conoce, por lo que resulta indispensable evaluar el cumplimiento de las medidas de seguridad, sus resultados y el cumplimiento de los SLAs.

Aunque no es imprescindible, es recomendable que estas evaluaciones se complementen con auditorías de seguridad externas y/o internas realizadas por personal independiente de la **Gestión de la Seguridad**.

Estas evaluaciones/auditorias deben valorar el rendimiento del proceso y proponer mejoras que se plasmarán en RFCs que habrán de ser evaluados por la Gestión de Cambios.

Independientemente de estas evaluaciones de carácter periódico, se deberán generar informes específicos cada vez que ocurra alguna incidencia grave relacionado con la seguridad. De nuevo, si la Gestión de la Seguridad lo considera oportuno, estos informes se acompañarán de las RFCs correspondientes.

4.3.6.4.2 Mantenimiento

La **Gestión de la Seguridad** es un proceso continuo y se han de mantener al día el Plan de Seguridad y las secciones de seguridad de los SLAs.

Los cambios en el Plan de Seguridad y los SLAs pueden ser resultado de la evaluación arriba citada o de cambios implementados en la infraestructura o servicios TI.

No hay nada más peligroso que la falsa sensación de seguridad que ofrecen medidas de seguridad obsoletas.

Es asimismo importante que la Gestión de la Seguridad esté al día en lo que respecta a nuevos riesgos y vulnerabilidades frente a virus, *spyware*, ataques de denegación de servicio, etcétera, y que adopte las medidas necesarias de actualización de equipos de hardware y software, sin olvidar el apartado de formación: el factor humano es normalmente el eslabón más débil de la cadena.

4.3.6.5 Control y Medición del proceso

Al igual que en el resto de procesos TI, es necesario realizar un riguroso control del proceso para asegurar que la Gestión de la Seguridad cumple sus objetivos.

Una buena **Gestión de la Seguridad** debe traducirse en:

- Disminución del número de incidencias relacionados con la seguridad.
- Un acceso eficiente a la información por el personal autorizado.
- Gestión proactiva, que permita identificar vulnerabilidades potenciales antes de que estas se manifiesten y provoquen una seria degradación de la calidad del servicio.

La correcta elaboración de informes permite evaluar el rendimiento de la Gestión de Seguridad y aporta información de vital importancia a otras áreas de la infraestructura TI.

Entre la documentación generada cabría destacar:

- Informes sobre el cumplimiento, en lo todo lo referente al apartado de seguridad, de los SLAs, OLAs y UCs en vigor.
- Relación de incidencias relacionados con la seguridad, calificados por su impacto sobre la calidad del servicio.
- Evaluación de los programas de formación impartidos y sus resultados.
- Identificación de nuevos peligros y vulnerabilidades a las que se enfrenta la infraestructura TI.
- Auditorías de seguridad.
- Informes sobre el grado de implementación y cumplimiento de los planes de seguridad establecidos.

4.3.7 Gestión de Proveedores

4.3.7.1 Introducción y Objetivos

La ventaja principal de una adecuada **Gestión de Proveedores** radica en que la organización TI obtiene mayores beneficios al contratar a aquellos suministradores que brindan el mejor servicio al menor coste.

Los principales objetivos de la Gestión de Proveedores consisten en:

- Aportar el máximo valor añadido al menor coste en aquellos servicios que prestan los proveedores.
- Asegurar que los contratos y acuerdos con proveedores están alineados con la estrategia y necesidades de negocio de la organización.
- Gestionar la relación con los proveedores.
- Gestionar el rendimiento de los proveedores.
- Negociar los contratos con los proveedores y gestionarlos a lo largo de su ciclo de vida.
- Mantener una política de proveedores y una Base de Datos de Proveedores y Contratos (SCD).

Los principales riesgos a los que se enfrenta la Gestión de Proveedores son:

- La Gestión de la Demanda no proporciona las directrices básicas para racionalizar el gasto, por lo que la Gestión de Proveedores se ve forzada a improvisar los niveles de capacidad a contratar de los suministradores.
- Los contratos en vigor son demasiado vagos y no contemplan objetivos fácilmente cuantificables como horas de trabajo, número de entregables, etc.
- Los contratos son demasiado exigentes en calidad-precio, por lo que las negociaciones con los proveedores se tornan auténticas discusiones bizantinas que acaban alargándose demasiado.
- La Gestión de Proveedores no tiene a su alcance indicadores de rendimiento del servicio o los recibe demasiado tarde, por lo que, si existen retrasos o disminuciones de calidad en el suministro, no podrá actuar con eficacia para corregirlo.

4.3.7.2 Conceptos básicos

A continuación, definimos los conceptos básicos de este proceso:

Cliente: es la empresa u organismo que contrata los servicios TI ofrecidos.

Usuarios: las personas que utilizan el servicio.

Proveedor: es la empresa u organismo que proporciona los servicios solicitados por el cliente.

Base de Datos de Proveedores y Contratos (SCD): La Base de Datos de Proveedores y Contratos (SCD) es un repositorio documental donde se archiva toda la información relacionada con los proveedores y los servicios que prestan, incluyendo por supuesto copias de los contratos (UCs) en vigor. Es aconsejable que la Base de Datos de Proveedores y Contratos esté integrada en el Sistema de Gestión de la Configuración (CMS) y en el Sistema de Gestión del Conocimiento del Servicio (SKMS).

4.3.7.3 Requisitos de contratación

La primera tarea que la **Gestión de Proveedores** debe llevar a cabo es analizar las estrategias generales de la organización y los servicios que se prestan para definir las necesidades de contratación.

Han de tenerse en cuenta, también, los informes económicos proporcionados por la Gestión Financiera, los niveles de calidad acordados con los clientes desde la Gestión de Niveles de Servicio, y la previsión de la capacidad necesaria para desplegar el servicio que haya definido la Gestión de la Demanda.

Por último, se deben estudiar a fondo en el Catálogo de Servicios las condiciones del servicio a prestar y el papel que desempeñarán los proveedores en el proceso.

Una vez recogidos y analizados estos inputs, la Gestión de Proveedores debe preparar:

- Requisitos que se van a exigir a los proveedores.
- Caso de Negocio inicial sobre el que trabajar durante las negociaciones con los proveedores.

Garantizando en todo momento que tanto los requisitos como las premisas básicas de negociación están alineados con la estrategia general de la organización TI.

4.3.7.4 Evaluación y Selección de proveedores

A la hora de elegir un nuevo suministrador han de tenerse en cuenta:

- Su adecuación a los requisitos previamente definidos.
- Referencias de otros competidores.
- Disponibilidad y capacidad.
- Aspectos financieros.

Una vez elegido el proveedor, se han de negociar los términos del servicio. El resultado debe quedar reflejado en el Contrato de Provisión del Servicio (UC), un documento legal que atestigua la relación entre la organización TI y el suministrador.

Es importante que en el UC queden reflejadas las metas y responsabilidades del proveedor de cara al cumplimiento de los SLAs.

4.3.7.5 Clasificación y Documentación de proveedores

Una vez que se han acordado y negociado los servicios de un determinado proveedor, es preciso crear una Base de Datos de Proveedores y Contratos (SCD) donde se recogerá toda la información relacionada:

- Contratos de provisión del servicio (UCs).
- El nivel de actuación del proveedor: Estratégico (directivos), táctico (mandos intermedios), operativo (nivel ejecutor).
- Relaciones con otros elementos del ciclo de vida.

4.3.7.6 Gestión del Rendimiento de los proveedores

A grandes rasgos, se trata de verificar si efectivamente se están cumpliendo los niveles de calidad y disponibilidad acordados en los contratos:

- ¿El suministrador se integra adecuadamente a los procesos de la organización TI?
- ¿Cuál es el procedimiento para informar al proveedor en caso de recibir una incidencia en el Centro de Servicios?
- Si un elemento de configuración relacionado con el proveedor cambia, ¿cuál es el procedimiento por seguir para actualizar el CMS?

4.3.7.7 Renovación o terminación de contratos

Esta actividad consiste en llevar a cabo renovaciones de contratos, asesorar a la dirección acerca de si éstos son relevantes y terminar la relación contractual en caso de que ya no se necesiten más los servicios del proveedor.

Los aspectos que considerar para tomar la decisión de renovar a un proveedor incluyen:

- El buen funcionamiento del contrato y su relevancia de cara al futuro.
- Cambios que es preciso acometer: servicios, productos, contratos, acuerdos, objetivos.
- Perspectivas futuras de la relación con el proveedor: crecimiento, estancamiento, cambio, terminación, transferencia, etc.
- Rendimiento comercial del contrato (criterios de cobro, estructura de precios, etc.)
- Buenas prácticas para la gestión de contratos.
- Administración de proveedores y contratos.

4.3.7.8 Control y Medición del proceso

Algunos indicadores clave que sirven para evaluar el proceso de Gestión de Proveedores:

- Indicadores de que el negocio no se ha visto afectado por el nivel de calidad en los servicios que prestan los proveedores:
    - Incremento en el número de proveedores que alcanzan los objetivos establecidos en el contrato.
    - Reducción del número de incumplimientos de objetivos contractuales.
- Indicadores de que los servicios de apoyo están alineados con las necesidades y objetivos de la organización:
    - Incremento en el número de servicios y revisiones de contrato.
    - Incremento en el número de proveedores y objetivos contractuales alineados con los objetivos contenidos en los SLA y SLR.
- Indicadores de que la disponibilidad de los servicios no se ve comprometida por el rendimiento de los proveedores:
    - Reducción en el número de interrupciones de servicio provocadas por los proveedores.

  - Reducción en el número de amenazas de interrupción de servicio provocadas por proveedores.
- Indicadores de que la organización es consciente de que pueden aparecer problemas en la gestión de proveedores y conoce quién debe ocuparse de ellos:
  - Incremento en el número de proveedores para los que se ha asignado un responsable.
  - Incremento en el número de contratos en los que figura un responsable.

4.4 Puesta en marcha

Los procesos asociados a la fase de Diseño son muy interdependientes entre sí por lo que resulta altamente recomendable su implementación simultánea.

Si por limitaciones presupuestarias o cualquier otra causa esto no fuera posible deberán establecerse prioridades dependientes de los planes existentes de Mejora del Servicio. Por ejemplo, en algunos casos, problemas preexistentes de capacidad pueden determinar que este sea el primer proceso que implementar o simplemente mejorar.

En cualquier caso, la organización TI debe ser consciente de que sin los *inputs* de los otros procesos cualquiera de éstos implementado de forma aislada corre un alto riesgo de fracaso.

Es esencial que todas las actividades desarrolladas en la fase de diseño estén regidas por:

- Los requisitos de los clientes y los SLAs ya en vigor.
- Las necesidades del negocio.
- La continuidad del servicio y la atenuación de riesgos.

Es imprescindible seguir una metodología adecuada en la fase de implementación. El modelo CSI ofrece una guía para ello:

- Disponer de una clara estrategia.
- Saber en qué posición nos encontramos.
- Tener objetivos bien definidos.
- Disponer de un plan de actuación.
- Establecer métricas que permitan evaluar el proceso.
- Disponer de mecanismos de mejora.

4.4.1 RACI

Para que la fase de diseño resulte exitosa es imprescindible organizar adecuadamente todos los procesos y actividades implicados.

El modelo RACI (matriz de asignación de responsabilidades) es un modelo muy útil para la asignación de responsabilidades en la ejecución de actividades o tareas asignadas a un proyecto. RACI es el acrónimo de:

***Responsible* (Encargado)**: persona encargada de hacer la tarea en cuestión.

***Accountable* (Responsable)**: único responsable de la correcta ejecución de la tarea.

Consulted (Consultado): personas que deben ser consultadas para la realización de la tarea.

Informed (Informado): personas que deben ser informadas sobre el progreso de ejecución de la tarea.

En cada tarea debe haber un único R (Encargado) y A (Responsable). Si esto no fuera así la tarea se subdividirá hasta que así sea. Recordemos que estamos hablando de roles, por lo que sería posible, a priori, que una persona fuese, R o A en múltiples tareas.

Una matriz RACI típicamente tiene un eje vertical donde se describen las tareas o entregables en orden cronológico y en el eje horizontal los perfiles o personas implicadas en los mismos.

Un ejemplo de matriz RACI viene dado por:

Ilustración 4-9 Ejemplo de modelo RACI. Actualización de un software

Existen variaciones menores de este modelo que incluyen nuevos roles.

Por ejemplo, en RASCI se incluye:

Support (Soporte): personas encargadas de facilitar el soporte necesario para la realización de la tarea.

4.4.2 Tecnología

Es conveniente disponer de herramientas que faciliten todo el proceso de Diseño del Servicio.

En líneas generales se debe tener en cuenta que todas las herramientas utilizadas deben estar al servicio de los procesos y no al contrario. Es habitual caer en el error de adaptar los procesos a las herramientas en vez de buscar o adaptar las herramientas para que se ajusten a nuestros requisitos, lo que puede empañar los esfuerzos de planificación y definición previos.

A la hora de escoger las herramientas adecuadas puede servir de ayuda el uso de un análisis MoSCoW:

M (*must have*): Funcionalidades esenciales de las que debe disponer la herramienta

S (*should have*): funcionalidades importantes de las que debe disponer la herramienta pero que "pueden esperar" y admiten soluciones temporales.

C (*could have*): funcionalidades adicionales que mejorarían el rendimiento o usabilidad de la herramienta.

W (*will not have it now*): funcionalidades accesorias que sería interesante añadir en el futuro pero que ahora son prescindibles.

Otras variables a tener en cuenta a la hora de hacer una determinada elección incluyen:

- Reputación del proveedor de la herramienta.
- Qué tipo de soporte se ofrece.
- Si el paquete incluye formación para los usuarios.
- Periodicidad y coste de las actualizaciones.
- Plataforma tecnológica.
- Compatibilidad con otras herramientas ya integradas dentro de la organización TI.

4.4.3 Factores de éxito y riesgos

Los principales **retos y riesgos** que afrontar en la implantación de la fase de Diseño del Servicio se resumen en:

- Falta de madurez en la organización para acometer y asimilar los cambios organizativos requeridos.
- Resistencias del personal a adoptar nuevos métodos de trabajo.
- Falta de preparación o pobre comunicación sobre los objetivos buscados.
- Tecnologías de apoyo inadecuadas.
- Desconocimiento de los requisitos de los clientes y las condiciones del mercado.
- Limitaciones presupuestarias.
- Desviaciones respecto a la estrategia predefinida.
- Sistemas ineficaces de monitorización del rendimiento.
- Problemas de sincronización entre todos los agentes implicados.
- Falta de recursos o infrautilización de los mismos.

4.5 Relación con otros ciclos

La **fase de Diseño** recibe sus *inputs* principales de la fase de Estrategia y Mejora del Servicio y a su vez sirve de principal input a las fases de Transición y Operación.

Un correcto diseño debe seguir de cerca las pautas estratégicas preestablecidas y debe a su vez tomar en cuenta las restricciones provenientes de la fase de Transición y especialmente Operación.

La fase de diseño representa la interfaz entre el mundo de las ideas y el mundo real. De nada sirve un servicio conceptualmente bien diseñado si se ignoran restricciones impuestas por la falta de recursos y ausencia de capacidades o si éstas no son correctamente asignadas.

4.5.1 Diseño y Estrategia

El principal *input* ofrecido a la fase de Diseño del Servicio por la fase de Estrategia es un Porfolio de Servicios orientado a cada segmento del mercado.

La estrategia debe aportar al diseño del servicio:

- Modelos de servicio que ofrezcan una guía sobre como aportar valor a los servicios propuestos.
- Información sobre restricciones derivadas de los clientes o política de precios, etcétera.

4.5.2 Diseño y Transición

Para elaborar los planes de cambio y realizar el despliegue del servicio, la fase de transición debe disponer de la siguiente documentación elaborada en los procesos de la fase de Diseño:

- Planes de capacidad
- Planes de disponibilidad
- Paquetes de servicio
- ANS
- Planes de continuidad TI

A su vez la fase de Transición debe asesorar al Diseño sobre los riesgos y posibles impactos del cambio en la calidad del servicio.

4.5.3 Diseño y Operación

La fase de operación es la más crítica y de ella depende la percepción final del cliente sobre la calidad del

servicio.

Por lo tanto, un factor esencial en el diseño del servicio es tener en cuenta la operativa del mismo.

El diseño debe:

- Ser usable.
- Ser sostenible y escalable.
- Ofrecer la funcionalidad requerida.
- Ser eficiente.
- Cumplir los protocolos de seguridad requeridos.
- Permitir el acceso sólo al personal autorizado.

4.5.4 Diseño y Mejora Continua

La fase de mejora del servicio tiene como principal objetivo generar planes de mejora para todos los procesos, actividades y servicios…

La satisfacción de los clientes depende en gran medida de los procesos y actividades desarrolladas en la fase de diseño:

- ¿Resulto la capacidad suficiente?
- ¿Se cumplieron los SLAs?
- ¿Se tuvieron en cuenta los requisitos del cliente?

Si esto no fuera así es necesario introducir planes de mejora que minimicen o eliminen los problemas encontrados y aporten una guía para las mejoras necesarias en las soluciones y arquitecturas empleadas.

5 TRANSICIÓN DEL SERVICIO

El objetivo de la fase de **Transición del Servicio** es conseguir la integración de los productos y servicios definidos en la fase de Diseño del Servicio en el entorno de producción, permitiendo el acceso a los clientes y usuarios autorizados.

Sus principales objetivos se resumen en:

- Supervisar y dar soporte a todo el proceso de cambio del servicio ya sea nuevo éste nuevo o una modificación.
- Asegurar que los nuevos servicios cumplen los requisitos y parámetros de calidad estipulados en las fases de Estrategia y la de Diseño.
- Minimizar los riesgos intrínsecos que conlleva cambio reduciendo el posible impacto sobre los servicios ya existentes.
- Mejorar el nivel de satisfacción del cliente respecto a los servicios prestados.
- Comunicar el cambio a todos los agentes implicados.

Para cumplir correctamente estos objetivos es necesario que durante la fase de Transición del Servicio:

- Se planifique todo el proceso de cambio.
- Se creen los entornos de pruebas y preproducción necesarios.
- Se realicen todas las pruebas necesarias para asegurar la adecuación del nuevo servicio a los requisitos predefinidos.
- Se establezcan planes de *roll-out* (despliegue) y *roll-back* (vuelta a la última versión estable).
- Se cierre el proceso de cambio con una detallada revisión post-implementación.

Como resultado de una adecuada Transición del Servicio:

- Los servicios están mejor alineados con las necesidades de negocio de los clientes.
- La implementación de nuevos servicios es más eficiente.
- Los servicios tienen una mejor respuesta a los cambios del mercado y a los requerimientos de los clientes.
- Se tiene un mayor control de los riesgos y se dispone de planes de contingencia que eviten una degradación prolongada del servicio.
- Se mantienen correctamente actualizadas las bases de datos de configuración y activos del servicio.
- Se dispone de una Base de Conocimiento actualizada a disposición del personal responsable de la operación del servicio y sus usuarios

5.1 Procesos de la fase de Transición

Las principales funciones y procesos asociados directamente a la Fase de Transición del Servicio son:

- **Planificación y soporte a la Transición**: responsable de coordinar y planificar todo el proceso de transición asociado a la creación o modificación de los servicios.
- **Gestión de Cambios**: responsable de aprobar y supervisar la implantación o modificación de los servicios prestados asegurando que todo el proceso ha sido planificado, evaluado, probado, implementado y documentado correctamente.

- **Gestión de la Configuración y Activos del Servicio**: responsable de la gestión y registro de los activos del servicio y de los elementos de configuración (CIs). Este proceso da soporte a prácticamente todos los aspectos de la Gestión del Servicio
- **Gestión de Entregas y Despliegues**: Responsable de desarrollar, hacer pruebas preliminares e implementar las nuevas versiones de los servicios según las directrices marcadas en la fase de Diseño del Servicio.
- **Validación y pruebas**: responsable de asegurar que los servicios cumplen los requisitos preestablecidos antes de su paso al entorno de producción.
- **Evaluación**: responsable de medir o valorar la calidad general de los servicios, su rentabilidad, su grado de utilización, la percepción de sus usuarios, etcétera
- **Gestión del Conocimiento**: gestiona toda la información importante para la prestación de los servicios asegurando que esté disponible para los agentes implicados en su concepción, diseño, desarrollo, implementación y operación.

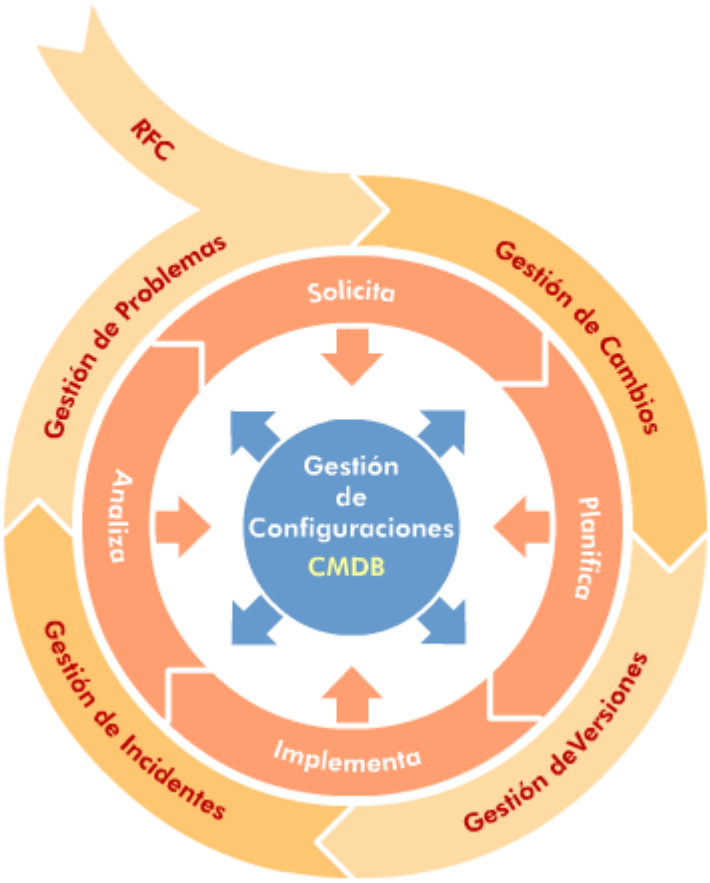


Ilustración 5-1 Procesos Transición del Servicio

5.1.1 Planificación y Soporte a la Transición

5.1.1.1 Introducción y objetivos

El principal cometido de este proceso consiste, como ya hemos esbozado, en coordinar y planificar los recursos necesarios para desplegar una nueva versión del servicio en el tiempo, coste y calidad requeridos en las especificaciones.

Para ello debe asegurarse de que todas las partes implicadas adoptan una metodología de trabajo común, proporcionando un plan de transición capaz de alinear el cambio con las necesidades del cliente.

Una correcta **Planificación de la Transición** trae consigo importantes ventajas que aportan valor al negocio:

- Incrementa la capacidad de la organización para manejar de forma simultánea un gran volumen de cambios y versiones.
- El servicio prestado está mejor alineado con los requisitos del cliente y los proveedores, e incluso con la propia estrategia interna de la organización.
- Al existir un cronograma general del que todos los procesos tienen conocimiento, se minimizan los tiempos muertos y por tanto los retrasos.

Entre las dificultades que pueden obstaculizar la **Planificación de la Transición** encontramos:

- La relación entre los recursos disponibles para prestar el servicio y la calidad exigida en los requisitos está desequilibrada, ocasionando el incumplimiento de plazos o de acuerdos con el cliente.
- La información sobre los elementos de configuración relacionados con el cambio no está actualizada.
- La valoración de la RFC en cuanto a su impacto y los recursos que precisará es incompleta o errónea.
- Los SACs no están alineados con los requisitos de diseño.
- Los elementos de configuración que intervienen en el cambio no están preparados llegado el momento, ocasionando retrasos en la planificación.
- Se monitoriza cada uno de los pasos de la transición, pero a menos que el cliente lo reclame no se hace una reflexión final sobre el rendimiento, la adecuación a los requisitos planteados inicialmente, etc.

5.1.1.2 Conceptos básicos

A continuación, definimos los conceptos básicos de este proceso

Petición de Cambio (RFC): Una Petición de Cambio o RFC es una petición formal para efectuar modificaciones en uno o más CIs.

Revisión Post-Implantación (PIR): La Revisión Post-Implantación o PIR es una fase de soporte posterior a la implementación de los cambios en la que la **Planificación y Soporte a la Transición** asesora a todas las partes implicadas. Estas labores de soporte consisten principalmente en informar sobre los procesos, sistemas y herramientas de apoyo a la Transición del Servicio.

5.1.1.3 Estrategia de transición

En primer lugar, la organización debe definir la **estrategia de transición** para llevar a cabo los cambios previstos en el servicio nuevo o a modificar.

Los puntos clave que debe contemplar dicha estrategia incluyen:

- Propósito, objetivos y metas.
- Contexto de prestación del servicio.
- Requisitos externos que deban tenerse en cuenta (estándares, legislación vigente, acuerdos contractuales, etc.). Requisitos particulares del servicio.
- Organizaciones y terceros interesados (socios estratégicos, proveedores, etc.)
- Marco de trabajo a adoptar (políticas, protocolos de autorización, etc.)
- Roles y responsabilidades. Requisitos de formación de la plantilla involucrada.
- Planificación de hitos y entregables. Frecuencia de entrega.
- Convenios de nomenclatura que se han adoptado para denominar las entregas (p. ej. “versión 1.1.3.65”)
- Criterios de evaluación y de aceptación de las RFCs.

- Criterios para dar por concluido el soporte post-implantación (ELS).

Las entregas pueden clasificarse de forma general en los siguientes tipos:

- **Entrega mayor**: Se consideran de esta clase los despliegues que incluyan la instalación de nuevo hardware y software, ya que suelen implicar un aumento de las funcionalidades.
- **Entrega menor**: Suelen consistir en paquetes de pequeñas mejoras, a menudo correspondientes a soluciones provisionales a problemas concretos.
- **Entrega de emergencia**: Se implementan de manera individual para resolver errores conocidos o problemas que no pueden esperar.

5.1.1.4 Preparación de la transición

La preparación consiste en una revisión general de toda la información recabada, así como de los elementos (recursos materiales, personal interno, proveedores, etc.) que intervendrán en la ejecución de los cambios.

- Revisión y aceptación de los inputs procedentes del resto de procesos del Ciclo de Vida.
- Revisión y comprobación del paquete de diseño del servicio (SDP) creado en la fase de Diseño.
- Revisión de los SACs.
- Identificación, desarrollo y planificación de las peticiones de cambio (RFCs).
- Comprobación de que la Gestión de la Configuración está actualizada.
- Comprobación de que la Transición está preparada para llevarse a cabo.

5.1.1.5 Planificación de la transición

Esta es la actividad principal del proceso, y consiste en la descripción pormenorizada del flujo de trabajo que hará posible la puesta en marcha del cambio. El plan ha de ser específico para cada nueva transición, ya que deben tomarse en cuenta aspectos concretos del servicio como el volumen de elementos de configuración (CIs) implicados en la prestación del mismo, los requisitos específicos acordados con el cliente, etc.

El desarrollo y despliegue de cada transición debe ser compartimentado en distintas etapas:

- Adquisición y evaluación de los CIs y otros componentes.
- Desarrollo de la entrega y evaluación preliminar.
- Validación y pruebas de la entrega.
- Comprobación de que el servicio está preparado para pasar a la fase de Operación.
- Despliegue de la nueva versión.
- Soporte post-implementación.
- Revisión y cierre de la transición.

Para cada una de estas etapas deben definirse los siguientes aspectos:

- Descripción de tareas y actividades.
- Recursos específicos asignados a cada tarea.
- Criterios de aceptación o SACs para determinar si se puede pasar a la siguiente etapa.
- Incidencias que pueden presentarse y riesgos asociados.
- Plazos previstos para cada fase.

Una buena **Planificación y Soporte a la Transición** tenderá a agrupar varias entregas y despliegues en una programación global, de tal manera que cada despliegue significativo será gestionado como un proyecto

aparte.

Por último, debe hacerse una revisión exhaustiva de los planes estratégicos una vez terminados.

5.1.1.6 Control y medición del proceso

El propietario de este proceso es el Jefe de Proyecto (*Project Manager*). En él recae la responsabilidad de controlar y medir los siguientes indicadores:

- **Número de proyectos gestionados**. Es decir, el número de versiones desplegadas (*rollout*) que han sido objeto de planificación y soporte.
- **Porcentaje de entregas** (respecto al total de entregables) que se ajustaron a lo acordado con el cliente en cuanto a coste, calidad y alcance.
- **Ajuste al presupuesto** del proyecto, comparando el consumo de recursos humanos y financieros previstos con los que se usaron realmente.
- **Retrasos** en proyectos, comparando las fechas de entrega reales con las que en un principio se habían definido en la planificación.

5.1.2 Gestión de Cambios

5.1.2.1 Introducción y Objetivos

El objetivo primordial de la **Gestión de Cambios** es que se realicen e implementen adecuadamente todos los cambios necesarios en la infraestructura y servicios TI garantizando el seguimiento de procedimientos estándar.

La **Gestión de Cambios** debe trabajar para asegurar que los cambios:

- Están justificados.
- Se llevan a cabo sin perjuicio de la calidad del servicio TI.
- Están convenientemente registrados, clasificados y documentados.
- Han sido cuidadosamente testeados en un entorno de prueba.
- Se ven reflejados en la CMDB.
- Pueden deshacerse mediante planes de *back-outs* (retirada del cambio) en caso de un incorrecto funcionamiento tras su implementación.

Las actividades principales de la **Gestión de Cambios** se resumen en el siguiente diagrama:

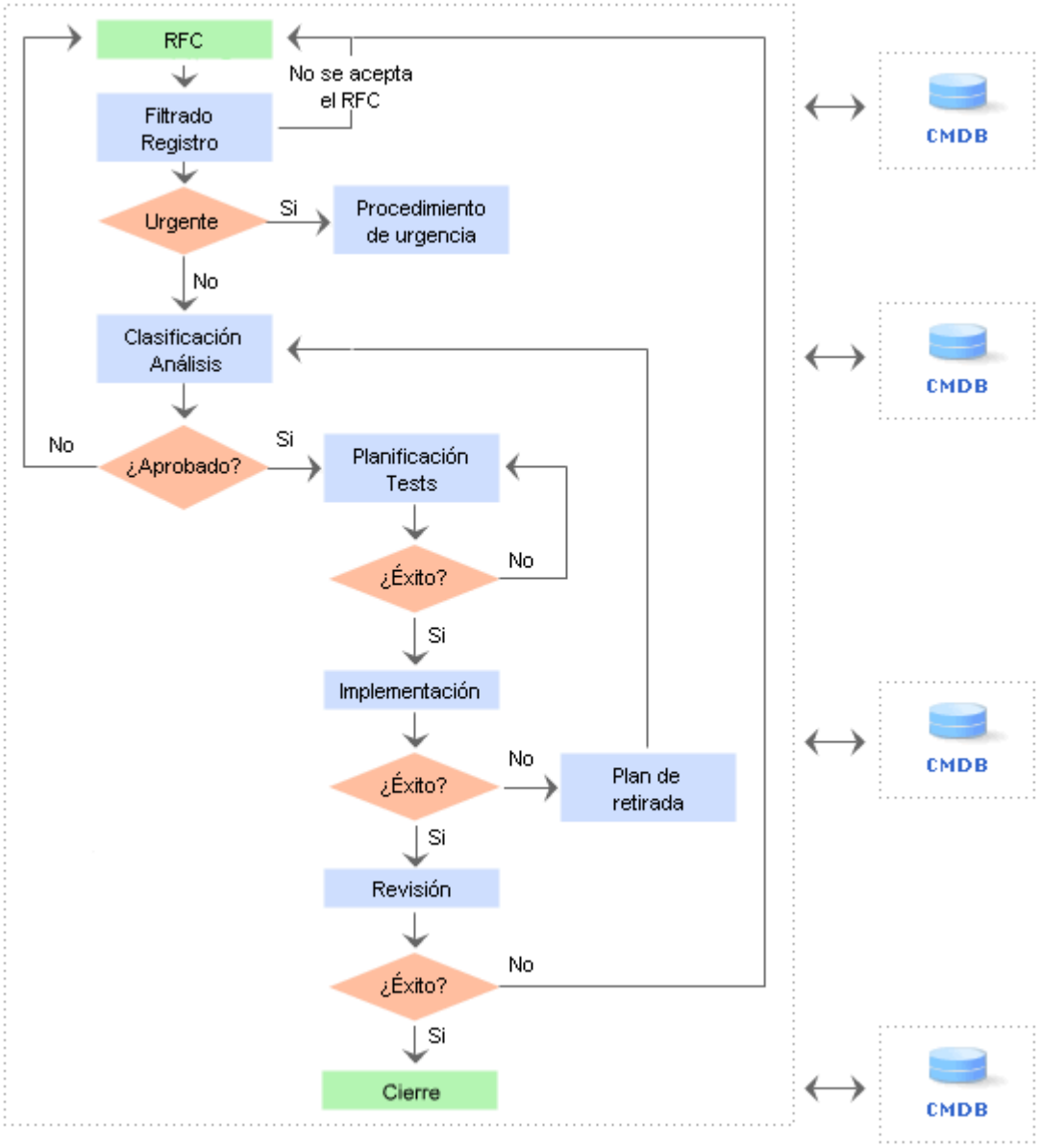


Ilustración 5-2 Actividades Gestión del Cambio

Los principales beneficios derivados de una correcta gestión del cambio son:

- Se reduce el número de incidencias y problemas potencialmente asociados a todo cambio.
- Se puede retornar a configuraciones estables de manera sencilla y rápida en caso de que el cambio tenga un impacto negativo en la estructura TI.
- Se reduce el número de back-outs necesarios.
- Los cambios son mejor aceptados y se evitan "tendencias inmovilistas".
- Se evalúan los costes reales asociados al cambio, y por lo tanto es más sencillo valorar el retorno real a la inversión.
- La CMDB está correctamente actualizada, algo indispensable para la correcta gestión del resto de procesos.
- Se desarrollan procedimientos de cambio estándar que permiten la rápida actualización de sistemas no críticos.

La implantación de una correcta política de gestión de cambios también se encuentra con algunas serias dificultades:

- Los diferentes departamentos deben aceptar la autoridad de la **Gestión de Cambios** sobre todo en lo que respecta al cambio, independientemente de que el motivo de su realización sea solucionar un problema, mejorar un servicio o adaptarse a requisitos legales.
- No se siguen los procedimientos establecidos y, en particular, no se actualiza correctamente la información sobre los CIs en la CMDB.
- Los encargados de la **Gestión de Cambios** no conocen a fondo las actividades, servicios, necesidades y estructura TI de la organización, lo que les incapacita para desarrollar correctamente su actividad.
- Los Gestores del Cambio no disponen de las herramientas de software adecuadas para monitorizar y documentar el proceso de forma apropiada.
- No existe el compromiso suficiente de la dirección por implementar rigurosamente los procesos asociados.
- Se adoptan procedimientos excesivamente restrictivos que dificultan la mejora o, por el contrario, el proceso de cambio se trivializa, provocando una falta de estabilidad que empobrece la calidad del servicio.

5.1.2.2 Conceptos básicos

Unos conceptos que se utilizarán con frecuencia en el resto de apartados de la fase de Transición del Servicio son el de Gestor de Cambios y el de Comité Asesor del Cambio (CAB), por lo que resulta conveniente describir y diferenciar sus respectivas atribuciones:

Gestor de Cambios: es el responsable del proceso y, por tanto, debe ser también el último responsable de todas las tareas asignadas a la **Gestión de Cambios**. En grandes organizaciones, el Gestor de Cambios puede apoyarse en una serie de asesores especialistas en determinadas áreas.

Comité Asesor del Cambio (CAB): es un órgano interno, presidido por el **Gestor de Cambios**, formado principalmente por representantes de las principales áreas de la gestión de servicios TI. Sin embargo, en algunos casos también puede incorporar:

- Consultores externos.
- Representantes de los colectivos de usuarios.
- Representantes de los principales proveedores de software y hardware.

Modelos de Cambio: es una serie de grupos de cambios que han sido previamente clasificados, analizados y autorizados, de tal manera que se predefinen ciertos mecanismos y actividades a realizar para cada grupo. De esta manera se alcanza un control más efectivo y una implementación mucho más ágil de las RFCs.

5.1.2.3 Alcance de la Gestión de Cambios

En principio, todo cambio no estándar debería ser tarea de la **Gestión de Cambios**. Sin embargo, a veces es inviable gestionar todos los cambios mediante ésta.

El alcance de la **Gestión de Cambios** debe ir en paralelo con el de la Gestión de la Configuración y Activos TI: todos los cambios de CIs inventariados en la CMDB deben ser correctamente registrados y supervisados.

Al igual que a la hora de implementar la **Gestión de la Configuración y Activos TI**, se sugirió la creación de "configuraciones de referencia" (por ejemplo, un PC de referencia con todos sus componentes hardware y software predefinidos) para simplificar el proceso, para la Gestión de Cambios es importante crear procesos de cambio cuyos protocolos estén previamente definidos y autorizados para, por ejemplo, realizar los cambios asociados a las configuraciones de referencia antes citadas.

Estos protocolos de cambio estándar deben ser cuidadosamente elaborados, pero una vez definidos permiten una gestión más rápida y eficiente de cambios menores o de bajo impacto en la organización TI.

5.1.2.3.1 Registro de peticiones

El primer paso del proceso de cambio es registrar adecuadamente las RFCs.

El origen de una RFC puede ser de muy distinta índole:

- **Gestión de Problemas:** se encarga de proponer soluciones a errores conocidos. En la mayoría de los casos, esta solución conlleva un cambio en la infraestructura TI. En este caso, la RFC debe ser registrada con información del error conocido asociado para que posteriormente pueda ser evaluado si procede o no realizar el cambio.
- **Nuevos Servicios**: el desarrollo de nuevos servicios normalmente necesita cambios en la infraestructura TI. Para asegurar que estos cambios cumplen las expectativas previstas y no deterioran la calidad de los otros servicios prestados es importante coordinar todo el proceso con las Gestiones de Capacidad, Disponibilidad y Niveles de Servicio.
- **Estrategia empresarial**: la dirección de la organización puede decidir una reorientación estratégica que puede afectar, por ejemplo, a los niveles de servicio ofrecidos o a la implantación de un nuevo CRM, etc. y que por regla general necesita cambios en el hardware, software y/o procedimientos.
- **Actualizaciones de software de terceros**: los proveedores pueden dejar de soportar versiones anteriores de paquetes de software o introducir nuevas versiones con grandes mejoras que recomienden la actualización.
- **Imperativo legal**: un cambio en la legislación (como, por ejemplo, la LOPD) puede exigir cambios en la infraestructura TI.
- **Sugerencias:** en principio cualquier cliente, empleado o proveedor puede sugerir mejoras en los servicios que pueden requerir cambios en la infraestructura.

No siempre un cambio implica una RFC. Para cambios de escaso impacto o que se repiten de forma periódica pueden acordarse procedimientos estándar que no requieran la aprobación de la **Gestión de Cambios** para cada caso.

Independientemente de su origen, el adecuado registro inicial de una RFC requerirá, cuando menos, de los siguientes datos:

- Fecha de recepción.
- Identificador único de la RFC.
- Identificador del error conocido asociado (dado el caso).
- Descripción del cambio propuesto:
    - Motivación.
    - Propósito.
    - CIs afectados.
    - Estimación de recursos necesarios para la implementación.
    - Tiempo estimado.
- Estado: que inicialmente será el de "registrado".

Este registro deberá ser actualizado con toda la información generada durante el proceso para permitir un detallado seguimiento del mismo desde su aprobación hasta la evaluación final y cierre.

La información de registro debe ser actualizada durante todo el proceso y debe incluir al menos:

- Estado actualizado: "aceptado", "rechazado", "implementado", etc.
- Fecha de aceptación (denegación) de la RFC.
- Evaluación preliminar de la Gestión del Cambio.

- Prioridad y categoría.
- Planes de *back-out*.
- Recursos asignados.
- Fecha de implementación.
- Plan de implementación.
- Cronograma.
- Revisión post-implementación.
- Evaluación final.
- Fecha de cierre.

5.1.2.4 Aceptación y Clasificación del cambio

5.1.2.4.1 Aceptación

Tras el registro de la RFC se debe evaluar preliminarmente su pertinencia. Una RFC puede ser simplemente rechazada si se considera que el cambio no está justificado o se puede solicitar su modificación si se considera que algunos aspectos de la misma son susceptibles de mejora o mayor definición. En los casos de rechazo la RFC debe ser enviada al departamento o persona solicitante para dar así la oportunidad de realizar nuevas alegaciones a favor de dicha RFC o modificarla.

La aceptación del cambio no implica su posterior aprobación por el CAB y es sólo indicación de que se ha encontrado justificado su posterior procesamiento.

5.1.2.4.2 Clasificación

Tras su aceptación se debe asignar a la RFC una categoría y prioridad dependiendo del impacto y la urgencia de la misma.

La categoría indica la dificultad e impacto de la RFC y será el parámetro principal para determinar la asignación de recursos, los plazos previstos y el nivel de autorización necesario para la implantación del cambio.

La prioridad determinará la importancia relativa de esta RFC respecto a otras RFCs pendientes y será el dato relevante para establecer una planificación en el tiempo de los cambios a realizar.

La determinación de la categoría se basa en el impacto sobre la organización y el esfuerzo requerido para su implementación. Las posibles categorías abarcarían desde cambios que apenas requieren la participación del personal TI y que apenas suponen alguna modificación en la calidad del servicio hasta cambios que necesiten grandes recursos y requieran de la aprobación directa de la Dirección.

Aunque se pueda definir un rango de prioridades tan amplio cómo se desee, se debería considerar una clasificación que incluyera, al menos, los siguientes niveles de prioridad:

- **Baja**: puede ser conveniente realizar este cambio junto a otros cuando, por ejemplo, se instale nuevo hardware, se actualice cierto software, se implemente un cambio de tecnología, etc.
- **Normal**: Es conveniente realizar el cambio, pero siempre que ello no interfiera con algún otro cambio de más alta prioridad. A su vez, los cambios de esta categoría se pueden dividir en menores, significativos y mayores.
- **Alta**: un cambio que debe realizarse sin demora, pues está asociado a errores conocidos que deterioran apreciablemente la calidad del servicio. El CAB debe evaluar este cambio en su próxima reunión y adoptar las medidas pertinentes que permitan una pronta solución.
- **Urgente**: es necesario resolver un problema que está provocando una interrupción o degradación grave del servicio. Un cambio de prioridad urgente desencadena un proceso denominado cambio de emergencia que trataremos posteriormente de forma independiente. Los cambios de esta categoría

pueden clasificarse a su vez en normales y de emergencia.

Los cambios menores pueden no necesitar la aprobación del CAB y ser implementados directamente. Cualquier otro cambio habrá de ser tratado en el CAB con la ayuda de personal especializado para realizar tareas de asesoramiento.

5.1.2.5 Aprobación y Planificación del cambio

La **planificación** es esencial para una buena gestión del cambio.

Los sistemas de gestión de la información son muy sensibles a los cambios de configuración por las complejas relaciones entre todos los CIs involucrados. Esto hace que un cambio qué en apariencia es menor puede provocar una reacción en cadena con resultados catastróficos. Es indispensable, como mínimo, disponer siempre de planes de *back-out* que permitan volver a la última configuración estable antes del cambio. Pero esto obviamente no es suficiente.

En primer lugar, el CAB debe celebrar reuniones periódicas para analizar y aprobar si procede, las RFCs pendientes y elaborar el FSC o calendario del cambio correspondiente.

Para su aprobación, el **cambio** se debe evaluar minuciosamente:

- Los beneficios esperados del cambio propuesto.
- La relación beneficio/coste del cambio.
- Los riesgos asociados al cambio.
- La disponibilidad de los recursos necesarios para llevar a cabo el cambio con garantías de éxito.
- La posibilidad de aplazar el cambio.
- El impacto general sobre la infraestructura y la calidad de los servicios.
- El posible impacto sobre los niveles establecidos de seguridad TI.

En el caso de cambios que tengan un alto impacto, debe también consultarse a la **dirección** pues pueden entrar en consideración aspectos de carácter económico, estratégico y de política general de la organización.

Una vez aprobado el cambio (en caso contrario se seguiría el proceso ya descrito para el caso de no aceptación) debe evaluarse si éste ha de ser implementado aisladamente o dentro de un "paquete de cambios", que formalmente equivaldrían a un solo cambio. Esto tiene algunas ventajas:

- Se optimizan los recursos necesarios.
- Se evitan posibles incompatibilidades entre diferentes cambios.
- Sólo se necesita un plan de *back-out*.
- Se simplifica el proceso de actualización de la CMDB y la PIR.

5.1.2.6 Implementación del cambio

Aunque la **Gestión de Cambios** no es la encargada de implementar el cambio, algo de lo que se encarga habitualmente la Gestión de Entregas y Despliegues, sí lo es de supervisar y coordinar todo el proceso.

En la fase de desarrollo del cambio se deberá monitorizar el proceso para asegurar que:

- Tanto el software desarrollado como el hardware adquirido se ajustan a las especificaciones predeterminadas.
- Se cumplen los calendarios previstos y la asignación de recursos es la adecuada.
- El entorno de pruebas es realista y simula adecuadamente el entorno de producción.
- Los planes de *back-out* permitirán la rápida recuperación de la última configuración estable.

Si es posible, debe permitirse el acceso restringido de usuarios al entorno de pruebas para que realicen una

valoración preliminar de los nuevos sistemas en lo que respecta a su:

- Funcionalidad.
- Usabilidad.
- Accesibilidad.

La opinión de los usuarios debe ser tomada en cuenta y la RFC debe ser revisada en caso de que se encuentren objeciones justificadas al cambio (debe tenerse en cuenta la resistencia habitual al cambio por parte de cierto tipo de usuarios).

Tanto clientes cómo proveedores no deben percibir el cambio como algo improvisado o inesperado. Es función tanto de la **Gestión de Cambios** como del Centro de Servicios mantener siempre informados a los usuarios de los futuros cambios y, en la medida de lo posible, hacerles partícipes del mismo:

- Escuchando sus sugerencias.
- Informando las ventajas asociadas.
- Aclarando sus dudas y dando soporte cuando sea necesario: los usuarios deben percibir la mejora producida por el cambio.

5.1.2.7 Evaluación del cambio

Antes de proceder al cierre del cambio, es necesario verificar que ha sido positivo para el servicio, ya sea porque se ha incrementado el nivel de calidad se ha visto aumentado o porque ha contribuido a mejorar la productividad de la organización. Aunque la Gestión de Cambios es la encargada de emitir el dictamen final, es la **Evaluación** del servicio la que ha de proporcionar a ésta los informes.

Los aspectos fundamentales a tener en cuenta son:

- Cumplimiento de los objetivos previstos.
- Desviación del proceso de las previsiones realizadas por la **Gestión de Cambios**.
- Aparición de problemas o interrupciones del servicio imprevistas provocados por el cambio.
- Percepción de los usuarios respecto al cambio.
- Puesta en marcha los planes de *back-out* en alguna fase del proceso y las causas de esa puesta en marcha.

Si la evaluación final determina que el proceso y los resultados han sido satisfactorios, se procederá al cierre de la RFC y toda la información se incluirá en la PIR asociada.

5.1.2.8 Cambios de emergencia

Se puede inferir que los cambios producidos mediante procedimientos de emergencia son resultado de una planificación deficiente. Desgraciadamente, a veces, por muy bien que se planifique, es inevitable realizar este tipo de cambios.

Cualquier interrupción del servicio de alto impacto, ya sea por el número de usuarios afectados o porque se han visto afectados servicios o sistemas críticos para la organización, debe encontrar una respuesta inmediata. Es frecuente que la solución al problema requiera un cambio y que éste haya de realizarse siguiendo un procedimiento de urgencia.

El procedimiento por seguir en estos casos debe estar debidamente previsto. Por ejemplo, se deben establecer protocolos de validación de los cambios urgentes que pueden requerir:

- La reunión urgente del CAB si esto fuera posible.
- En ciertos casos en los que el número de integrantes o sus circunstancias hagan de ello algo inviable, puede ser necesario constituir un equipo específico, más reducido, que se denomina CAB de Emergencia (ECAB).

- Una decisión del Gestor del Cambio no es posible aplazar la resolución del problema o éste sucede cuando los miembros del CAB o ECAB no están disponibles (fin de semana, periodo vacacional).

Como lo más prioritarios en estos casos es restaurar el servicio, es a menudo frecuente que los procesos asociados sigan un orden inverso al usual: tanto los registros en la CMDB como la documentación asociada al cambio podrían realizarse a posteriori.

Sin embargo, es muy importante que al cierre del cambio de emergencia se disponga de la misma información de la que dispondríamos tras un cambio normal. Si esto no fuera así, en el futuro se podrían generar nuevas incidencias o problemas al realizar cambios qué no son compatibles con el cambio de emergencia no documentado.

5.1.2.9 Control y Medición del proceso

Es imprescindible elaborar informes que permitan evaluar el rendimiento de la **Gestión de Cambios**.

Para que estos informes ofrezcan una información precisa y de fácil valoración, es imprescindible crear métricas de referencia que cubran aspectos tales como:

- RFCs solicitados.
- Porcentaje de RFCs aceptados y aprobados.
- Número de cambios realizados clasificados por impacto y prioridad y filtrados temporalmente.
- Tiempo medio del cambio dependiendo del impacto y la prioridad.
- Número de cambios de emergencia realizados.
- Porcentaje de cambios exitosos en primera instancia, segunda instancia, etc.
- Numero de *back-outs* con una detallada explicación de los mismos.
- Evaluaciones post-implementación.
- Porcentajes de cambios cerrados sin incidencias ulteriores.
- Incidencias asociadas a cambios realizados.
- Número de reuniones del CAB con información estadística asociada: número de asistentes, duración, nº de cambios aprobados por reunión, etc.

5.1.3 Gestión de la Configuración y Activos del Servicio

5.1.3.1 Introducción y Objetivos

Es esencial conocer en detalle la infraestructura TI de nuestras organizaciones para obtener el mayor provecho de la misma. La principal tarea de la **Gestión de la Configuración y Activos TI** es llevar un registro actualizado de todos los elementos de configuración de la infraestructura TI, junto con sus interrelaciones.

Esto no es una labor sencilla y requiere la colaboración de los Gestores de los otros procesos, en particular, de la Gestión de Cambios y la de Entregables y Despliegues.

Los objetivos principales de la Gestión de la Configuración y Activos TI se resumen en:

- Proporcionar información precisa y fiable al resto de la organización de todos los elementos que configuran la infraestructura TI.
- Mantener actualizada la **Base de Datos de Gestión de Configuración y Activos TI**:
    - Registro actualizado de todos los CIs: identificación, tipo, ubicación, estado...
    - Interrelación entre los CIs.
    - Servicios que ofrecen los diferentes CIs.
- Servir de apoyo a los otros procesos, en particular, a la Gestión de Incidencias, Problemas y Cambios.

Los beneficios de una correcta Gestión de la Configuración y Activos TI incluyen, entre otros:

- Resolución más rápida de los problemas, que redunda en una mayor calidad de servicio. Una fuente habitual de problemas es la incompatibilidad entre diferentes CIs, drivers desactualizados, etc. La detección de estos errores sin una CMDB actualizada alarga considerablemente el ciclo de vida de un problema.
- Una Gestión de Cambios más eficiente. Es imprescindible conocer la estructura previa para diseñar un cambio que no genere nuevas incompatibilidades y/o problemas.
- Reducción de costes: El conocimiento detallado de todos los elementos de configuración permite, por ejemplo, eliminar duplicidades innecesarias.
- Control de licencias. Se pueden identificar copias ilegales de software que pueden suponer tanto peligros para la infraestructura TI en forma de virus, etc. como incumplimientos de los requisitos legales que pueden tener una repercusión negativa en la organización.
- Mayores niveles de seguridad. Una CMDB actualizada permite, por ejemplo, detectar vulnerabilidades en la infraestructura.
- Mayor rapidez en la restauración del servicio. Si se conocen todos los elementos de configuración y sus interrelaciones será mucho más sencillo recuperar la configuración de producción en el tiempo más breve posible.

Las principales dificultades con las que topa la Gestión de la Configuración y Activos TI son:

- Una incorrecta planificación: es esencial programar correctamente las actividades necesarias para evitar duplicaciones o incorrecciones.
- Estructura inadecuada de la CMDB: mantener actualizada una Base de Datos de Gestión de Configuración y Activos TI excesivamente detallada y completa puede ser una tarea engorrosa y que consuma demasiados recursos.
- Herramientas inadecuadas: es necesario disponer del software adecuado para agilizar los procesos de registro y sacar el máximo provecho de la CMDB.
- Falta de Coordinación con la Gestión de Cambios y la de Entregables y Despliegues, que imposibilita el correcto mantenimiento de la CMDB.
- Falta de organización: es importante que haya una correcta asignación de recursos y responsabilidades. Es preferible, cuando sea posible, que la Gestión de la Configuración y Activos TI sea llevada a cabo por personal independiente y especializado.
- Falta de compromiso: los beneficios de la Gestión de la Configuración y Activos TI no son inmediatos y son casi siempre indirectos, lo que puede provocar el desinterés de la gestión de la empresa y, consecuentemente, de los agentes implicados.

5.1.3.2 **Conceptos básicos**

A lo largo de la descripción de la Fase de Transición del servicio hemos utilizado y utilizaremos con profusión conceptos tales como elementos de configuración (CI) y base de datos de Gestión de la Configuración y Activos TI (CMDB) es por lo tanto conveniente que nos detengamos para dar una definición precisa de ambos.

- **Elementos de configuración (CI)**: todos, tanto los componentes de los servicios TI como los servicios que éstos nos ofrecen, constituyen diferentes elementos de configuración. A modo de ejemplo citaremos:
    - Dispositivos de hardware como PCs, impresoras, routers, monitores, etc. así como sus componentes: tarjetas de red, teclados, lectores de CDs, etc.
    - Software: sistemas operativos, aplicaciones, protocolos de red, etc.
    - Documentación: manuales, acuerdos de niveles de servicio, etc.

- **Base de Datos de la Gestión de la Configuración y Activos TI (CMDB):** La CMDB no se limita a una mera enumeración del stock de piezas, sino que nos brinda una imagen global de la infraestructura TI de la organización. Esta base de datos debe incluir:
    - Información detallada de cada elemento de configuración.
    - Interrelaciones entre los diferentes elementos de configuración, como, por ejemplo, relaciones "padre-hijo" o interdependencias tanto lógicas como físicas.
- **Sistema de Gestión de la Configuración (CMS):** es un sistema de apoyo diseñado para infraestructuras de servicios TI de gran complejidad

5.1.3.3 Planificación de la configuración

La **Gestión de la Configuración y Activos TI** es uno de los pilares de la metodología ITIL por sus interrelaciones e interdependencias con el resto de procesos. Por ello, su implantación es particularmente compleja.

Aunque ofrecer un detallado plan de implementación de la Gestión de la Configuración y Activos TI va mucho más allá de lo que aquí podemos ofrecer, creemos conveniente, al menos, destacar algunos puntos que consideramos esenciales:

- Designar un responsable: una descentralización excesiva puede generar descoordinación y llevar al traste todo el proceso.
- Invertir en alguna herramienta de software adecuada a las actividades requeridas: una organización manual es impracticable.
- Realizar un cuidadoso análisis de los recursos ya existentes: gestión de stocks, activos, etc.
- Establecer claramente:
    - El alcance y objetivos.
    - El nivel de detalle.
    - El proceso de implementación: orden de importancia, cronograma...
- Coordinar el proceso estrechamente con la Gestión de Cambios, Gestión de Entregas y Despliegues y los Departamentos de Compras y Suministros.

Una falta de planificación conducirá con total certeza a una **Gestión de la Configuración y Activos TI** defectuosa con las graves consecuencias que esto supondrá para el resto de los procesos.

5.1.3.4 Clasificación y Registro de CIs

La principal tarea de la **Gestión de la Configuración y Activos TI** es mantener la CMDB. Es imprescindible, para llevar a cabo esta labor con éxito, predeterminar la estructura del CMDB de manera que:

- Los objetivos sean realistas: una excesiva profundidad o detalle puede sobrecargar de trabajo a la organización y resultar, a la larga, en una dejación de responsabilidades.
- La información sea suficiente: debe existir, al menos, un registro de todos los sistemas críticos para la infraestructura TI.

5.1.3.4.1 Alcance

En primer lugar, habremos de determinar qué sistemas y componentes TI van a ser incluidos en la CMDB:

- Es esencial incluir al menos todos los sistemas de hardware y software implicados en los >servicios críticos.
- Se debe determinar qué CIs deben incluirse dependiendo del estado de su ciclo de vida. Por ejemplo, pueden obviarse componentes que ya han sido retirados.
- Es recomendable incorporar, al menos, la documentación asociada a proyectos, SLAs y licencias.

En general, cualquier servicio o proceso es susceptible de ser incluido en la CMDB, pero unos objetivos en exceso ambiciosos pueden resultar contraproducentes.

5.1.3.4.2 Nivel de detalle y Profundidad

Una vez determinado el alcance de la CMDB, es imprescindible establecer el nivel de detalle y profundidad deseados:

- Determinar los atributos que describen a un determinado CI.
- Tipo de relaciones lógicas y físicas registradas entre los diferentes CIs.
- Subcomponentes registrados independientemente.

Por ejemplo, si se decide incluir Servidores en la CMDB:

- Atributos: Fabricante, CPU, sistema operativo, etc.
- Relaciones: conexiones de red, aplicaciones alojadas, etc.
- Profundidad: Memoria RAM, discos duros, tarjetas gráficas, etc.

5.1.3.4.3 Nomenclatura

Aunque este sea un aspecto muy técnico, es de vital importancia predefinir los códigos de clasificación de los CIs para que el sistema sea funcional:

- La identificación debe ser, por supuesto, única y si es posible interpretable por los usuarios.
- Este código debe ser utilizado en todas las comunicaciones referentes a cada CI y si es posible debe ir físicamente unido al mismo (mediante una etiqueta de difícil eliminación).
- Los códigos no deben ser sólo utilizados para componentes de hardware sino también para documentación y software.

5.1.3.5 **Monitorización**

Es imprescindible conocer el estado de cada componente en todo momento de su ciclo de vida. Esta información puede ser de gran utilidad, por ejemplo, a la Gestión de la Disponibilidad para conocer qué CIs han sido responsables de la degradación de la calidad del servicio.

Puede representar una ayuda para el análisis el uso de herramientas de software que ofrezcan representaciones visuales del ciclo de vida de los componentes, organizados por diferentes filtros (tipo, fabricante, responsable, costes, etc.).

Por ejemplo, puede resultar interesante para la Gestión Financiera la monitorización del ciclo de vida de, digamos, los switches instalados a la hora de adoptar decisiones de compra de nuevo material:

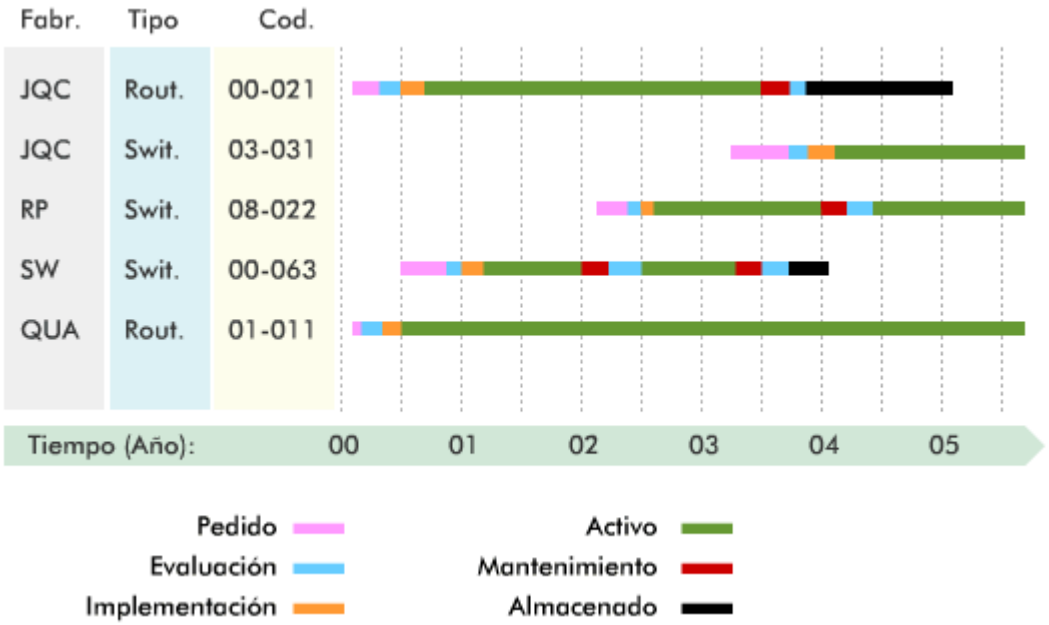


Ilustración 5-3 Ejemplo de monitorización

5.1.3.6 Control de CIs

La **Gestión de la Configuración y Activos TI** debe estar puntualmente informada de todos los cambios y adquisiciones de componentes para mantener actualizada la CMDB.

El registro de todas las componentes de hardware debe iniciarse desde la aprobación de su compra y debe mantenerse actualizado su estado en todo momento de su ciclo de vida. Asimismo, debe estar correctamente registrado todo el software "en producción".

Las tareas de control deben centrarse en:

- Asegurar que todos los componentes están registrados en la CMDB.
- Monitorizar el estado de todos los componentes.
- Actualizar las interrelaciones entre los CIs.
- Informar sobre el estado de las licencias.

5.1.3.7 Auditorías

El objetivo de las auditorías es asegurar que la información registrada en la CMDB coincide con la configuración real de la estructura TI de la organización.

Existen herramientas que permiten una gestión remota, centralizada y automática de los elementos de configuración de hardware y software. La información recopilada puede ser utilizada para actualizar la CMDB.

Si el alcance de la CMDB incluye aspectos como documentación, SLAs, personal, etc. es necesario complementar estos datos con auditorías manuales. Éstas deben realizarse con cierta frecuencia y al menos:

- Tras la implementación de una nueva CMDB.
- Antes y después de cambios mayores en la infraestructura.
- Si existen fundadas sospechas de que la información almacenada en la CMDB es incorrecta o incompleta.

Las auditorías deben dedicar especial atención a aspectos tales como:

- Uso correcto de la nomenclatura en los registros de los CIs.

- Comunicación con la Gestión de Cambios: información sobre RFCs, cambios realizados, etc.
- Estado de los CIs actualizado.
- Cumplimiento de los niveles de alcance y detalle predeterminados.
- Adecuación de la estructura de la CMDB con la de la estructura TI real.

5.1.3.8 Control y Medición del proceso

Una correcta **Gestión de la Configuración y Activos TI** necesita la colaboración de toda la estructura TI para mantener actualizada la información almacenada en la CMDB.

Es imprescindible elaborar informes que permitan evaluar el rendimiento de la Gestión de la Configuración y Activos TI, tanto para conocer la estructura y adecuación de la CMDB como para aportar información de vital importancia a otras áreas de la infraestructura TI.

Entre la documentación generada cabría destacar:

- Alcance y nivel de detalle de la CMDB.
- Desviaciones entre la información almacenada en la CMDB y la obtenida de las auditorias de configuración.
- Información sobre CIs que han estado involucrados en incidencias.
- Costes asociados al proceso.
- Sistemas de clasificación y nomenclatura utilizados.
- Informes sobre configuraciones no autorizadas y/o sin licencias.
- Calidad del proceso de registro y clasificación.
- Información estadística y composición de la estructura TI.

En pequeñas organizaciones, es a veces conveniente combinar la Gestión de la Configuración y Activos TI y la de Cambios para simplificar el proceso de control. La coordinación entre ambos procesos es un factor crítico para el éxito y esta unificación puede resultar beneficiosa en aquellos casos en el que el volumen de la infraestructura no justifica la total separación de estos procesos.

5.1.4 Gestión de Entregas y Despliegues

5.1.4.1 Introducción y Objetivos

Las complejas interrelaciones entre todos los elementos que componen una infraestructura TI convierten en tarea delicada la implementación de cualquier cambio.

Si la Planificación y Soporte de la Transición es la encargada de diseñar el Plan del Cambio, la Gestión de Cambios de aprobarlo y supervisarlo, y la Validación y Pruebas de testear cada nueva versión, es la **Gestión de Entregas y Despliegues** la que realmente pone en marcha el proceso.

Todo ello requiere de una cuidadosa planificación y coordinación con el resto de procesos asociados a la Gestión de Servicios TI.

Entre los principales objetivos de la Gestión de Entregas y Despliegues se incluyen:

- Establecer una política de implementación de nuevas versiones de hardware y software.
- Implementar las nuevas versiones de software y hardware en el entorno de producción después de que la Validación y Pruebas las haya verificado en un entorno realista.
- Garantizar que el proceso de cambio cumpla las especificaciones de la RFC correspondiente.
- Asegurar, en colaboración con la Gestión de Cambios y la de Configuración y Activos TI, que todos los cambios se ven correctamente reflejados en la CMDB.

- Archivar copias idénticas del software en producción, así como de toda su documentación asociada, en la DML.
- Mantener actualizado el DS.

Los **beneficios** de una correcta Gestión de Entregas y Despliegues se resumen en:

- El proceso de cambio se realiza sin deterioro de la calidad de servicio.
- Las nuevas versiones cumplen los objetivos propuestos.
- El correcto mantenimiento de la DML impide que se pierdan (valiosas) copias de los archivos fuente.
- Se reduce el número de copias de software ilegales.
- Control centralizado del software y hardware desplegado.
- Protección contra virus y problemas asociados a versiones de software incontroladas.

Las **principales dificultades** con las que topa la Gestión de Entregas y Despliegues son:

- No existe una clara asignación de responsabilidades y/o la organización TI no acepta la figura dominante de la Gestión de Entregas y Despliegues en todo el proceso de implementación del cambio.
- No se dispone de un entorno de pruebas adecuado en donde se puedan testear de forma realista las nuevas versiones de software y hardware.
- Hay resistencia en los diferentes departamentos a la centralización del proceso de cambio. Es habitual que existan reticencias a adoptar sistemas estandarizados en toda la organización, sobre todo cuando ésta no ha sido la política tradicional de la misma.
- Se realizan cambios sin tener en cuenta a la Gestión de Entregas y Despliegues argumentado que éstos sólo son responsabilidad de un determinado grupo de trabajo o que su "urgencia" requería de ello.
- Hay resistencias a aceptar posibles planes de "*back-out*". Ciertos entornos de producción pueden elegir "ignorar" lo problemas que una nueva versión puede provocar en otras áreas y resistirse a volver a la última versión estable.
- La implementación sincronizada de versiones en entornos altamente distribuidos.

La solución a estos problemas pasa por:

- Un firme compromiso de la organización con la Gestión de Entregas y Despliegues y sus responsables.
- Un adecuado plan de comunicación que informe a todos los responsables y usuarios de la organización TI de las ventajas de una correcta gestión de todo el proceso de cambio.

5.1.4.2 **Conceptos básicos**

A continuación, definimos los conceptos básicos de este proceso.

5.1.4.2.1 Versión

Una versión es un grupo de CIs de nueva creación o modificados que han sido validados para su instalación en el entorno de producción. Las especificaciones funcionales y técnicas de una versión están determinadas en la RFC correspondiente.

Las versiones pueden clasificarse, según su impacto en la infraestructura TI, en:

- **Versiones mayores**: representan importantes despliegues de software y hardware e introducen modificaciones importantes en la funcionalidad, características técnicas, etc.
- **Versiones menores**: suelen implicar la corrección de varios errores conocidos puntuales y habitualmente son modificaciones que vienen a implementar de una manera correctamente documentada soluciones de emergencia.

- **Versiones de emergencia**: modificaciones que subsanan de forma rápida un error conocido.

Como pueden llegar a existir múltiples versiones, es conveniente definir un código o referencia que los identifique unívocamente. El sistema universalmente aceptado es:

- **Versiones mayores**: 1.0, 2.0, etc.
- **Versiones menores**: 1.1, 1.2, 1.3, etc.
- **Versiones de emergencia**: 1.1.1, 1.1.2, etc.

Aunque en algunos casos esta clasificación se refina aún más (vea, por ejemplo, en la ayuda la versión de su navegador).

En su ciclo de vida, una versión puede encontrase en diversos estados: desarrollo, pruebas, producción y archivado.

El siguiente diagrama nos ilustra gráficamente la evolución temporal de una versión:

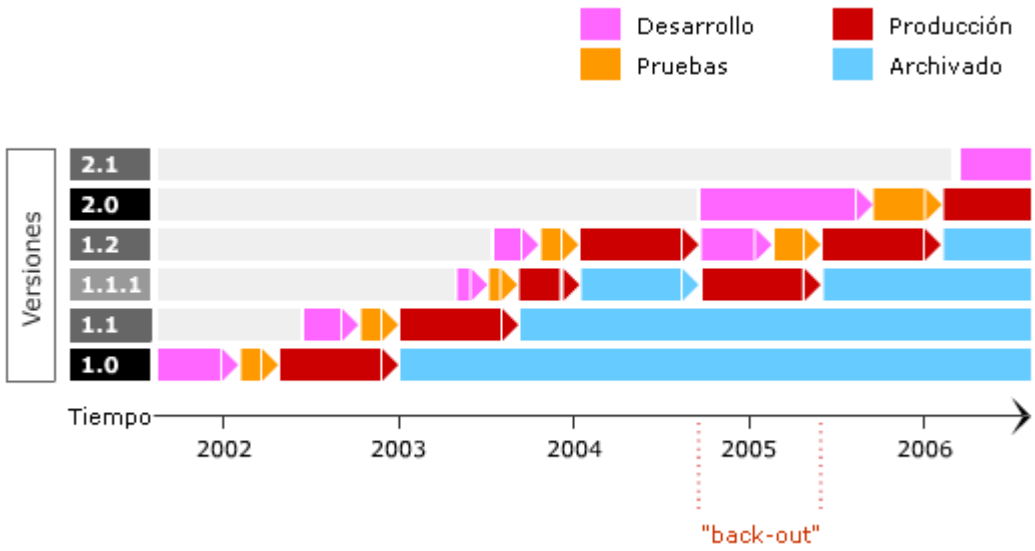


Ilustración 5-4 Evolución temporal de una versión

El despliegue de nuevas versiones puede realizarse de diferentes maneras y es responsabilidad de la Gestión de Cambios el determinar la forma más conveniente de hacerlo. Entre las opciones más habituales cabe contar:

- **Versión delta**: sólo se testean e instalan los elementos modificados. Esta opción tiene como ventaja su mayor simplicidad, pero conlleva el peligro de que puedan aparecer problemas e incompatibilidades en el entorno de producción.
- **Versión completa**: Se distribuyen todos los elementos afectados, ya hayan sido modificados o no. Aunque esta opción es obviamente más trabajosa, es más improbable que se generen incidencias tras la instalación si se han realizado las pruebas pertinentes.
- **Paquete de Versiones**: La Gestión de Cambios puede optar por distribuir de forma sincronizada diferentes paquetes de versiones: de esta forma se ofrece una mayor estabilidad al entorno TI. En algunos casos esta opción es obligada por incompatibilidades entre una nueva versión con software o hardware previamente instalado. Pensemos, por ejemplo, en la migración a un nuevo sistema operativo que requiere hardware más avanzado y/o nuevas versiones de los programas ofimáticos.

5.1.4.2.2 Biblioteca de Medios Definitivos (DML)

La **Biblioteca de Medios Definitivos** (DML) debe contener una copia de todo el software instalado en el entorno TI. Esto incluye no sólo sistemas operativos y aplicaciones, sino también controladores de dispositivos y documentación asociada.

La DML debe contener el histórico completo de versiones de un mismo software para proporcionar la versión

necesaria en caso de que se deban implementar los planes de *back-out*.

La DML debe ser almacenada en un entorno seguro y es conveniente que se realicen *back-up* periódicos.

5.1.4.2.3 Recambios Definitivos (DS)

El almacén de **Recambios Definitivos** (DS) contiene piezas de repuesto para los CIs en el entorno de producción.

Los activos almacenados deben incorporarse a la CMDB en el caso de que los CIs correspondientes se hallen registrados en la misma (esto puede depender del alcance y nivel de detalle de la CMDB).

5.1.4.3 Planificación de entregas

Es crucial establecer un marco general para el lanzamiento de nuevas versiones que fije una metodología de trabajo. Esto es especialmente importante para los casos de versiones menores y de emergencia, pues en el caso de lanzamientos de gran envergadura se deben desarrollar planes específicos que tomen en cuenta las peculiaridades de cada caso.

A la hora de planificar correctamente el lanzamiento de una nueva versión se deben de tomar en cuenta los siguientes factores:

- Cómo puede afectar la nueva versión a otras áreas del entramado TI.
- Qué CIs se verán directa o indirectamente implicados durante y tras el lanzamiento de la nueva versión.
- Cómo ha de construirse el entorno de pruebas para que éste sea fiel reflejo del entorno de producción.
- Qué planes de *back-out* son necesarios.
- Cómo y cuándo se deben implementar los planes de back-out para minimizar el posible impacto negativo sobre el servicio y la integridad del sistema TI.
- Cuáles son los recursos humanos y técnicos necesarios para llevar a cabo la implementación de la nueva versión con garantías de éxito.
- Quiénes serán los responsables directos en las diferentes etapas del proceso
- Qué planes de comunicación y/o formación deben desarrollarse para que los usuarios estén puntualmente informados y puedan percibir la nueva versión como una mejora.
- Qué tipo de despliegue es el más adecuado: completo, delta, sincronizado en todos los emplazamientos, gradual...
- Cuál es la vida media útil esperada de la nueva versión.
- Qué impacto puede tener el proceso de lanzamiento de la nueva versión en la calidad del servicio.
- Si es posible establecer métricas precisas que determinen el grado de éxito del lanzamiento de la nueva versión.

Una herramienta clave para formular la planificación de entregas es el **Modelo en V**, que sirve para identificar los diferentes niveles de test necesarios para aceptar una versión durante el proceso de Validación y Pruebas.

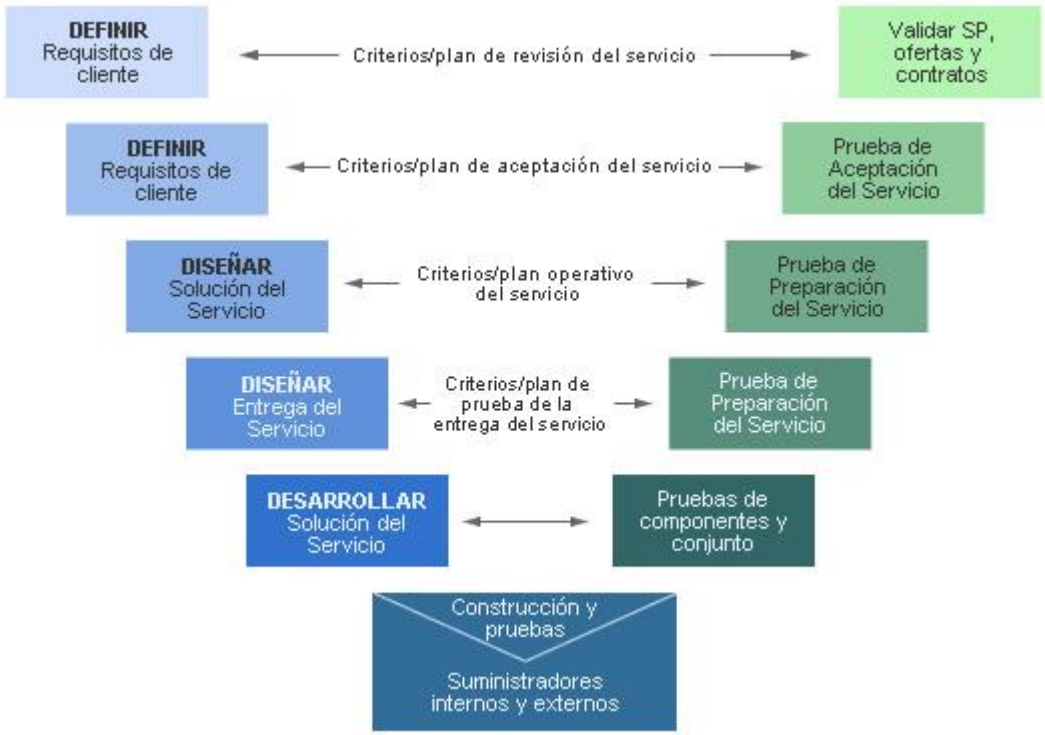


Ilustración 5-5 Modelo en V

La metodología del Modelo en V consiste en definir, en el brazo izquierdo de la V, las especificaciones del servicio que es necesario cumplir para aceptar una versión. En el brazo derecho se van indicando, de forma paralela, las pruebas mediante las cuales se van a comprobar cada una de las especificaciones de la izquierda.

5.1.4.4 Desarrollo del despliegue

La **Gestión de Entregas y Despliegues** es la encargada del diseño y construcción de las nuevas versiones siguiendo las pautas marcadas en las RFCs correspondientes.

A veces el desarrollo se realizará "en casa" y muchas otras requerirá la participación de proveedores externos. En este segundo caso, la tarea de la Gestión de Entregas y Despliegues será la de asegurar que el paquete o paquetes de software o hardware ofrecidos cumple o cumplen las especificaciones detalladas en la RFC. Asimismo, la Gestión de Entregas y Despliegues será la responsable de todo el proceso de configuración necesario.

El desarrollo debe incluir, si esto fuera necesario o simplemente recomendable, todos los scripts de instalación requeridos para el despliegue de la versión. Estos scripts deberán tener en cuenta aspectos tales como:

- Back-up automático de datos.
- Actualizaciones necesarias de las Bases de Datos asociadas.
- Instalación de las nuevas versiones en diferentes sistemas o emplazamientos geográficos.
- Creación de logs asociados al proceso de instalación.

Parte integrante del desarrollo lo componen los planes de back-out asociados. Éstos tendrán que tomar en cuenta la disponibilidad acordada con los clientes en los SLAs correspondientes.

5.1.4.5 Implementación de la entrega

Llegó el momento de la verdad: la distribución de la nueva versión, también conocida como *rollout*.

El *rollout* puede ser de varios tipos:

- **Completo y sincronizado**: se realiza de manera integral y simultánea en todos los emplazamientos.

- **Fragmentado**: ya sea bien espacial o temporalmente. Por ejemplo, introduciendo la nueva versión por grupos de trabajo o incrementando progresivamente la funcionalidad ofrecida.

El procedimiento de *rollout* debe ser cuidadosamente documentado para que todas las partes conozcan sus tareas y responsabilidades específicas. En particular, los usuarios finales deben estar puntualmente informados del calendario de lanzamiento y de cómo éste puede afectar a sus actividades diarias.

Es imprescindible determinar claramente:

- Los CIs que deben borrarse e instalarse y en qué orden debe realizarse este proceso.
- Cuando debe realizarse este proceso para diferentes grupos de trabajo y/o localizaciones geográficas.
- Qué métricas determinan la puesta en marcha de los planes de *back-out* y si éstos deben ser completos o parciales.

Tras la distribución, la **Gestión de Entregas y Despliegues** debe asegurarse de que:

- Se incluya una copia de la versión en la DML.
- El DS incorpore repuestos funcionales de los nuevos CIs.
- La CMDB esté correctamente actualizada.
- Los usuarios están debidamente informados de las nuevas funcionalidades y han recibido la formación necesaria para poder sacar el adecuado provecho de las mismas.

Tras la implementación, la Gestión de Entregas y Despliegues debe ser puntualmente informada por el Centro de Servicios de los comentarios, quejas, incidencias, etc. que la nueva versión haya podido suscitar. Toda esta información deberá ser analizada para asegurar que las próximas versiones incorporen las sugerencias recibidas y que se tomen las medidas correctivas necesarias para minimizar el impacto negativo que puedan tener futuros cambios.

5.1.4.6 Comunicación y Formación

Es frecuente, y a su vez un grave error, que cuando se aborden cuestiones de carácter técnico se obvie el factor humano.

Salvo contadas excepciones, es necesaria la interacción usuario-aplicación y ésta suele representar el eslabón más débil de la cadena.

Es inútil disponer de un sofisticado servicio TI si los usuarios, debido a una incompleta (in)formación, no se encuentran en disposición de aprovechar sus ventajas.

La (in)formación debe estructurarse en distintos niveles:

- Los usuarios deben conocer el próximo lanzamiento de una nueva versión y conocer con anterioridad la nueva funcionalidad planificada o los errores que se pretenden resolver para participar, a su discreción, en el proceso.
- Cuando se considere oportuno, se impartirán cursos presenciales o remotos mediante módulos de e-learning sobre el funcionamiento de la nueva versión.
- Se desarrollará una página de FAQs donde los usuarios puedan aclarar las dudas más habituales y puedan solicitar ayuda o soporte técnico en el uso de la nueva versión.

5.1.4.7 Control y Medición del proceso

Es imprescindible elaborar informes que permitan evaluar el rendimiento de la **Gestión de Entregas y Despliegues**.

Para que estos informes ofrezcan una información precisa y de sencilla evaluación es necesario elaborar métricas de referencia que cubran aspectos tales como:

- Número de lanzamientos de nuevas versiones.

- Número de *back-outs* y razones de los mismos.
- Incidencias asociadas a nuevas versiones.
- Cumplimientos de los plazos previstos para cada despliegue.
- Asignación de recursos en cada caso.
- Corrección y alcance de la CMDB y la DS.
- Existencia de versiones ilegales de software.
- Adecuado registro de las nuevas versiones en la CMDB.
- Incidencias provocadas por uso incorrecto (formación inadecuada) de la nueva versión por parte de los usuarios.
- Disponibilidad del servicio durante y tras el proceso de lanzamiento de la nueva versión.

5.1.5 Validación y Pruebas

5.1.5.1 Introducción y Objetivos

La **Validación y Pruebas del Servicio** es la encargada de probar cada nueva versión en un entorno idéntico al real antes de proceder a su implantación. El objetivo último del proceso consiste en detectar y prevenir aquellos errores causados por incompatibilidades imprevistas, y verificar que se cumplen los niveles de utilidad y garantía establecidos.

Para cumplir este cometido, la Validación y Pruebas del Servicio se encarga de:

- Diseñar y mantener un entorno de pruebas, es decir, una réplica exacta del escenario en el que el servicio desarrolla su actividad.
- Conocer a fondo las funcionalidades del servicio y mantener listados actualizados de todos los casos de uso para poder hacer chequeos completos.
- Conocer a fondo los requisitos de calidad del servicio acordados con el cliente para poder garantizar que las nuevas versiones los cumplen.
- Planificar y llevar a cabo un calendario de pruebas que cubra todas las funcionalidades registradas para el servicio.

Los **beneficios** de una correcta Validación y Pruebas del Servicio se resumen en:

- Se reduce el número de incidencias por incompatibilidades con otro software o hardware instalado.
- Al haber menos incidencias, también se reduce significativamente el volumen de llamadas que llegan al Centro de Servicios.
- Los problemas y errores conocidos pueden ser detectados, aislados y diagnosticados en el entorno de pruebas mucho mejor que en el entorno real.
- Se ahorran costes, puesto que es mucho menos “caro” resolver errores en un entorno de pruebas que en uno real.
- El proceso de pruebas asociado no sólo permite asegurar la calidad del software y hardware a instalar, sino que también permite conocer la opinión de los usuarios sobre la funcionalidad y usabilidad de las nuevas versiones.

La **Validación y Pruebas del Servicio** puede encontrarse con las siguientes dificultades:

- El Catálogo de Servicios Técnico omite algunas funcionalidades del servicio, ya sea por no estar suficientemente actualizado o por falta de detalle, por lo que la Validación y Pruebas del Servicio no las incluye en su plan de pruebas.
- La Gestión de Entregas y Despliegues no actualiza con suficiente frecuencia su entorno de desarrollo,

lo que deriva en la necesidad de efectuar varias pruebas previas hasta pulir la versión desde un punto de vista técnico antes de examinar su utilidad y garantía.

- La Gestión de Entregas y Despliegues no conoce o a fondo los requisitos definidos en los SLRs y SLAs, por lo que son necesarias evaluaciones preliminares hasta alcanzar el nivel de rendimiento mínimo.
- No se define suficiente con claridad la metodología a emplear durante las pruebas, o ésta se aparta demasiado de los SLRs acordados con el cliente, por lo que las pruebas resultan ser ineficaces.

5.1.5.2 Validación, planificación y verificación de tests

Un bien planificado **protocolo de tests** es absolutamente indispensable para lanzar al entorno de producción una nueva versión con razonables garantías de éxito.

Las pruebas no deben limitarse a una validación de carácter técnico (ausencia de errores) sino que también deben realizarse pruebas funcionales con usuarios reales para asegurarse de que la versión cumple los requisitos establecidos y es razonablemente usable (siempre existe una inevitable resistencia al cambio en los usuarios que debe ser tenida en consideración). Cuanto mayor sea el alcance del plan de pruebas, mayores serán las garantías de fiabilidad de la nueva versión.

Es importante que las pruebas incluyan los planes de *back-out* para asegurarnos de que se podrá volver a la última versión estable de una forma rápida, ordenada y sin pérdidas de valiosa información.

Estas consideraciones se registran y estructuran en el modelo de pruebas, que incluye:

- El propio **objeto de las pruebas**, proporcionado por la Gestión de Entregas y Despliegues.
- **Plan de Pruebas**, que recoge la planificación y la estimación de plazos para cada una de las pruebas: técnicas, funcionales, etc. Puede haber uno o varios, dependiendo de las circunstancias y magnitud de los cambios.
- **Guiones de pruebas**, que recogen el método a emplear: cómo se va a testear cada elemento, qué datos se van a tomar como indicadores y los baremos de calidad que determinarán si la prueba ha sido un éxito o un fracaso.

La **Dirección y Validación de Pruebas** es la unidad encargada de supervisar el correcto desempeño de las tareas descritas en el Plan de Pruebas. Al final de todo el proceso, será también la responsable de elaborar el registro final de todas las tareas realizadas y de verificar que la planificación se cumplió punto por punto.

Una vez planificado el proceso, el siguiente paso consiste en la validación de los paquetes de servicios, las ofertas y los contratos (UCs). El objetivo último es asegurar que el servicio TI se corresponde con la utilidad y garantía esperadas, y que el proveedor o proveedores correspondientes están preparados para poner en funcionamiento el nuevo servicio a partir de su despliegue.

Llegado este punto, también se repasan los diseños y planes de pruebas para verificar que todo está completo y que se ajusta a los perfiles de riesgo previstos (teniendo en cuenta, por ejemplo, los picos de demanda) y a todos los casos de uso (interfaces, perfil tecnológico de los usuarios, roles, etc.).

5.1.5.3 Construcción de tests

En esta etapa, la **Validación y Pruebas del Servicio** se ocupa de recopilar todos los componentes de la versión y de poner a punto el entorno de pruebas en las condiciones necesarias para su correcto desarrollo.

La fiabilidad de las pruebas está condicionada al entorno en el que éstas tienen lugar. Si no es idéntico al escenario real en que se desplegará el servicio nuevo o modificado, los resultados de las pruebas se verán distorsionados y por tanto no servirán. De ahí la importancia de que el escenario de pruebas tenga:

- Las mismas versiones de software que la plataforma en producción.
- Los mismos dispositivos de hardware.
- Clones de las bases de datos. Sólo si se utilizan las bases de datos reales pueden obtenerse informes precisos sobre, por ejemplo, el rendimiento de las consultas, con resultados que no aparecerían de

utilizar bases de datos de ejemplo con sólo unas pocas entradas.

Antes de dar comienzo a las pruebas, todos estos componentes son pre-testeados para garantizar que sólo participarán en ellas aquellos que cumplen con los más estrictos criterios de calidad.

5.1.5.4 Pruebas

En esta etapa del proceso se llevan a cabo las **pruebas** propiamente dichas: todos los componentes, herramientas y mecanismos que participan en el despliegue, la migración y el *back-out* son examinados uno por uno. El desarrollo de las pruebas puede ser automático o manual.

Las principales actividades realizadas en el subproceso de pruebas deben incluir:

- Pruebas del correcto funcionamiento de la versión.
- Pruebas de los procedimientos automáticos o manuales de instalación.
- Pruebas de los planes de *back-out*.
- Pruebas por grupo objetivo (roles), para medir la utilidad del servicio.

Siempre que sea posible, las pruebas de carácter funcional deben ser realizadas por un selecto grupo de usuarios finales. Durante este proceso de prueba se documentará y analizará:

- La experiencia subjetiva del usuario.
- Los comentarios y sugerencias sobre usabilidad y funcionalidad o las dudas que hayan surgido durante el uso de la nueva versión.
- La claridad de la documentación que se pondrá a disposición del usuario final.

5.1.5.5 Aceptación y reporte

La **aceptación** consiste en la comparación de los datos reales obtenidos en las pruebas con los SACs. Si la versión no cumple los requisitos mínimos preestablecidos, es devuelta como "no aceptada" a la Gestión de Cambios para su reevaluación.

En cambio, si el análisis es favorable y existen garantías de que la versión cumple las condiciones necesarias para obtener el consentimiento del cliente, se procede a la elaboración de un informe completo de resultados de las pruebas.

Este documento incluye:

- Reporte de actividades realizadas.
- Listas de *bugs* o errores detectados, si se diera el caso.
- Ideas de mejora, que se envían a la fase de CSI.
- Información y conocimiento para el SKMS.

Este documento es el que más adelante servirá a la Evaluación para elaborar informes de rendimiento del servicio que a su vez serán tenidos en cuenta por la Gestión de Cambios a la hora de validar o no el cambio.

5.1.5.6 Limpieza y cierre

Por último, se procede a la **limpieza** del entorno de pruebas, revirtiendo los cambios incorporados durante los test (instalación de aplicaciones, importación de datos, etc.) hasta la situación inicial.

En esta última etapa, el equipo encargado de las pruebas revisa el planteamiento de las mismas y verifica si la planificación se cumplió conforme a los recursos, SACs y plazos acordados. Así, se detectan aspectos mejorables para perfeccionar el proceso.

5.1.5.7 Control y Medición del proceso

La eficacia de la **Validación y Pruebas del Servicio** puede ser evaluada teniendo en cuenta los siguientes indicadores:

- Porcentaje de componentes que no superan los test de aceptación.
- Número de errores conocidos que se registran durante la etapa de pruebas.
- Tiempo de demora en la subsanación de errores.
- Número de incidencias atribuibles a las nuevas versiones.
- Porcentaje de test de aceptación del servicio que no obtienen la aprobación del cliente.

5.1.6 Evaluación

5.1.6.1 Introducción y Objetivos

La **Evaluación** es un proceso transversal encargado de valorar el rendimiento de un elemento específico o conjunto de elementos del servicio y de generar un informe completo al respecto. No debe confundirse esta labor con la de verificar si el servicio cumple los requisitos mínimos de calidad, eficacia y utilidad, que corresponde a la Validación y Pruebas del Servicio.

El objetivo principal de la Evaluación consiste en facilitar la información suficiente para determinar con seguridad si un aspecto del servicio es útil para el negocio, ya sea porque aumenta su calidad o porque proporciona una mejora en la productividad.

Algunas dificultades que pueden obstaculizar las actividades de la Evaluación son:

- Las evaluaciones no se gestionan con suficiente agilidad y se generan cuellos de botella que retrasan la implementación del cambio.
- Los resultados de la Validación y Pruebas del Servicio son incompletos o poco detallados, lo que puede resultar en una evaluación sesgada.
- El modelo de rendimiento no refleja el servicio en toda su complejidad, ocasionando un constante desequilibrio entre las estimaciones iniciales de rendimiento previsto y el rendimiento real del servicio una vez implantados los cambios.
- No se analiza el rendimiento del servicio con suficiente celo, por lo que algunos efectos imprevistos del cambio no llegan a advertirse.

5.1.6.2 Planificación de la evaluación

El propósito de la Evaluación es, como se ha dicho, analizar el impacto de un cambio en el servicio con el fin de recabar toda la información relevante para tomar una decisión respecto a la implantación del mismo.

Con el fin de predecir el impacto de un cambio, la **Evaluación** considerará los siguientes factores:

- **Capacidad del proveedor de Servicios (S)**. La capacidad de un proveedor o de una unidad de servicio para desempeñar su trabajo.
- **Tolerancia (T)**. La capacidad que tiene el servicio para absorber cambios.
- **Configuración de la Organización (O)**. La capacidad que tiene la organización TI para absorber cambios.
- **Recursos (R)**. Disponibilidad de la necesaria infraestructura, personal cualificado, fondos económicos, etc. para llevar a cabo la transición.
- **Modelado y medidas (M)**. Grado en que las predicciones formuladas a partir del modelo de rendimiento coinciden con el comportamiento real del servicio modificado.
- **Personas (P)**. Las personas dentro del sistema y el efecto del cambio en ellas.

- **Uso (U)**. Grado en que el servicio cumple con las expectativas de uso (p.ej. disponibilidad, capacidad, seguridad, etc.)
- **Propósito (P)**. Grado en que el servicio se ajusta al propósito inicial.

La mejor manera de garantizar que el impacto del cambio se ha comprendido en profundidad es examinarlo desde dos perspectivas:

- Efectos deliberados. En general, son beneficiosos para el servicio y deben estar alineados con los SACs definidos por la Planificación y Soporte a la Transición. Algunos ejemplos: reducción del coste del servicio, incremento del rendimiento, optimización de recursos, etc.
- Efectos imprevistos. Son muy difíciles de predecir e incluso de detectar, ya que a menudo no se manifiestan hasta que se despliega el cambio en producción.

Por lo general, suelen ser perjudiciales para el servicio y son difíciles de medir: impacto en los clientes/usuarios, sobrecarga de la red…

5.1.6.3 Evaluación de rendimiento previsto

Consiste en una evaluación de los riesgos derivados de la ejecución de un cambio, que toma como referencia:

- Requisitos del cliente (SLRs, SLAs).
- Rendimiento esperado o rendimiento que está previsto que el servicio obtenga una vez implantado el cambio.
- Modelo de rendimiento, que no es sino una representación de la utilidad y garantía del servicio.

Si la **Evaluación** concluye que el rendimiento real no coincide con lo previsto, acarrea riesgos inaceptables o bien se desvía de los criterios de aceptación, entonces se interrumpen las actividades de evaluación y se genera un Informe Intermedio de Valoración, que será enviado a la Gestión de Cambios y que contemplará:

- Perfil de riesgos.
- Reporte de desviaciones (rendimiento esperado vs. real).
- Recomendaciones.
- Control de calidad.

Si, en cambio, la Evaluación concluye que el rendimiento previsto coincide con lo esperado, se procede al despliegue del cambio y a la evaluación del rendimiento real.

5.1.6.4 Evaluación de rendimiento real

Una vez ya se ha implantado el cambio, desde la fase de Operación se envían a la Evaluación los **informes del rendimiento real** que está registrando el servicio. De nuevo, se analizarán los riesgos comparando estos datos con los requisitos del cliente, el rendimiento esperado y el modelo de rendimiento.

Si todo marcha según lo esperado, se genera un **informe de evaluación final** y se da por concluido el proceso de Evaluación.

Si, en cambio, se determina que el cambio está comportando riesgos inaceptables, se están incumpliendo los criterios de aceptación o el rendimiento no alcanza las expectativas iniciales, es responsabilidad de la Evaluación alertar a la Gestión de Cambios y hacerle llegar un **Informe Intermedio de Valoración** en los términos descritos en el apartado anterior.

Este desenlace también cierra el proceso de Evaluación, ya que, si la Gestión de Cambios desea corregir la situación, se generará una nueva RFCs conforme a los planes de retirada.

5.1.6.5 Control y Medición del proceso

El proceso de **Evaluación** puede medirse a través de los siguientes indicadores:

- Número de evaluaciones solicitadas para nuevos servicios o cambios en un periodo determinado.
- Número de evaluaciones entregadas en un periodo determinado.
- Número de evaluaciones que permanecen en la cola de tareas.
- Tiempo medio de elaboración de una evaluación desde que ésta es solicitada hasta que se entrega.
- Desviación de las evaluaciones de rendimiento previsto respecto de las evaluaciones reales.

5.1.7 Gestión del Conocimiento

5.1.7.1 Introducción y Objetivos

La **Gestión del Conocimiento** es la encargada de reunir, analizar, almacenar y compartir el conocimiento e información de la organización. El objetivo principal del proceso consiste en mejorar la eficiencia, reduciendo la necesidad de redescubrir el conocimiento.

La Gestión del Conocimiento contribuye a mejorar la calidad de las decisiones que se adoptan en una organización, al garantizar que aquellos a quienes compete tomarlas disponen de información segura y fiable.

Sin embargo, una organización puede tener las herramientas adecuadas para registrar y organizar los datos, pero las buenas intenciones pueden no llegar a materializarse nunca si no existe una unidad de Gestión del Conocimiento que impulse, coordine y estructure el proceso para:

- Garantizar que el personal hace uso de las herramientas, tanto para registrar como para consultar los datos disponibles.
- Evaluar los datos recogidos, velando por que estén permanentemente actualizados.
- Analizar las necesidades de información de ciertos departamentos y coordinar la adecuada transferencia de conocimiento desde aquellos que poseen los datos.

Estas funciones requieren que los encargados de desempeñar las labores de Gestión del Conocimiento tengan entendimiento profundo de los procesos que se desarrollan en la organización, así como una constante monitorización del aprovechamiento, organización y registro de los datos.

Los beneficios obtenidos de una correcta Gestión del Conocimiento son numerosos:

- No se duplica el trabajo innecesariamente. Si surge un problema que ya se presentó en el pasado, pueden recuperarse con facilidad los detalles de la solución aplicada entonces, ahorrando tiempo y esfuerzo.
- Mejor aprovechamiento de los recursos existentes.
- Prevención de situaciones de desinformación en caso de faltar los "propietarios" de los datos de acceso a una aplicación, de contacto con un cliente, etc.

Las principales dificultades que se presentan a la hora de abordar la Gestión del Conocimiento consisten en:

- Los miembros del personal están saturados de trabajo y no disponen de tiempo para documentar los datos o dan prioridad a otras tareas más urgentes.
- Los miembros del personal no confían en los datos registrados, de modo que recurren a otras vías a la hora de buscar información.
- Los datos están mal estructurados, son incompletos o no están adaptados a la audiencia a la que van destinados, por lo que en la práctica resultan inservibles.
- Los datos se registran, pero no se revisan, por lo que la información disponible está desactualizada o incompleta.

5.1.7.2 Conceptos básicos

A continuación, definimos los conceptos básicos de este proceso.

5.1.7.2.1 Sistema de Gestión del Conocimiento del Servicio (SKMS)

Un **Sistema de Gestión del Conocimiento del Servicio** o SKMS es una herramienta que proporciona funcionalidades de presentación, procesamiento y gestión para interactuar con la Base de Datos de Gestión del Conocimiento del Servicio de la organización IT.

Un SKMS está estructurado de forma estratificada, en varias capas que se articulan en torno a la base de datos donde se almacena la información propiamente dicha:

- Capa de presentación. Es la interfaz que permite buscar, explorar, almacenar, recuperar y actualizar los datos a través de una serie de interfaces específicas para cada proceso interesado: vista de Gestión de la Calidad, vista de Activos y Configuración, etc.
- Capa de procesamiento de conocimiento. Las funciones asociadas a esta capa incluyen el análisis de los datos, la elaboración de informes, la planificación, el modelado de los datos y la monitorización de los cambios a través de paneles de control.
- Capa de Integración de la Información. Es donde está la Base de Datos de Gestión, propiamente dicha, y donde se desarrollan todas las actividades de integración de datos: minería de datos, gestión de metadatos, sincronización, etc.
- Herramientas y fuentes de datos e información. En esta capa es donde se estructura la información

5.1.7.2.2 Estructura DIKW

El **concepto DIKW** (Datos-Información-Conocimiento-Saber) recoge y relaciona las distintas unidades de conocimiento en un proceso lineal que va de menor a mayor. Esta estructura es un reflejo del modo en que la Gestión del Conocimiento procesa y transforma los Datos en Saber, que es lo relevante en la toma de decisiones.

- Los **Datos** consisten en mediciones cuantificables y objetivas.
- Al aportar contexto a los datos (contrastando con otras fuentes de datos, interpretándolos, etc.) obtenemos **Información**.
- El **Conocimiento** se alcanza al completar la información con las experiencias, ideas y juicios de cada individuo.
- El **Saber**, por último, radica en tomar las decisiones adecuadas aplicando el conocimiento y el sentido común.

Los Datos, la Información y el Conocimiento pueden ser registrados en bases de datos, y por lo tanto ser consultados y transferidos. El Saber, sin embargo, no puede ser capturado puesto que se refiere a la capacidad individual para hacer juicios válidos y tomar decisiones correctas.

5.1.7.3 Estrategia de conocimiento

A la hora de planificar el proceso de **Gestión del Conocimiento** es preciso definir, desarrollar y difundir:

- Una serie de políticas generales referentes a los datos: qué registrar, cuándo hacerlo, cómo estructurar los datos, etc.
- Las condiciones de administración: qué clase de información es susceptible de ser corregida o eliminada.
- Los roles: quién registra la información, quién la revisa, quién la valida, quienes la pueden consultar libremente.
- Procedimientos de registro, revisión y validación de la información.

5.1.7.4 Transferencia de conocimiento

Es tarea de la **Gestión del Conocimiento**, en primera instancia, transmitir a todos los miembros de la organización TI la importancia de registrar la información relacionada con su trabajo en las herramientas

dispuestas para ello.

Por otro lado, es también su labor instalar una cultura de aprendizaje constante entre los miembros del personal. No sólo se trata de hacer que los empleados registren los datos, sino también motivarlos a que acudan a las fuentes de conocimiento para completar aquello que no saben.

Asimismo, la Gestión del Conocimiento se ocupa de:

- Detectar las necesidades de conocimiento existentes en la organización, tanto a nivel particular como grupal.
- Conocer en todo momento quién o quiénes poseen esa información.
- Establecer el canal adecuado para que los "propietarios" del conocimiento puedan transferirlo a quienes lo necesitan: seminarios, anuncios, boletín, periódico.

5.1.7.5 Gestión del conocimiento

La **Gestión del Conocimiento** debe garantizar que la información disponible sea completa y esté puntualmente actualizada, ya que de otro modo puede resultar inútil.

Las labores de gestión comportan una monitorización exhaustiva de los cambios registrados en el SKMS, y una serie de tareas asociadas a esta revisión:

- Iniciar y gestionar procesos de borrado de información.
- Determinar la periodicidad de las revisiones.
- Detectar y subsanar incoherencias en los datos registrados.

5.1.7.6 Uso del SKMS

En el SKMS han de estar disponibles todos los documentos generados por el resto de procesos:

- **Gobierno de TI**: Cartera de Servicios, informes, CSI, Riesgos y otras cuestiones.
- **Calidad**: Políticas, procesos, procedimientos, formularios, plantillas, listas de comprobación.
- **Servicios**: Catálogo de Servicios, SPs, informes del servicio.
- **Activos y Configuración**: Activo financiero, información del CMS, informes de estado, datos de la CMDB, fuentes definitivas.
- **Centro de Servicios / Soporte**: Catálogo de Servicios, clientes, usuarios, grupos de interés, CIs, incidencias, problemas, cambios, entregas, rendimiento de las configuraciones.

5.1.7.7 Control y Medición del proceso

Las métricas de referencia para evaluar si la **Gestión del Conocimiento** está desarrollando correctamente su labor son:

- Número de solicitudes de entradas nuevas recibidas en un periodo específico.
- Número de solicitudes de modificaciones/actualizaciones enviadas en un periodo específico.
- Número de entradas nuevas publicadas en la base de datos del SKMS en un periodo específico.
- Número de entradas modificadas en la base de conocimiento en un periodo específico.
- Número de incidencias que recurrieron a entradas existentes en la base de conocimiento en un periodo específico.
- Tiempo ahorrado gracias al uso de la base de conocimiento. Se calcula comparando el tiempo medio de resolución de incidencias que se cerraron empleando la base de conocimiento con los que no la usaron.

- Número de peticiones de autoayuda que declararon que la base de conocimiento ayudó en la resolución de un asunto en un periodo determinado.

5.1.8 Puesta en marcha

La **puesta en marcha** de la Transición del servicio puede ser un proceso complejo. En organizaciones no lo suficientemente maduras se puede percibir como una simple burocratización del proceso asociado al cambio.

Es evidente que es imprescindible dimensionar correctamente toda la estructura organizativa asociada y en el caso de pequeñas organizaciones TI, aunque no sea la solución óptima, asumir que diferentes roles puedan recaer en la misma persona o equipo.

Para que la implementación sea un éxito:

- Se deben analizar los problemas surgidos en el pasado debidos a una deficiente implementación de los cambios.
- Se debe comunicar adecuadamente a clientes y miembros de la organización TI las ventajas asociadas y como una correcta gestión de la Transición podría haber evitado estas situaciones.
- La puesta en marcha debe ser incremental incorporando la fase de Transición principalmente a nuevos servicios y proyectos evitando en lo posible interferencias con proyectos ya consolidados o en marcha.

Se deben evaluar cuidadosamente en cada caso las ventajas e inconvenientes asociados y planificar consecuentemente el proceso de introducción de la fase de transición.

5.1.8.1 Organización

Los cambios y los nuevos productos y servicios provocan con frecuencia los consecuentes **cambios organizativos**.

Estos cambios organizativos pueden implicar:

- Transferencia de personal
- Reorganizaciones jerárquicas
- Cambios procedimentales
- Recapacitación del personal

Todos estos cambios pueden ser percibidos positivamente por los miembros de la organización TI o por el contrario pueden ser causa de tensiones internas y problemas de carácter personal.

Las personas son un componente esencial en los procesos de cambio y evolución y es habitual que las personas muestren sus resistencias y miedos.

Es esencial que la fase de transición tome en cuenta este componente emocional actuando en consecuencia:

- Analizando las consecuencias organizativas del cambio incluyendo factores tecnológicos y humanos.
- Dando soporte a todas las personas y equipos implicados.
- Evaluando la capacitación del personal involucrado tanto en el proceso de transición como de operación del servicio.
- Garantizando que el personal involucrado dispone de los recursos necesarios.
- Asegurando el correcto acceso a toda la información necesaria asociada a los nuevos productos y servicios:
    - Estrategias.
    - Análisis de mercados.
    - Guías técnicas y manuales.

  - Matrices RACI.
  - Plan de comunicación.
- Supervisando y documentando todo el proceso.

5.1.8.2 Tecnología

La tecnología juega un papel crucial en dos aspectos primordiales:

- Como apoyo a los procesos involucrados en la fase de transición.
- Como requisito para la implementación de los propios cambios.

La fase de transición puede ser intrínsecamente compleja en organizaciones con una fuerte dependencia tecnológica. La organización del workflow, las pruebas y la generación de toda la documentación asociada al cambio requieren por regla general disponer de herramientas de apoyo que permitan:

- Gestionar adecuadamente la base de datos de configuración y activos del servicio para asegurar que está refleja en todo momento una instantánea actualizada de la infraestructura TI.
- Gestionar el versionado de los servicios.
- Gestionar de forma ágil y flexible toda la documentación generada.
- Acceder rápidamente a todo el conocimiento necesario.
- Supervisar las pruebas realizadas sobre calidad y rendimiento de los nuevos servicios.
- Supervisar el despliegue de los nuevos servicios.
- Mantener puntualmente informados a todos los agentes participantes en esta fase de transición.

Por otro lado, es imprescindible que la infraestructura TI disponga de la tecnología adecuada para la prestación de los servicios nuevos o modificados. Aunque esto pueda parecer una verdad de Perogrullo es habitual que organizaciones TI "reactivas" no afronten actualizaciones tecnológicas necesarias hasta que éstas se hacen imperativas por una clara degradación del servicio.

Habitualmente nuevos servicios requieren actualizaciones de hardware y software que impidan una degradación de la calidad cuando estos se ven forzados a sus límites de capacidad. Normalmente estas actualizaciones desembocan en procesos de cambio secundarios que es necesario analizar, planificar y supervisar de igual manera y con los mismos niveles de exigencia.

5.1.8.3 Factores de éxito y riesgos

Entre los **factores de éxito y retos** a los que se debe confrontar la correcta implementación de la Fase de Transición del Servicio se encuentran:

- Encontrar el equilibrio entre estabilidad y (r)evolución: los clientes y usuarios quieren servicios estables y siempre operativos, pero tienen necesidades cambiantes a las que debe dar respuesta la organización TI.
- Coordinar los procesos asociados a la Transición del servicio entre ellos y con los asociados a las otras fases del ciclo de vida.
- Evitar la burocratización del proceso de cambio sin por ello perder el control sobre el mismo.
- Crear una cultura de intercambio de información y conocimiento que evite los "guetos de *know-how*".
- Disponer de la adecuada estructura tecnológica y organizativa.
- Crear los necesarios mecanismos de control y métricas asociadas para la supervisión de todos los procesos, tareas y procedimientos.
- Desarrollar un *workflow* que permita la integración de todos los agentes implicados.

Los principales riesgos se resumen en:

- Incrementos injustificados del gasto.
- Deficiente comunicación entre los agentes implicados.
- Inmadurez de la organización para asumir los cambios culturales necesarios.
- Incumplimiento de los protocolos por supuestas razones de urgencia.
- Falta de recursos para una implementación en exceso ambiciosa.

5.2 Relación con otros ciclos

Aunque la fase de Transición es una de las mejor delimitadas no debe interpretarse como un compartimento estanco del ciclo de vida del servicio.

La fase de Transición recibe sus inputs principales de la fase de Diseño del Servicio y a su vez sirve de principal input a la fase de Operación, pero tiene a su vez un fuerte impacto en las restantes fases.

5.2.1 Transición y Estrategia

A la hora de establecer una correcta Estrategia del Servicio es necesario conocer en profundidad sus implicaciones en la fase de Transición del Servicio. Cada cambio y evolución implica costes e inevitablemente tiene un impacto en clientes y usuarios.

Es indispensable sopesar los riesgos y potenciales beneficios asociados para establecer una estrategia que minimice los primeros maximizando a su vez los segundos.

Por otra parte, la Transición del Servicio debe colaborar, en aquello que le corresponde, a dar soporte a la perspectiva y posicionamiento del servicio establecidos en la fase de estrategia.

5.2.2 Transición y Diseño

La fase de diseño debe proveer de toda la documentación necesaria para elaborar los planes de cambio y realizar el despliegue del servicio:

- Planes de capacidad y disponibilidad
- SPs
- SLAs
- Planes de continuidad TI

A su vez la fase de Transición debe asesorar al Diseño sobre los riesgos y posibles impactos del cambio en la calidad del servicio.

5.2.3 Transición y Operación

La Operación del Servicio debe suministrar información relevante sobre:

- El entorno de producción
- El conocimiento asociado (incidencias, percepción de clientes y usuarios…) a servicios similares a los que se han de desplegar.

La Transición del Servicio debe poner a disposición de la fase de Operación:

- Toda la documentación necesaria asociada al uso y mantenimiento de los nuevos o actualizados servicios.
- La información relativa a los procesos de prueba y evaluación.

5.2.4 Transición y Mejora Continua

La principal misión de la fase de Mejora Continua es mejorar todos los procesos y tareas involucrados en la prestación del servicio con el objetivo último de mejorar la calidad, rendimiento y rentabilidad de estos y la consecuente percepción de clientes, usuarios y organización TI.

La fase de Transición es clave en este aspecto. Los cambios son la fuente principal de incidencias y problemas tanto a nivel interno (componente tecnológica) como a nivel externo (calidad del servicio).

La fase de Mejora Continua es por sí misma una de las principales fuentes de cambio introduciendo mejoras en los procesos y ajustando la calidad y rentabilidad de los servicios.

6 OPERACIÓN DEL SERVICIO

La fase de **Operación del Servicio** es, sin duda, la más crítica entre todas. La percepción que los clientes y usuarios tengan de la calidad de los servicios prestados depende en última instancia de una correcta organización y coordinación de todos los agentes involucrados.

Todas las otras fases del Ciclo de Vida del Servicio tienen como objetivo último que los servicios sean correctamente prestados aportando el valor y la utilidad requerida por el cliente con los niveles de calidad acordados. Es evidente que de nada sirve una correcta estrategia, diseño y transición del servicio si falla la "entrega".

Por otro lado, es prácticamente imposible que la fase de Mejora Continua del Servicio sea capaz de ofrecer soluciones y cambios sin toda la información recopilada durante la fase de operación.

Los **principales objetivos** de la fase de Operación del Servicio incluyen:

- Coordinar e implementar todos los procesos, actividades y funciones necesarias para la prestación de los servicios acordados con los niveles de calidad aprobados.
- Dar soporte a todos los usuarios del servicio.
- Gestionar la infraestructura tecnológica necesaria para la prestación del servicio.

Uno de los aspectos principales en la Operación del Servicio es la búsqueda de un equilibrio entre capacidad de respuesta y estabilidad.

La estabilidad es necesaria, ya que los clientes requieren disponibilidad y presentan resistencias al cambio. Por otra parte, las necesidades de negocio pueden cambiar rápidamente y eso hace necesario la rapidez en las respuestas.

Normalmente los cambios correctamente planificados no tienen que afectar a la estabilidad del servicio, pero esto requiere la colaboración de todos los agentes implicados en la Operación del Servicio que deben aportar el *feedback* necesario.

Para evitar los problemas de inestabilidad es conveniente adoptar una actitud proactiva que permita dar respuestas a las nuevas necesidades de negocio de una forma progresiva. La actitud reactiva provoca que los cambios sólo se implementen cómo respuesta a estímulos externos, cómo las incidencias o problemas, lo que habitualmente provoca un estado de "urgencia" que no lleva a una correcta planificación del cambio.

Es también muy importante encontrar un correcto equilibrio entre las demandas externas de los clientes y los procesos de gestión internos orientados a gestionar y mantener los recursos humanos y tecnológicos necesarios para la prestación del servicio. Si no se dispone de esos recursos la organización TI no debe comprometerse a prestar el servicio solicitado. Tampoco debe caer en el error de engordar en exceso la infraestructura TI encareciendo innecesariamente el coste de los servicios prestados.

6.1 Procesos de la Fase de Operación del Servicio

Los principales de la Fase de Operación del Servicio son:

- **Gestión de Eventos:** responsable de monitorizar todos los eventos que se dan en la infraestructura TI con el objetivo de asegurar su correcto funcionamiento y ayudar a prever incidencias futuras.
- **Gestión de Incidencias:** responsable de que queden registradas todas las incidencias que afecten a la calidad del servicio y restaurarlo a los niveles acordados de calidad lo antes posible.
- **Petición de Servicios TI:** responsable de gestionar las peticiones de clientes y usuarios que habitualmente hacen necesaria la realización de pequeños cambios en la prestación del servicio. Se corresponderían con RFCs de muy bajo impacto y urgencia sujetas a protocolos estándar, para no

necesitar ser aprobadas por el CAB para su implementación.

- **Gestión de Problemas:** responsable de analizar y ofrecer soluciones a aquellas incidencias repetitivos o recurrentes que degradan la calidad del servicio
- **Gestión de Acceso a los Servicios TI:** relacionada con la seguridad de los servicios. Es el responsable de asegurar que sólo puedan acceder a información de carácter restringido las personas autorizadas para ello.

A continuación, se describen cada uno de ellos.

6.1.1 Gestión de Eventos

6.1.1.1 Introducción y Objetivos

La principal misión de la **Gestión de Eventos**, en su función de monitorizar todos los sucesos importantes, consiste en detectar y escalar condiciones excepcionales para así contribuir a una operación normal del servicio:

- Proporcionando puntos de entrada (inputs) para varios procesos de la fase de Operación (p. ej. Gestión de Incidencias).
- Posibilitando la comparación entre el rendimiento real del servicio con los estándares de diseño y los ANS.
- Contribuyendo a la Mejora Continua del Servicio mediante informes de mejora.

Algunas de las **ventajas** que una correcta Gestión de Eventos aporta a la organización TI son:

- Ayuda a la detección temprana de incidencias, llegando incluso a evitar que éstos se manifiesten a los usuarios.
- Además, la coordinación directa con otros procesos hace posible que éstos reaccionen con mayor rapidez, resultando en una mayor eficiencia de toda la organización TI.
- Posibilita la monitorización automatizada de determinadas actividades. Es más barata que una monitorización en tiempo real y disminuye considerablemente el periodo de inactividad del servicio que media entre la aparición de la incidencia y su resolución definitiva.
- Proporciona la base para las operaciones automatizadas, que incrementan la eficiencia y descargan de trabajo a los recursos humanos que, así, pueden ser empleados en otras tareas como diseñar nuevas funcionalidades, etc.

Entre los **principales desafíos** que pueden obstaculizar la labor de la Gestión de Eventos encontramos:

- Dificultades en la obtención de fondos para contratar las herramientas necesarias y el esfuerzo necesario para configurarlas y explotar sus beneficios.
- Los niveles de filtrado no son adecuados, bien por exceso (se gestionan eventos sin impacto real en el servicio) o por defecto (algunos eventos de importancia no se detectan hasta que es demasiado tarde)
- No existe suficiente compromiso con la Gestión de Eventos en otros procesos del ciclo de vida, ocasionando retrasos en la repuesta a los eventos.
- Adquirir las habilidades necesarias exige tiempo y dinero.

Las actividades de la Gestión de Eventos son

- Aparición de eventos. El proceso se inicia cuando ocurre el suceso, ya sea detectado o no.
- Notificación de eventos. El evento es notificado al equipo o responsable de gestión.
- Detección y filtrado de eventos. La notificación llega a un agente o herramienta de gestión que la lee e interpreta el suceso con el fin de determinar si merece mayor atención o no.
- Clasificación de eventos. Se le asigna una categoría y un nivel de prioridad.

- Correlación. Se analiza si existen eventos similares, así como la importancia del evento en sí mismo y se decide si es necesario tomar medidas.
- Disparadores. Se ponen en marcha los mecanismos necesarios para dar respuesta al evento.
- Opciones de respuesta. Se eligen las soluciones a adoptar.
- Revisión de acciones y cierre. Se revisan las excepciones o eventos importantes para determinar si se han tratado correctamente. Se cierra el proceso de Gestión de Eventos.

6.1.1.2 Aparición de eventos

El flujo de trabajo del proceso de **Gestión de Eventos** se inicia cuando aparece un evento. Los eventos ocurren continuamente, pero no todos son detectados o registrados.

Por ello, es importante que todos los implicados en el diseño, desarrollo, gestión y soporte de los servicios IT y la infraestructura IT comprendan cuáles son los eventos que es preciso detectar.

6.1.1.3 Notificación de eventos

La mayoría de los elementos de configuración (CIs) son diseñados para comunicar información sobre sí mismos de las siguientes formas:

- Una herramienta de gestión demanda periódicamente determinados datos a un dispositivo del CI.
- El propio CI genera un informe al darse unas determinadas condiciones definidas previamente.

Las notificaciones de eventos pueden estar registradas en un formato propietario, aunque la mayoría de los CIs emplean el estándar SNMP (*Simple Network Management Protocol*).

En general, cuanta más información acerca del evento quede recogida en la notificación, y cuanto mejor se determine el destinatario de dicha información, más fácil resultará tomar decisiones respecto al mismo. A menudo, se registran mensajes de error codificados y el personal encargado de resolver los problemas no alcanza a comprender su significado completo.

Si los roles y responsabilidades no han sido bien definidos desde la fase de Diseño, es muy probable que cuando se presente un evento que requiera una respuesta, nadie sepa quién está haciendo qué. En tal caso, hay que redactar una RFC.

6.1.1.4 Detección y filtrado de eventos

Una vez generada la notificación, ésta llega a su destinatario, que puede ser un agente que trabaje sobre el sistema o bien una herramienta de gestión diseñada específicamente para recibir los datos relacionados con el evento e interpretarlos.

El filtrado consiste en decidir si el suceso merece una consideración en profundidad por parte de otra unidad de gestión o si, por el contrario, una vez leído puede ser ignorado. Por ejemplo, cuando se trata de un grupo de notificaciones relacionadas que se emiten de forma seriada, es habitual optar por transmitir sólo la primera.

En otros CIs, en cambio, todos los eventos son significativos y se trasladan directamente a un sistema de correlación automatizado, incluso aunque la notificación esté duplicada.

6.1.1.5 Clasificación de eventos

No todos los eventos son iguales ya que no tienen la misma importancia para el servicio ni la infraestructura TI y, por tanto, no deben tratarse de la misma manera.

La mejor manera de asignar distintas prioridades a cada evento, pero que al mismo tiempo guarden cierta coherencia, es confeccionar una clasificación de eventos. Lo más habitual es que cada organización TI disponga de su propia categorización, ya que es lo más eficaz. Sin embargo, existen tres categorías que no pueden faltar:

- **Informativo**. Se asigna a aquellos eventos que no requieren, en principio, ninguna respuesta y que por

tanto no representan una excepción.

- **Alerta**. Se asigna a aquellos eventos que indican que el servicio se aproxima a un umbral. Su objetivo es notificar a las personas, herramientas o procesos apropiados para que revisen la situación y tomen las medidas necesarias para evitar que se produzca una excepción.
- **Excepción**. Se asigna a los eventos cuando indican que el servicio está operando de manera irregular: los SLAs y OLAs se han incumplido, etc. Las excepciones pueden representar un fallo total, un cese en una funcionalidad o una disminución del rendimiento. Sin embargo, no tienen por qué ser errores.

6.1.1.6 Correlación

La **Correlación** consiste en dimensionar la importancia del evento y, si se diera el caso, establecer conexiones con otros eventos relacionados para ahorrar tiempo. La importancia y significado del evento en sí mismo depende de los siguientes factores:

- Número de eventos similares registrados con anterioridad.
- Número de elementos de configuración (CIs) que generan eventos similares.
- Si existe alguna acción asociada al evento.
- Si el evento representa una excepción.
- Comparación de la cantidad de información utilizada en el evento respecto a un estándar.
- Si se requieren datos adicionales para investigar el evento con posterioridad o incluso datos procedentes de otros sistemas de información.
- Categorización asignada al evento.
- Nivel de prioridad asignado al evento.

6.1.1.7 Disparadores

Una vez que la Correlación ha reconocido la importancia de un evento, es preciso poner en marcha los mecanismos pertinentes para que se produzca una respuesta desde dentro de la organización TI. A este mecanismo, que sirve como desencadenante de una tarea o serie de tareas, lo denominamos “disparador”.

Existen varios tipos de disparadores:

- Disparadores de Incidencias. Crean un registro en el Sistema de Gestión de Incidencias, generando un input para este proceso de la fase de Operación.
- Disparadores de Cambios. Generan una solicitud de cambio (RFC) y enviándola a la Gestión de Cambios, en la fase de Transición.
- Disparadores procedentes de una RFC aprobada o desautorizada. Se envía toda la información relacionada para que la Gestión de Cambios investigue lo ocurrido.
- Scripts automatizados que ejecutan acciones específicas (p. ej. reiniciar un equipo).
- Notificaciones por teléfono móvil.
- Disparadores de base de datos, que restringen el acceso de un usuario a determinados registros o campos, o que crean/eliminan entradas en la base de datos.

6.1.1.8 Opciones de respuesta

Existen numerosas respuestas posibles a la hora de actuar frente a un evento. Entre las más comunes están:

- Registro de eventos. Independientemente de las acciones que se lleven a cabo, se documenta lo ocurrido.
- Respuesta automática. En algunos casos, se pueden programar respuestas automáticas a determinados eventos que la organización TI conoce en profundidad. Por ejemplo: reiniciar un dispositivo, cambiar

un parámetro, bloquear una aplicación para evitar accesos no autorizados, etc.

- Alerta e intervención humana. La alerta tiene como objeto advertir e informar a la persona más cualificada para que desempeñe una acción específica, probablemente en un tiempo determinado y en un dispositivo concreto.
- Emisión de una solicitud de cambio (RFC). Las solicitudes de cambio pueden crearse en cuanto ocurre la excepción o en el momento en que la actividad de Correlación concluye que es necesario hacer cambios.
- Apertura de un registro de incidencia. Al igual que con la RFC, el registro de incidencias puede efectuarse en cuanto se detecta la excepción o cuando la Correlación lo considera necesario.
- Apertura de un vínculo a un registro de problema. Los problemas suelen estar asociados a uno o más incidencias. Esto ayuda al equipo encargado de la Gestión de Problemas para determinar el impacto y la severidad del problema.

Estas respuestas no tienen por qué darse de manera aislada, es decir, que la organización puede combinar dos o más de ellas para ofrecer una solución más completa al evento.

Puede presentarse el caso de un evento que representa una excepción pero que no tiene un impacto directo en el servicio. Se trata de incidencias especiales en los que el registro debe hacerse de acuerdo con un Modelo de Incidencias, pero que no tienen ninguna influencia en el rendimiento al no ocasionar interrupciones del servicio.

6.1.1.9 Revisión de acciones y cierre

Antes de dar por terminado el proceso de **Gestión de Eventos**, es preciso revisar todas las excepciones o eventos importantes para garantizar que se han tratado correctamente.

6.1.1.10 Control y medición del proceso

A la hora de evaluar la eficiencia y efectividad del proceso de **Gestión de Eventos** deben verificarse los siguientes indicadores:

- Número de eventos, por categorías.
- Número de eventos, por importancia.
- Número y porcentaje de eventos que requirieron de intervención humana y cómo fue esa intervención.
- Número y porcentaje de eventos que desembocaron en el registro de una nueva incidencia o solicitud de cambio.
- Número y porcentaje de eventos ocasionados por problemas ya existentes o errores conocidos.
- Número y porcentaje de eventos repetidos o duplicados. Esto es relevante para optimizar la función de Correlación.
- Número y porcentaje de eventos relacionados con problemas de rendimiento.
- Número y porcentaje de eventos que indican futuros problemas de disponibilidad.
- Número y porcentaje de cada tipo de evento, por plataforma o aplicación.
- Número y ratio de eventos por comparación al número de incidencias.

6.1.2 Gestión de Incidencias

6.1.2.1 Introducción y Objetivos

El objetivo del proceso de **Gestión de Incidencias** es resolver, de la manera más rápida y eficaz posible, cualquier incidencia que cause una interrupción en el servicio.

La Gestión de Incidencias no debe confundirse con la Gestión de Problemas, pues al contrario que esta última,

no se preocupa de encontrar y analizar las causas subyacentes a una determinada incidencia sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que ambas están fuertemente relacionadas.

Por otro lado, también es importante diferenciar la Gestión de Incidencias de la Gestión de Peticiones, que se encarga de las solicitudes que los usuarios plantean para mejorar el servicio, al margen de que esté fallando en ese momento.

Los objetivos principales de la **Gestión de Incidencias** son:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA correspondiente.

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el Centro de Servicios debe jugar un papel esencial en el mismo.

El siguiente diagrama resume el proceso de Gestión de Incidencias:

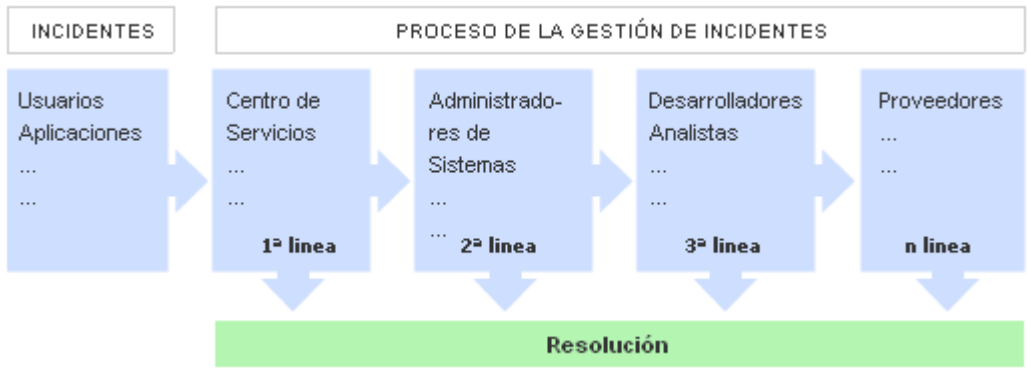


Ilustración 6-1 Gestión de Incidencias

Aunque el concepto de incidencia se asocia naturalmente con cualquier malfuncionamiento o degradación del servicio, según se define en ITIL una incidencia 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".

Con esta definición se puede considerar casi cualquier llamada al Centro de Servicios como una incidencia, exceptuando las Peticiones de Servicio tales como concesión de nuevas licencias, cambio de información de acceso, etc.

Cualquier cambio que requiera una modificación de la infraestructura no se considera un servicio estándar y requiere el inicio de una Petición de Cambio (RFC) que debe ser tratada según los principios de la Gestión de Cambios.

Los **principales beneficios** de una correcta Gestión de Incidencias incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio acordados en el SLA.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Una CMDB más precisa, pues se registran las incidencias en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

Por otra parte, una **incorrecta Gestión de Incidencias** puede acarrear efectos adversos tales como:

- Reducción de los niveles de servicio.
- Se dilapidan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución de la incidencia.
- Se pierde valiosa información sobre las causas y efectos de las incidencias para futuras reestructuraciones y evoluciones.
- Se crean clientes y usuarios insatisfechos por la mala y/o lenta gestión de sus incidencias.

Las **principales dificultades** a la hora de implementar la Gestión de Incidencias se resumen en:

- No se siguen los procedimientos previstos y se resuelven las incidencias sin registrarlas o se escalan innecesariamente y/u omitiendo los protocolos preestablecidos.
- En casos de que se den muchas incidencias concurrentes ("picos de incidencias"), al no haber un margen operativo, puede ocurrir que las incidencias no se registren adecuadamente, impidiendo así la correcta operación de los protocolos de clasificación y escalado.

6.1.2.2 Conceptos básicos

A continuación, definimos los conceptos básicos de este proceso.

6.1.2.2.1 Clasificación y Registro

Es frecuente que existan múltiples incidencias simultáneas, por lo que es necesario definir un nivel de prioridad para la resolución de las mismas.

La **priorización** se basa esencialmente en dos parámetros:

- Impacto: determina la importancia de la incidencia en función de cómo ésta afecta a los procesos de negocio y/o del número de usuarios afectados.
- Urgencia: depende del tiempo máximo que el cliente pueda esperar para la resolución de la incidencia y/o el nivel de servicio acordado en el SLA.

También se deben tener en cuenta otros factores auxiliares tales como el tiempo de resolución previsto y los recursos necesarios para su resolución: las incidencias "fáciles" se gestionarán cuanto antes.

En función de la prioridad, se asignarán los recursos necesarios para la resolución de la incidencia.

La prioridad de la incidencia puede variar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que permitan funcionar al servicio de forma aceptable, permitiendo así demorar el cierre de la incidencia sin que el cliente perciba degradación del servicio.

Es recomendable establecer un protocolo para determinar, en primera instancia, la prioridad de la incidencia. El siguiente diagrama nos muestra un posible "diagrama de prioridades" en función del impacto de la incidencia:

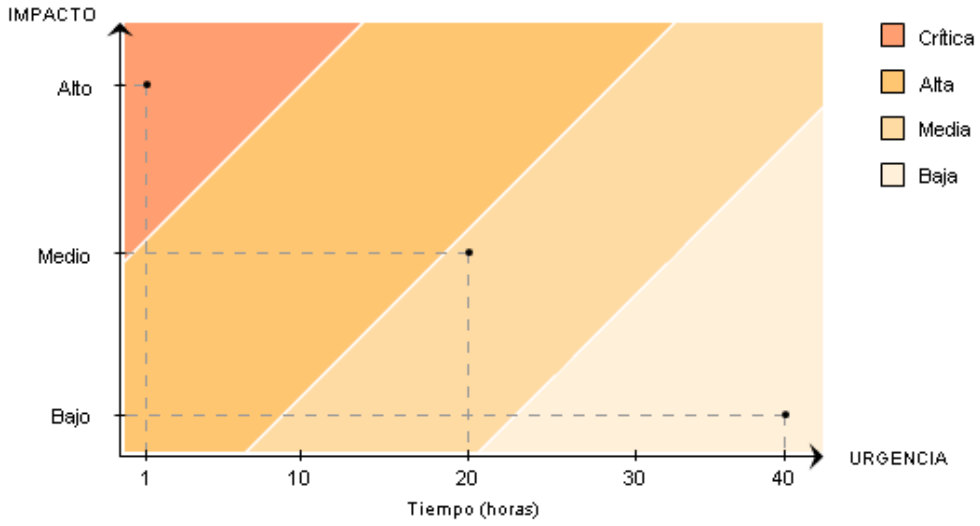


Ilustración 6-2 Determinación de prioridad

6.1.2.2.2 Escalado y Soporte

Es habitual que el Centro de Servicios no sea capaz de resolver en primera instancia una incidencia. En esos casos deberá recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado.

Básicamente hay dos tipos de escalado:

- Escalado funcional: Se requiere el apoyo de un especialista de más alto nivel para resolver la incidencia.
- Escalado jerárquico: Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapan de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de una incidencia específica.

El proceso de escalado puede resumirse gráficamente como sigue:

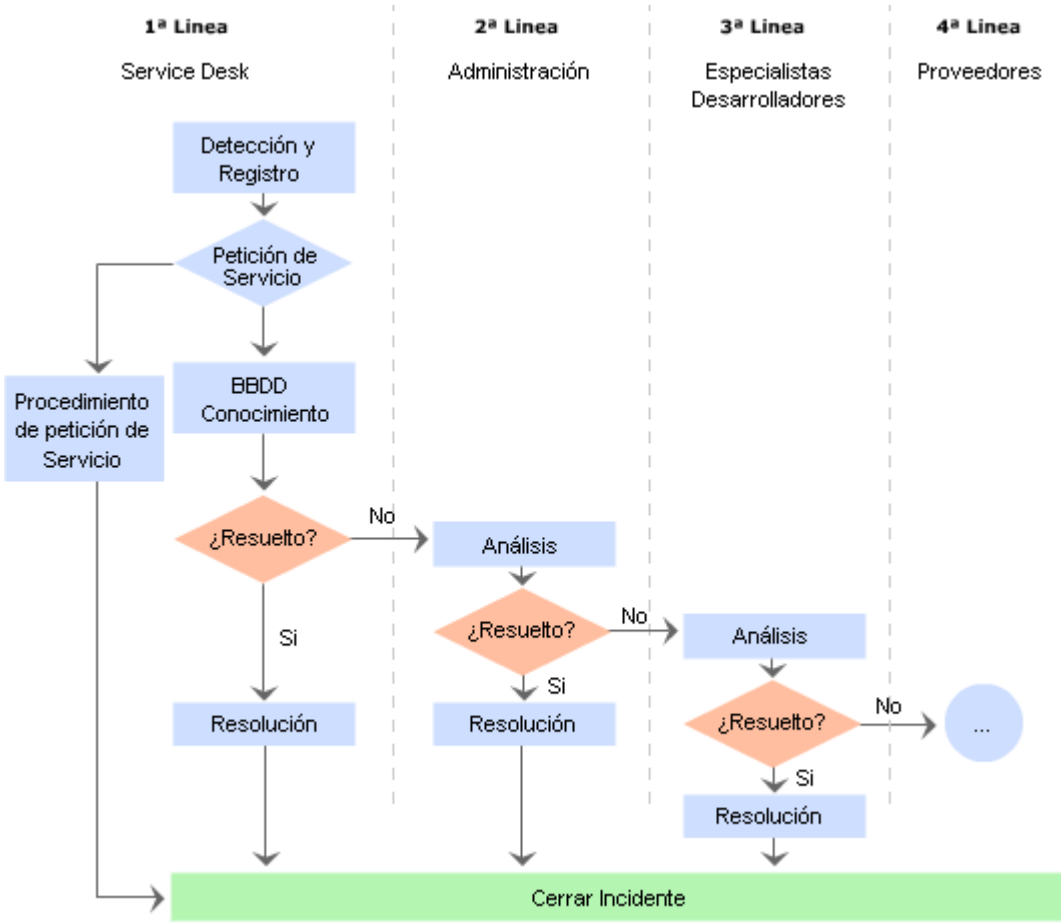


Ilustración 6-3 Proceso de escalado

El escalado puede incluir más niveles en grandes organizaciones, o, por el contrario, en el caso de PYMES, integrar diferentes niveles.

6.1.2.3 Registro y Clasificación

6.1.2.3.1 Registro

La admisión y registro de la incidencia es el primer y necesario paso para una correcta gestión del mismo.

Las incidencias pueden provenir de diferentes fuentes tales como usuarios, gestión de aplicaciones (incidencias reactivas), el mismo Centro de Servicios o el soporte técnico (incidencias proactivas), entre otras posibilidades.

El proceso de registro debe realizarse inmediatamente, pues resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

- La admisión a trámite de la incidencia: el Centro de Servicios debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el SLA del cliente y en caso contrario reenviarlo a una autoridad competente.
- Comprobación de que esa incidencia aún no ha sido registrada: es muy habitual que más de un usuario notifique la misma incidencia y por lo tanto hay que evitar la aparición de duplicidades.
- Asignación de referencia: a la incidencia se le debe dar un código que la identifique unívocamente, tanto internamente cómo en las comunicaciones con el cliente.
- Registro inicial: se debe introducir en la base de datos asociada, la información básica necesaria para la atención de la incidencia (hora, descripción de la incidencia, elementos afectados...).
- Información de apoyo: se incluirá cualquier información relevante para la resolución de la incidencia que puede ser solicitada al cliente a través de un formulario específico, o que puede ser obtenida de la

propia CMDB (configuración del hardware, versión del software, etc.).

- Notificación de la incidencia: en los casos en que la incidencia pueda afectar a otros usuarios, se les debe notificar la incidencia para que conozcan cómo ésta puede afectar su trabajo.

6.1.2.3.2 Clasificación

El objetivo principal de la clasificación de una incidencia es recopilar toda la información que pueda ser utilizada para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- Categorización o Tipificación: se asigna una categoría o tipificación (que a su vez se puede dividir en más niveles) dependiendo del tipo de incidencia o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por la incidencia.
- Establecimiento de la prioridad: al igual que con las RFCs, en función del impacto y la urgencia se determina, siguiendo criterios preestablecidos, un nivel de prioridad.
- Asignación de recursos: si el Centro de Servicios no puede resolver la incidencia en primera instancia, la asignará al personal de soporte técnico responsable de su resolución (segundo nivel).
- Monitorización del estado y tiempo de respuesta esperado: se asocia un estado a la incidencia (por ejemplo: registrada, en curso, parada, resuelta o cerrada) y se estima el tiempo de resolución de la incidencia en base al ANS correspondiente y la prioridad.

6.1.2.4 **Análisis, Resolución y Cierre**

Primero se examina la incidencia con ayuda de la Base de Datos de Conocimiento para ver si se puede identificar con alguna incidencia ya resuelta y aplicar la misma solución.

Si el Centro de Servicios no es capaz de resolver la incidencia, éste informa a un nivel superior para su investigación por los expertos asignados. Si estos expertos tampoco no son capaces de resolver la incidencia, se escalará la incidencia de acuerdo con los protocolos de escalado predeterminados.

Durante todo el ciclo de vida de la incidencia se debe actualizar la información del estado de la incidencia para que los agentes involucrados dispongan de cumplida información sobre su evolución.

Si fuera necesario, paralelamente a la resolución de la incidencia se puede emitir una Petición de Cambio (RFC) que se enviaría a la Gestión de Peticiones. Por otro lado, si la incidencia fuera recurrente y no se encontrase una solución definitiva, se deberá informar a la Gestión de Problemas para el estudio detallado de las causas subyacentes.

Cuando se haya solucionado la incidencia se:

- Confirma con los usuarios la solución satisfactoria del mismo.
- Incorpora el proceso de resolución al SKMS.
- Reclasifica la incidencia si fuera necesario.
- Actualiza la información en la CMDB sobre los elementos de configuración (CIs) implicados en la incidencia.
- Cierra la incidencia.

6.1.2.5 **Control y medición del proceso**

La correcta elaboración de informes es una parte fundamental del proceso de **Gestión de Incidencias**.

Estos informes deben aportar información necesaria para, por ejemplo:

- La Gestión de Niveles de Servicio: es fundamental que los clientes dispongan de información actualizada sobre los niveles de cumplimiento de los SLAs y que se tomen las medidas correctivas necesarias en caso de incumplimiento.
- Monitorizar el rendimiento del Centro de Servicios: supervisar el correcto funcionamiento de la

primera línea de soporte y atención al cliente y conocer el grado de satisfacción del cliente por el servicio prestado.

- Optimizar la asignación de recursos: los gestores deben conocer si se han seguido los protocolos establecidos para un escalado y si se han evitado duplicidades en el proceso de gestión.
- Identificar errores: es posible que los protocolos especificados no se adaptan a la estructura de la organización o a las necesidades del cliente, por lo que se deberán tomar medidas correctivas.
- Disponer de Información Estadística: esta información se puede usar para hacer proyecciones futuras sobre asignación de recursos, costes asociados al servicio, etc.

Por otra parte, una correcta Gestión de Incidencias necesita una infraestructura que facilite su adecuada implementación. Entre ellos cabe destacar:

- Un correcto sistema automatizado de registro de incidencias y relación con los clientes
- Un SKMS que permita comparar nuevas incidencias con incidencias ya registrados y resueltos. Un SKMS actualizado permite:
    - Evitar escalados innecesarios.
    - Convertir el *know how* de los técnicos en un activo duradero de la empresa.
    - Poner directamente a disposición del cliente parte o la totalidad de estos datos (a la manera de FAQs) en una extranet, lo que puede permitir que a veces el usuario no necesite siquiera notificar la incidencia.
- Una CMDB que permita conocer todas las configuraciones actuales y el impacto que éstas puedan tener en la resolución de la incidencia.

Para el correcto seguimiento de todo el proceso, es imprescindible el uso de métricas que permitan valorar del modo más objetivo posible el funcionamiento del servicio. Algunos de los aspectos clave a considerar son:

- Número de incidencias clasificados temporalmente y por prioridades.
- Tiempos de resolución clasificados en función del impacto y la urgencia de las incidencias.
- Nivel de cumplimiento del SLA.
- Costes asociados.
- Uso de los recursos disponibles en el Centro de Servicios.
- Porcentaje de incidencias, clasificados por prioridades, resueltos en primera instancia por el Centro de Servicios.
- Grado de satisfacción del cliente.

6.1.3 Gestión de Peticiones

6.1.3.1 Introducción y Objetivos

La **Gestión de Peticiones**, como su nombre indica, es la encargada de atender las peticiones de los usuarios proporcionándoles información y acceso rápido a los servicios estándar de la organización TI.

Es importante aclarar qué entendemos por petición de servicio, un concepto que engloba las solicitudes que los usuarios pueden plantear al departamento de TI:

- Solicitudes de información o consejo.
- Peticiones de cambios estándar (por ejemplo: cuando el usuario olvida su contraseña y solicita una nueva)
- Peticiones de acceso a servicios TI.

La Gestión de Peticiones recibe las siguientes entradas para poder iniciar su labor:

- Peticiones de servicio, planteadas por los usuarios.
- RFCs, también de la misma fuente.
- Descripción detallada del servicio, proporcionada por el Porfolio de Servicios.
- Políticas de Seguridad, de la Gestión de Seguridad.

Las principales razones que respaldan la implementación del proceso de Gestión de Peticiones en la organización TI son:

- Proporciona al departamento comercial un acceso rápido y efectivo a servicios estándar. Esto mejora su productividad, la calidad de los servicios comerciales y los propios productos.
- Reduce la burocracia asociada al proceso de petición de acceso a servicios nuevos o ya existentes, reduciendo asimismo los costes.
- Incrementa el nivel de control sobre los servicios al centralizar la concesión de acceso a los mismos.
- Reduce costes al centralizar la negociación con proveedores respecto al acceso a los servicios, y también al reducir el coste del soporte.

Los objetivos de la **Gestión de Peticiones** incluyen:

- Proporcionar un canal de comunicación a través del cual los usuarios puedan solicitar y recibir servicios estándar para los que existe una aprobación previa.
- Proporcionar información a los usuarios y clientes sobre la disponibilidad de los servicios y el procedimiento para obtenerlos.
- Localizar y distribuir los componentes de servicios estándar solicitados.
- Ayudar a resolver quejas o comentarios ofreciendo información general.

Las **dificultades y desafíos** a los que se puede enfrentar la Gestión de Peticiones son:

- A la hora de documentar y definir claramente el tipo de peticiones que van a ser gestionadas.
- Al establecer funcionalidades de autoayuda para que los usuarios interactúen mejor con el proceso de envío de peticiones.
- Si el alcance del proceso de Gestión de Peticiones no está bien definido, las personas implicadas no tendrán una idea clara sobre cómo se desarrollará.
- Si las interfaces de envío de peticiones tienen un diseño pobre o la implementación no es correcta, resultará muy complicado a los usuarios remitir sus sugerencias, quejas, etc.
- Si las aplicaciones de gestión interna no son adecuadas, la Gestión de Peticiones puede ver disminuida considerablemente su capacidad para asumir gran cantidad de trabajo.
- Una monitorización insuficiente o ineficaz.

6.1.3.2 Selección de peticiones de un menú

La **Gestión de Peticiones** hace posible que los propios usuarios emitan sus peticiones de servicio a través de una interfaz web. En ella, el cliente podrá escoger de entre las "peticiones tipo" predefinidas la que más se ajusta a su caso.

Esto se puede combinar con otras herramientas destinadas a enviar la petición directamente al equipo de *back-end*.

6.1.3.3 Aprobación financiera

La mayoría de las peticiones conllevan un gasto, independientemente de los acuerdos financieros en vigor. Por eso, antes de autorizar una petición es principal determinar primero los costes que ésta acarreará de ser cursada.

Se pueden definir, para determinadas peticiones estándares, unos precios fijos que ayuden a gestionar con

rapidez aquellos casos más frecuentes.

6.1.3.4 Tramitación y cierre

Esta actividad consiste en cursar la propia petición, por lo que las acciones a desempeñar dependerán de la naturaleza de la misma.

El Centro de Servicios puede encargarse de las más simples, mientras que otras precisarán de una intervención especializada. Algunas organizaciones disponen de grupos de expertos para cursar cada tipo de petición, o incluso derivan ciertas actividades a proveedores externos.

El Centro de Servicios, independientemente de si la unidad que tramita la petición es interna o externa, debe monitorizar todo el proceso y perseguir nuevos progresos.

Una vez resuelta la petición, se notifica al Centro de Servicios para que compruebe si el usuario está satisfecho con el resultado y proceda a su cierre.

6.1.3.5 Control y medida del proceso

Algunos de los indicadores que suelen usar para el control y medición de este proceso son los siguientes:

- Número total de peticiones de servicio.
- Ruptura de peticiones de servicio en cada etapa.
- Tamaño de la copia de seguridad de las peticiones más destacadas.
- Tiempo medio que dura la gestión de cada tipo de petición de servicio.
- Número y porcentaje de peticiones de servicio completadas en los tiempos acordados.
- Coste medio de cada tipo de petición de servicio.
- Nivel de satisfacción del cliente con la gestión de las peticiones de servicio.

6.1.4 Gestión de Problemas

6.1.4.1 Introducción y Objetivos

Como se explicó en la sección de Gestión de Incidencias, esta última tiene como exclusivo objetivo el restablecer lo más rápidamente la calidad del servicio y no el determinar cuáles han sido los orígenes y causas del mismo.

Cuando algún tipo de incidencia se convierte en recurrente o tiene un fuerte impacto en la infraestructura TI, es la función de la **Gestión de Problemas** el determinar sus causas y encontrar posibles soluciones.

Cabe diferenciar entre:

- **Problema**: causa subyacente, aún no identificada, de una serie de incidencias o una incidencia aislada de importancia significativa.
- **Error conocido**: Un problema se transforma en un error conocido cuando se han determinado sus causas.

Los principales conceptos involucrados en el proceso de Gestión de Problemas y su relación con la Gestión de Incidencias se resumen en el siguiente interactivo:

Entre las funciones principales de la Gestión de Problemas figuran:

- Identificar, registrar y clasificar los problemas.
- Dar soporte a la Gestión de Incidencias, proporcionando información y soluciones temporales o parches.
- Analizar y determinar las causas de los problemas y proponer soluciones.
- Elevar RFCs a la Gestión de Cambios para llevar a cabo los cambios necesarios en la infraestructura

TI.

- Realizar un seguimiento post-implementación de todos los cambios para asegurar su correcto funcionamiento.
- Realizar informes que documenten no sólo los orígenes y soluciones a un problema, sino que también sirvan de soporte a la estructura TI en su conjunto.
- Analizar tendencias para prevenir incidencias potenciales.

Los principales beneficios de una correcta Gestión de Problemas:

- Un aumento de la calidad general de los servicios TI.
- Se minimiza el número de incidencias.
- Las incidencias se solucionan más rápidamente y, generalmente, en la primera línea de soporte TI, ahorrando recursos e innecesarios escalados.
- La documentación desarrollada es de gran utilidad para la Gestión de la Capacidad, Disponibilidad y Niveles de Servicio.

Las principales dificultades a la hora de implementar la Gestión de Problemas se resumen en:

- Establecer una estrecha colaboración entre la Gestión de Incidencias y la de Problemas. Sin ésta, la Gestión de Incidencias no dispondrá de toda la información necesaria para la rápida solución de las incidencias y la Gestión de Problemas carecerá de la información necesaria para determinar, clasificar y resolver los problemas.
- Mantener actualizadas las bases de datos asociadas requiere un compromiso por parte de todos los agentes implicados y la supervisión de los responsables de la infraestructura TI.
- Aumento de los costes por la contratación de personal especializado, aunque estos se vean sobradamente compensados por los beneficios derivados.

Las principales actividades de la **Gestión de Problemas** son:

- Control de Problemas: se encarga de registrar y clasificar los problemas para determinar sus causas y convertirlos en errores conocidos.
- Control de Errores: registra los errores conocidos y propone soluciones a los mismos mediante la generación de RFCs que son enviadas a la Gestión de Cambios. Además, efectúa la PIR de los mismos en estrecha colaboración con la Gestión de Cambios.

Se recomienda, en la medida de lo posible, desarrollar una **Gestión de Problemas Proactiva** que ayude a detectar problemas incluso antes de que éstos se manifiesten provocando un deterioro en la calidad del servicio.

6.1.4.2 Control de Problemas

El principal objetivo del **Control de Problemas** es conseguir que estos se conviertan en Errores Conocidos para que el Control de Errores pueda proponer las soluciones correspondientes.

Ilustración 6-4 Control de Problemas

El Control de Problemas se compone fundamentalmente de tres fases:

- Identificación y Registro.
- Clasificación y Asignación de Recursos.
- Análisis y Diagnóstico: Error conocido

6.1.4.2.1 Identificación y Registro

Una de las principales tareas de la Gestión de Problemas es identificar los mismos. Las principales fuentes de información utilizadas son:

- La Base de Datos de Incidencias: en principio, cualquier incidencia del que no se conocen sus causas y que se ha cerrado mediante un *workaround* (solución temporal) es potencialmente un problema. Sin embargo, se habrá de analizar si esta incidencia es aislada o su impacto en la estructura TI antes de elevarla a la categoría de problema.
- Análisis de la infraestructura TI: en colaboración con la Gestión de Disponibilidad y de Capacidad, la Gestión de Problemas debe analizar los diferentes procesos y determinar en qué aspectos se debe reforzar los sistemas y estructuras TI para evitar futuros problemas.
- Deterioro de los Niveles de Servicio: el descenso del rendimiento puede ser una indicación de la existencia de problemas subyacentes que no se hayan manifestado de forma explícita como incidencias.

Todas las áreas de la infraestructura TI deben colaborar con la Gestión de Problemas para identificar problemas reales y potenciales, informando a ésta de cualquier síntoma que pueda ser señal de un deterioro en el servicio TI.

El registro de problemas es, en principio, similar al de las incidencias, aunque el énfasis debe hacerse no en los detalles específicos de las incidencias asociados sino más bien en su naturaleza y posible impacto.

El registro debe incorporar, entre otras, información sobre:

- Los CIs implicados.
- Causas del problema.
- Síntomas asociados.
- Soluciones temporales.
- Servicios involucrados.
- Niveles de prioridad, urgencia e impacto.
- Estado: activo, error conocido, cerrado.

6.1.4.2.2 Clasificación y Asignación de Recursos

La clasificación del problema engloba desde las características generales de éste, tales como si es un problema de hardware o software, qué áreas funcionales se ven afectadas y detalles sobre los diferentes elementos de configuración (CIs) involucrados en el mismo.

Un factor esencial es la determinación de la prioridad del problema, que al igual que en el caso de las incidencias, se determina tanto a partir de la urgencia (demora aceptable para la solución del problema) como de su impacto (grado de deterioro de la calidad del servicio).

Al igual que en la Gestión de Incidencias, la prioridad puede cambiar en el curso del ciclo de vida del problema, por ejemplo, si se encuentra una solución temporal al mismo que reduce considerablemente su impacto.

Una vez clasificado el problema y determinada su prioridad, se deben asignar los recursos necesarios para su solución. Estos recursos deben ser suficientes para asegurar que los problemas asociados son tratados eficazmente y así minimizar su impacto en la infraestructura TI.

6.1.4.2.3 Análisis y Diagnóstico: Error conocido

Los objetivos principales del proceso de análisis son:

- Determinar las causas del problema.
- Proporcionar soluciones temporales a la Gestión de Incidencias para minimizar el impacto del problema hasta que se implementen los cambios necesarios que lo resuelvan definitivamente.

Es esencial tener en cuenta que no siempre el origen del problema es un error de hardware o software. Es frecuente que el problema esté causado por:

- Errores de procedimiento.
- Documentación incorrecta.
- Falta de coordinación entre diferentes áreas.

Es también posible que la causa del problema sea un *bug* bien conocido de alguna de las aplicaciones utilizadas. Por lo tanto, es conveniente establecer contacto directo con el entorno de desarrollo, en caso de aplicaciones desarrolladas "en la casa", o investigar en Internet información sobre errores conocidos aplicables al problema en cuestión.

Una vez determinadas las causas del problema, éste se convierte en un Error Conocido y se remite al Control de Errores para su posterior procesamiento.

6.1.4.3 **Control de Errores**

Una vez que el Control de Problemas ha determinado las causas de un problema, es responsabilidad del Control de Errores el registro del mismo como error conocido.

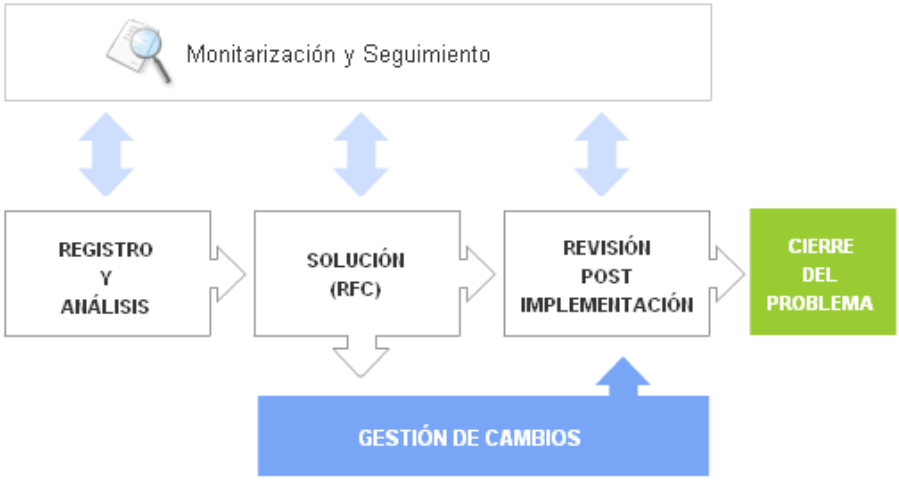


Ilustración 6-5 Control de errores

6.1.4.3.1 Identificación y Registro de errores

El registro de los errores conocidos es de vital importancia para la Gestión de Incidencias, pues debe llevar asociado, siempre que esto sea posible, algún tipo de solución temporal (también llamada ***workaround***) que permita minimizar el impacto de las incidencias asociados.

6.1.4.4 Análisis y Solución

Se deben investigar diferentes soluciones para el error evaluando en cada momento:

- El posible impacto de las mismas en la infraestructura TI.
- Los costes asociados.
- Sus consecuencias sobre los SLAs.

En algunos casos en los que el impacto del problema puede tener consecuencias graves en la calidad del servicio, puede emitirse una RFC de emergencia para su procesamiento urgente por la Gestión de Cambios.

Una vez determinada la solución óptima al problema y antes de elevar una RFC a la Gestión de Cambios han de tenerse en cuenta las siguientes consideraciones:

- Conveniencia de demorar la solución. Bien porque se prevén cambios significativos en la infraestructura TI a corto plazo o por el escaso impacto del problema en cuestión.
- Evaluación del nivel de calidad de la solución provisional. ¿Es aceptable?
- Relación beneficio/coste. ¿Vale la pena el beneficio obtenido por el coste soportado?

Sea cual sea la respuesta, toda la información sobre el error y su solución se registrará en las bases de datos asociadas. En el caso en el que se considere que el problema necesita ser solucionado, se emitirá una RFC. Será responsabilidad de la Gestión de Cambios la implementación de los cambios de infraestructura propuestos.

6.1.4.4.1 Revisión Post Implementación y Cierre

Antes de dar el problema por resuelto y cambiar su estado a “cerrado” se debe analizar el resultado de la implementación de la RFC elevado a la Gestión de Cambios.

Si los resultados de esta PIR son los deseados y se pueden cerrar todas las incidencias relacionados con este problema, se considera concluido el proceso y se emiten los informes correspondientes. Por último, es indispensable actualizar la Base de Datos de Errores Conocidos (KEDB) para futuras ocasiones.

Adicionalmente, en el caso de problemas de carácter grave, todo el proceso se somete a una Revisión de Problemas Graves para prevenir la reaparición del problema.

6.1.4.5 Control y medición del proceso

El objetivo de la **Gestión de Problemas** no es otro que el de mejorar el funcionamiento de la infraestructura TI, y para evaluar su eficacia es imprescindible realizar un continuo seguimiento de los procesos relacionados y evaluar su rendimiento.

En particular, una buena gestión de problemas debe traducirse en una:

- Disminución del número de incidencias y una más rápida resolución de los mismos.
- Mayor eficacia en la resolución de problemas.
- Gestión proactiva, que permita identificar problemas potenciales antes de que éstos se manifiesten o provoquen una seria degradación de la calidad del servicio.

La adecuada elaboración de informes permite valorar el rendimiento de la Gestión de Problemas y aporta información de vital importancia a otras áreas de la infraestructura TI.

Entre la documentación generada cabría destacar:

- **Informes de Rendimiento de la Gestión de Problemas**: donde se detalle el número de errores resueltos, la eficacia de las soluciones propuestas, los tiempos de respuesta y el impacto en la Gestión de Incidencias
- **Informes de Gestión Proactiva**: donde se especifiquen las acciones ejercidas para la prevención de nuevos problemas y los resultados de los análisis realizados sobre la adecuación de las estructuras TI a las necesidades de la empresa.
- **Informes de Calidad de Productos y Servicios**: donde se evalúe el impacto en la calidad del servicio de los productos y servicios contratados y que eventualmente pueda permitir adoptar decisiones informadas sobre cambios de proveedores, etc.

Una eficaz Gestión de Problemas también requiere determinar claramente quiénes son los responsables de cada proceso. Sin embargo, en pequeñas organizaciones es recomendable no segmentar en exceso las responsabilidades para evitar los costes asociados: sería poco eficaz y contraproducente asignar unos recursos humanos desproporcionados al proceso de identificación y solución de problemas.

6.1.5 Gestión de Acceso

6.1.5.1 Introducción y Objetivos

El objetivo de la **Gestión de Acceso a los Servicios TI** es otorgar permisos de acceso a los servicios a aquellos usuarios autorizados e impedírselo a los usuarios no autorizados.

La Gestión de Acceso a los Servicios TI se relaciona con algunos procesos de la fase de Diseño:

- La Gestión de la Seguridad establece las políticas de seguridad que luego la Gestión de Acceso debe tener en cuenta a la hora de otorgar el acceso a los servicios TI.
- El Catálogo del Servicio aporta la documentación sobre los servicios cuyo acceso solicitan los usuarios.

También se relaciona con otros procesos de la fase de Operación, como es el caso de la Gestión de Peticiones o el Centro de Servicios, procesos desde los cuales pueden llegar solicitudes de acceso a servicios.

Asimismo, proporciona información de salida para:

- Gestión de Incidencias, que se hará cargo de aquellas peticiones de acceso o actividades relacionadas con los accesos que representen una excepción.
- Gestión Técnica y Gestión de Aplicaciones, que deben monitorizar los accesos y comprobar si son autorizados o no.

La Gestión de Acceso a los Servicios TI proporciona una serie de **ventajas** a la organización TI que justifican su implantación:

- Mayor garantía de confidencialidad de la información, gracias a un acceso controlado a los servicios.
- Mayor efectividad de los empleados, al minimizarse los conflictos y problemas derivados de la asignación de permisos.
- Menor probabilidad de errores en servicios críticos relacionados con la actividad de usuarios no cualificados.
- Capacidad de monitorizar el uso de los servicios y detectar casos de abuso de los mismos.
- Mayor rapidez y eficacia al revocar permisos en caso de ser necesario, algo que puede ser crítico para la seguridad en determinadas circunstancias.
- La Gestión de Acceso puede, además, ser un requisito indispensable para la adecuación a determinados estándares de calidad e incluso, a la legislación vigente (en el sector sanitario, por ejemplo).

Los **principales retos** a que se enfrenta habitualmente la Gestión de Acceso a los Servicios TI son:

- Verificar la identidad de los usuarios.
- Verificar la identidad de la persona u organismo que autoriza la asignación de permisos.
- Verificar que el usuario está solicitando el acceso a un determinado servicio.
- Integrar múltiples niveles de permisos para un usuario concreto.
- Determinar con rapidez y fiabilidad el nivel de permisos del usuario en cualquier momento.
- Gestionar cambios en los requisitos de acceso de los usuarios.
- Restringir los permisos de acceso a los usuarios no autorizados.
- Mantener una base de datos actualizada donde figuren todos los usuarios y los derechos de los que gozan.

Las actividades de la **Gestión de Acceso a los Servicios TI** incluyen:

- Petición de acceso, que puede llegar por distintas vías como el departamento de RRHH, una solicitud de cambio, una instrucción autorizada…
- Verificación. Se comprueba la identidad del usuario que solicita el acceso, así como de aquellos que lo autorizan. También se examina si los motivos para otorgar el acceso son pertinentes.
- Monitorización de identidad. Los cambios en la asignación de permisos suelen estar asociados a un cambio de estatus dentro de la organización: ascensos, despidos, jubilaciones…
- Registro y monitorización de accesos. La Gestión de Accesos es responsable de asegurar que los permisos que ha otorgado se están usando apropiadamente.
- Eliminación y restricción de derechos. En algunos casos, los derechos pueden ser eliminados por completo: fallecimiento, dimisión, despido, traslados…

6.1.5.2 Petición de acceso

La petición de acceso puede llegar a través de numerosas vías:

- Una petición estándar generada por el sistema de Recursos Humanos. Por ejemplo, al contratar a una persona, al ascenderla, transferirla o cuando abandonan la empresa.
- Una solicitud de cambio (RFC).
- Una petición de servicio enviada por la Gestión de Peticiones.
- Al ejecutar una tarea automática previamente autorizada.

Las reglas para establecer las peticiones de acceso normalmente están documentadas en el Catálogo de Servicios.

6.1.5.3 Verificación

La **Gestión de Acceso** debe verificar cada petición desde dos perspectivas:

- El usuario que solicita el acceso, ¿es realmente quien dice ser?
- ¿Tiene un motivo válido para usar el servicio?

El primer punto se comprueba, habitualmente, comprobando el nombre y la clave del usuario. En la mayor parte de organizaciones, estos datos bastan para acreditar al usuario, aunque depende de las políticas de seguridad y de lo sensible que sea la información registrada en el sistema del servicio (p.ej. datos biométricos).

El segundo punto requiere una comprobación paralela e independiente de la que aporta el usuario. En caso de que se trate de un nuevo empleado, por ejemplo, será necesaria una notificación por escrito procedente del departamento de Recursos Humanos.

6.1.5.4 Monitorización de identidad

A medida que los usuarios trabajan en la organización, sus roles van cambiando y, con ellos, sus necesidades de acceso a servicios. Algunos ejemplos de cambios incluyen:

- **Cambio de tarea**. En este caso, es muy posible el usuario necesite acceso a nuevos servicios, o incluso a otros completamente diferentes.
- **Ascensos**. Lo más probable es que el usuario requiera niveles de permisos superiores en los mismos servicios a los que ya tenía acceso.
- **Dimisión o fallecimiento**. Es preciso eliminar por completo el acceso para evitar que la cuenta de usuario se convierta en un agujero de seguridad.
- **Jubilación**. En muchas organizaciones, los empleados ya retirados todavía conservan el privilegio de acceder a ciertos servicios, como por ejemplo descuentos en sus compras en determinadas plataformas de e-commerce.
- **Acción disciplinar**. En algunos casos, es posible que la organización necesite restringir el acceso durante un tiempo para evitar que el usuario acceda a determinados servicios. Esta circunstancia debería estar prevista en el sistema de asignación de permisos, evitando así tener que eliminar los derechos y luego crearlos de nuevo.
- **Despido**. Cuando un empleado es despedido, o cuando se emprenden acciones legales contra un cliente, el acceso debe ser revocado inmediatamente. Además, la Gestión de Accesos, en conjunto con la Gestión de Seguridad, debe tomar medidas para prevenir, detectar y evitar ataques contra la organización procedentes de ese usuario.

La Gestión de Accesos debe comprender en profundidad el ciclo de vida de cada tipo de usuario y documentarlo. Esto puede servir para automatizar el proceso y ahorrar tiempo.

6.1.5.5 Registro y monitorización de accesos

Además de responder a las peticiones, la **Gestión de Acceso** es responsable de asegurar que los permisos que ha otorgado se están usando apropiadamente. Por este motivo es necesario que la monitorización y control de los accesos esté incluida entre las actividades de las funciones de la Gestión Técnica y Gestión de Aplicaciones y en todos los otros procesos de operación de servicio.

En caso de detectarse abusos, habrá que documentar la situación como una excepción y enviarla a la Gestión de Incidencias para que proceda a su resolución.

La Gestión de la Seguridad de la Información juega un papel fundamental a la hora de detectar accesos no autorizados y en compararlos con los permisos que se habían asignado desde la Gestión de Accesos.

Si se sospecha que un usuario está vulnerando las normas de acceso, haciendo un uso inapropiado de los recursos o utilizando datos de forma fraudulenta, corresponderá la Gestión de Accesos proporcionar evidencias de los datos, tiempos e incluso contenido al que el usuario tiene acceso en determinados servicios.

6.1.5.6 Eliminación y restricción de derechos

Naturalmente, la **Gestión de Acceso** no sólo se encarga de otorgar permisos, sino también de revocarlos o limitarlos.

Las circunstancias que suelen motivar la eliminación de derechos:

- Fallecimiento.
- Dimisión.
- Despido.
- Cambio de roles dentro de la organización, por lo que ya no se necesita acceder al servicio
- Traslado del usuario a otra área donde existe un acceso regional distinto.

6.1.5.7 Control y medición del proceso

La eficacia del proceso de **Gestión de Acceso a los Servicios TI** puede controlarse mediante los siguientes indicadores:

- Número de peticiones de acceso.
- Instancias de acceso garantizado, por servicio, usuario, departamento, etc.
- Instancias de acceso garantizado por derechos de acceso de departamento o individuo.
- Número de incidencias que requirieron la revocación de los permisos de acceso.
- Número de incidencias causados por una configuración incorrecta de los accesos.

6.1.6 Funciones

Una **función** es una unidad especializada en la realización de una cierta actividad y es la responsable de su resultado. Las funciones incluyen todos las capacidades y recursos necesarios para el adecuado desarrollo de dicha actividad.

Las funciones que participan en la fase de Operación del servicio son las responsables de que los servicios cumplan los objetivos solicitados por los clientes y de gestionar toda la tecnología necesaria para la prestación de dichos servicios:

- Centro de Servicios: responsable de todos los procesos de interacción con los usuarios de los servicios TI.
- Gestión de Operaciones TI: responsable de la operación diaria del servicio.
- Gestión Técnica: es una unidad funcional en la que se encuentran todos los equipos, grupos y departamentos involucrados en la gestión y soporte de la infraestructura TI.
- Gestión de Aplicaciones: esta unidad funcional es la responsable de la gestión del ciclo de vida de las aplicaciones TI

6.1.6.1 Centro de Servicios

6.1.6.1.1 Introducción y Objetivos

El objetivo principal, aunque no único, del **Centro de Servicios** es ser el punto de contacto entre los usuarios y la Gestión de Servicios TI.

Un Centro de Servicios, en su concepción más actual, debe funcionar como centro neurálgico de todos los procesos de soporte al servicio:

- Monitorizando y registrando incidencias.

- Aplicando soluciones temporales a errores conocidos en colaboración con la Gestión de Problemas.
- Colaborando con la Gestión de Configuraciones para asegurar la actualización de las bases de datos correspondientes.
- Gestionando las RFCs generadas por los clientes y usuarios mediante peticiones de servicio en colaboración con Gestión de Cambios y Gestión de Entregas y Despliegues.

También debe jugar un papel importante dando soporte al negocio, identificando nuevas oportunidades en sus contactos con clientes y usuarios.

Los clientes demandan, cada vez con mayor frecuencia, un soporte al servicio de alta calidad, eficiente y continuo e independiente de su localización geográfica.

Es esencial para el buen desarrollo del negocio que los clientes y usuarios perciban que están recibiendo una atención personalizada y ágil que les ayude a:

- Resolver rápidamente las interrupciones del servicio.
- Emitir peticiones de servicio.
- Informarse sobre el cumplimiento de los SLAs.
- Recibir información comercial en primera instancia.

El punto de contacto con el cliente puede tomar diversas formas, dependiendo de la amplitud y profundidad de los servicios ofrecidos:

- ***Call Center***: Su objetivo es gestionar un alto volumen de llamadas y redirigir a los usuarios, excepto en los casos más triviales, a otras instancias de soporte y/o comerciales.
- **Centro de Soporte** (*Help Desk*): Su principal objetivo es ofrecer una primera línea de soporte técnico que permita resolver en el menor tiempo las interrupciones del servicio.
- **Centro de Servicios** (*Service Desk*): representa la interfaz para clientes y usuarios de todos los servicios TI ofrecidos por la organización, con un enfoque centrado en los procesos de negocio. Aparte de ofrecer los servicios citados anteriormente, ofrece servicios adicionales a clientes, usuarios y la propia organización TI tales como:
    - Supervisión de los contratos de mantenimiento y niveles de servicio.
    - Canalización de las Peticiones de Servicio de los clientes.
    - Gestión de las licencias de software.
    - Centralización de todos los procesos asociados a la Gestión TI.

Los principales beneficios de una correcta implementación del Centro de Servicios se resumen en:

- Reducción de costes mediante una eficiente asignación de recursos.
- Una mejor atención al cliente, que repercute en un mayor grado de satisfacción y fidelización del mismo.
- Apertura de nuevas oportunidades de negocio.
- Centralización de procesos que mejoran la gestión de la información y la comunicación.
- Soporte al servicio proactivo.

6.1.6.1.2 Implementación

La implementación de un **Centro de Servicios** requiere una meticulosa planificación. En primera instancia deben establecerse los siguientes puntos:

- Cuáles son las necesidades.
- Cuáles han de ser sus funciones.
- Quiénes serán los responsables del mismo.

- Qué cualificaciones profesionales poseerán sus integrantes.
- Si se deben externalizar ciertos servicios como, por ejemplo, el soporte técnico del hardware.
- Qué estructura de Centro de Servicios (distribuido, central o virtual) se adapta mejor a nuestras necesidades y las de nuestros clientes.
- Qué herramientas tecnológicas necesitamos.
- Qué métricas determinarán el rendimiento del Centro de Servicios.

Además de estas cuestiones de carácter técnico, es imprescindible ponderar otros aspectos más directamente relacionados con el "factor humano" y que son tan importantes o más que los puramente técnicos para el éxito del Centro de Servicios:

- Establecer estrictos protocolos de interacción con el cliente.
- Motivar al personal encargado de la relación directa con el cliente.
- Informar a los clientes de los beneficios de este nuevo servicio de atención y soporte.
- Asegurar el compromiso de la dirección con la filosofía del Centro de Servicios.
- Sondear a los clientes para conocer mejor sus expectativas y necesidades.

El objetivo NO es implementar lo más rápidamente posible un Centro de Servicios, sino implantar un Centro de Servicios cuyos objetivos se alineen con nuestros procesos de negocio, mejore la satisfacción de nuestros clientes, optimice la imagen externa de nuestra organización y nos sirva de plataforma para identificar nuevas oportunidades de negocio.

6.1.6.1.3 Estructura

Como ya se ha comentado anteriormente, el **Centro de Servicios** es "EL" punto de contacto de toda la organización TI con clientes y usuarios. Es por lo tanto imprescindible que:

- Sea fácilmente accesible.
- Ofrezca un servicio de calidad consistente y homogéneo.
- Mantenga puntualmente informados a los usuarios y lleve un registro de toda la interacción con los mismos.
- Sirva de soporte al negocio.

Para cumplir estos objetivos es necesario implantar la adecuada estructura física y lógica.

6.1.6.1.3.1 Estructura lógica

Las personas que forman parte del Centro de Servicios deben:

- Conocer todos los protocolos de interacción con el cliente: guiones, checklists…
- Disponer de herramientas software que permitan llevar un registro de la interacción con los usuarios (por ejemplo: una web de gestión de incidencias).
- Tener claro cuando se debe realizar un escalado a instancias superiores o entrar en discusiones sobre cumplimiento de SLAs.
- Tener rápido acceso a las bases de conocimiento para ofrecer un mejor servicio a los usuarios.
- Recibir formación sobre los productos y servicios de la organización TI.

6.1.6.1.3.2 Estructura física

A la hora de elegir la estructura del Centro de Servicios deben tenerse muy presentes las necesidades del servicio: locales, globales, 24x7, etc.

De acuerdo con estos factores, existen distintas opciones que el Centro de Servicios puede adoptar:

- Local
- Centralizado
- Virtual
- 24x7
- Especializado

En la práctica, cada organización configurará su Centro de Servicios de acuerdo con sus circunstancias y necesidades particulares. A continuación, profundizaremos en las opciones enumeradas anteriormente:

6.1.6.1.4 Centro de Servicios Local

Un Centro de Servicios Local está ubicado en el mismo lugar donde están los usuarios a los que atiende. Es muy habitual recurrir a este modelo cuando existen diferencias lingüísticas, políticas o culturales entre la organización y sus usuarios.

- Mayor fluidez en la comunicación con los usuarios.
- Mayor presencia frente a los usuarios

En cambio, su mantenimiento es caro y puede darse el caso de que el volumen de trabajo no sea suficiente para justificar el gasto.

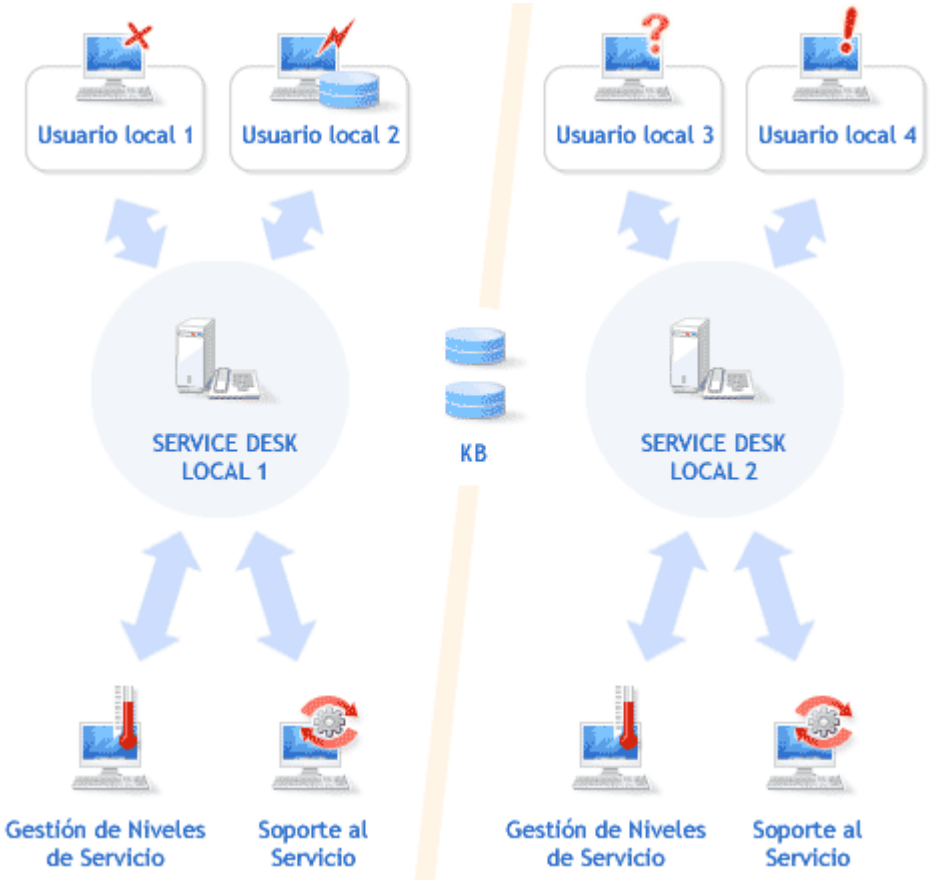


Ilustración 6-6 Centro de servicios local

6.1.6.1.5 Centro de Servicios Centralizado

Si se desea ahorrar costes, se pueden concentrar los centros de servicio locales en uno solo y canalizar el contacto con los usuarios a través de una sola estructura central.

Sus ventajas principales consisten en:

- Se reducen los costes.

- Se optimizan los recursos.
- Se simplifica la gestión.

Sin embargo, surgen importantes inconvenientes cuando:

- Los usuarios se encuentran en diversos emplazamientos geográficos: diferentes idiomas, productos y servicios.
- Es preciso dar servicios de mantenimiento *on-site*.

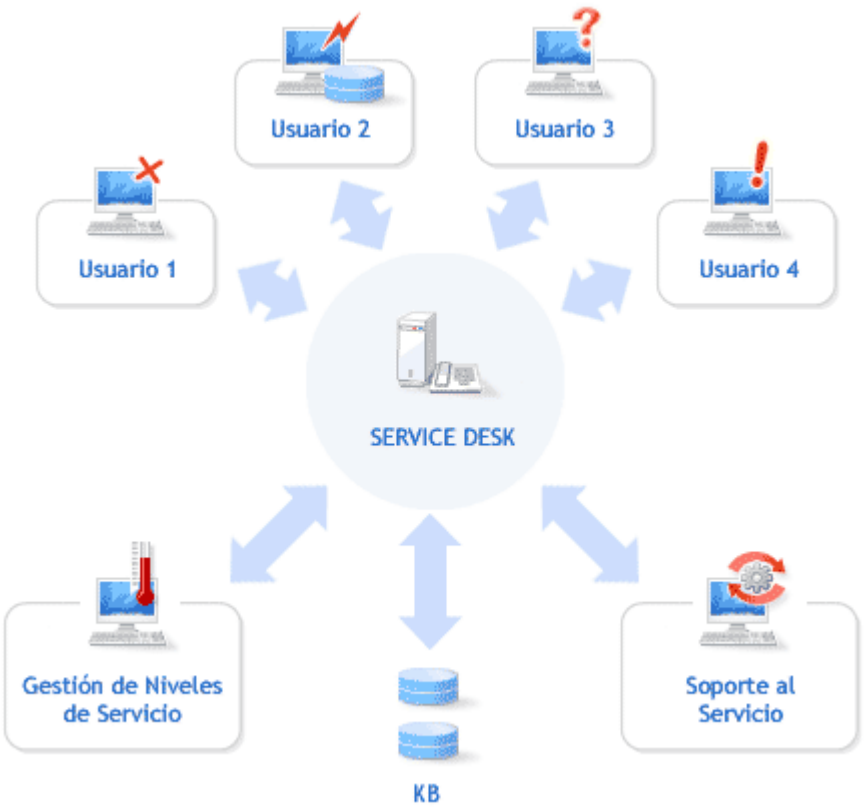


Ilustración 6-7 Centro de servicios centralizado

6.1.6.1.6 Centro de Servicios Virtual

En la actualidad, gracias a que se disponen de rápidas redes de comunicaciones, la situación geográfica de los Centros de Servicios es cada vez más irrelevante. Puede ocurrir que los Centros de Servicios se encuentren ubicados incluso en un continente distinto al que prestan en servicio. Mientras los componentes del Centro de Servicios hablen con fluidez el mismo idioma que los usuarios, no debería haber problema alguno.

El principal objetivo del Centro de Servicios virtual es aprovechar las ventajas de los Centros de Servicios centralizados y distribuidos.

En un Centro de Servicios virtual:

- El conocimiento está centralizado.
- Se evitan duplicidades, con el correspondiente ahorro de costes.
- Es posible ofrecer un servicio local sin incurrir en costes adicionales.
- La calidad del servicio es consistente y homogénea.

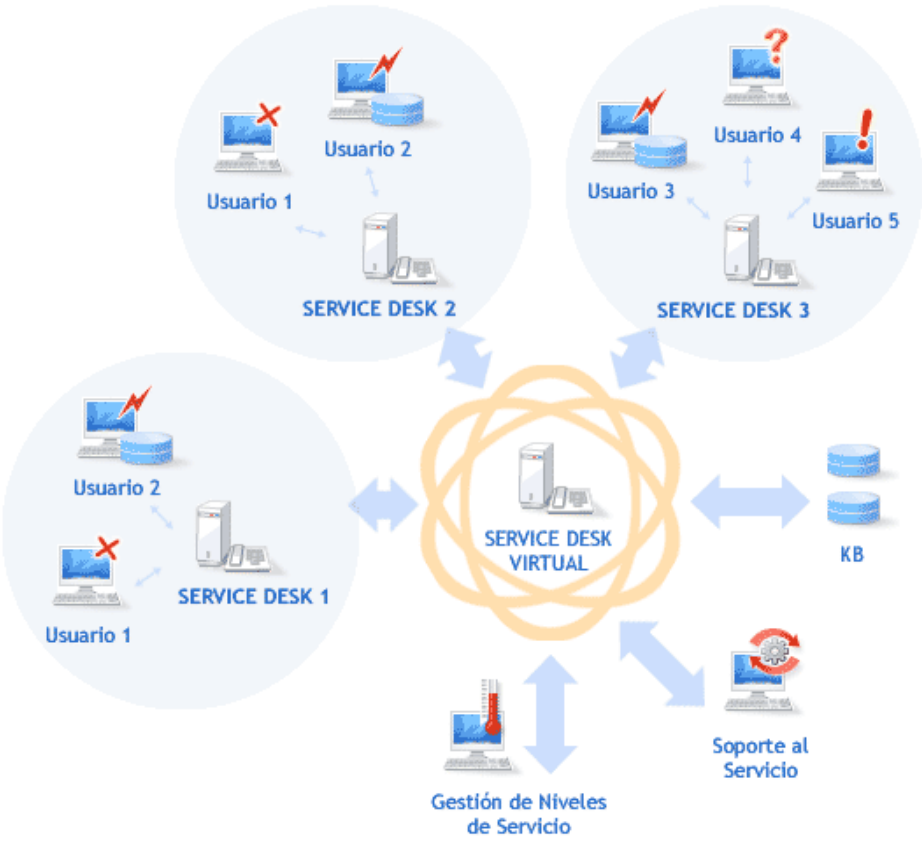


Ilustración 6-8 Centro de servicios virtual

6.1.6.1.7 Centro de Servicios 24/7

Este modelo, también conocido como *follow the sun*, consiste en ubicar una serie de Centros de Servicios Locales en distintas zonas horarias con el fin de cubrir de forma conjunta las 24 horas del día durante los 7 días de la semana. Esta configuración es adoptada principalmente por organizaciones internacionales.

6.1.6.1.8 Centros de Servicios Especializados

En ciertas organizaciones en las que los Servicios IT son muy específicos, las incidencias relacionados con éstos se derivan a grupos especializados mejor capacitados para resolverlos.

6.1.6.1.9 Actividades

Las actividades del **Centro de Servicios** abarcan prácticamente casi todos los aspectos de la Gestión de Servicios TI. No obstante, no debemos olvidar de que su función principal es gestionar la relación con los clientes y usuarios, manteniéndoles puntualmente informados de todos aquellos procesos de su interés.

En los siguientes apartados se describen algunas de las actividades que un Centro de Servicios debería ofrecer.

6.1.6.1.10 Gestión de Incidencias

Independientemente de que la completa gestión de las incidencias requiera la colaboración de otros departamentos y personal, el Centro de Servicios debe ofrecer siempre una primera línea de soporte para la resolución de todas las incidencias y/o peticiones de servicio que puedan cursar los clientes y usuarios.

Entre sus tareas específicas se incluyen:

- Registro y monitorización de cada incidencia.
- Verificación de que el servicio de soporte requerido se incluye en el SLA asociado.
- Seguimiento del proceso de escalado, si procede.
- Identificación de problemas.

- Cierre de la incidencia y confirmación con el cliente.

6.1.6.1.11 Centro de información

El Centro de Servicios debe ser la principal fuente de información de los clientes y usuarios, informando sobre:

- Nuevos servicios.
- El lanzamiento de nuevas versiones para la corrección de errores.
- El cumplimiento de los SLAs.

Este contacto directo con los clientes debe permitir también:

- Evaluar las necesidades de los clientes y usuarios.
- Valorar el grado de satisfacción de clientes y usuarios con el servicio.
- Identificar nuevas oportunidades de negocio.

El Centro de Servicios se encuentra en una posición inmejorable para ofrecer también información privilegiada a todos los procesos de gestión de los servicios TI. Es por ello indispensable que se lleve un correcto registro de toda la interacción con los clientes y usuarios.

6.1.6.1.12 Relaciones con los proveedores

El Centro de Servicios es también el responsable de la relación con los proveedores de servicios de mantenimiento externos.

Para ofrecer un servicio de calidad es imprescindible que el Centro de Servicios canalice el establecimiento de una estrecha relación entre los responsables externos del mantenimiento y la Gestión de Incidencias.

6.1.6.1.13 Control de la unidad

La mejor forma de medir el éxito de un **Centro de Servicios** es medir la satisfacción del cliente, aunque dicha satisfacción no sea responsabilidad exclusiva de éste.

Es importante que se establezcan métricas bien definidas para medir el rendimiento del Centro de Servicios y la percepción que los usuarios tienen de éste.

En los informes de control hay que considerar cuestiones tales como:

- Tiempo medio de respuesta a las solicitudes recibidas por correo electrónico y teléfono.
- Porcentaje de incidencias que se cierran en primera línea de soporte.
- Porcentaje de consultas respondidas en primera instancia.
- Análisis estadísticos de los tiempos de resolución de incidencias organizados según su impacto y urgencia.
- Cumplimiento de los ANS.
- Número de llamadas gestionadas por cada integrante del Centro de Servicios.

Otra tarea de control importante es la supervisión del grado de satisfacción del cliente. Una forma de conseguir esto, es realizar de encuestas que permitan evaluar la percepción del cliente respecto a los servicios prestados.

Una opción sería realizar un control de calidad contactando con el cliente o usuario poco después del cierre de una incidencia o petición para, mediante una serie de preguntas valorar el nivel de calidad percibido por el usuario. Toda la información obtenida, debe ser recopilada y analizada periódicamente para mejorar la calidad del servicio.

6.1.6.2 **Gestión de Operaciones**

6.1.6.2.1 Introducción y Objetivos

La **Gestión de Operaciones** es el proceso responsable del mantenimiento y la gestión continua de la

infraestructura de la organización TI. Se centra especialmente en garantizar que los servicios cumplen los niveles acordados.

A continuación, resumiremos algunos aspectos clave de la Gestión de Operaciones:

- Trabaja para asegurar que un dispositivo, sistema o proceso está funcionando.
- Lleva a cabo los planes.
- Está enfocada a las actividades a corto plazo, aunque éstas generalmente se repiten durante un largo periodo de tiempo.
- El equipo que ejecuta estas actividades ha de estar muy especializado, por lo que a menudo requiere de una formación específica.
- Hay una tendencia a establecer acciones repetitivas y fiables para asegurar el éxito de la operación del servicio.
- Es en la Gestión de Operaciones es donde el valor real de la organización se mide y distribuye.
- Depende directamente de las inversiones tanto en equipamiento como recursos humanos.
- El valor generado debe superar el coste de la inversión y otros gastos indirectos.

Los objetivos de la **Gestión de Operaciones TI** consisten en:

- Mantenimiento del estatus quo de los procesos y actividades de la organización para alcanzar estabilidad en el día a día.
- Escrutinio regular y mejoras para alcanzar un servicio mejorado con costes reducidos, manteniendo la estabilidad.
- Aplicación rápida de habilidades operacionales para diagnosticar y resolver cualquier fallo que ocurra en las operaciones.

6.1.6.2.2 Implementación

Esta labor se desarrolla de acuerdo con los estándares de rendimientos definidos durante la fase de Diseño. Los requisitos generales para que la Gestión de Operaciones desempeñe correctamente su trabajo son:

- Comprender en profundidad cómo se emplea la tecnología para prestar servicios.
- Comprender la importancia relativa y el impacto de esos servicios en el negocio.
- Los procedimientos y manuales que delimitan los roles operacionales tanto en la gestión de la tecnología como en la prestación de servicios.
- Disponer de un conjunto de métricas claramente diferenciadas que informen sobre la culminación de objetivos de servicio, y mantengan informados a los gestores TI sobre la eficiencia y efectividad de las Operaciones TI.
- Los equipos de operaciones TI deben comprender exactamente cómo afecta el rendimiento de la tecnología a la prestación de servicios.
- Una estrategia de gasto orientada a equilibrar los requisitos de las distintas unidades de negocio con los ahorros disponibles gracias a la optimización de la tecnología existente o la inversión en nueva tecnología.
- Una estrategia de inversión basada en retorno del valor, más que retorno del gasto.

6.1.6.2.3 Estructura

En algunas organizaciones, un solo departamento se ocupa de desarrollar las actividades de la **Gestión de Operaciones TI**, mientras que en otros algunas actividades se centralizan y otras las asumen otros departamentos especializados de la organización.

Las dos funciones de la Gestión de Operaciones, que trataremos en profundidad en el siguiente apartado, suelen conformar estructuras organizacionales por sí mismas:

- **Control de Operaciones**, cuya plantilla generalmente se organiza en turnos de operadores encargados de asegurar que las tareas rutinarias se llevan a cabo. El Control de Operaciones también desempeña tareas de monitorización y control, para lo que a menudo recurre a unidades específicas como el Puente de Operaciones o un Centro de Operaciones en Red.
- **Gestión de Instalaciones**, encargada de supervisar el mantenimiento de todo el equipamiento físico. A menudo está ubicada junto a la Gestión Técnica y de Aplicaciones en grandes centros de datos.

6.1.6.2.4 Actividades

Las actividades de la **Gestión de Operaciones TI** tienen una fuerte relación con la monitorización y supervisión, al ser ésta la responsable de que la infraestructura de la organización funcione, especialmente en lo referente a la prestación de servicios.

A continuación, se describen algunas de las funciones que realiza la Gestión de Operaciones TI dentro de la organización.

6.1.6.2.4.1 Control de Operaciones

El objetivo de esta función consiste, tal y como su propio nombre indica, en supervisar la ejecución y monitorización de la prestación de servicios, así como de los eventos relacionados con la infraestructura de la organización. En esta labor pueden colaborar, como ya se ha dicho, el Puente de Operaciones o el Centro de Operaciones en Red.

El Control de Operaciones desempeña las siguientes tareas:

- Gestión de Consolas: determina cómo se va a llevar a cabo la observación central y valora la capacidad de monitorización. Con este objetivo, las consolas son sometidas a ejercicios de monitorización y control de actividades.
- Programación de tareas, que gestiona los trabajos rutinarios o automáticos.
- *Back-up* (respaldo) y restauración de archivos en beneficio de los equipos de Gestión Técnica y de Aplicaciones, así como de los usuarios.
- Gestión de Impresión y salidas, para la recopilación y distribución de documentos impresos u otros entregables electrónicos.
- Actividades de rendimiento o mantenimiento en beneficio de los equipos de Gestión Técnica o de Aplicaciones.

6.1.6.2.4.2 Gestión de Instalaciones

Esta función se ocupa de gestionar el entorno físico de la infraestructura TI: el centro de datos, los cuartos de ordenadores, todo el equipamiento energético y de enfriamiento de los mismos, etc.

La Gestión de Instalaciones también abarca la coordinación de proyectos de consolidación a gran escala, ya que necesitan el despliegue de una infraestructura independiente. Esta función puede contratarse a un proveedor externo, especialmente la gestión del centro de datos.

6.1.6.2.5 Control de la unidad

El rendimiento de la unidad puede monitorizarse mediante la comprobación periódica de los siguientes indicadores:

- Finalización con éxito de las tareas programadas.
- Número de excepciones que se presentaron en las tareas y actividades programadas.
- Número de restauraciones del sistema o de datos requeridas.
- Estadísticas de instalación de equipo, incluyendo el número de elementos instalados por tipo, instalaciones exitosas, etc.
- Métricas del proceso. La Gestión de Operaciones TI ejecuta muchas actividades de otros procesos de la gestión de servicios. Su capacidad para desempeñar este trabajo se cuantificará como parte de las métricas de los otros procesos:

  - Tiempo de respuesta a eventos.
  - Tiempos de resolución de incidencias.
  - Número de incidencias relacionados con la seguridad.
  - Número de escalado de incidencias y razones.
  - Número de cambios implementados y retirados.
  - Número de cambios no autorizados que se detectaron.
  - Número de versiones desplegadas de forma total y exitosa.
  - Rastreo de SIPs.
  - Gasto por comparación al presupuesto.
- Si se delegaron tareas de mantenimiento, entonces las métricas relacionadas con estas actividades también deben reflejar:
  - Rendimiento según planificación.
  - Número de ventanas de mantenimiento superadas.
  - Objetivos de mantenimiento alcanzados (número y porcentaje).
- Las métricas relacionadas con el Mantenimiento de Instalaciones son exhaustivas, y suelen incluir:
  - Costes vs. presupuesto asociado al mantenimiento, construcción, seguridad, reparto, etc.
  - Incidencias relacionadas con el edificio (p.ej. reparaciones)
  - Informes de acceso a las instalaciones.
  - Número de eventos e incidencias relacionados con la seguridad y cómo se resolvieron.
  - Estadísticas de uso eléctrico, especialmente relacionado con cambios en la distribución y las estrategias de responsabilidad ambiental.
  - Eventos o incidencias relacionados con el reparto y la distribución.

6.1.6.3 Gestión Técnica

6.1.6.3.1 Introducción y Objetivos

El objetivo principal de la **Gestión Técnica** consiste en ayudar en la planificación, implementación y mantenimiento de una infraestructura técnica estable para apoyar los procesos de negocio de la organización mediante:

- Una topología técnica bien diseñada, elástica y económica.
- Uso de habilidades técnicas adecuadas para mantener la infraestructura técnica en condiciones óptimas.
- Uso ágil de habilidades técnicas para una diagnosis rápida y resolución de cualquier error técnico que pueda ocurrir.

6.1.6.3.2 Implementación

La **Gestión Técnica** debe procurar que exista un equilibrio entre el nivel de habilidad, la utilización y el coste de los recursos. Se trata de corregir situaciones como, por ejemplo, que se contrate un recurso de alto nivel a un coste elevado y que después sólo se utilice un 10% de sus capacidades.

Algunas de las estrategias a emplear para equilibrar el gasto en recursos en Gestión Técnica son:

- Identificar cuándo se necesitan determinadas habilidades de alto nivel
- Contratar a terceros sólo en los momentos puntuales en que se necesitan sus habilidades.
- Montar un equipo táctico que, además de sus tareas propias, desempeñe tareas que requieran

habilidades específicas.

6.1.6.3.3 Estructura

La estructura de la **Gestión Técnica** depende de las dimensiones de la organización TI. Si ésta es pequeña, a menudo se centralizan las actividades en un solo departamento, mientras que en las de mayor tamaño se subdividen en varios departamentos especializados técnicamente. El criterio principal es, por lo tanto, la especialización: los trabajadores se agrupan de acuerdo con sus habilidades técnicas, que a su vez dependen de la tecnología que hay que gestionar.

Algunos ejemplos de equipos o departamentos de Gestión Técnica:

- Equipo/departamento central
- Equipo/departamento de servidor
- Equipo/departamento de almacenamiento de datos
- Equipo/departamento de soporte de redes
- Equipo/departamento de aplicaciones de escritorio
- Equipo/departamento de base de datos
- Equipo/departamento de software intermedio
- Equipo/departamento del directorio de servicios
- Equipo/departamento de web
- Equipo/departamento de telefonía basada en IP

6.1.6.3.4 Actividades

Las actividades de la **Gestión Técnica** engloban:

- Identificar el conocimiento y experiencia necesarios para prestar servicios y gestionar la infraestructura TI:
    - Documentando las habilidades que posee la organización.
    - Identificando las necesidades de formación.
- Diseñar y desarrollar (aunque no impartir) programas de formación relacionados con los recursos técnicos.
    - Formación técnica de los usuarios.
    - Formación técnica del Centro de Servicios
    - Formación técnica de otros equipos del ciclo de vida.
- La Gestión Técnica a menudo participa en la contratación de:
    - Recursos humanos, cuando no es posible desarrollar las habilidades requeridas debido a que no hay suficiente personal con los conocimientos mínimos requeridos.
    - Comerciales, ya que a menudo los miembros del equipo de la Gestión Técnica son los únicos que saben exactamente los conocimientos técnicos que debe tener un comercial y cómo evaluarlos en los candidatos.
- La Gestión Técnica también se ocupa de definir estándares para:
    - El diseño de nuevas arquitecturas, colaborando además en la definición de las mismas durante las fases de Estrategia y Diseño.
    - Las herramientas de Gestión de Eventos y respuestas “tipo” a ciertos tipos de eventos.
    - Estándares de rendimiento que luego serán usados por la Gestión de la Disponibilidad y la Gestión de la Capacidad.

- La Gestión Técnica participa en el diseño de:
    - Nuevos servicios, interviniendo sobre todo en la arquitectura técnica y las actividades necesarias para gestionar la infraestructura.
    - Tests de funcionalidad, rendimiento y facilidad de uso de los servicios.
- La Gestión Técnica, como garante de todo el conocimiento tecnológico de la infraestructura de la organización TI, pone dicho conocimiento al servicio del resto de la organización en:
    - La Gestión Financiera, determinando los costes de la recursos humanos y tecnológicos que participan en la prestación de servicios.
    - La Gestión de Problemas, ayudando en su diagnóstico y resolución. También contribuye a mantener y validar el KEDB.
    - La Gestión de Incidencias y la Gestión de Problemas, ayudando a definir la forma en la que se codificarán.
    - La Gestión de Incidencias, ya que es habitual que los integrantes de la Gestión Técnica participen como línea de soporte especializado para el Centro de Servicios. También colaboran en la definición de los casos de escalado.
    - La Gestión de Cambios, para evaluar las RFCs, muchas de las cuales son ejecutadas por la Gestión Técnica.
    - Asesoramiento sobre riesgos, identificando dependencias y definiendo contramedidas.
    - La Gestión Técnica suministra información al sistema de Gestión de Configuraciones, y en colaboración con la Gestión de Aplicaciones se ocupa de garantizar que se creen los atributos y relaciones correctas entre CIs, tanto en el despliegue como en el mantenimiento del ciclo de vida de los mismos.
    - En la Mejora Continua del Servicio, apoyando en la tarea de identificar oportunidades de mejora.
    - La Gestión Técnica también participa en la actualización de la documentación del sistema, asegurando que la información esté actualizada y sea bien conocida por el personal.
- La Gestión Técnica, además, se ocupa de investigar y desarrollar soluciones que ayuden a ampliar los servicios, o a simplificar los que ya están en marcha.

6.1.6.3.5 Control de la unidad

La **Gestión Técnica** puede medirse a través de los siguientes indicadores:

- Métricas de los entregables acordados. Esto puede incluir:
    - Contribución a logros para el negocio
    - Porcentajes de transacción y disponibilidad en transacciones de negocio críticas
    - Formación del Centro de Servicios
    - Resolución de problemas de grabación en la KEDB
    - Mediciones de la calidad de los entregables
    - Instalación y configuración de componentes bajo su control
- Mediciones de procesos. Los equipos de Gestión Técnica se ocupan de ejecutar numerosas actividades de otros procesos de la gestión de servicios, como, por ejemplo:
    - Tiempos de respuesta medios a eventos y porcentajes de completado de eventos.
    - Tiempos de resolución de incidencias en segunda y tercera líneas de soporte.
    - Estadísticas de resolución de problemas.
    - Número de incidencias escalados y razones para esos escalados.

  - Número de cambios implementados y retirados.
  - Número de cambios no autorizados detectados.
- Rendimiento de la tecnología.
- Tiempo promedio entre incidencias de determinado equipamiento.
- Medición de las actividades de mantenimiento.
- Formación y desarrollo de habilidades.

6.1.6.4 Gestión de Aplicaciones

6.1.6.4.1 Introducción y Objetivos

La **Gestión de Aplicaciones** tiene como principal objetivo identificar los requisitos funcionales del software de aplicaciones, prestar apoyo en el diseño y desarrollo de dichas aplicaciones y colaborar en el soporte y mejora que siguen a su despliegue.

Para lograr este fin, se precisa:

- Aplicaciones bien diseñadas, elásticas y que optimicen costes.
- Garantizar que la funcionalidad requerida está disponible para alcanzar los resultados de negocio deseados.
- Organizar las habilidades técnicas adecuadas para mantener aplicaciones operacionales en condiciones óptimas.
- Uso ligero de habilidades técnicas para una diagnosis rápida y la resolución de cualquier fallo técnico que pueda presentarse.

La Gestión de Aplicaciones se encarga de que exista un equilibrio entre el nivel de los recursos y su coste.

6.1.6.4.2 Implementación

Es habitual en las organizaciones TI dividir la **Gestión de Aplicaciones** en departamentos según el catálogo de aplicaciones. Esto permite una mayor especialización y un soporte más centrado.

A pesar de que todos los equipos, departamentos o grupos de Gestión de Aplicaciones desempeñan actividades similares, cada aplicación o conjunto de aplicaciones precisa un conjunto específico de requisitos de gestión y operación, en función de:

- El propósito de la aplicación. Los equipos deben tener en cuenta los objetivos de negocio.
- La funcionalidad de la aplicación.
- La plataforma en la que corre la aplicación.
- El tipo/marca de tecnología empleada.

6.1.6.4.3 Estructura

Los equipos y departamentos de **Gestión de Aplicaciones** suelen organizarse según las distintas categorías de aplicaciones a las que dan soporte. Algunos ejemplos típicos son:

- Aplicaciones financieras.
- Aplicaciones de mensajería y colaboración.
- Aplicaciones de RRHH
- Aplicaciones de soporte industrial
- Aplicaciones de automatización de fuerza de ventas (CRM)
- Aplicaciones de procesamiento de ventas.
- Aplicaciones del centro de llamadas y marketing

- Aplicaciones específicas del negocio (sanidad, seguros, banca, etc.)
- Aplicaciones TI, como Centro de Servicios, Sistemas de Gestión de la Empresa (SKMS, CMS, etc.)
- Portales web.
- Tienda online.

6.1.6.4.4 Actividades

Mientras la mayoría de equipos/departamentos de **Gestión de Aplicaciones** se dedican a aplicaciones específicas o conjuntos de ellas, existen ciertas funciones comunes, que cómo se observará coinciden con las del proceso de Gestión Técnica:

- Ayudar a la Gestión Técnica en la tarea de identificar el conocimiento y experiencia necesarios para gestionar las aplicaciones a la hora de prestar servicios TI.
- Diseñar y desarrollar (aunque no impartir) programas de formación destinados al usuario final. Aunque otros equipos o incluso terceros pueden ser quienes la impartan finalmente, la Gestión de Aplicaciones es responsable de que ésta sea adecuada.
- La Gestión de Aplicaciones también interviene en labores de contratación:
    - En caso de que ciertas habilidades no se puedan desarrollar a nivel interno (por falta de personal o de nivel), la Gestión de Aplicaciones es la encargada de seleccionar y contratar los recursos adecuados.
    - Comerciales, ya que a menudo los miembros del equipo de la Gestión de Aplicaciones son los únicos que saben exactamente los conocimientos técnicos que debe tener un comercial y cómo evaluarlos en los candidatos.
- La Gestión de Aplicaciones también se encarga de definir estándares para
    - Diseñar nuevas arquitecturas, participando además en la definición de las mismas durante las fases de Estrategia y Diseño.
    - Las herramientas de Gestión de Eventos y respuestas “modelo” a ciertos tipos de eventos.
    - Estándares de rendimiento que luego serán utilizados por la Gestión de la Disponibilidad y la de la Capacidad.
- La Gestión de Aplicaciones interviene en el diseño de:
    - Nuevos servicios, contribuyendo a la definición de la arquitectura técnica y rendimiento estándar, así como en la adecuación a los niveles de servicio preestablecidos. Además, la Gestión de Aplicaciones es responsable de especificar las actividades necesarias para mantener dichas aplicaciones.
    - Tests de funcionalidad, rendimiento y manejabilidad de servicios.
- La Gestión de Aplicaciones, como guardiana del conocimiento relacionado con las aplicaciones, lo pone al servicio del resto de la organización en:
    - La Gestión Financiera, identificando el coste de las aplicaciones que intervienen en la prestación de servicios.
    - La Gestión de Problemas, ayudando a diagnosticar y resolver aquellos que guardan relación con las aplicaciones.
    - La Gestión de Incidencias y la de Problemas, ayudando a definir los sistemas de codificación de los mismos.
    - La Gestión de Incidencias, ya que es habitual que los equipos de la Gestión Técnica actúen como línea de soporte especializado para el Centro de Servicios. También participan en la definición de los casos de escalado.
    - La Gestión de Cambios, para evaluar las RFCs, muchas de las cuales son ejecutadas por la Gestión de Aplicaciones.

- Asesoramiento sobre riesgos, identificando dependencias y definiendo contramedidas.
- La Gestión de Aplicaciones es, a menudo, quien dirige el despliegue de las nuevas versiones durante la fase de Transición.
- La Gestión de Aplicaciones proporciona información al sistema de Gestión de Configuraciones, y en colaboración con la Gestión Técnica garantiza que se creen los atributos y relaciones correctas entre CIs, tanto en el despliegue como en el mantenimiento del ciclo de vida de los mismos.
- En la Mejora Continua, ayudando en la tarea de identificar oportunidades de mejora.
- Colaborar en la actualización de la documentación del sistema, garantizando que la información está actualizada y es bien conocida por el personal.
- Participar en las actividades operacionales que se llevan a cabo como parte de la Gestión de Operaciones.
- La Gestión de Aplicaciones también contribuye a mantener actualizadas las políticas de configuración de software.

- Investigación y desarrollo de soluciones que ayuden a expandir el Porfolio de Servicios o al menos a mejorar la prestación de los mismos.
- Proporcionar asesoramiento en riesgos, identificando servicios críticos y dependencias de sistema y definiendo e implementando contramedidas.

6.1.6.4.5 Control de la unidad

Las métricas que reflejan el rendimiento de la **Gestión de Aplicaciones** dependen de las aplicaciones que se estén gestionando, pero las más típicas son:

- Métricas de los entregables acordados. Esto puede incluir:
  - Capacidad de los usuarios para acceder a la aplicación y sus funcionalidades.
  - Reportes y archivos enviados a los usuarios.
  - Porcentajes de éxito y disponibilidad para determinadas transacciones críticas para el negocio.
  - Formación del Centro de Servicios.
  - Registro de resolución de problemas en el sistema de Gestión del Conocimiento.
  - Percepción que los usuarios tienen de la calidad, en comparación con los requisitos definidos en los SLAs.
- Métricas de procesos
  - Tiempo de respuesta a eventos y porcentajes de finalización.
  - Tiempos de resolución de incidencias en la segunda y tercera líneas de soporte.
  - Estadísticas de resolución de problemas.
  - Número de incidencias escaladas y razones que motivaron su escalado.
  - Número de cambios implementados y revertidos.
  - Número de cambios no autorizados que se detectaron.
  - Número de versiones desplegadas (total y exitosas)
  - Problemas de seguridad detectados y resueltos
  - Utilización real del sistema comparada con las previsiones del Plan de Capacidad.
  - Seguimiento de sesiones.

  - Gasto en comparación con el presupuesto.
- Rendimiento de aplicaciones. Estas métricas se basan en las especificaciones de la fase de Diseño y el rendimiento técnico contenido en los OLAs. Suelen incluir:
  - Tiempos de respuesta.
  - Disponibilidad de la aplicación.
  - Integridad de los datos e informes.
- Métricas de las actividades de mantenimiento.
  - Mantenimiento llevado a cabo según la planificación.
  - Número de ventanas de mantenimiento que se prolongaron.
  - Objetivos de mantenimiento alcanzados (número y porcentaje)
- Probabilidad de la colaboración entre los equipos de Gestión de Aplicaciones y los equipos de Desarrollo de Aplicaciones en proyectos. Métricas de:
  - Tiempo invertido en proyectos.
  - Satisfacción del cliente y el usuario con el entregable del proyecto.
  - Costes de involucrarse en el proyecto.
- Formación y desarrollo de habilidades. Estas métricas garantizan que la plantilla tiene las habilidades y formación necesarias para gestionar la tecnología de la que son responsables, además de identificar áreas en las que se requiere formación adicional.

6.1.7 Puesta en marcha

6.1.7.1 Introducción y Objetivos

Una de las principales dificultades para la adecuada puesta en marcha de la fase de Operación del Servicio se encuentra en el "abismo" que hay entre teoría y práctica.

Las fases previas del ciclo de vida del servicio se han ocupado de diseñar, planificar y desplegar una serie de procesos que ahora han de ponerse en marcha y es frecuente que ello conlleve las siguientes dificultades:

- Los responsables del diseño no conocen en detalle las complicaciones asociadas a las labores de mantenimiento y tareas recurrentes de la fase de operación con las consiguientes consecuencias indeseables:
  - Se toman "atajos" que rompen con las buenas prácticas de gestión.
  - Se crean resistencias a la aplicación de los protocolos diseñados.
- No se han asignado los recursos necesarios para implementar correctamente la fase de operación y el personal la percibe como una nueva capa "burocrática" que sólo dificulta su trabajo.
- Las estructuras de gestión no son lo suficientemente flexibles y por tanto no son capaces de asimilar la complejidad de los nuevos procesos y actividades.
- Las métricas definidas se centran en exceso en aspectos "internos" de la organización TI y obvian importantes aspectos "externos" relativos a la percepción de los clientes.

Para impedir que todo esto ocurra es imprescindible:

- Involucrar al personal de operación en el diseño de los servicios.
- Asegurarse una rápida evaluación del impacto de todos los cambios en la fase de operación.
- Que el personal a cargo de la fase de operación disponga desde el primer momento de todas las herramientas y tecnología necesarias para desempeñar correctamente su función según los protocolos preestablecidos.

6.1.7.2 Monitorización y control

La **monitorización** consiste en la observación atenta de una determinada situación con el fin de detectar cambios a lo largo del tiempo. En el contexto de la fase de Operación del servicio, la monitorización implica:

- Monitorizar los CIs y actividades clave.
- Asegurarse de que se cumplen las condiciones establecidas y, en caso contrario, advertir al grupo adecuado.
- Asegurar que el rendimiento y utilización de los componentes, sistemas, etc. están dentro de un rango previsto.
- Detectar niveles anormales de actividad en la infraestructura.
- Detectar cambios no autorizados.
- Asegurar el cumplimiento de las políticas de la empresa.
- Rastrear las salidas al negocio y garantizar que casan con los requisitos de calidad y rendimiento acordados.
- Rastrear cualquier información empleada para medir los KPIs.

El modelo más extendido para definir el control es el **Ciclo de Monitorización-Control**. Este ciclo puede ser de dos tipos:

- **Ciclo Abierto**: se programan actividades específicas sin tener en cuenta las condiciones del entorno. Un backup periódico, que se lanza con independencia de las circunstancias, es un buen ejemplo de control de ciclo abierto.
- **Ciclo Cerrado**: se monitoriza un entorno con el fin de responder sólo a los cambios que se produzcan. Un ejemplo de esto sería un balance de carga de una red, en el que se ejercen tareas de control sólo si la monitorización indica que se está sobrepasando el tráfico normal.

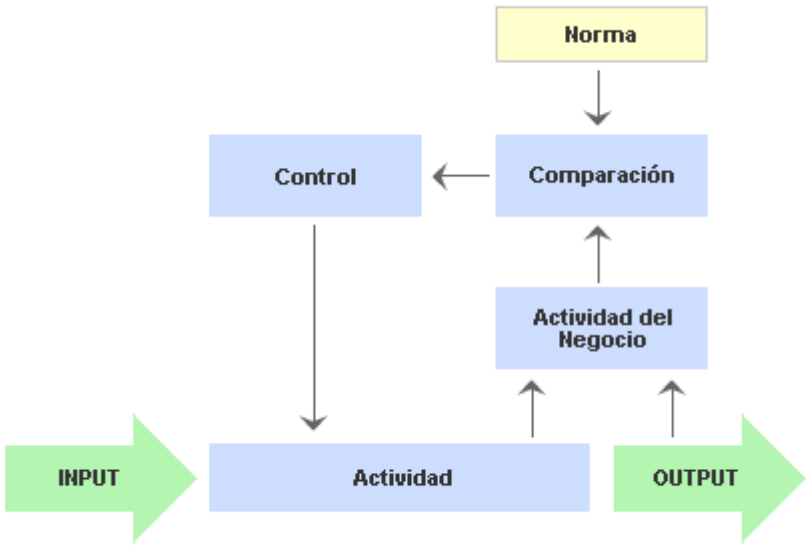


Ilustración 6-9 Ciclo de Monitorización-Control

La monitorización tiene dos niveles de actuación:

- **Monitorización y control interno**, cuando desde un equipo o departamento se controlan los elementos y actividades de esa misma unidad.
- **Monitorización y control externo**, cuando un equipo o departamento realiza el control de elementos y actividades que dependen de otros grupos, procesos o funciones.

Podemos distinguir distintos tipos de monitorización según tres factores:

- **Monitorización activa vs. pasiva**. La monitorización activa consiste en hacer una comprobación directa del estado de un sistema o dispositivo. La pasiva, en cambio, genera y transmite eventos a un agente de monitorización de forma automática. La pasiva es más frecuente, reservándose la activa para la diagnosis.
- **Monitorización reactiva vs. proactiva**. La primera está diseñada para ejecutar acciones al producirse cierto tipo de eventos o fallos. La monitorización proactiva, por otro lado, se utiliza para detectar los patrones de eventos que predicen el fallo de un dispositivo.
- **Medición continuada vs. basada en excepciones**. La medición continua enfoca la monitorización como un registro del rendimiento en tiempo real, mientras que la medición basada en excepciones se limita a notificar las interrupciones.

6.1.7.3 Factores de éxito y riesgos

Entre los factores de éxito y retos a los que se debe confrontar la correcta implementación de la Fase de Operación del Servicio se encuentran:

- Contar con el personal convenientemente formado sobre los procesos y actividades necesarias para una correcta gestión del servicio.
- Disponer del adecuado soporte tecnológico que facilite y automatice, siempre que sea posible, las actividades asociadas a la gestión y prestación del servicio.
- Contar con el apoyo necesario de los órganos de dirección de la organización TI para disponer de las capacidades y recursos y necesarios.
- Disponer de las métricas adecuadas para evaluar la calidad de la operación del servicio.
- Generar los informes y documentación necesarios para la futura mejora del servicio.
- Trabajar en estrecha colaboración con las unidades de negocio para conocer sus necesidades y garantizar que estas son cubiertas.

Los principales riesgos se resumen en:

- Diseños defectuosos del servicio que impiden una operación eficiente.
- Recursos y capacidades insuficientes.
- Falta de soporte de la organización TI.

6.2 Relación con otros ciclos

Aunque la fase de Operación del Servicio tenga entidad propia no puede ser correctamente interpretada sin conocer sus interrelaciones con las otras fases del Ciclo de Vida del Servicio.

La fase de operación recibe sus datos de entrada principales de la fase de Transición del Servicio y a su vez sirve de principal entrada de datos a la fase de Mejora del Servicio.

6.2.1 Operación y Estrategia

La fase de Operación es la más importante desde el punto de vista del cliente, los servicios pueden ser adecuados y estar bien diseñados, pero si el eslabón de la operación falla los resultados no serán los buscados y la percepción del cliente será negativa.

Por lo tanto, un factor esencial en el enfoque estratégico de los servicios es asegurar que son operacionalmente viables.

Recíprocamente, la Operación del Servicio debe de resultar en la fuente más fiable sobre las demandas y restricciones de los clientes que servirán de guía para dar forma a la estrategia más adecuada.

6.2.2 Operación y Diseño

Un factor esencial en el diseño del servicio es tener en cuenta la operativa del mismo.

El diseño debe:

- Ser usable
- Ser sostenible y escalable.
- Ofrecer la funcionalidad requerida.
- Ser eficiente.
- Cumplir los protocolos de seguridad requeridos.
- Permitir el acceso sólo al personal autorizado.

Para conseguir estos objetivos los responsables de la Fase de Diseño deben recibir la información necesaria de la Fase de Operación sobre el uso de los servicios y las percepciones de los clientes.

6.2.3 Operación y Transición

La Operación del Servicio debe suministrar a los responsables de la fase de Transición toda la información relevante sobre:

- El entorno de producción.
- El conocimiento asociado (incidencias, percepción de clientes y usuarios, …) a servicios similares a los que se han de desplegar.

La Transición del Servicio debe poner a disposición de la fase de Operación:

- Toda la documentación necesaria asociada al uso y mantenimiento de los nuevos o actualizados servicios.
- La información relativa a los procesos de prueba y evaluación.

6.2.4 Operación y Mejora Continua

La fase de Mejora Continua del Servicio depende directamente de la fase de Operación pues ésta representa la principal fuente de información para la optimización de los procesos y actividades involucrados en la prestación del servicio.

Los informes generados en la fase de Operación del Servicio deben, en particular, incorporar información detallada sobre:

- Incidencias en la prestación del servicio.
- Soluciones propuestas a los problemas detectados en la fase de operación.
- Peticiones de los usuarios y clientes.

7 MEJORA CONTINUA DEL SERVICIO

La fase de Mejora Continua del Servicio se basa en el principio de que todos los servicios son susceptibles de ser mejorados.

Los principales objetivos de esta mejora son:

- Adaptarse a las necesidades cambiantes del cliente.
- Mejorar la satisfacción del cliente.
- Conseguir un mayor retorno de la inversión.

Pero este objetivo de mejora sólo se puede alcanzar mediante la continua monitorización y medición de todas las actividades y procesos involucrados en la prestación de los servicios:

- **Conformidad**: los procesos se adaptan a los nuevos modelos y protocolos.
- **Calidad**: se cumplen los objetivos establecidos en forma y plazo.
- **Rendimiento**: los procesos son eficientes y rentables para la organización TI.
- **Valor**: los servicios ofrecen el valor esperado y se diferencian de los de la competencia.

Los **principales objetivos** de la fase de Mejora Continua del Servicio se resumen en:

- Proponer mejoras para todas las actividades y procesos que participan en la gestión y prestación de los servicios.
- Analizar y monitorizar los parámetros de seguimiento de Niveles de Servicio y contrastarlos con los SLAs en vigor.
- Recomendar mejoras que aumenten el ROI y VOI asociados a los servicios.
- Dar soporte a la fase de estrategia y diseño para la definición de nuevas actividades, procesos y servicios asociados a los mismos.

Los resultados de esta fase del ciclo de vida han de verse reflejados en **Planes de Mejora del Servicio** que incorporen toda la información necesaria para:

- Mejorar la calidad de los servicios prestados.
- Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- Mejorar y hacer más eficientes los procesos internos de la organización TI.

7.1 Ciclo de Deming

El ciclo **PDCA**: *Plan* (Planificar), *Do* (Hacer), *Check* (Verificar) y *Act* (Actuar) también conocido como **ciclo de Deming** en honor a su creador, Edwards Deming, forma la columna vertebral de todos los procesos de mejora continua:

- **Plan:** definir los objetivos y los recursos para conseguirlos.
- **Do:** implementar la visión preestablecida.
- **Check:** comprobar que se alcanzan los objetivos previstos con los recursos asignados.
- **Act:** analizar y corregir las desviaciones detectadas respecto a los objetivos previstos, así como recomendar mejoras a los procesos utilizados.

La fase de **Mejora Continua del Servicio** tiene un papel fundamental en las etapas de Check y Act, aunque

también debe participar en las etapas de Plan y Do:

- Colaborando en la definición los objetivos y las métricas de cumplimiento asociadas.
- Monitorizando y valorando la calidad de los procesos involucrados.
- Definiendo y supervisando las mejoras propuestas.

7.2 Métricas

Para poder mejorar algo, primero hay que conocerlo, y para conocerlo es necesario poder medirlo. Por ello, es imprescindible que la organización TI defina una serie de métricas que permitan valorar si se han conseguido alcanzar los objetivos propuestos, así como la calidad y rendimiento de las funciones y procesos que han participado.

Una organización TI debe utilizar tres tipos de métricas:

- **Técnicas o Tecnológicas**: miden la capacidad, disponibilidad y rendimiento de las aplicaciones e infraestructuras.
- **De procesos**: miden la calidad y el rendimiento de los procesos de gestión de los servicios.
- **De servicios**: valoran los servicios ofrecidos en términos de sus componentes individuales.

Las métricas deben adaptarse a los **Factores Críticos de Éxito** (CSFs) que describen aquello que debe ocurrir para que se cumplan los objetivos que se hayan establecido. Asociados a cada CSF es necesario definir una serie de **Indicadores Críticos de Rendimiento** (KPIs) que permitan evaluar la calidad y el rendimiento de los procesos, así como su adecuación y valor.

Los KPIs deben medir aspectos cualitativos y cuantitativos y deben permitir valorar el cumplimiento de los objetivos.

Si la organización TI se ha propuesto, por ejemplo, como CSF la mejora en la atención al usuario los KPIs incluirían:

- Tiempo medio de respuesta.
- Tiempo medio de resolución de las incidencias.
- Adecuación de los procesos de escalado.
- Percepción de los usuarios respecto a la atención prestada mediante encuestas de satisfacción.

Es importante que los KPIs no obvien aspectos clave y que su cumplimiento sea una medida objetiva del cumplimiento de los CSFs asociados. Por ejemplo, en el caso anterior no se hace mención a los costes y una reducción de los mismos podría ser parte de los objetivos preestablecidos por lo que en ese caso los KPIs utilizados no proporcionarían todas las métricas necesarias.

7.3 DIKW

DIKW es el acrónimo de:

- ***Data*** (Dato): o materia prima, que está compuesta de mensajes o símbolos sin procesar, por ejemplo, la lista de elementos de configuración de una infraestructura TI.
- ***Information*** (Información): que proviene del análisis de un conjunto de datos, que, por ejemplo, se correspondería en el caso anterior a una distribución de proveedores por inversiones y tecnologías utilizadas.
- ***Knowledge*** (Conocimiento): este proviene del proceso de interpretación de la información en términos de experiencia y reflexión. Por ejemplo, ciertos proveedores tecnológicos que participan en servicios clave corren el riesgo de no saberse adaptar al mercado y utilizar tecnologías que pueden

quedar obsoletas a corto plazo.

- ***Wisdom*** (Sabiduría): la capacidad de tomar la mejor decisión posible basada en el conocimiento, información y datos disponibles. Por ejemplo, optar por cambiar de proveedor tecnológico para minimizar los riesgos asociados a depender de proveedores que no están correctamente alineados con las necesidades futuras del negocio.

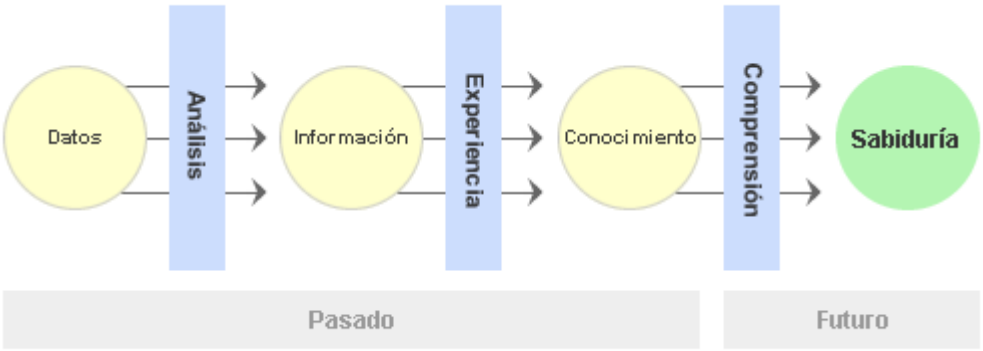


Ilustración 7-1 DIKW

La sabiduría es el componente esencial en lo que respecta al proceso de Mejora Continua. A partir de los datos, información y conocimiento obtenidos durante todas las fases del ciclo de vida del servicio se deben elaborar unos Planes de Mejora que incorporen los cambios necesarios para aumentar la satisfacción del cliente mejorando el rendimiento, calidad y gestión de todos los procesos implicados.

7.4 Modelo CSI

Nunca podremos saber si hemos llegado si primero no decidimos adónde queremos ir.

El proceso de Mejora Continua requiere de una serie de metas y objetivos que determinen la dirección de avance y sirvan de pilares para el resto de las actividades involucradas en el mismo.

Pero la determinación de esas metas y objetivos está asimismo sometido a un proceso de constante revisión que forma parte de un ciclo descrito por el **modelo CSI.**

Este ciclo continuo se compone de 6 fases:

- **Establecer la visión:** se deben establecer metas y objetivos alineados con el modelo de negocio de la organización.
- **Conocer el estado actual:** saber de dónde partimos (organización, recursos, capacidades, procesos…) para poder utilizar ese estado como referencia de base.
- **Establecer objetivos cuantificables:** a partir de la visión establecer hitos y entregables que permitan realizar un seguimiento del proceso.
- **Planificar:** establecer un SIP (Plan de mejora de Servicio) que determine las acciones requeridas para obtener los objetivos buscados en los plazos previstos y con el nivel de calidad predeterminado.
- **Comprobar:** valorar si los planes se han cumplido y si se han seguido lo procesos establecidos.
- **Integrar los cambios:** asegurase de que los cambios realizados forman parte de la cultura de la organización permitiéndonos así reiniciar el ciclo con nuevo impulso.

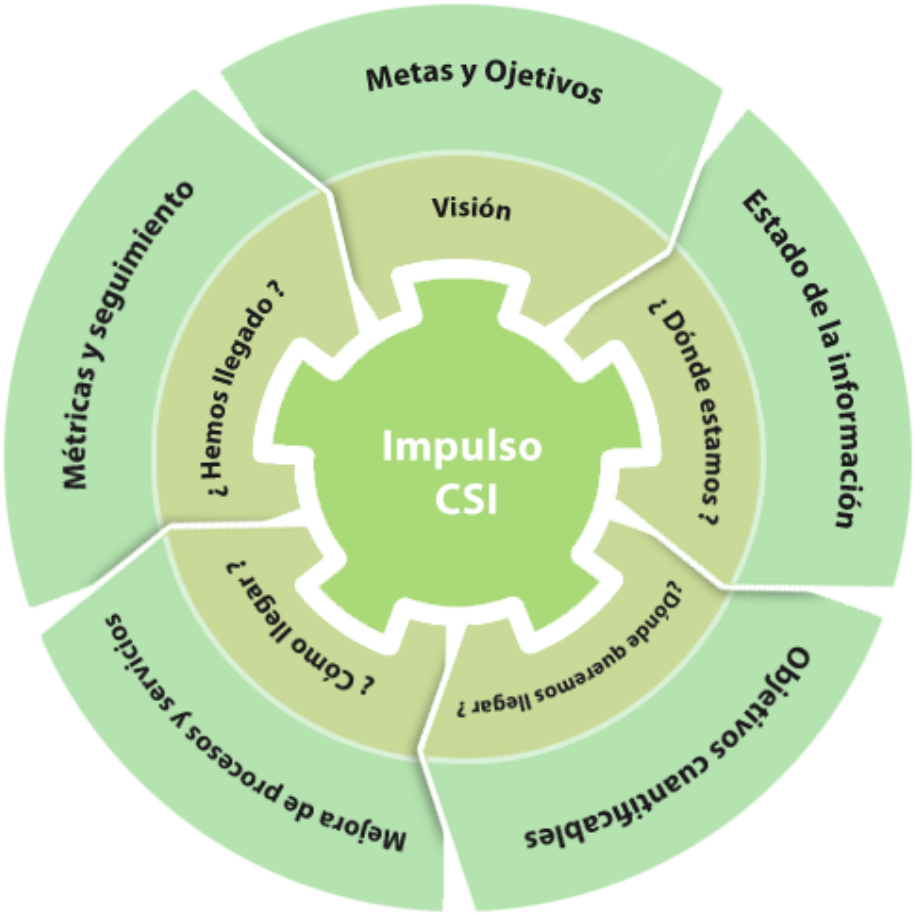


Ilustración 7-2 Ciclo del modelo CSI

7.5 Herramientas y metodologías

Una mejora propuesta no siempre implica una mejora real. Incluso tras exhaustivos procesos de análisis y planificación de las posibles mejoras se han podido obviar aspectos críticos o imponderables que pueden afectar negativamente a los servicios y procesos. Es indispensable disponer de metodologías y herramientas que permitan valorar las mejoras introducidas y comparar el "estado de situación" antes y después de la introducción de los cambios.

Es imposible enumerar todas las herramientas y metodologías disponibles por lo que aquí nos centraremos en algunas de las más populares. Éste listado, aunque manifiestamente incompleto, puede servirnos como punto de partida para ahondar en el tema.

7.5.1 Análisis comparativo

Consiste en comparar el rendimiento de las actividades y procesos llevados a cabo por la organización con aquellos que han sido considerados como "mejores prácticas".

Este análisis puede ser realizado a distintos niveles:

- Interno: comparando con otros procesos o funciones de la propia organización.
- Externo: comparando con otras organizaciones competidoras o directamente con los estándares del sector.

Los resultados de este análisis deben incluir:

- Información sobre el rendimiento de la organización.
- Factores de éxito y riesgos.
- Propuestas sobre nuevas líneas de actuación.

7.5.2 Análisis de brechas (Gap analysis)

El análisis de brechas se basa en contrastar el "estado de la situación actual" y el "estado esperado o ideal". Las diferencias entre ambas situaciones suponen las brechas que se desea eliminar.

Este análisis se puede realizar a diferentes niveles: estratégico, táctico y operativo.

7.5.3 Análisis DAFO

Se centra en el análisis de las **Debilidades**, **Amenazas**, **Fortalezas** y **Oportunidades**.

Las Debilidades y Fortalezas son de carácter interno y dependientes en este caso de la propia organización TI mientras que las Amenazas y Oportunidades provienen de factores de mercado u otros factores externos.

El **análisis DAFO** puede realizarse a diferentes niveles, desde una componente o función hasta englobar a toda la organización TI.

Sus principales objetivos consisten en:

- Determinar las Debilidades y buscar métodos para eliminarlas.
- Valorar las Amenazas e intentar minimizar su impacto.
- Conocer las propias Fortalezas y buscar la mejor manera de rentabilizarlas.
- Estudiar las Oportunidades y desarrollar estrategias que permitan aprovecharlas.

7.5.4 Cuadro de Mando Integral (CMI)

Es un método diseñado por Robert Kaplan y David Norton para evaluar la actividad de una organización en términos de cumplimiento de su plan estratégico.

El **Cuadro de Mando Integral** (CMI) propone analizar la actividad de una organización respecto a diferentes perspectivas:

- Financiera
- Clientes
- Procesos
- Innovación y Aprendizaje

Es imprescindible determinar los KPIs asociados a cada una de estas perspectivas y cuáles son los objetivos buscados. Se recomienda buscar un conjunto reducido de KPIs que luego pueda ir ampliándose con el tiempo para evitar CMIs excesivamente complejos que dificulten su implementación.

7.6 Procesos de la fase de Mejora Continua del Servicio

Los principales procesos asociados directamente a la **fase de Mejora del Servicio** son:

- Proceso de Mejora: este es un proceso compuesto por siete pasos que describen como se deben medir la calidad y rendimiento de los procesos para que se generen los informes adecuados que permitan la elaboración de un SIP.
- Informes de Servicios TI: es el responsable de la generación de los informes que permiten valorar los servicios ofrecidos y los resultados de las mejoras propuestas.

7.6.1 Proceso de Mejora CSI

7.6.1.1 Introducción y Objetivos

El **Proceso de Mejora Continua** (CSI) tiene como misión implementar el ciclo de Deming para la mejora de los servicios TI.

El CSI permite a la organización TI:

- Conocer en profundidad la calidad y rendimiento de los servicios TI ofrecidos.
- Detectar oportunidades de mejora.
- Proponer acciones correctivas.
- Supervisar su implementación.

Para que el CSI sea efectivo tiene, además, que adaptarse a la visión y estrategia del negocio. Sin unos objetivos claros es imposible determinar cuáles han de ser los aspectos prioritarios en el proceso de mejora y la organización TI puede terminar volcando sus esfuerzos en aspectos irrelevantes para el desarrollo del negocio.

El **Proceso de Mejora CSI** se compone de siete pasos que permiten, a partir de los datos obtenidos, elaborar Planes de Mejora del Servicio que modifiquen procesos o actividades susceptibles de optimización:

- Paso 1: qué debemos medir
- Paso 2: qué podemos medir
- Paso 3: recopilar los datos necesarios.
- Paso 4: procesar los datos (información).
- Paso 5: analizar los datos (conocimiento).
- Paso 6: proponer medidas correctivas (sabiduría).
- Paso 7: implementar las medidas correctivas.

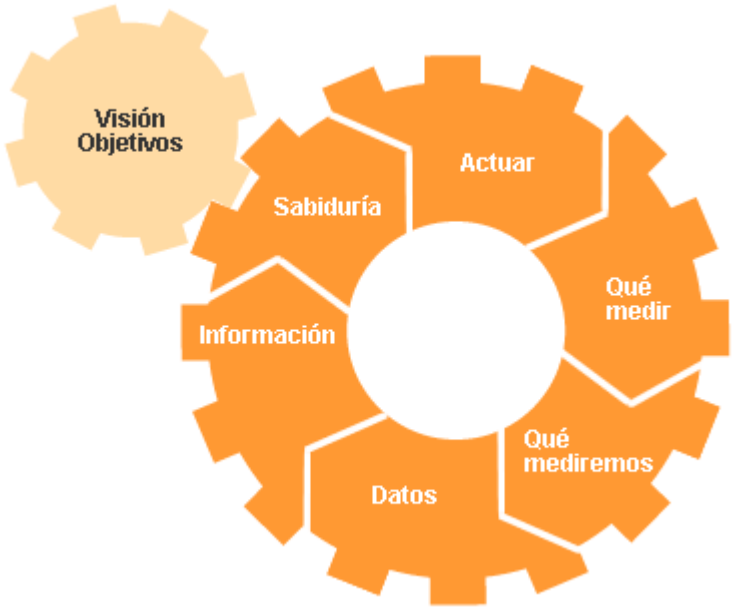


Ilustración 7-3 Pasos proceso de mejora CSI

Es imprescindible tener en cuenta cuál es la visión y estrategia de la organización TI con el objetivo de que aquello que se mide se alinee con las necesidades de negocio.

El proceso de medición nunca debe ser un objetivo en sí mismo y debe ser periódicamente revisado para

asegurar su continua adecuación a los objetivos marcado por la gestión de los servicios TI.

Es necesario contar con referencias que permitan procesar y analizar correctamente los datos obtenidos. Estas referencias pueden ser internas de la organización, datos obtenidos previamente, o externas, como las provenientes de "mejores prácticas" como la propia ITIL.

Las principales actividades del **Proceso de Mejora Continua** se resumen en:

- Decidir qué se debe medir.
- Definir lo que finalmente se medirá.
- Realizar dichas mediciones.
- Procesar los datos recogidos.
- Analizar la información recabada.
- Proponer y documentar posibles mejoras en base al conocimiento adquirido.
- Implementar las mejoras propuestas.

7.6.1.2 Qué medir

Es imposible iniciar el **proceso de Mejora Continua** sin una idea clara de que es aquello que, en principio, debemos mejorar. Luego, en primer lugar, debemos conocer en profundidad la misión y estrategia previamente trazados por los máximos responsables de la organización TI de acuerdo con las necesidades de negocio.

A partir de esa información y de la recogida a través de:

- El catalogo actual de servicios.
- Los SLAs en vigor: compromisos alcanzados con nuestros clientes.
- Los SLRs: peticiones y requisitos expresados para que los servicios se adecúen a las necesidades del negocio.
- Información de carácter legal y financiero.

Debemos determinar aquello que se debe medir, así como los CSFs y KPIs correspondientes.

En todo este proceso es necesaria la colaboración de los propietarios del servicio que conocen en profundidad las actividades necesarias para la prestación de los servicios y los procesos de gestión asociados.

7.6.1.3 Qué se puede medir

Cuando ya dispongamos de una lista de todo aquello que deseamos medir es necesario asegurarse que nuestros objetivos son realistas.

En algunos casos puede ocurrir, ya sea porque no se dispone de las herramientas necesarias o simplemente porque la organización carece del grado de madurez necesario, que no se puedan implementar, con una mínima garantía de éxito, ciertas métricas.

Para limitar los procesos de medida a aquellos realmente asequibles a la organización TI es necesario tener en cuenta los:

- Procesos de medida ya existentes.
- Informes generados.
- Flujos de trabajo establecidos.
- Protocolos y procedimientos en vigor.

Tras el análisis de la situación debe generarse:

- Una lista de definitiva de métricas, CSFs y KPIs a implementar
- Un informe con los requisitos necesarios (recursos y capacidades) para llevar a cabo las mediciones

propuestas.

Es importante tener en cuenta a la hora de alcanzar un compromiso sobre lo que realmente se va a medir cuáles son los riesgos de ignorar ciertas métricas:

- ¿Se puede resentir gravemente la calidad de los servicios prestados?
- ¿Se puede ver seriamente afectado el rendimiento de algún proceso?

Por otra parte, sólo aquello que sea finalmente medible debe incorporarse a los SLAs.

7.6.1.4 Recopilación de datos

Una vez decidido lo qué se va a medir hay que decidir cómo y ponerse manos a la obra.

Aunque muchas de las mediciones se pueden realizar de forma automática monitorizando la actividad de la organización TI en algunos casos esto no es posible, por ejemplo, en lo que respecta a la calidad de los informes emitidos, el cumplimiento de ciertos protocolos, etcétera.

Es importante que cada proceso de medición tenga claramente asignada la persona responsable del mismo, que ésta disponga de las herramientas automáticas necesarias y se haya definido claramente el procedimiento.

Las actividades habituales en el proceso de medición incluyen:

- Definición del calendario o frecuencia de toma de datos (en el caso automático este proceso puede ser continuo).
- Análisis de las herramientas necesarias para el proceso de medición y registro.
- Instalación, configuración, personalización y pruebas de funcionamiento de dichas herramientas.
- Analizar la disponibilidad y capacidad de la infraestructura necesaria.
- Monitorizar la calidad y adecuación al propósito de los datos recogidos: establecer métricas.
- Preparar los datos para que sean accesibles y útiles.
- Documentar todo el proceso.

7.6.1.5 Procesamiento de datos

Para que los datos sean de utilidad deben ser previamente procesados para que sean inteligibles y útiles desde la perspectiva de negocio.

Este proceso debe transformar los datos en información para así estar dispuesta para su posterior análisis. Esto no es posible sin la previa realización de ciertas tareas:

- Definir las necesidades de procesamiento en función de la estrategia predefinida.
- Analizar los SLAs vigentes para determinar los que información puede ser de utilidad para evaluar su cumplimiento.
- Establecer protocolos para el procesamiento de datos:
    - Frecuencia:
        - Tiempo real
        - Por lotes (diariamente, semanalmente...)
    - Procedimientos:
        - Estructuración de los datos
        - Evaluación de la calidad de los datos
- Determinar los recursos y capacidades necesarios.
- Seleccionar e instalar las herramientas a utilizar.

- Formar el personal asignado a las tareas de procesamiento de datos.
- Definir la estructura de los informes a entregar (plantillas).

Como resultado de todo ello los responsables del proceso de análisis deben recibir los informes correspondientes en un formato eminentemente práctico (obviando información no relevante para el negocio) que permita su correcta interpretación.

7.6.1.6 Análisis de datos

El análisis de la información previamente "digerida" permite transformar a esta en "conocimiento" orientado a determinar cuáles son los aspectos susceptibles de mejora.

El principal objetivo del análisis es comprobar que:

- Se cumplen los SLAs.
- Los servicios son rentables y eficientes.
- Se siguen los procedimientos preestablecidos.
- Los servicios TI cumplen los objetivos propuestos y dan soporte a la estrategia de negocio.

Es de particular importancia analizar las tendencias pues estas nos permiten prever a corto y medio plazo posibles problemas u oportunidades.

7.6.1.7 Creación de informes

El último paso, antes de entrar en lo que es la propia "acción correctiva", es utilizar toda la información y conocimiento adquiridos a través de los pasos anteriores del proceso para permitir la toma de decisiones con "conocimiento de causa".

Esto se debe hacer mediante la presentación de informes específicamente orientados a los diferentes agentes involucrados en la gestión y prestación de los servicios TI. Se deben ajustar tanto los contenidos como el estilo de presentación (técnico, conceptual...) a cada público objetivo:

- Dirección.
- Gestores TI.
- Personal técnico.
- Clientes y usuarios.

El objetivo principal de estos informes es ofrecer "inteligencia" a la organización TI y sus clientes para mejorar la calidad del servicio y alinearlo con las necesidades de negocio.

Es recomendable establecer una estructura clara y, en la medida de lo posible, estandarizada para toda la documentación generada que facilite el acceso a la información relevante a cada público objetivo. La documentación no debe ser excesivamente prolija y debe centrarse exclusivamente en los elementos que aporten valor.

Si es posible, todos los informes generados deben estar disponibles en una intranet/extranet que permita el rápido acceso (con la jerarquía de permisos adecuada) a toda la información relevante con diferentes grados de profundidad.

Los informes deben ser una herramienta eminentemente práctica. Si el público al que van dirigidos los considera farragosos o se requiere un excesivo esfuerzo para la extracción de información relevante serán probablemente ignorados y todo el proceso se verá gravemente afectado.

7.6.1.8 Acciones correctivas

Todo este complejo **proceso de Mejora Continua** sería poco más que una pérdida de tiempo y dinero sino aseguramos que las medidas correctivas propuestas son correctamente implementadas.

Sin embargo, es conveniente establecer un calendario realista para la implementación de dichas mejoras. No es

siempre la mejor solución poner en marcha simultáneamente todas las mejoras propuestas.

Es imprescindible establecer prioridades que respondan a las prioridades del negocio en términos de su estrategia y visión. Una vez hecho esto las mejores propuestas han de pasar por la fase de Diseño (desarrollo) y Transición (despliegue) para su despliegue, antes de incorporarse a la decisiva fase de Operación.

Durante todo este proceso es indispensable seguir midiendo y analizando para asegurar que no han cambiado las necesidades o estrategia de negocio y asegurar que todos los agentes implicados están correctamente informados y han sido capacitados para afrontar los cambios previstos.

7.6.1.9 Control y medición del proceso

El proceso de mejora continua es a la vez susceptible de aplicarse a sí mismo, aunque, claro está, deban evitarse bucles infinitos :).

El CSI debe aplicarse los mismos fundamentos que postula por lo que el ciclo de 7 pasos que lo componen debe ser utilizado para monitorizar el propio proceso de mejora y proponer las mejoras que se consideren oportunas.

Para todo ello es necesario determinar:

- Los objetivos de los propios planes de mejora.
- Las métricas que se aplicaran para evaluar dicho proceso.
- Los datos que es necesario recopilar.
- La información y conocimiento que se generan de ellos.
- Los informes o inteligencia que se esperan generar.
- Como se implementarán dichos cambios.

Es imprescindible que todo el proceso este adecuadamente documentado y se incorporen evaluaciones periódicas de todo el proceso.

Se designará un gestor del CSI que será responsable de:

- Gestionar toda la comunicación asociada al proceso.
- Asignar y monitorizar los recursos disponibles.
- Determinar las principales áreas de mejora en colaboración con la dirección y los propietarios de los diferentes servicios.
- Elaborar el Plan de Mejora del servicio en colaboración con la Gestión de Niveles de Servicio.
- Supervisar todo el proceso y garantizar que se adecúa a los objetivos propuesto en concepto y forma.

7.6.2 Informes de Servicios TI

7.6.2.1 Introducción y Objetivos

Es imposible realizar proyecciones, establecer estrategias y proponer mejoras si se desconoce el estado actual de las cosas. El proceso de **Gestión de Informes** tiene como principal objetivo proporcionar a todos los agentes implicados en la gestión de los servicios TI una visión objetiva, basada en datos y métricas, de la calidad y rendimiento de los servicios prestados.

Este proceso tiene como *input* los datos recopilados a través de toda la organización TI y ofrece como output una serie de informes que aporten el conocimiento necesario para implementar mejoras funcionales, estructurales o para el negocio.

Por su naturaleza este proceso requiere la estrecha colaboración de los otros procesos pues sin ésta se carecerá del adecuado punto de partida para determinar qué datos deben ser registrados, procesados, analizados y posteriormente “digeridos” y presentados como informes.

El objetivo principal de la **Gestión de Informes** consiste en mantener puntualmente informados a los responsables y personal de la organización TI sobre la calidad, rendimiento de los actuales servicios TI y desarrollos realizados o planificados cara al futuro.

La Gestión de Informes es esencial para:

- Garantizar que todos los responsables de la gestión de procesos TI disponen del conocimiento necesario para tomar decisiones informadas.
- Se dispone de todas las métricas necesarias para evaluar de forma global la calidad de los servicios prestados.
- Crear un marco unificado para la generación y difusión de informes que simplifique el acceso a la información.

Los **beneficios** de una correcta gestión de este proceso se resumen en:

- Ofrecer al conjunto de la organización TI una instantánea periódica sobre el estado de los servicios TI prestados.
- Facilitar la toma de decisiones estratégicas en base a información objetiva.
- Comunicar la percepción de los clientes y usuarios sobre la calidad de los servicios ofrecidos.

Las **principales dificultades** a las que se enfrenta la gestión de Generación de Informes incluyen:

- No están bien delimitadas las responsabilidades de cada uno de los agentes implicados.
- La recogida de datos no se realiza correctamente o la calidad de los datos es deficiente.
- Los informes generados son meramente técnicos y apenas aportan "inteligencia" al negocio.
- La presentación de los informes no se adecua a su público objetivo: insuficiente información gráfica, lenguaje excesivamente técnico, falta de precisión…

Las principales actividades de la **Gestión de Informes** de servicios TI se resumen en:

- Selección y recopilación de los datos necesarios para la generación de informes.
- Procesado y análisis de los datos para su posterior uso.
- Preparación de los contenidos para los diferentes públicos objetivo.
- Publicación de los informes predeterminados.

7.6.2.2 Recopilación de datos

Los modernos sistemas TI son capaces de registrar, manipular y procesar ingentes cantidades de datos, capacidad que no comparten sus gestores, al menos mientras las máquinas no nos sustituyan en tareas de "alto nivel" :).

Es por ello imprescindible que desde el mismo inicio del proceso de recogida de datos para la elaboración de informes se seleccionen y filtren los aquellos susceptibles de aportar valor al negocio y a la gestión de los procesos TI.

Es necesario determinar en primaria instancia:

- Qué informes se generarán.
- Cuáles son los datos que se necesitan.
- A quién van a ir dirigidos los informes.
- Qué nivel de detalle incluirán.
- Qué formato se utilizará.

Esto permitirá a los responsables del proceso optimizar las actividades necesarias de recogida de datos.

No debemos caer en la tentación de pensar que los datos nunca sobran. Aunque si bien es cierto que al simple

nivel de registro es posible y conveniente guardar la mayor cantidad posible de datos, ya que el coste de esta operación es marginal, la recopilación y preparación de los datos para su posterior análisis y proceso puede ser una tarea infinitamente más compleja y devoradora de recursos, tanto tecnológicos como humanos.

7.6.2.3 Análisis de datos

Una vez recopilados los datos necesarios es necesario **procesarlos y analizarlos** de forma que ofrezcan información útil al negocio y a los responsables de los servicios TI.

Todos los datos e información deben transformarse en conocimiento de forma que los receptores de los informes generados puedan tomar decisiones inteligentes sobre las acciones que se deban tomar (proceso DIKW).

Durante el proceso y análisis de los datos se deben destacar aquellos que han tenido un impacto apreciable en el pasado y puedan tener un impacto futuro. Los datos no son sólo una fuente necesaria para tomar acciones correctivas sino también pueden ser de utilidad para futuras decisiones estratégicas o de marketing.

Durante el proceso de análisis se deben evaluar la calidad y cantidad de los datos corregidos y proponer los cambios necesarios para asegurar que se dispone de la información necesaria para evaluar la calidad y rendimiento de los servicios TI prestados.

7.6.2.4 Generar documentación

Tras procesar y analizar toda la información recopilada es el momento de darle forma a través de informes para proceder a su comunicación a su público objetivo.

Los informes deben ser claros y comprensibles a sus lectores. Por ejemplo, todos los informes dirigidos a los responsables del negocio deben obviar complicados aspectos técnicos que no aporten valor para la toma de decisiones de carácter estratégico.

En principio los diferentes públicos objetivos incluyen:

- Los responsables del negocio: los informes que tengan este grupo como destinatario deben concentrarse en aspectos relacionados con el cumplimiento de los compromisos de nivel de servicio recogidos en los SLAs.
- Los gestores de procesos TI: están principalmente interesados en la calidad y rendimiento de los procesos TI y deben ser informados sobre el cumplimiento de los CSFs y KPIs.
- Personal técnico: necesita información (métricas, KPIs) que les permita mejorar aspectos operativos en la prestación de servicio TI.

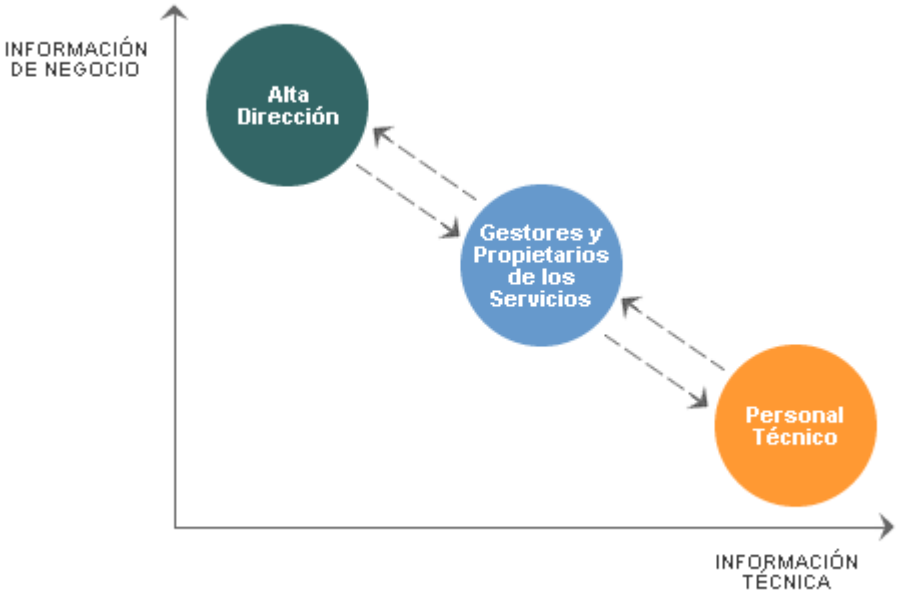


Ilustración 7-4 Públicos objetivos de la documentación

Cuando esto sea posible se debe mostrar la información de una forma gráfica que permita su rápida interpretación y oriente a los responsables sobre los aspectos que necesitan una lectura más detallada y productiva.

7.6.2.5 Control y medición del proceso

Los responsables del proceso de **Generación de Informes** deben velar por la calidad y adecuación al propósito de toda la documentación generada y al mismo tiempo generar los informes necesarios para el control y seguimiento del propio proceso.

La documentación generada sobre las actividades llevadas a cabo por el proceso de Generación de Informes de incluir:

- Calendarios de entrega de toda la documentación aportada:
  - Descripción individual de los informes generados
  - Destinatarios
- Informes sobre las características y calidad de los datos recogidos:
  - Origen
  - Calidad de los mismos
  - Periodicidad: continua, diaria, semanal, mensual...
  - Recogida manual o automática
- Metodologías utilizadas para el procesado y análisis de los datos.
- Recursos utilizados.
- *Feedback* recibido: dirección, gestores y propietarios de servicios y procesos, personal técnico
- Propuestas de mejora.

En particular los gestores deberán velar porque los informes:

- Estén correctamente escritos en un lenguaje sencillo y directo.
- Contengan toda la información necesaria.

- Faciliten la "digestión" de la información a través de gráficas y diagramas.
- Tengan una dimensión y profundidad acorde con las necesidades y conocimientos de sus destinatarios.
- Sean fácilmente accesibles a todas las personas a las que van dirigidos.

7.6.3 Puesta en marcha

La puesta en marcha de esta fase puede ser bastante compleja y requiere una preparación previa que asegure la calidad de sus resultados:

- Se dispone de una clara visión de los objetivos.
- Se han elaborado planes de comunicación para informar a todos los agentes implicados y garantizar que estos comprenden la importancia del proceso de mejora continua.
- Todas las métricas requeridas han sido definidas y se dispone de las herramientas necesarias para su utilización.
- Está disponible la estructura organizativa necesaria y los roles necesarios se hayan cubiertos.
- Existe una estrategia para implementar ágilmente los cambios que puedan tener un impacto positivo sin grandes costes y/o esfuerzo para impulsar el CSI.

7.6.3.1 Caso de negocio

Una de las herramientas básicas para la puesta en marcha del CSI es la realización de un "Caso de Negocio" que permita evaluar, en términos del negocio, los potenciales beneficios de la implantación del CSI.

Este caso de negocio debe ofrecer una clara respuesta a preguntas iniciales tales como:

- ¿Cuáles son nuestros objetivos?
- ¿Dónde nos encontramos respecto a esos objetivos?
- ¿Qué necesitamos para alcanzarlos?
- ¿Cuál será el retorno previsto?
- ¿Cómo se evaluará lo obtenido?

Que se deberán complementar con la progresiva implantación del CSI en respuestas a:

- ¿Se han cumplido los objetivos?
- ¿Qué otras posibles mejoras podemos implementar?

Como parte de este caso de negocio es imprescindible establecer de forma explícita:

- Los costes:
  - Personal
  - Formación
  - Tecnología
  - Gestión
  - Comunicación
- Los beneficios esperados en términos de:
  - Mejoras en la calidad y rendimiento de servicios y procesos
  - Retorno a la Inversión (ROI)
  - Valor de la Inversión (VOI): que incluye aspectos de valor añadido de difícil medida a corto plazo: satisfacción del cliente, recompensas emocionales para la fuerza de trabajo…

7.7 Relación con otros ciclos

La fase de **Mejora Continua del Servicio** debe estar, por su propia naturaleza, estrechamente ligada a todas las restantes fases del ciclo de vida del servicio. La fase de mejora Continua del servicio recibe inputs de todas las demás fases y debe proporcionar input a cada una de ellas pues su objetivo es mejorar tanto la calidad de los servicios prestados como todos los procesos de gestión asociados.

7.7.1 Mejora continua y estrategia

En un mundo en constante desarrollo tecnológico las estrategias no deben ser inamovibles. La estrategia debe ser continuamente rediseñada atendiendo a múltiples factores.

La Mejora del Servicio debe ofrecer información a la fase de Estrategia sobre aspectos que pueden ser optimizados, tales como calidad y rendimiento, pero esto siempre debe hacerse partiendo de la perspectiva de negocio establecida durante la fase de estrategia.

7.7.2 Mejora Continua y Diseño

La satisfacción de los clientes depende en gran medida de los procesos y actividades desarrolladas en la fase de diseño:

- ¿Resulto la capacidad suficiente?
- ¿Se cumplieron los SLAs?
- ¿Se tuvieron en cuenta los requisitos del cliente?

Si esto no fuera así es necesario introducir planes de mejora que minimicen o eliminen los problemas encontrados y aporten una guía para las mejoras necesarias en las soluciones y arquitecturas empleadas.

7.7.3 Mejora Continua y Transición

La principal misión de la fase de Mejora Continua es mejorar todos los procesos y tareas involucrados en la prestación del servicio con el objetivo último de mejorar la calidad, rendimiento y rentabilidad de estos y la consecuente percepción de clientes, usuarios y organización TI.

La fase de Transición es clave en este aspecto. Los cambios son la fuente principal de incidencias y problemas tanto a nivel interno (componente tecnológica) como a nivel externo (calidad del servicio).

La fase de Mejora Continua es por sí misma una de las principales fuentes de cambio introduciendo mejoras en los procesos y ajustando la calidad y rentabilidad de los servicios.

7.7.4 Mejora Continuación y Operación

La fase de Mejora Continua del Servicio depende directamente de la fase de Operación pues ésta representa la principal fuente de información para la optimización de los procesos y actividades involucrados en la prestación del servicio.

Los informes generados en la fase de Operación del Servicio deben, en particular, incorporar información detallada sobre:

- Incidencias en la prestación del servicio.
- Soluciones propuestas a los problemas detectados en la fase de operación.
- Peticiones de los usuarios y clientes.

8 GESTIÓN Y MANTENIMIENTO DE LOS PUNTOS DE INFORMACIÓN DE LA ETSI DE SEVILLA

En este apartado se va a representar cómo se plantearía un servicio de gestión y mantenimiento de los puntos de información que hay en la Escuela Técnica Superior de Ingenieros (ETSI) de siguiendo las recomendaciones de ITIL. Se planteará un escenario ficticio en el que no se trabaja siguiendo estas recomendaciones y se observará como se van aplicando en la descripción del servicio.

8.1 Escenario inicial

La Escuela Técnica Superior de Ingenieros cuenta con una serie de puntos de información en sus instalaciones del Edificio Plaza de América. Dichos puntos de información se corresponden con unas pantallas situadas en las plantas baja y primera y de un servidor de contenidos situado en el centro de cálculo en la entre planta 2. Este sería el plano de la situación actual:

Ilustración 8-1 Mapa planta baja

Ilustración 8-2 Mapa planta 1ª

Ilustración 8-3 Mapa Entreplanta 2

Las pantallas de los puntos información se conectan con el servidor de contenidos a través de la red interna del edificio:

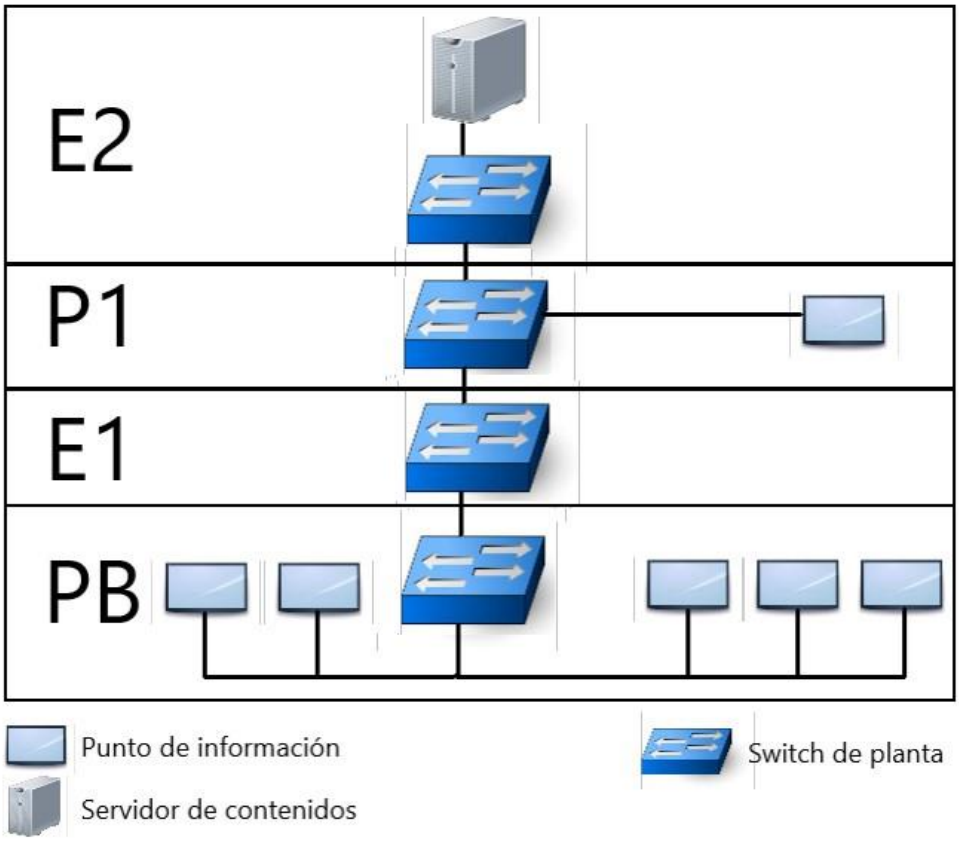


Ilustración 8-4 Mapa de red del servicio

En total hay 6 pantallas y un servidor central. En los siguientes apartados se describen estos elementos

8.1.1 Pantallas

El modelo de pantalla instalado en los puntos de información es el modelo TX-40ES513 del fabricante Panasonic. A continuación, se muestran sus especificaciones:

Ilustración 8-5 Pantallas usadas en el servicio

Pantalla		Panel	LED LCD
		Bright Panel	Bright Panel
		Resolución de la pantalla	1,920 (W) x 1,080 (H)
		Unidad de Panel	800 Hz BMR
		Modo de imagen	Dinámico / Normal / Cine / Cine verdadero / Usuario
		Contraste	Alto Contraste
		Adaptive Backlight Dimming	Sí
Calidad de sonido		Surround	VR-Audio True Surround
		Altavoces	Full Range x 2
		Salida de altavoz	20 W (10 W x 2)
		Modo sonido	Estándar/Música/Ambiente/Usuario
Funciones inteligentes	my Home Screen		Sí
	Guía por voz		Sí
	EPG		Sí
	Idiomas de menú en pantalla		27 idiomas*12
	Sintonizador HD idéntico/Sintonizador triple HD		— / Sí
	LAN inalámbrica integrada		Sí
	Panasonic Media Center (aplicación)	Panasonic Media Center (aplicación)	—
		TV Anywhere	—
		In-House TV Streaming	Sí (cliente)
	Aplicaciones Panasonic TV Remote	Aplicaciones Panasonic TV Remote	Sí
		Swipe & Share	Sí
		Calibración inteligente	—

	Internet Apps	Internet Apps	Sí
		Explorador web	Sí
	Réplica de pantalla sencilla		Sí
	DLNA		Sí (DTCP-IP/DMP/DMR/DMS)
	Bluetooth		—
	Control de IP doméstica (Crestron/Control4)		Sí
	Media Player	Media Player	Sí
		Compatibilidad con formatos	AVI/HEVC/MKV/WMV/MP4/M4v/FLV/3GP P/VRO/VOB/TS/PS, MP3/AAC/WMA Pro/FLAC/Apple Lossless/WAV, JPEG
	HbbTV		Sí
	Recepción de teletexto		1000P
	Multi ventana		PAT
	Grabación de USB-HDD (con rebobinado de emisión de TV en directo)		Sí
	Modo Hotel		Sí
	Modo videojuegos		—
	Control HDAVI		Sí
Información energética		Proveedor de Marcas	Panasonic
		Modelo ID	TX-40ES513E
		Clase de eficiencia energética	A+
		Tamaño de pantalla visible (en diagonal)	100 cm/40 pulgadas
		Promedio de consumo de energía en modo Encendido	44 W
		Consumo anual de energía	62 kWh
		Consumo energético en Standby	0,50 W

		Consumo de energía en Modo Apagado	0.30 W
		Alimentación	AC 220 - 240 V, 50/60 Hz
		Resolución de la pantalla	1,920 (W) x 1,080 (H)
		Consumo energético	77 W
		Sensor de ambiente (CATS)	Sí
Terminal	Recepción de sintonizador digital		DVB-T/T2/DVB-S2/DVB-C
	Sintonizador analógico		Sí
	HDMI	HDMI	2 (traseros)
		HDMI (4K 60/50p con HDCP2.2)	—
		Compatibilidad de las características	Canal de retorno de audio (entrada 2)
	USB		2 (2 laterales, USB 2.0 x 2)
	Puerto LAN		1
	CI (Common Interface)		1 (CI Plus, Versión 1.3)
	Tarjeta SD		—
	conector SCART		—
	Entrada video por componentes compartidos con compuesto		RCA phono type x 1 (rear)
	Salida de audio digital (Óptico)		1 (trasero)
	Salida de Auriculares		1 (cara)
General		Accesorio incluido	TV Remote
		Dimensiones (A x A x P) (sin soporte)	902 x 521 x 90 mm
		Peso (sin soporte)	8.0 kg
		Dimensiones (An. x Al. x F.) (con pedestal)	902 x 561 x 202 mm
		Peso (con soporte)	9.5 kg

	Compatible con VESA	Sí
	Dimensión VESA	200 x 200 mm
	Unidad en caja exterior (anchura x altura x profundidad)	983 x 649 x 154 mm
	Peso total de unidad en caja	12.0 kg

Tabla 8-1 Especificaciones pantalla

8.1.2 Servidor de contenidos

El servidor de contenidos es un HP ProLiant MicroServer Gen10 con las siguientes especificaciones

Ilustración 8-6 Servidor de contenidos

Procesador	Frecuencia	1,6 GHz
	Modelo	AMD Opteron X3216
	Número de núcleos	2
	Tipo de caché	L2
	Cantidad de caché	1 MB
	Frecuencia en modo turbo	3 GHz
Memoria	Memoria Interna	8 GB
	Tipo de memoria interna	DDR4-SDRAM
	Memoria interna máxima	32 GB
	Ranuras de memoria	24 DIMM
	Velocidad de memoria	2400 MHz

	ECC	Sí
Puertos e interfaces	Cantidad de puertos USB 2.0	2
	Cantidad de puertos VGA (D-Sub)	1
	Ethernet LAN (RJ-45) cantidad de puertos	2
	Cantidad de puertos tipo A USB 3.0 (3.1 Gen 1)	4
	Cantidad de DisplayPorts	2
Peso y dimensiones	Ancho	235 mm
	Profundidad	230 mm
	Altura	254 mm
Control de energía	Suministro de energía redundante (RPS), soporte	No
	Fuente de alimentación	200 W
	Número de fuentes de alimentación	1
Conexión	Ethernet	Sí
	Controlador LAN	Broadcom BCM5720
	Tipo de interfaz ethernet	Gigabit Ethernet
Almacenamiento	Tamaño de disco duro	3.5"
	Interfaz del disco duro	SATA
	Compatibilidad con RAID	Sí
	Capacidad máxima de almacenaje	16 TB
	Niveles RAID	0, 1, 10
	Compatibilidad con Hot-Plug	No
	Número de discos duros soportados	4
	Número de discos duros instalados	2
	Modelo discos duros instalados	WD NAS Red 4TB SATA3
	Capacidad discos duros instalados	4 TB
Aprobaciones reguladoras	Certificado Energy Star	No

Diseño	Tipo de chasis	Ultra Micro Tower
	Tipo de unidad óptica	No

Tabla 8-2 Especificaciones del servidor

8.2 Necesidades de la ETSI

La ETSI requiere que los puntos de información estén operativos la mayor cantidad de tiempo posible durante su horario de apertura. Dado que no dispone de recursos propios especializados en el mantenimiento de este hardware ha decidido contratar con un proveedor externo un servicio de mantenimiento.

La ETSI exigirá que el servicio cumpla con los siguientes requisitos:

- Disponibilidad de los puntos de información el mayor tiempo posible durante el horario de apertura del centro.
- La cobertura horaria del servicio deberá ser similar al horario de apertura de la ETSI.
- La comunicación de las incidencias y peticiones deberá poder realizarse por diferentes vías.
- El proveedor deberá responder a la incidencia o petición como máximo una hora después de su comunicación.
- Las incidencias deberán quedar resueltas cómo máximo un día después de su comunicación.
- El proveedor tendrá que aportar los recursos humanos y materiales necesarios para el servicio de mantenimiento.
- La gestión de la garantía del hardware será llevada a cabo por el proveedor.
- El proveedor realizará una revisión preventiva de los equipos con al menos una periodicidad de un año.
- La ETSI podrá solicitar al proveedor informes puntuales sobre la actuación realizada por el proveedor ante una determinada incidencia.
- El proveedor deberá entregar, con periodicidad mensual, a la ETSI un informe en el que aparezcan datos suficientes para tener una visión de la calidad de prestación del servicio.

8.3 Descripción del servicio

En este apartado se describe el servicio prestado por el proveedor externo para satisfacer las necesidades de la ETSI.

El proveedor externo ofrece un servicio de mantenimiento correctivo unido a dos revisiones anuales de los equipos para prevenir incidencias, que harán las veces de mantenimiento preventivo.

Denominaremos mantenimiento correctivo cómo aquel que corrige los defectos observados en los equipamientos o instalaciones.

8.3.1 Organización

La estructura organizativa del proveedor para la prestación del servicio se muestra en la siguiente imagen:

Ilustración 8-7 Organización del proveedor

A continuación, se describen cada una de estas figuras.

8.3.1.1 Gestor del Servicio

El Gestor del Servicio es una persona con gran experiencia en este tipo de servicios. Entre sus atribuciones se encuentran:

- Responsable último del servicio ante la ETSI.
- Interlocución directa con cliente para escalados y tratamiento de la calidad del servicio
- Presentación de informes.
- Supervisión del resto áreas que componen este servicio para asegurar la calidad del servicio.
- Realizar propuestas de mejoras para el servicio.
- Soporte al CAU sobre las peticiones de cliente.
- Primer nivel de escalado ante incidencias.
- Comunicación a la ETSI de facturación adicional.

El Gestor del Servicio no tendrá una dedicación exclusiva. Su horario de cobertura será de lunes a viernes laborables de 09:00 a 18:00, aunque en función de la necesidad podrá ampliar este horario.

La ETSI podrá contactar con el Gestor del Servicio por vía el proveedor o por correo electrónico.

En ITIL equivaldría al Jefe de Proyecto.

8.3.1.2 CAU

El Centro de Atención al Usuario (CAU) está compuesto por un número de recursos humanos suficiente para garantizar la atención del servicio. El CAU actúa como Ventanilla Única de Recepción de Tickets. Algunas de sus funciones son:

- Recepción de Tickets
- Actualización del estado de los Tickets

- Realización de la actuación en remoto para la resolución de las incidencias
- Programación de la actuación in-situ para la resolución de la incidencia
- Monitorización y Seguimiento de los Tickets
- Análisis y tratamiento de las peticiones de cliente.
- Encargado de registrar en la CMDB cualquier cambio de hardware o de contactos de la ETSI

El horario de atención del CAU será de lunes a domingo de 00:00 a 24:00 incluyendo festivos.

El CAU no tiene dedicación exclusiva a este servicio.

La ETSI podrá contactar con el CAU a través del correo electrónico, teléfono o la aplicación web de gestión de incidencias del proveedor.

En ITIL el CAU sería el Centro de Servicios

8.3.1.3 Técnicos In-situ

Este grupo está compuesto por un pool de técnicos especialistas en labores de mantenimiento de hardware similar al cubierto por este servicio. Los técnicos In-situ, realizarán las actuaciones necesarias en las dependencias de la ETSI para resolver las incidencias o peticiones. También serán los encargados de realizar los mantenimientos preventivos.

Este grupo equivaldría en ITIL a un soporte especializado o al Help Desk

8.3.1.4 Garantías y Repuestos

Para poder cumplir con los Acuerdos de Nivel de Servicio, es necesario dotar a los técnicos in-situ de los repuestos necesarios. Para reponer dicho respuestas es necesario realizar las gestiones necesarias con los fabricantes para hacer efectiva la garantía. Este grupo es el encargado de realizar todas estas gestiones.

La ETSI no tendrá contacto directo con este grupo, cuya labor debe ser transparente para los clientes.

8.3.2 Gestión de la Disponibilidad

Dada la naturaleza de los elementos de configuración del servicio, estos no pueden ser monitorizados, por lo que no será posible actuar de forma proactiva para garantizar la disponibilidad.

En este servicio el elemento más crítico para la disponibilidad del servicio es el servidor de contenidos. Cómo se comenta posteriormente se dispondrá de un repuesto dedicado de este servidor para que, en caso de avería, se pueda restituir el servicio lo antes posible.

Para garantizar, en la medida de lo posible, disponibilidad del servicio cobra especial importancia velar por el cumplimiento de los OLAs (tarea realizada por el Gestor del Servicio) y los UCs (tarea realizada por el grupo de garantías y repuestos).

8.3.3 Gestión de la Capacidad

Los recursos técnicos que el prestador del servicio pondrá a disposición del servicio, consistirán en repuestos de los elementos y en el portal Web de gestión de tickets.

Los repuestos son descritos en apartados posteriores, mientras que, respecto al portal Web, el proveedor garantiza disponer de suficientes recursos para que éste esté siempre disponible.

Aunque la Gestión de Capacidad se refiere a recursos técnicos, en este servicio podríamos ampliar su definición para que abarque también a los recursos humanos.

La capacidad de este servicio vendrá entonces marcada por el número de recursos de los que dispone el CAU para atender los tickets y el número de técnicos que hay para realizar intervenciones in-situ.

El proveedor se compromete a poner el número de recursos humanos necesarios para dotar de la “capacidad”

suficiente al servicio.

8.3.4 Gestión de la Continuidad

Para garantizar en la medida de lo posible la continuidad del servicio, el prestador del servicio realizará al menos dos actuaciones anuales de Mantenimiento Preventivo.

8.3.4.1 Mantenimiento preventivo

El mantenimiento preventivo consiste en realizar pruebas y comprobaciones sobre elementos que no sufren ninguna incidencia en ese momento. El objetivo es evitar en la medida de lo posible que se produzcan dichas incidencias.

El mantenimiento preventivo en este servicio se dedicará principalmente al servidor, ya que tiene una estructura más modular y por su naturaleza está preparado para soportar más pruebas. Aun así, también se realizará una breve revisión de las pantallas.

Tal y como se indicaba en anteriores apartados el prestador del servicio tendrá que realizar al menos dos mantenimientos preventivos al año. En este caso se realizará uno en el mes de enero y otro en julio.

Las actuaciones necesarias para este mantenimiento preventivo serán realizadas fuera del horario habitual de funcionamiento de los puntos de información, para que así no tenga impacto en el servicio.

El prestador del servicio desplazará a los técnicos necesarios para realizar la actuación con algunos repuestos, para sustituir los componentes en los que se detecte algún problema. Como mínimo se deberán llevar los siguientes repuestos:

- Memoria RAM para el servidor
- Disco Duro para el servidor
- Fuente de alimentación del servidor
- 3 latiguillos de red.
- 2 cables de alimentación.
- Una pantalla

Si se agotan los repuestos, o no se dispone de ellos para el componente afectado, se coordinará con la ETSI una actuación correctiva posterior para proceder a la sustitución de este componente. La fecha de dicha actuación se determinará en función de la severidad del problema.

Una vez finalizadas todas las revisiones y actuaciones el prestador del servicio entregará un informe a la ETSI con las revisiones y actuaciones realizadas, así como algunas recomendaciones.

8.3.4.1.1 Preventivo pantallas

Las actuaciones que se realizarán en el mantenimiento preventivo de las pantallas serán las siguientes:

- Revisión del cableado de red y alimentación conectado a las pantallas.
- Revisión superficial (detección de ruido o temperatura excesiva).

8.3.4.1.2 Preventivo Servidor

Las actuaciones que se realizarán en el mantenimiento preventivo del servidor serán las siguientes:

- Revisión del cableado de red y alimentación conectado al servidor.
- Comprobación del estado de la memoria RAM, mediante el uso del software adecuado para ello. Por ejemplo: Memtest.
- Comprobación del estado del disco duro con chkdsk (Windows) o fsck (Linux)
- Revisión de la CPU con el test Prime95
- Extracción de imagen de seguridad del sistema.

8.3.5 Los Tickets.

En el servicio se definen los tickets cómo la unidad de comunicación entre la ETSI y el proveedor. Cuando la ETSI

quiera notificar una incidencia o realizar una petición se dará de alta en el Sistema de Gestión de Tickets del proveedor un Ticket del tipo correspondiente. A este ticket se le asignará un código con el que el cliente podrá hacer un seguimiento del mismo si así lo desea.

Los tickets podrán ser del tipo Incidencia, Petición o Problema. Para simplificar la redacción, hablaremos siempre directamente de Incidencias, Peticiones o Problemas y no de Tickets tipo Incidencia, Tickets tipo Petición o Tickets tipo Problema.

8.3.6 Gestión de Incidencias.

En este caso será la ETSI la encargada de comunicar al proveedor externo el mal funcionamiento de alguno de los elementos incluidos en el servicio. Esta comunicación supondrá la apertura de un ticket del tipo incidencia (a partir de ahora lo llamaremos incidencia para simplificar) que el prestador del servicio tendrá que resolver.

El diagrama de flujo típico de una incidencia será el siguiente:

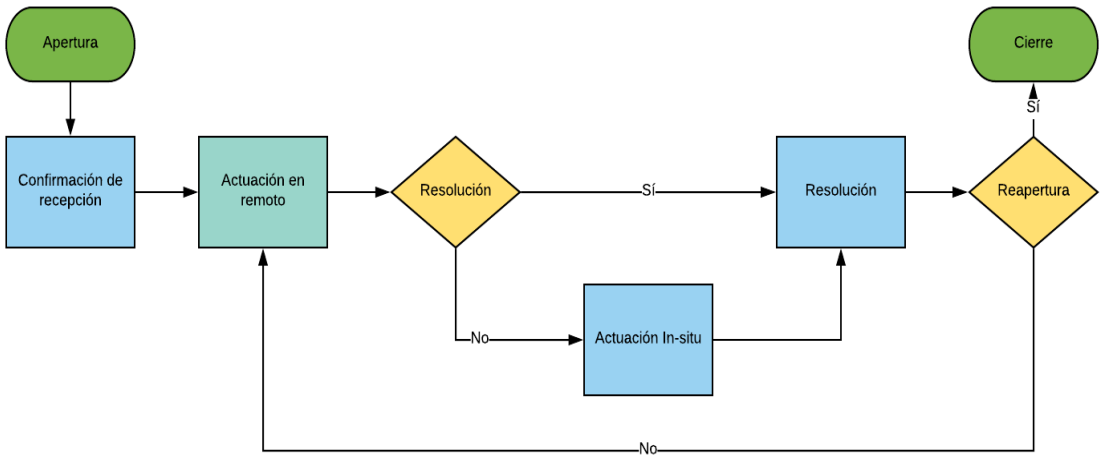


Ilustración 8-8 Diagrama de flujo de la Gestión de Incidencias

Tal y como se indica en el apartado anterior, el proveedor que presta el servicio dispone un Centro de Atención al Usuario (en adelante CAU) que actuará como Ventanilla Única de Recepción de Incidencias.

El CAU se encargará de confirmar la recepción de la incidencia, así como realizar alguna actuación en remoto con el usuario que notificó la incidencia para intentar resolverla lo antes posible. De no ser posible la resolución en remoto, el CAU enviará a un técnico de campo para que realice las acciones necesarias in-situ para resolver la incidencia.

El CAU, si procede, marcará la incidencia cómo masiva y lo comunicará al contacto de la ETSI.

El proveedor dispone de un sistema de gestión y seguimiento de incidencias al que dará acceso a la ETSI.

Veremos ahora con más detalle cada una de las fases que atraviesa una incidencia.

8.3.6.1 Apertura

La ETSI será la encargada de notificar al proveedor externo el mal funcionamiento de algunos de los elementos que componen los puntos de información. Esta notificación conllevará la apertura de una incidencia.

El proveedor externo pone a disposición de la ETSI tres vías para la notificación y apertura de incidencias:

- Teléfono: El proveedor externo habilitará un número de teléfono exclusivo para la ETSI. Dentro del horario de cobertura de servicio, siempre habrá al menos un operador disponible que se encargará de recoger los datos sobre la incidencia que le proporcione el usuario de la ETSI.

- Correo electrónico: Se habilitará un buzón de correo electrónico para este servicio. El usuario de la ETSI podrá escribir un email a este buzón danto los detalles de la incidencia.
- Aplicación web: El proveedor externo dará acceso a la ETSI a su propia herramienta de gestión de tickets. Dicha herramienta se trata de una aplicación web que permite el registro y seguimiento de incidencias/peticiones desde un navegador web. La ETSI podrá registrar directamente las incidencias/peticiones desde esta aplicación.

Los datos que deberá aportar la ETSI en la apertura de la incidencia son los siguientes:

- Elemento afectado: Se indicará si el elemento en el que se observa un mal funcionamiento es una pantalla o el servidor. Si es posible se indicará el número de serie de dicho elemento.
- Contacto de ETSI: Se indicará la persona con el que el CAU podrá contactar para realizar las actuaciones en remoto y/o coordinar la visita de un técnico in-situ si fuese necesario. Se podrá indicar más de un contacto por si alguno no estuviera disponible.
- Descripción: Se hará una descripción del problema observado. Cuanto más detallada sea dicha descripción más fácil será hacer un diagnóstico de la incidencia.
- Impacto: Se indicará si el impacto de la incidencia en el servicio es baja, media, alta o crítica.
- Urgencia: Se indicará si la urgencia de la petición es baja, media, alta o crítica.

Nunca se abrirá una incidencia que incluya más de un elemento afectado, si por cualquier motivo aparece una avería en más de un elemento, habrá que abrir una incidencia por elemento. El servidor se considera cómo un elemento en conjunto.

La incidencia pasará al estado “Abierta”.

8.3.6.2 Confirmación de recepción

Una vez que la incidencia quede registrada en el Sistema de Gestión de Tickets del proveedor, el usuario que ha realizado la apertura recibirá un email en su dirección de correo electrónico confirmando la correcta recepción de la incidencia.

El registro de la incidencia será prácticamente inmediato independientemente de la vía elegida por el usuario para su notificación.

La incidencia pasará al estado “En curso”.

8.3.6.3 Actuación en remoto

El CAU solicitará, vía el proveedor, al usuario que realice una serie de comprobaciones mínimas sobre el elemento afectado para intentar resolver la incidencia o al menos poder diagnosticar de forma más aproximada la avería que sufre el equipo.

Ejemplos de comprobaciones mínimas:

- Verificar que el equipo está correctamente conectado a la alimentación eléctrica.
- Comprobar que el equipo está correctamente conectado a la red de datos de la ETSI.
- Reiniciar el equipo.
- Comprobar que el equipo no se ha mojado.

Si tras estas comprobaciones la incidencia no queda resuelta, el CAU se la notificará a un técnico de campo, para que acuda a la sede para sustituir el equipo afectado. El CAU también notificará al usuario que es necesario realizar una actuación in-situ, indicándole la fecha y hora aproximada a la que el técnico se desplazará a la sede.

Si la incidencia queda resuelta se pasará al estado “Resuelta”, si no, continuará en el estado “En curso”.

8.3.6.4 Actuación in-situ

La actuación in-situ consistirá en la sustitución del equipo afectado por parte de un técnico de campo del proveedor externo. Los técnicos que realicen sustituciones de equipos seguirán el siguiente procedimiento:

- Desembalaje del equipo.
- Retirar el equipo averiado.
- Instalación del nuevo equipo y pruebas de funcionamiento.
- Recepción de la conformidad del usuario y cierre de la incidencia en el Sistema de Gestión de Incidencias.
- Embalaje del equipo averiado para retirarlo.

En el caso de que el equipo a sustituir sea el servidor, el nuevo equipo deberá llevar precargada una imagen del anterior con el fin de acortar el tiempo de la actuación.

En técnico de campo tendrá que informar al CAU de los datos del nuevo equipo (número de serie, modelo, etc.). Con estos datos el CAU podrá actualizar la CMDB.

8.3.6.5 Resolución de la incidencia

Una vez realizada las actuaciones necesarias y comprobado con alguno de los contactos de la ETSI indicados en la apertura de la incidencia que el elemento afectado por la incidencia funciona de nuevo correctamente, se considerará que la incidencia está resuelta y se pasará al estado "Resuelta".

Si antes de que transcurran 24 horas de la resolución se reproduce el problema que generó la incidencia la ETSI podrá reabrir la incidencia para que se vuelva a tratar, pasándose de nuevo al estado "En curso".

Transcurridas 24 horas de la resolución y si no se recibe nueva notificación de la ETSI, se procederá a pasar la incidencia al estado "Cerrada". Cualquier problema que surja sobre este elemento pasado este tiempo tendrá que tratarse como una nueva incidencia. Este detalle es importante de cara al cumplimento de los Acuerdos de Nivel de Servicio, ya que cuando se reabre una incidencia el tiempo de resolución cuenta desde la apertura original de la incidencia. Mientras que con una nueva incidencia este tiempo se "reinicia". En el apartado de Acuerdos de Nivel de Servicio se detallará más este proceso.

8.3.7 Gestión de Problemas

El objetivo es la identificación, registro, seguimiento y corrección (proactiva o reactivamente) de los problemas que afectan a la prestación del servicio.

El flujo que seguir se resume a continuación:

- El primer paso es detectar el problema, por lo que habrá que hacer seguimiento de todas aquellas incidencias recurrentes e incidencias especialmente graves. Asimismo, el CAU, los técnicos in-situ, usuarios o suministradores son fuente para la identificación de problemas.
- Registro del problema una vez identificado, mediante un ticket del tipo "Problema".
- Se categoriza y prioriza el problema para su posterior diagnóstico de causas y raíces.
- Se plantea y planifica una solución provisional hasta el diagnóstico final.
- Cuando se conozca la causa del error se registrará el error conocido y se buscará una solución definitiva.
- Se procede a la resolución y posterior cierre del problema.

8.3.8 Gestión de Peticiones

Se denominará Petición a toda notificación del cliente sobre el servicio que no se categoriza como incidencia. Un ejemplo de petición sería la solicitud de un informe sobre una incidencia en concreto o la solicitud de la planta actual en funcionamiento. Las peticiones se registrarán mediante tickets del tipo "Petición" serán tratadas siempre por el CAU con el soporte e intervención del Gestor del Servicio si fuese necesario. El

diagrama de flujo típico de una petición sería:

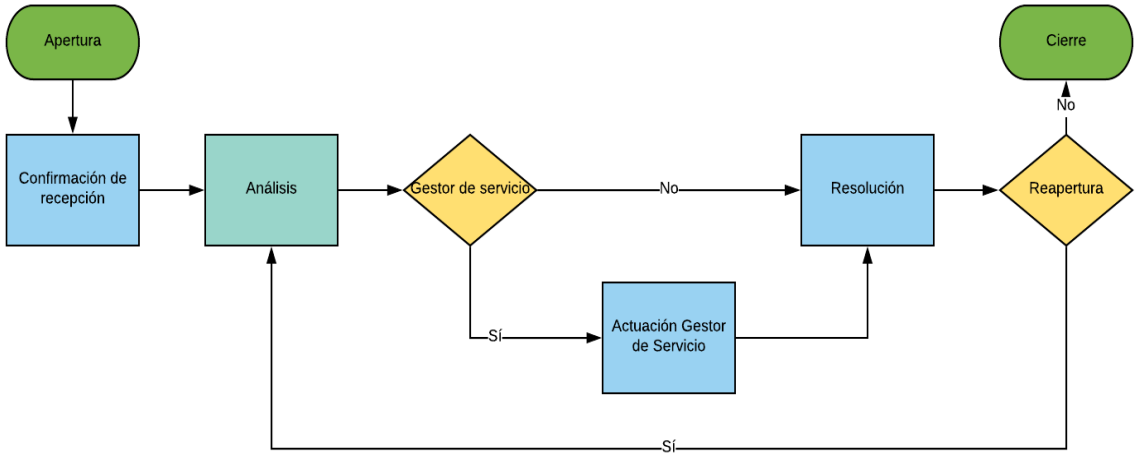


Ilustración 8-9 Diagrama de flujo de la Gestión de Peticiones

Se describen a continuación las fases por las que atravesaría una Petición.

8.3.8.1 Apertura

Por su naturaleza, las Peticiones serán realizadas por la ETSI. La ETSI dispone de los mismos medios para notificación que para la apertura de incidencias, es decir, Teléfono, Correo electrónico y aplicación WEB.

Los datos que deberá aportar la ETSI en la apertura de la petición son los siguientes:

- Contacto de ETSI: Se indicará la persona con el que el CAU podrá contactar para realizar las consultas necesarias para atender la petición. Se podrá indicar más de un contacto por si alguno no estuviera disponible.
- Descripción: Se hará una descripción de lo solicitado. Cuanto más detallada sea dicha descripción más fácil será analizar la petición y resolverla.
- Elemento: Elemento al que afecta la petición, si son varios se pondrá al principal afectado.
- Impacto: Se indicará si el impacto de la petición en el servicio es bajo, medio, alto o crítico.
- Urgencia: Se indicará si la urgencia de la petición es baja, media, alta o crítica.

La petición pasará al estado “Abierta”.

8.3.8.2 Confirmación de recepción

Una vez que la petición quede registrada en el Sistema de Gestión de Tickets del proveedor, el usuario que ha realizado la apertura recibirá un email en su dirección de correo electrónico confirmando la correcta recepción de la incidencia.

El registro de la petición será prácticamente inmediato independientemente de la vía elegida por el usuario para su notificación.

La incidencia pasará al estado “En curso”.

8.3.8.3 Análisis

El CAU analizará la petición, pudiendo consultar con los contactos facilitados las dudas que puedan surgir. Una vez realizado el análisis decidirá si es necesaria la intervención del Gestor del Servicio. También, tras consultar con el usuario podrá se podrá modificar el impacto y la urgencia de la petición.

Motivos por los que puede ser necesaria la intervención del Gestor del Servicio:

- Se trata de la petición de un informe.
- La petición se sale de la operación estándar del servicio y podría considerarse cómo una RFC.

Si no es necesaria la intervención del Gestor del Servicio, el CAU procederá a resolver la petición realizando lo indicado en la descripción de la petición

Si la petición queda resuelta se pasará al estado "Resuelta", si no, continuará en el estado "En curso".

8.3.8.4 Actuación Gestor del Servicio

El Gestor del Servicio revisará la petición y actuará en función de la naturaleza de la misma:

- Si se trata de la petición de un informe, el Gestor del Servicio lo realizará y lo entregará a la ETSI, resolviendo de esta forma la incidencia. Además, lo comunicará al CAU para que lo registre en la base de datos de gestión de tickets.
- Si es una petición que excede el alcance del servicio se considerará cómo una RFC y se iniciará el proceso de Gestión del Cambio.

Tras la actuación del Gestor del Servicio, la petición pasará al estado resuelta.

8.3.8.5 Resolución de la petición

Una vez realizada las actuaciones necesarias y comprobado con alguno de los contactos de la ETSI indicados en la apertura de la petición que ésta ha quedado satisfecha, se considerará que la petición está resuelta y se pasará al estado "Resuelta".

La ETSI tendrá 2 día laborables a partir de la resolución para reabrir la petición si hay algo con lo que no está conforme, pasándose de nuevo al estado "En curso".

Transcurridos 2 días laborables de la resolución, se procederá a pasar la petición al estado "Cerrada" si no se ha recibido ninguna notificación de la ETSI al respecto.

8.3.9 Gestión de Informes

En el servicio se contemplan hasta tres tipos de informes:

- Informe sobre una incidencia: Documento en el que se detalla lo sucedido en una incidencia.
    - Periodicidad: Puntual, se realizará mediante una Petición de la ETSI.
    - ANS entrega: 3 días laborables a partir de la petición de la ETSI.
- Informe de Calidad de Servicio: Documento en el que se hace un balance mensual del servicio, mostrando datos generales y comparativas sobre el mismo.
    - Periodicidad: Mensual.
    - ANS entrega: Antes del día 6 del mes siguiente al evaluado.
- Informe de Mantenimiento Preventivo: Documento en el que se describen las actuaciones realizadas durante el mantenimiento preventivo.
    - Periodicidad: Al menos dos veces al año.
    - ANS entrega: 3 días laborables después de la elaboración.

En los apartados anexos se muestran ejemplos de estos informes.

8.3.10 Gestión del Cambio

El proceso de Gestión del cambio comenzará cuando la ETSI o el proveedor detecte la necesidad de algún

cambio en el servicio. Dicha necesidad podrá provenir de las siguientes fuentes:

- Peticiones expresas de los usuarios finales a la ETSI.
- Mecanismos internos de la ETSI para la detección de la necesidad de cambio.
- Proceso de Gestión de Problemas o Incidencias.
- Resultado del proceso de Mejora Continua implementado por el proveedor.

Dichas necesidades, una vez realizada una primera evaluación positiva de la misma, generará una RFC ("Petición de Cambio").

En el proveedor el Gestor del Servicio asumirá el rol de Gestor del Cambio. El Gestor del Cambio será el representante del proveedor en las reuniones del Comité Asesor del Cambio de la ETSI (si lo hubiese) en las que el proveedor sea convocado.

A continuación, se presentan con más detalle los flujos de las peticiones en función de que estas sean "reactivas" (peticiones generadas por la ETSI) o "proactivas" (peticiones generadas por el proveedor):

a) Peticiones reactivas:
    1. La ETSI genera un ticket del tipo “petición” por alguna de las vías que tiene a su disposición.
    2. El CAU analiza el ticket, y al ver que lo solicitado va más allá de un cambio “estándar”, lo traslada al Gestor el Servicio, identificándolo con una RFC.
    3. El Gestor del Servicio, asumiendo el rol de Gestor del Cambio se pone en contacto con la ETSI para informar de que la petición se va a tratar cómo RFC.
    4. El Gestor del Cambio con la colaboración de otras áreas de su organización (comercial, especialistas técnicos, dirección, etc.) realiza un análisis de la RFC. Los posibles resultados de este análisis son:
        i. Aceptación del cambio.
        ii. Envío de propuesta de modificación del cambio.
        iii. Ejecución del cambio condicionada a aceptación de propuesta comercial.
        iv. Rechazo del cambio por ser técnicamente inviable. Se resuelve el ticket justificando adecuadamente el rechazo del cambio.
    5. El Gestor del Cambio, además de actualizar el estado del ticket, comunica a la ETSI el resultado de este análisis justificándolo debidamente.
    6. ETSI decide si seguir adelante con el cambio y comunica su decisión al Gestor del Cambio. Si la decisión es continuar con el cambio el Gestor del Cambio inicia los procedimientos necesarios para implementarlo y verificar su correcta implantación (PIR). Si la decisión es no continuar con el cambio, se resuelve y cierra el ticket.
    7. En los cambios aprobados por ambas partes, el Gestor del Cambio coordina su implantación con la ETSI.
    8. Una vez implementado el cambio, el Gestor del Cambio se ocupa de que se realicen las pruebas necesarias para verificar tanto la correcta ejecución cómo que los efectos del cambio son los deseados. Estas pruebas de verificación se podrán realizar de forma conjunta con la ETSI
    9. Si el resultado de las pruebas es satisfactorio el Gestor del Cambio, lo comunica al CAU para que actualice la CMDB con el cambio realizado y resuelve el ticket una vez esté recogido el cambio en la CMDB.
    10. Si el resultado no es satisfactorio se procede a realizar el roll-back. El Gestor del Cambio, con el soporte técnico que necesite, analiza lo sucedido, ejecuta las medidas correctivas oportunas y vuelve a coordinar con la ETSI la implementación del cambio.

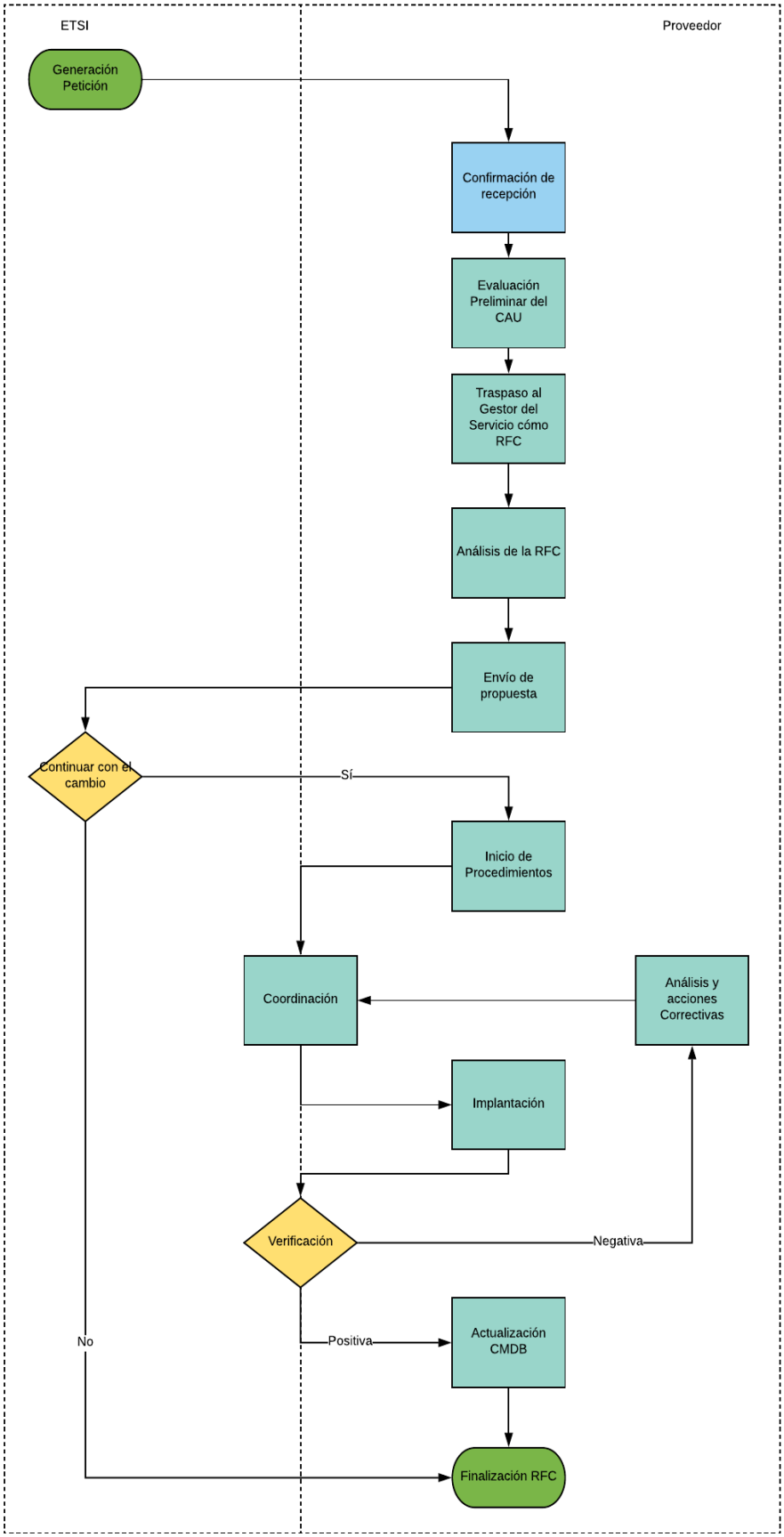


Ilustración 8-10 Diagrama de flujo RFCs reactivas

b) Peticiones proactivas:
    1. El Gestor del Servicio, asumiendo el rol de Gestor del Cambio comunica la necesidad de realizar un cambio a la ETSI, detallando la propuesta técnica, el impacto y la mejora que supondría el cambio.
    2. La ETSI evalúa la solicitud y comunica su decisión al Gestor del Cambio.
    3. Si se rechaza el cambio se da por concluido el proceso.
    4. Si se acepta el cambio, la ETSI registra un ticket de tipo "Petición" indicando que se trata de una RFC, para que el CAU la traslade directamente al Gestor del Servicio.
    5. El Gestor del Cambio inicia los procedimientos. necesarios para implementarlo y verificar su correcta.
    6. El Gestor del Cambio coordina su implementación con la ETSI.
    7. Una vez implementado el cambio, el Gestor del Cambio se ocupa de que se realicen las pruebas necesarias para verificar tanto la correcta ejecución cómo que los efectos del cambio son los deseados. Estas pruebas de verificación se podrán realizar de forma conjunta con la ETSI
    8. Si el resultado de las pruebas es satisfactorio el Gestor del Cambio, lo comunica al CAU para que actualice la CMDB con el cambio realizado y resuelve el ticket una vez esté recogido el cambio en la CMDB.
    9. Si el resultado no es satisfactorio se procede a realizar el roll-back. El Gestor del Cambio, con el soporte técnico que necesite, analiza lo sucedido, ejecuta las medidas correctivas oportunas y vuelve a coordinar con la ETSI la implementación del cambio.

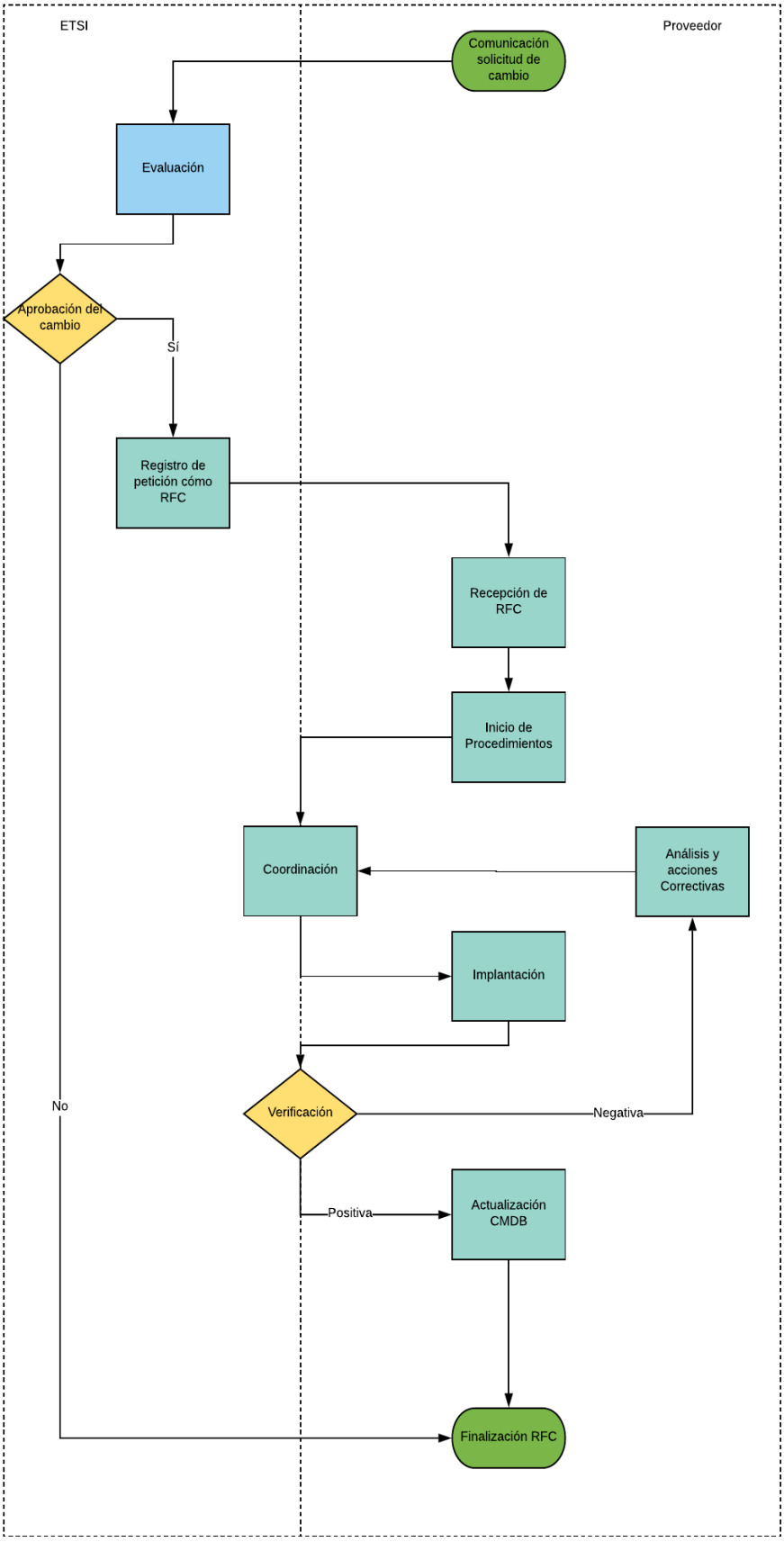


Ilustración 8-11 Diagrama de flujo de RFCs proactivas

Si el cambio solicitado implica coste adicional para el proveedor (cambio de hardware, adquisición de nuevas licencias), el proveedor podrá repercutirlo a la ETSI en forma de factura adicional. En estos casos, la ETSI tendrá que validar el importe propuesto por el proveedor antes de proceder con el cambio.

8.3.11 Gestión de Niveles de Servicio

El Acuerdo de Nivel de Servicio entre la ETSI y el proveedor del servicio establece los siguientes KPIs con sus correspondientes valores umbrales.

Nombre	Valor
Cobertura	Lunes a Viernes Laborables de 8:30 a 20:30
Tiempo de respuesta máximo ante incidencia/petición	1 hora
Tiempo de resolución máximo de incidencia crítica	4 horas
Tiempo de resolución máximo de incidencia	24 horas (siguiente día laborable)
Tiempo de resolución máximo de incidencia masiva	3 días laborables
Tiempo máximo de entrega de informe de incidencia	3 días laborables
Tiempo de resolución máximo de petición	3 días laborables
Entrega informe de calidad de servicio	Antes del día 6 del mes siguiente al evaluado
Tiempo máximo de entrega de informe de mantenimiento preventivo	3 días laborables

Tabla 8-3 ANS

Con el fin de cumplir con estos ANS el proveedor define en su OLA que, cuando sea necesario, el CAU tendrá que comunicar la incidencia a los técnicos in-situ el mismo día que se abrió la incidencia.

A continuación, se define cada uno de los KPIs:

- Cobertura: Horario durante el que proveedor de servicio debe atender las incidencias. Este horario es el único computable de cara a medir los tiempos descritos posteriormente.
- Tiempo de respuesta: Tiempo que transcurre entre que la ETSI notifica al proveedor del servicio una incidencia y el proveedor le confirma su recepción.
- Tiempo de resolución: Tiempo que transcurre la apertura del ticket y la resolución definitiva de la misma.
- Tiempo de entrega de informe de incidencia: Tiempo transcurrido entre la solicitud por parte de la ETSI de un informe sobre una incidencia y la entrega del mismo por parte del proveedor.
- Entrega de informe de calidad de servicio: Fecha tope para la entrega del informe.
- Tiempo de entrega de informe de mantenimiento preventivo: Tiempo transcurrido entre la finalización de las actuaciones de mantenimiento preventivo y la entrega a la ETSI del informe de mantenimiento por parte del proveedor.

Para ilustrar cómo se miden estos tiempos pondremos con unos ejemplos:

- Apertura de incidencia un martes laborable a la 15:00
    - El proveedor tendría que confirmar la recepción de la incidencia antes de las 16:00 de ese

mismo día.

  - La incidencia debe quedar resuelta el siguiente día laborable.

- Apertura de incidencia un sábado a las 09:00
  - El proveedor tendría que confirmar la recepción de la incidencia antes de las 09:30 del siguiente día laborable (supondremos el lunes)
  - La incidencia debe quedar resuelta el segundo día laborable después de la apertura (en este ejemplo supondremos que el martes).
- La ETSI solicita un informe sobre una incidencia un miércoles laborable a las 17:00.
  - Suponiendo que no haya días festivos, el proveedor tiene de plazo hasta el lunes siguiente a las 20:30 para entregar el informe.
- El mantenimiento preventivo finaliza un sábado a las 15:00.
  - Suponiendo que no haya días festivos, el proveedor tiene de plazo hasta el miércoles siguiente a las 20:30 para entregar el informe.

8.3.11.1 Tiempos no imputables. Las paradas de reloj.

Durante el tiempo de vida de un ticket pueden darse circunstancias ajenas al proveedor que pueden retrasar la resolución del ticket. Dicho retraso no debe ser imputado al tiempo de resolución. Cuando se de alguna de estas circunstancias se "parará el reloj" del ticket, pasándose este al estado "Parado", es decir, dejará de contarse el tiempo que transcurre. Una vez se produzca un cambio que haga posible que el proveedor pueda retomar la resolución del ticket se "reactivará" el reloj del ticket, pasándose de nuevo al estado "En curso"

Ejemplos de causas de paradas de reloj:

- Fuera del horario de cobertura del servicio: Por definición todo el tiempo transcurrido fuera del horario de cobertura del servicio no se computa de cara a los KPIs.
- Contactos ilocalizables: El proveedor puede localizar a ninguno de los contactos indicados por la ETSI para realizar las actuaciones remotas sobre la incidencia o coordinar la visita de un técnico.
- Cita concertada: Es posible que por disponibilidad de su personal u otras causas la ETSI prefiera coordinar la visita de un técnico de campo para un día determinado. En este caso el reloj se pararía hasta la fecha de esa cita. Momento en el que se reactivaría.
- Acceso a la sede: Causas de fuerza mayor como incendio en la sede, atentados terroristas, condiciones climatológicas muy adversas (huracanes, nevadas muy abundantes, etc.) que imposibiliten el acceso de un técnico de campo a la sede.
- Indisponibilidad de la sede: Falta de fluido eléctrico en la sede, obras, etc.
- Espera de contestación por parte de la ETSI ante un presupuesto presentado para una petición.

Nótese que también se producirá "parada de reloj" cuando el ticket se pase a resuelto.

8.3.11.2 Incidencias fuera del alcance del servicio

Se considera que una incidencia está fuera del alcance del servicio cuando es producida por causas ajenas al normal funcionamiento normal de los elementos.

Como mejora del servicio, el proveedor atenderá estas incidencias, pero estas no computarán de cara al cálculo de los ANS, es decir, no existirá un tiempo máximo de respuesta ni un tiempo máximo de resolución.

En función de la naturaleza de la incidencia, el proveedor podrá emitir una factura a la ETSI. Dicha factura será adicional a la facturación normal del servicio. En caso de que sea necesario emitir una factura adicional, no se procederá con la resolución hasta que la ETSI no apruebe dicha factura.

Las causas que pueden hacer que una incidencia se considere fuera del alcance del servicio son las siguientes:

- Robo o desaparición de alguno de los componentes.
- Deficiencias en las instalaciones de la ETSI: Goteras, humedades, picos de tensión, derrumbes.
- Vandalismo.
- Mal uso por parte de la ETSI (golpes, cableado mal conectado).
- Acción de animales (ratas y otros roedores, por ejemplo).
- Desastres naturales.

8.3.11.3 Incidencias masivas

El proveedor podrá catalogar a las incidencias como masivas cuando se reciba más de una incidencia en un mismo día para el mismo tipo de elemento.

El CAU deberá notificar al contacto de la ETSI de la incidencia del marcado de la misma como masiva, vía correo electrónico.

Tal y como se indica en el apartado anterior estas incidencias tienen un ANS diferente.

Ejemplos:

- En un mismo día la ETSI notifica una incidencia que afecta al servidor y otra que afecta a una pantalla. Estas incidencias NO podrían catalogarse cómo masivas y por tanto aplicaría el ANS de una incidencia norma.
- Durante el transcurso de un día la ETSI notifica el mal funcionamiento de 2 pantallas. Estas incidencias SÍ podrían marcarse cómo masivas.

8.3.11.4 Penalizaciones

La ETSI podrá descontar ciertas cantidades de la facturación mensual del proveedor por el servicio sí se incumplen los ANS. En el siguiente cuadro se muestran las penalizaciones aplicables por cada KPI:

KPI	Valor umbral	Importe
Tiempo de respuesta de incidencia/petición	Incumplimiento en el 5% o más de las incidencias	10% de la facturación mensual
Tiempo de resolución de incidencia crítica	4 horas	5% de la facturación mensual por cada hora excedida
Tiempo de resolución de incidencia	24 horas (siguiente día laborable)	5% de la facturación mensual por cada día excedido
Tiempo de resolución de incidencia masiva	3 días laborables	5% de la facturación mensual por cada día excedido
Tiempo de resolución de petición	3 días laborables	5% de la facturación mensual por cada día excedido
Tiempo de resolución del problema	1 mes	5% de la facturación mensual por cada mes excedido
Tiempo de entrega de informe de incidencia	3 días laborables	5% de la facturación mensual por cada día excedido

Entrega informe de calidad de servicio	Antes del día 6 del mes siguiente al evaluado	5% de la facturación mensual por cada día excedido
Tiempo de entrega de informe de mantenimiento preventivo	3 días laborables	5% de la facturación mensual por cada día excedido

Tabla 8-4 Penalizaciones

8.3.12 Gestión de Garantía, Repuestos y Proveedores

De cara a garantizar en la medida de lo posible el cumplimiento del ANS de resolución de incidencia se ha dimensionado el servicio con un stock dedicado de equipos compuesto por los siguientes elementos:

- 1 Servidor Completo
- 1 Pantalla

Con este dimensionamiento, salvo que se averíen de forma simultánea dos pantallas, será posible resolver en tiempo todas las incidencias.

Este stock pasará a ser propiedad de la ETSI transcurridos 4 años del servicio, aunque durante la vigencia del mismo será el proveedor el encargado de almacenarlo y gestionar su garantía.

Para reponer rápidamente este stock, el proveedor dispone de acuerdos de garantía avanzados tanto con HP cómo con Panasonic. Estos acuerdos garantizan la reposición de las piezas averiadas 48 horas después de la apertura de caso de garantía con fabricante, así como amplían su vigencia a 4 años, siendo posible renovar esos acuerdos.

El procedimiento para hacer uso efectivo de estas garantías son las siguientes:

- Se informa al fabricante de la avería del equipo.
- El fabricante realiza el envío del equipo o pieza de sustitución.
- Se envía a fabricante el equipo o pieza averiada.

Nótese que el fabricante realiza el envío antes de recibir el equipo averiado, esto es tremendamente importante para garantizar la reposición del stock en el tiempo adecuado.

Todas estas gestiones son realizadas de forma transparente para la ETSI por el grupo de garantías y repuestos.

8.3.13 Gestión de Accesos y Seguridad de la Información

Para este servicio se han agrupado estos dos procesos en uno solo debido a la simplicidad de ambos.

Los elementos críticos del servicio en relación con este servicio son:

- Correo electrónico de la ETSI y el proveedor: La ETSI y el proveedor se comprometen al uso de software de seguridad para el correo electrónico que los proteja de virus, spam, ataques DDoS, etc. En el caso del proveedor, cómo medida adicional de seguridad y para controlar el acceso, cada usuario se identificará de forma unívoca con una matrícula y usará una contraseña que cumpla con los estándares de seguridad de Microsoft (uso de mayúsculas, minúsculas y números) que tendrá que modificar cada 30 días.
- Servidor de Contenidos: La ETSI será la responsable de velar por la seguridad de la información del servidor, así como de controlar quien accede. Por su parte el proveedor se compromete a realizar las mismas tareas para el servidor de repuesto que tendrá almacenado.
- Aplicación WEB de Gestión de Tickets: El proveedor, solo asignará un alias para registrarse en la aplicación WEB a aquellas personas que la ETSI (sus gestores) soliciten. El proveedor garantiza que, aunque la aplicación web es usada por otros clientes, ningún cliente tiene visibilidad de los tickets de

otro cliente.

8.3.14 Bases de Datos del Servicio

Para el este servicio se ha definido dos Bases de Datos:

- Base de datos de Tickets
- CMDB (Configuration Management DataBase)

Estas dos Bases de Datos se relacionan entre sí a través de ciertos campos de sus tablas cómo se verá en los siguientes apartados.

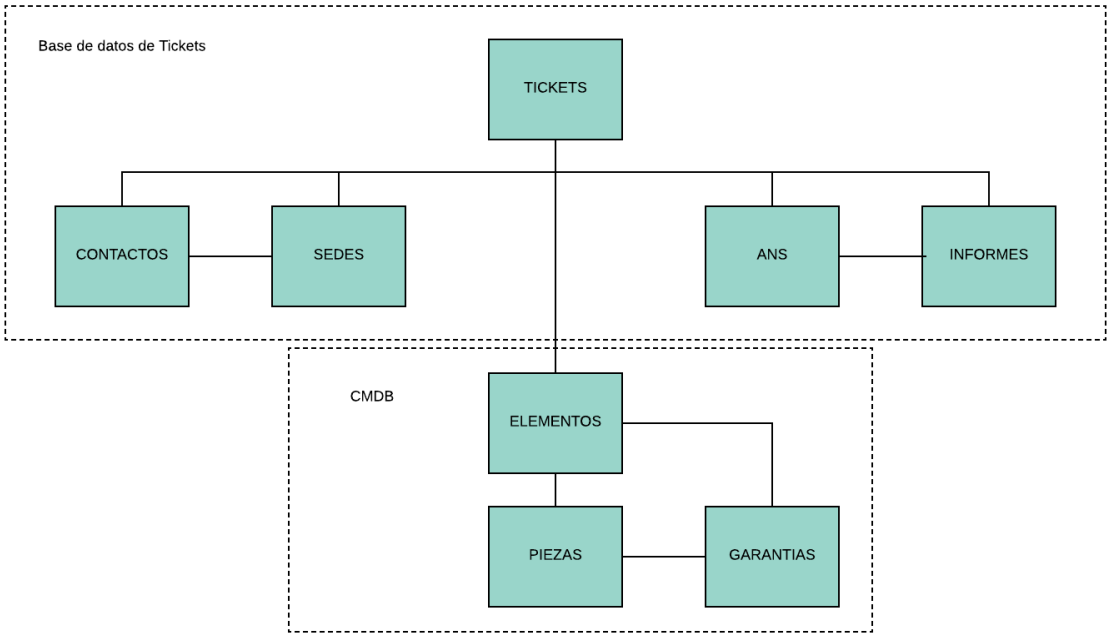


Ilustración 8-12 Estructura Bases de datos

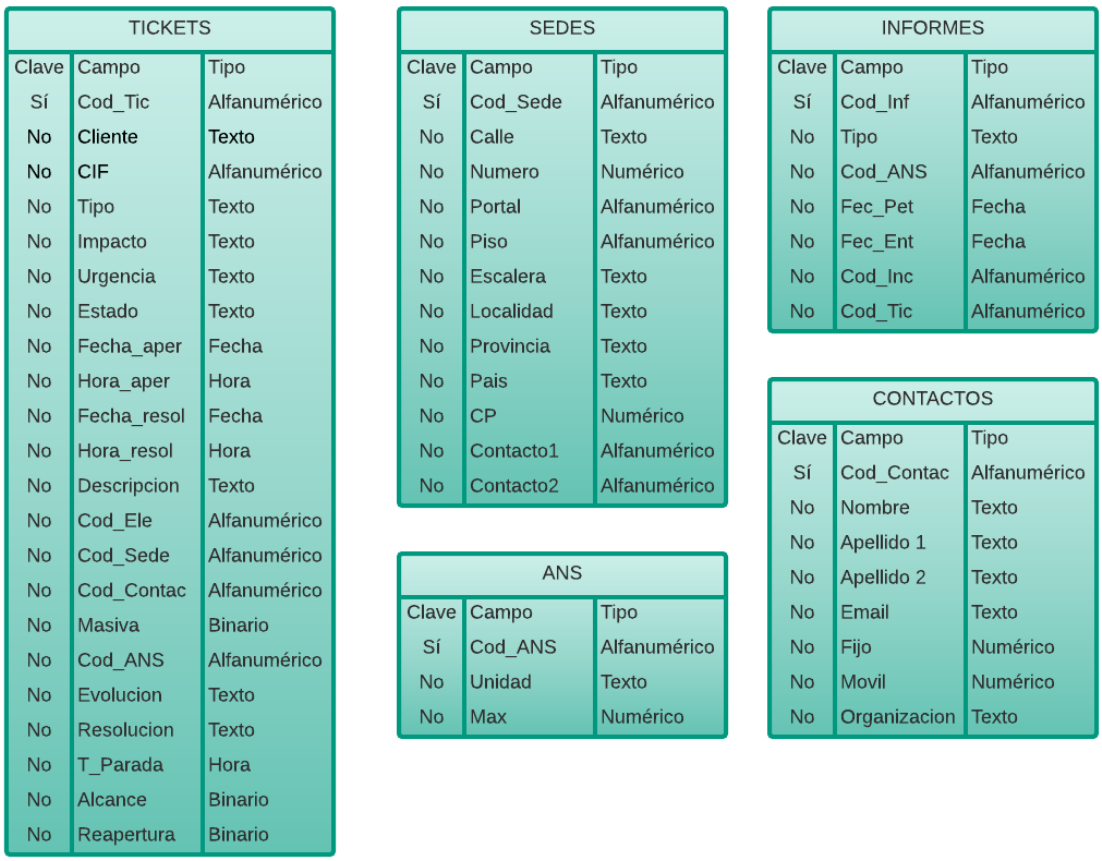
8.3.14.1 Base de Datos de Tickets

En esta Base de Datos se registran todos los tickets generados durante el servicio. Sirve pues, como base de datos para incidencias, peticiones y problemas.

Adicionalmente también almacena toda la información sobre los informes, por lo que contiene prácticamente toda la información sobre el desarrollo del servicio.

Este base de datos sirve también cómo base de datos del conocimiento, ya que en la información de los tickets aparecerá siempre el procedimiento seguido para resolverlos. De esta forma quien esté tratando un ticket podrá consultar en esta base de datos si ha habido algún ticket similar y la forma en la que se resolvió.

A continuación, se detallan las tablas que componen esta base de datos:



TICKETS		
Clave	Campo	Tipo
Sí	Cod_Tic	Alfanumérico
No	Cliente	Texto
No	CIF	Alfanumérico
No	Tipo	Texto
No	Impacto	Texto
No	Urgencia	Texto
No	Estado	Texto
No	Fecha_aper	Fecha
No	Hora_aper	Hora
No	Fecha_resol	Fecha
No	Hora_resol	Hora
No	Descripcion	Texto
No	Cod_Ele	Alfanumérico
No	Cod_Sede	Alfanumérico
No	Cod_Contac	Alfanumérico
No	Masiva	Binario
No	Cod_ANS	Alfanumérico
No	Evolucion	Texto
No	Resolucion	Texto
No	T_Parada	Hora
No	Alcance	Binario
No	Reapertura	Binario

SEDES		
Clave	Campo	Tipo
Sí	Cod_Sede	Alfanumérico
No	Calle	Texto
No	Numero	Numérico
No	Portal	Alfanumérico
No	Piso	Alfanumérico
No	Escalera	Texto
No	Localidad	Texto
No	Provincia	Texto
No	Pais	Texto
No	CP	Numérico
No	Contacto1	Alfanumérico
No	Contacto2	Alfanumérico

ANS		
Clave	Campo	Tipo
Sí	Cod_ANS	Alfanumérico
No	Unidad	Texto
No	Max	Numérico

INFORMES		
Clave	Campo	Tipo
Sí	Cod_Inf	Alfanumérico
No	Tipo	Texto
No	Cod_ANS	Alfanumérico
No	Fec_Pet	Fecha
No	Fec_Ent	Fecha
No	Cod_Inc	Alfanumérico
No	Cod_Tic	Alfanumérico

CONTACTOS		
Clave	Campo	Tipo
Sí	Cod_Contac	Alfanumérico
No	Nombre	Texto
No	Apellido 1	Texto
No	Apellido 2	Texto
No	Email	Texto
No	Fijo	Numérico
No	Movil	Numérico
No	Organizacion	Texto

Ilustración 8-13 Tablas base de datos de Tickets

A continuación, se describe cada uno de los campos para cada tabla:

- TICKETS:
  - Cod_Tic: Código alfanumérico único que identificará al ticket. Este código se generará automáticamente al registrar el ticket. Ejemplo: TIC0000000000001.
  - Cliente: Nombre del cliente. En este caso "ETSI".
  - CIF: Cif del cliente.
  - Tipo: Categorización del ticket. Los tipos son:
    - Incidencia: Anomalía en el funcionamiento de cualquier elemento del servicio.
    - Petición: Solicitudes de la ETSI sobre el servicio.
    - Problema: Anomalía recurrente en el funcionamiento del servicio.
  - Impacto: Importancia del ticket para el funcionamiento del servicio. Para este servicio se definen cuatro niveles de impacto:
    - Bajo: Sin apenas afectación del servicio.
    - Medio: Un elemento tiene afectación total.
    - Alto: Dos o más elementos tienen afectación total.
    - Crítico: Corte total del servicio.
  - Urgencia: Rapidez con la que se requiere la resolución del ticket. Para este servicio se definen cuatro niveles de urgencia:

        - Baja
        - Media
        - Alta
        - Crítica
    - Estado: Indica cómo se encuentra el ticket. Los posibles estados son:
        - Abierto: Se ha registrado el ticket, pero no se ha enviado su confirmación al usuario.
        - En curso: Se ha notificado al usuario la correcta recepción del ticket y se están realizando las actuaciones necesarias para su resolución.
        - Parado: No se puede continuar con la resolución por motivos ajenos al proveedor o por estar fuera del horario.
        - Resuelto: El elemento afectado ya funciona correctamente o en el caso de la petición, se ha satisfecho la misma. Es posible reabrir el ticket.
        - Cerrado: Estado al que pasa el ticket automáticamente transcurridas 24 horas de paso a Resuelto si no hay nueva notificación. El ticket no puede ser reabierto.
    - Fecha_aper: Fecha de apertura del ticket. Ejemplo: 29/04/2018.
    - Hora_aper: Hora de apertura del ticket. Ejemplo: 09:11:01.
    - Fecha_resol: Fecha de resolución definitiva del ticket. Ejemplo: 30/04/2018.
    - Hora_resol: Hora de resolución definitiva del ticket. Ejemplo: 11:23:58
    - Descripción: Campo de texto donde se explica los síntomas que presente el o los elementos afectados. Ejemplo: “Pantalla no enciende”.
    - Cod_Ele: Código del elemento afectado. Este código identifica de manera unívoca al elemento. Su valor será igual al de alguno de los elementos de la tabla “Elementos”. Ejemplo: ELE_ETSI_00001
    - Cod_Sede: Código de la sede afectada. Este código identifica de manera unívoca a la sede. Su valor será igual al de alguno de los elementos de la tabla “Sedes”. Ejemplo: SEDE_ETSI_00001
    - Cod_Contac: Código del contacto de la ETSI para el ticket. Este código identifica de manera unívoca al contacto. Su valor será igual al de alguno de los elementos de la tabla “Contactos”. Ejemplo: CON_ETSI_00001
    - Masiva: Indica si la incidencia se ha marcado o no cómo masiva.
    - Cod_ANS: Código del ANS que aplica a el ticket. Este código identifica de manera unívoca al ANS. Su valor será igual al de alguno de los elementos de la tabla “ANS”. Ejemplo: ANS_ETSI_00001
    - Evolucion: En este campo se irá describiendo la evolución del ticket (cambios de estado, descripción de las actuaciones, motivos de paradas, etc.). En cada nuevo registro que se incluya en este campo se indicará siempre la fecha y la hora del registro. Ejemplo: 29/04/2018 09:11:01 Apertura del ticket: 29/04/2018 09:12:00 Confirmación de recepción. 30/04/2018 10:12:00 Se contacta con el usuario para actuación en remoto. 30/04/2018 11:23:58. Incidencia/petición resuelta 01/05/2018 11:23:58 Incidencia/petición cerrada.
    - Resolucion: Descripción de la solución dada a el ticket. Ejemplo: Durante actuación en remoto el usuario que reajusta el cable de alimentación en la toma de corriente y comprueba que la pantalla enciende.
    - T_Parada: Tiempo que ha estado el ticket en estado Parado.
    - Alcance: Indica si lo indicado en el ticket está dentro del alcance del servicio.

  - Reapertura: Indica si el ticket se ha reabierto después de una primera resolución.

- SEDES:
  - Cod_Sede: Código alfanumérico único que identificará a la sede. Este código se generará automáticamente al dar de alta a la sede en la CMDB.
  - Calle: Nombre de la calle donde se encuentra la sede.
  - Numero: Número de la calle donde se encuentra la sede.
  - Portal: Número del portal donde se encuentra la sede.
  - Piso: Código del piso donde se encuentra la sede.
  - Escalera: Código de la escalera donde se encuentra la sede.
  - Localidad: Localidad. donde se encuentra la sede.
  - Provincia: Provincia donde se encuentra la sede.
  - Pais: País donde se encuentra la sede.
  - CP: Código Postal que corresponde a la ubicación de la sede.
  - Contacto1: Código de un contacto de la ETSI para la sede. Este código identifica de manera unívoca al contacto. Su valor será igual al de alguno de los elementos de la tabla “Contactos”. Ejemplo: CON_ETSI_00001
  - Contacto2: Código de un contacto de la ETSI para la sede. Este código identifica de manera unívoca al contacto. Su valor será igual al de alguno de los elementos de la tabla “Contactos”. Ejemplo: CON_ETSI_00001
- ANS:
  - Cod_ANS: Código alfanumérico único que identificará al ANS. Este código se generará automáticamente al dar de alta el ANS en la CMDB Ejemplo: ANS_ETSI_00001
  - Unidad: Indica la unidad del KPI para este ANS. Ejemplo: horas.
  - Max: Umbral de ANS para el KPI.
- INFORMES:
  - Cod_Inf: Código alfanumérico único que identificará al informe. Este código se generará automáticamente al dar de alta el informe en la CMDB Ejemplo: INFO_ETSI_00001
  - Tipo: Indica si es un informe de calidad de servicio, de mantenimiento preventivo o de una incidencia.
  - Cod_ANS: Código del ANS que aplica a este informe. Este código identifica de manera unívoca al ANS. Su valor será igual al de alguno de los elementos de la tabla “ANS”. Ejemplo: ANS_ETSI_00001
  - Fec_Pet: Fecha en la que se solicita el informe.
  - Fec_Ent: Fecha de entrega del informe.
  - Cod_Inc: Código del ticket tipo incidencia, si aplica, sobre el que versa el informe. Su valor será igual al de alguno de los elementos de la tabla “Tickets”. Ejemplo: TIC0000000000001.
  - Cod_Tic: Código del ticket tipo petición donde se solicitó el informe. Su valor será igual al de alguno de los elementos de la tabla “Tickets”. Ejemplo: TIC0000000000002.
- CONTACTOS:
  - Cod_contac: Código alfanumérico único que identificará al contacto. Este código se generará automáticamente al dar de alta al contacto en la CMDB. Ejem: CON_ETSI_00001
  - Nombre: Nombre del contacto.

- Apellido 1: Primer apellido del contacto.
- Apellido 2: Segundo apellido del contacto.
- Email: Dirección de correo electrónico del contacto.
- Fijo: Número de teléfono fijo del contacto.
- Móvil: Número de teléfono móvil del contacto.
- Organización: Cliente al que pertenece el contacto. En este caso sería la ETSI.
- Cod_Sede: Código de la sede en la que se ubica el contacto. Este código identifica de manera unívoca a la sede. Su valor será igual al de alguno de los elementos de la tabla "Sedes". Ejemplo: SEDE_ETSI_00001.

8.3.14.2 **CMDB**

La CMDB (Configuration Management DataBase) es la base de datos donde se administrarán y gestionarán todos los elementos de configuración del servicio (Configuration Ítems o CIs). Esta base de datos está compuesta por una serie de tablas relacionadas entre sí:

ELEMENTOS		
Clave	Campo	Tipo
Sí	Cod_Ele	Alfanumérico
Sí	Num_Ser	Alfanumérico
No	Cod_Prod	Alfanumérico
No	Fabricante	Texto
No	Modelo	Texto
No	Tipo	Texto
No	Caract	Texto
No	Cod_Sede	Alfanumérico
No	Cod_ANS	Alfanumérico
No	Fin_Garantia	Fecha
No	Cod_Gar	Alfanumérico

PIEZAS		
Clave	Campo	Tipo
Sí	Cod_Pie	Alfanumérico
Sí	Num_Ser	Alfanumérico
No	Cod_Prod	Alfanumérico
No	Fabricante	Texto
No	Modelo	Texto
No	Tipo	Texto
No	Caract	Texto
No	Cod_Ele	Alfanumérico
No	Fin_Garantia	Fecha
No	Cod_Gar	Alfanumérico

GARANTIAS		
Clave	Campo	Tipo
Sí	Cod_Gar	Alfanumérico
No	Proveedor	Texto
No	Calle	Texto
No	Numero	Numérico
No	Portal	Alfanumérico
No	Piso	Alfanumérico
No	Escalera	Texto
No	Localidad	Texto
No	Provincia	Texto
No	Pais	Texto
No	CP	Texto
No	Email	Texto
No	Telefono	Numérico
No	Unidad	Texto
No	Tiempo Rep	Tiempo Rep

Ilustración 8-14 Tablas CMDB

A continuación, se describe cada uno de los campos para cada tabla:

- ELEMENTOS:
  - Cod_Ele: Código alfanumérico único que identificará al elemento. Este código se generará automáticamente al dar de alta el elemento en la CMDB. Ejem: ELE_ETSI_00001
  - Num_Ser: Número de serie del elemento.
  - Cod_Prod: Código de producto o part number del elemento.
  - Fabricante: Fabricante del elemento. En este caso será HP o Panasonic.
  - Modelo: Nombre comercial del elemento. Ejemplo: HP ProLiant MicroServer Gen10
  - Tipo: Catalogación del elemento. En este caso podrá ser Pantalla o Servidor.
  - Caract: Breve resumen de las características del elemento. Ejemplos: número de pulgadas de la pantalla, cantidad de memoria de disco duro del servidor.

  - Cod_Sede: Código de la sede en la que se ubica el elemento. Este código identifica de manera unívoca a la sede. Su valor será igual al de alguno de los elementos de la tabla "Sedes". Ejemplo: SEDE_ETSI_00001
  - Cod_ANS: Código del ANS que aplica a este elemento. Este código identifica de manera unívoca al ANS. Su valor será igual al de alguno de los elementos de la tabla "ANS". Ejemplo: ANS_ETSI_00001
  - Fin_Garantia: Fecha de fin de garantía de fabricante.
  - Cod_Gar: Código de la garantía que afecta al elemento. Este código identifica de manera unívoca a la garantía. Su valor será igual al de alguno de los elementos de la tabla "Garantias". Ejemplo: GAR_00000001.

- PIEZAS:
  - Cod_Pie: Código alfanumérico único que identificará a la pieza. Este código se generará automáticamente al dar de alta la pieza en la CMDB. Ejemplo: PIE_ETSI_00001
  - Num_Ser: Número de serie de la pieza.
  - Cod_Prod: Código de producto o part number de la pieza.
  - Fabricante: Fabricante de la pieza. Ejemplo: AMD.
  - Modelo: Nombre comercial del elemento. Ejemplo: AMD Opteron X3216
  - Tipo: Catalogación de la pieza. Ejemplos: Microprocesador, memoria RAM, etc.
  - Caract: Breve resumen de las características de la pieza. Ejemplos: Velocidad del microprocesador, tamaño del módulo de memoria RAM.
  - Cod_Ele: Código del elemento al que pertenece la pieza. Este código identifica de manera unívoca al elemento. Su valor será igual al de alguno de los elementos de la tabla "Elementos". Ejemplo: ELE_ETSI_00001.
  - Fin_Garantia: Fecha de fin de garantía de fabricante.
  - Cod_Gar: Código de la garantía que afecta al elemento. Este código identifica de manera unívoca a la garantía. Su valor será igual al de alguno de los elementos de la tabla "Garantias". Ejemplo: GAR _00000001.

- GARANTIAS:
  - Cod_Gar: Código alfanumérico único que identificará a la garantía. Este código se generará automáticamente al dar de alta la garantía en la CMDB Ejemplo: GAR_00000001.
  - Proveedor: Nombre del fabricante o interlocutor con el que gestionar la garantía de la pieza o elemento.
  - Calle: Nombre de la calle donde se encuentra el proveedor.
  - Numero: Número de la calle donde se encuentra el proveedor.
  - Portal: Número del portal donde se encuentra el proveedor.
  - Piso: Código del piso donde se encuentra el proveedor.
  - Escalera: Código de la escalera donde se encuentra el proveedor.
  - Localidad: Localidad. donde se encuentra el proveedor.
  - Provincia: Provincia donde se encuentra el proveedor.
  - Pais: País donde se encuentra el proveedor.
  - CP: Código Postal que corresponde a la ubicación del proveedor.
  - Email: Dirección de correo electrónico del proveedor con el que gestionar la garantía.

- Telefono: Número de teléfono del proveedor con el que gestionar la garantía.
- Unidad: Indica en qué se va a medir el tiempo de reposición de la pieza o elemento. Ejemplo: Días, horas.
- Tiempo_Rep: Tiempo de reposición por parte del proveedor del elemento o pieza.

8.3.15 Gestión de la Configuración y Activos del Servicio

En este servicio este proceso consistirá en mantener debidamente actualizada la CMDB. El grupo encargado de realizar estás actualizaciones será el CAU.

Cada vez que se produzca alguna modificación en algún CI, ya sea por sustitución de hardware por una incidencia, problema o cambio, traslado, modificación de la persona de contacto, etc. el CAU actualizará la CMDB recogiendo dicha modificación.

En Cualquier caso, el Gestor del Servicio será el responsable último de velar por la integridad y coherencia de la CMDB.

8.3.16 Gestión del Conocimiento

Cómo se ha comentado anteriormente todas las resoluciones de las incidencias estarán almacenadas dentro de la Base de datos de Tickets. Al margen de esto, el proveedor dispone de un repositorio interno de documentación sobre los servicios que presta. Que puede ser consultado por todas las áreas de su organización.

8.3.17 Mejora Continua del Servicio

La Mejora Continua del Servicio tiene como objetivo evaluar la calidad del servicio prestado e identificar los aspectos susceptibles de ser modificados para ofrecer una mayor calidad.

Se trata de un proceso iterativo, basado en el ciclo de Deming (Plan, Do, Check, Act).

La aplicación de este proceso abarca todo el ciclo de vida del servicio, lo que garantiza asegurar la calidad de extremo a extremo.

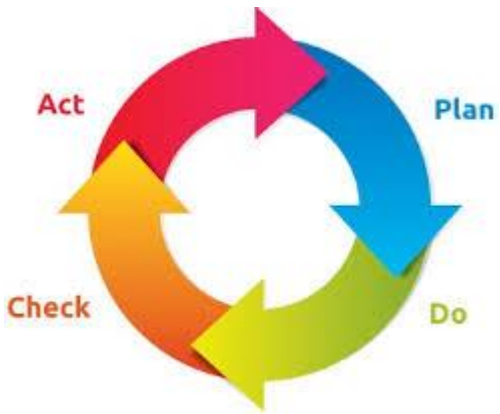


Ilustración 8-15 Ciclo PDCA

1. Plan: Esta fase tiene como objetivo la identificación de las mejoras del servicio ya sea a través de la realización de encuesta de satisfacción a los usuarios, análisis de los informes de Calidad del Servicio, Incidencias y Mantenimiento Preventivo, así como de los procesos de Gestión de Incidencias y Gestión de Problemas. Comprende las siguientes actividades:

- Análisis de la situación actual: El Gestor del Servicio asumirá el rol de Responsable de Mejora Continua. Se encargará de realizar un análisis de los diversos inputs indicados anteriormente, con el objetivo de identificar puntos de mejora. Entre las tareas a realizar se encuentran las siguientes:
  - Análisis de los principales KPIs del proceso.

  - Análisis de la información recogida en la base de datos de conocimiento.
  - Análisis de los problemas e incidencias vigentes para identificar puntos de mejora en el servicio.
- Identificación de mejoras: Tras el análisis de la situación, el responsable de la Mejora Continua identificará las posibles mejoras a implementar.
- Valoración de las mejoras: El Gestor del Servicio será el encargado de valorar las mejoras identificadas. El Gestor del Servicio se podrá apoyar en el departamento comercial o técnico que corresponda dentro de su organización

2. Do: El Gestor del Servicio solicitará a la ETSI la generación de una Petición para poder aplicar la mejora. En caso de que la ETSI apruebe dicha solicitud se procederá a implementar la mejora siguiendo el proceso de Gestión del Cambio.

3. Check: El Gestor del Cambio verificará que la mejora ha tenido el efecto esperado dentro de un margen aceptable. Se recopilarán los datos de las pruebas realizadas

4. Act: En esta fase, el Gestor del Cambio usará los datos obtenidos de la fase anterior, para ajustar los parámetros de la mejora implementada con el objetivo de que la mejora tenga un efecto más cercano al deseado

Si la mejora queda fuera del alcance del contrato de servicio subscrito entre el proveedor y la ETSI, el proveedor podrá realizar a la ETSI una oferta económica adicional a la del servicio para implantar dicha mejora.

8.4 Valoración económica

Para la prestación del servicio se adquirirán repuestos dedicados por el siguiente importe:

Descripción	Unidades	Importe total
HP ProLiant MicroServer Gen10	1	384,72€
Panasonic TX-40ES513	1	449,00€

Tabla 8-5 Valoración repuestos

Estas cantidades serán prorrateadas dentro del importe mensual del servicio de mantenimiento.

En la valoración económica están incluidos los siguientes conceptos:

- Visitas y actuaciones de mantenimiento preventivo.
- Gestor de Servicio con dedicación no exclusiva.
- Prorrateo de los Repuestos.
- Técnicos in-situ para las actuaciones.
- CAU.

Teniendo en cuanto todos estos conceptos y considerando una duración del contrato de 24 meses se calcula que la valoración del servicio será:

Descripción	Importe mensual
Servicio de mantenimiento de puntos de información	110,00€

Tabla 8-6 Valoración Servicio

9 CONCLUSIONES Y LÍNEAS DE DESARROLLO FUTURAS

En este proyecto se ha explicado en qué consiste la metodología ITIL v3. Recordemos que ITIL es una filosofía, una guía de buenas prácticas orientada a la prestación de servicios de TI (Tecnología de la Información).

ITIL se basa en establecer procesos dentro de la organización que presta un servicio y dentro del propio servicio en sí para poder aportar al usuario la máxima calidad posible.

Recordemos que un usuario que hace uso de un servicio TI no tienen por qué saber cómo funciona, ni a nivel técnico ni siquiera a nivel organizativo, lo que realmente le interesa es que funcione de acuerdo con sus expectativas.

Si contrato un nuevo servicio de Internet en casa y sufro una avería, lo que me interesa es que me solucionen la avería lo más pronto posible y mientras la reparan tener la posibilidad de saber en qué estado se encuentra. Si el prestador del servicio consigue que sus clientes perciban que se atienden sus problemas con rapidez, informando de los pasos a dar y solucionándolo correctamente al primer intento, el usuario se verá menos tentado de acudir a la competencia. Si a esto le unimos que la organización realice mejoras en el servicio que el usuario demande (mejorar la velocidad, proactividad ante averías), tendremos prácticamente fidelizado al cliente, será muy complicado para la competencia hacer que los contrate a ellos.

Nótese que en esta fidelización se han seguido las cinco fases del ciclo de vida del servicio que se definen en ITIL:

- Estrategia del servicio: Antes de ofrecer el servicio se ha realizado un estudio de mercado para ver si es algo que los clientes puedan necesitar.
- Diseño del servicio: De acuerdo con lo obtenido en la fase anterior, se ha diseñado un servicio de acceso a Internet que se adapta a lo que demandan los usuarios.
- Transición del servicio: Se ha dotado de los recursos humanos (operadores, técnicos especialistas) y materiales necesarios (routers, teléfonos, etc.) para poder prestar el servicio. Además, se han hecho todos los test necesarios y se ha creado una base de datos (CMDB) con todos los elementos que forman parte del servicio. También se han definido todos los procesos para operación del servicio.
- Operación del servicio: Se ha coordinado eficientemente la gestión de la avería reportada por el usuario, consiguiendo que su resolución sea correcta y rápida, además de mantener informado al usuario.
- Mejora Continua del servicio: Se ha estudiado lo que los usuarios parecen demandar y se ha aumentado por ejemplo la velocidad del acceso a internet.

Esto es lo que se ha intentado mostrar en el servicio de ejemplo explicado en este proyecto, el cómo siguiendo las buenas prácticas de ITIL es posible definir cualquier servicio.

El ejemplo de este proyecto es un servicio relativamente sencillo, de mantenimiento de hardware. La potencia de ITIL está en que la organización que presta este servicio tan simple se puede adaptarse con relativa facilidad para prestar un servicio más complejo.

Supongamos que la ETSI requiere que además del mantenimiento del hardware, la misma organización gestione los contenidos que se muestran en los puntos de información, es decir, que administre el servidor. La empresa que presta el servicio tan sólo tendría que definir un nuevo grupo especializado en la gestión de contenidos e incorporarlo a su estructura y definir su rol en os procesos ya implementados.

Los procesos de ITIL son totalmente independientes de la tecnología empleada. Esto confiere a la organización una capacidad de adaptación que es de vital importancia en el mercado de las TI. No olvidemos

que las TI evolucionan continuamente y las organizaciones que no se adaptan a esta evolución terminan desapareciendo o formando parte de otras que sí lo han hecho. Adelantarse a la competencia es muy importante en este mercado.

A nivel interno aporta ventajas, el flujo de los procesos de ITIL es casi siempre horizontal, por ejemplo, el CAU habla directamente con los Técnicos In-situ de una forma estructurada que reduce el riesgo de errores y las posibilidades de confusión, así como agiliza la gestión. En otros modelos más tradicionales se tiende más a que la comunicación sea vertical, provocando a veces que se pierda la información en ese tránsito y teniendo el riesgo de generar un cuello de botella en la unidad jerárquica superior (las unidades superiores suelen tener una dimensión menor que las inferiores).

A pesar de todo lo expuesto no conviene olvidar que los procesos los aplican en última instancia las personas, las cuales pueden cometer errores, lo cual puede llevar a una menor calidad del servicio. Con ITIL no se consigue "inmunizar" a la organización ante errores puntuales, pero sí minimizar el riesgo de que sucedan y minimizar su impacto.

ITIL a su vez también va evolucionando, actualmente ha cambiado la nomenclatura, ITIL v3 vendría a equivaler a ITIL 2011. Aunque desde 2011 se han ido realizando pequeñas modificaciones, por lo que actualmente tendríamos ITIL 2018. Estas modificaciones vienen a corregir algún error en la definición de algún proceso, pero no conlleva ningún cambio tan profundo como el que se produjo entre ITIL v2 e ITIL v3. En cualquier caso, no es descartable que en futuro no muy lejano se reformule la estructura de ITIL y tengamos una especie de ITIL v4, la propia ITIL también está sujeta al ciclo de vida del servicio y por lo tanto le aplica la fase de mejora continua del servicio.

10 REFERENCIAS

- Libros oficiales ITIL:
  - AXELOS. *ITIL® Service Strategy 2011 edition*. Editor: THE STATIONERY OFFICE. Fecha de publicación: 29/07/2011. ISBN: 9780113313044
  - AXELOS. *ITIL® Service Design 2011 edition*. Editor: THE STATIONERY OFFICE. Fecha de publicación: 29/07/2011. ISBN: 9780113313051
  - AXELOS. *ITIL® Service Transition 2011 edition*. Editor: THE STATIONERY OFFICE. Fecha de publicación: 29/07/2011. ISBN: 9780113313068
  - AXELOS. *ITIL® Service Operation 2011 edition*. Editor: THE STATIONERY OFFICE. Fecha de publicación: 29/07/2011. ISBN: 9780113313075
  - AXELOS. *ITIL® Continual Service Improvement 2011 edition*. Editor: THE STATIONERY OFFICE. Fecha de publicación: 29/07/2011. ISBN: 9780113313082

- Otras referencias:
  - *Curso online ITIL Osiatis*. ©2010-2017 [consulta: 10 de enero de 2017] Disponible en http://itilv3.osiatis.es/
  - Panasonic España: https://www.panasonic.com/es/
  - HP: http://www8.hp.com/es/

ÍNDICE DE CONCEPTOS

GLOSARIO

Accountable: Responsable

ANS: Acuerdo de Nivel de Servicio

Back-out: Marcha atrás o retirada del cambio.

Back-up: Copia de seguridad

BCM: Business Continuity Management. Gestión de la Continuidad del Negocio.

Benchmark: Prueba de rendimiento comparativa

Bug: Error, fallo.

CAB: Change Advisory Board. Comité Asesor del Cambio.

Call Center: Centro de llamadas.

CAU: Centro de Atención al Usuario.

CCTA: Central Computer and Telecommunications Agency. Agencia Central de Informática y Telecomunicaciones.

CDB: Capacity Database. Base de Datos de la Capacidad.

CFIA*:* Component Failure Impact Analysis. Análisis del Impacto del Fallo del Componente.

CI: Configuration Item. Elemento de configuración.

CIF: Código de Identificación Fiscal.

CMDB: Configuration Management Database. Base de Datos de la Gestión de la Configuración.

CMI: Cuadro de Mando Integral.

CMS: Configuration Management System. Sistema de Gestión de la Configuración.

Cold standby: Método de redundancia, en el que el respaldo sólo es utilizado cuando cae el principal.

Consulted: Consultado

CPU: Central Processing Unit. Unidad Central de Procesamiento

CRAMM: CCTA Risk Analysis and Management Method. Método de Gestión y Análisis de Riesgos de la CCTA

CRM: Customer Relationship Management. Gestión de la Relación con el Cliente.

CSF: Critical success factor. Factor Crítico de Éxito.

CSI: Continual Service Improvement. Mejora continua del Servicio.

DAFO: Debilidades Amenazas Fortalezas Oportunidades.

DDoS: Distributed Denial-of-Service. Denegación de Servicio Distribuida.

DIKW: Data Information Knowledge Wisdom. Datos Información Conocimiento Sabiduría.

DML: Definitive Media Library. Biblioteca de Medios Definitivos**.**

DS: Definitive Spare. Repuesto Definitivo.

Early-access: Acceso anticipado.

ELS: Early Life Support. Soporte post-implantación.

ETSI: Escuela Técnica Superior de Ingeniería.

Feedback: Respuesta recibida por un interlocutor o sistema.

FSC: Checklist Forward Schedule of Changes. Calendario de cambios.

FTA: Failure Tree Analysis. Análisis del Árbol de Fallos.

Función: Unidad especializada en realizar una cierta actividad

Help Desk: Centro de Soporte

Hot standby: Método de redundancia, en el que el respaldo funciona en paralelo con el principal, conteniendo ambos siempre la imsma información.

Incidencia: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.

Informed: Informado.

ITSCM: IT Service Continuity Management. Gestión de la continuidad del Servicio de TI.

KEDB: Known Error Database. Base de Datos de Errores Conocidos.

KPI: Key Performance Indicator. Indicador Clave de Rendimiento.

LOPD: Ley Orgánica de Protección de Datos.

MTBF: Mean Time Between Failures. Tiempo Medio Entre Fallos.

MTBSI: Mean Time Between Service Incidents. Tiempo Medio Entre Incidencias del Servicio.

MTTR: Mean Time To Repair. Tiempo Medio Para Reparar.

OLA: Operational Level Agreement. Acuerdo de Nivel de Operación.

PDCA: Plan Do Check Act. Planificar Hacer Verificar Actuar.

Petición: Solicitud sobre el servicio.

PIR: Post Implementation Review. Revisión Post Implementación.

Problema: causa subyacente, aún no identificada, de una serie de incidencias o una incidencia aislada de importancia significativa

Project Manager: Gestor o Jefe de Proyecto.

Puntos de información: Lugares de la ETSI en los que hay instaladas una o más pantanllas mostrando diversa información.

RACI: Responsible Accountable Consulted Informed. Encargado Responsable Consultado Informado.

RAD: Rapid Application Development. Desarrollo Rápido de Aplicaciones.

RAM: Random Access Memory. Memoria de Acceso Aleatorio.

Responsible: Encargado

RFC: Request For Change. Petición de Cambio.

ROI: Return On Investment. Retorno de la Inversión.

Rol: Conjunto de actividades y responsabilidades asignada a una persona o grupo.

Roll-back: Retorno a la última versión estable.

Roll-out: Despliegue.

RRHH: Recursos Humanos.

SAC: Service Acceptance Criteria. Criterios de Aceptación del Servicio.

SCD: Supplier and Contract Database. Base de Datos de Suministradores y Contratos

SDP: Service Design Package. Paquete de Diseñe del Servicio.

Service Desk: Centro de Servicios.

SIP: Service Improvement Plan. Plan de Mejora del Servicio.

SLA: Service Level Agreement. Acuerdo de Nivel de Servicio.

SLR: Service Level Requirements. Requisitos de Nivel de Servicio.

SKMS: Service Knowledge Management System. Sistema de Gestión del Conocimiento en Servicios.

SOA: Service Outage Analysis. Análisis de Interrupción del Servicio.

SP: Service Packet. Paquete de Servicios.

SQP: Service Quality Plan. Plan de Calidad del Servicio.

Support: Apoyo, Soporte.

TCO: Total Cost of Ownership. Coste Total de la Propiedad.

Ticket: Unidad de comunicación entre el cliente y el proveedor.

UC: Underpinning Contract.

VOI: Value on Investment. Valor de la Inversión

Warm standby: Método de redundancia intermedio entre Cold standby y Hot standby. En este caso el respaldo trabaja en paralelo con el principal, pero la información del principal se vuelca en el respaldo con menos frecuencia que en el Hot standby

Workaround: Solución temporal.

Workflow: Flujo de trabajo.

ANEXO A: INFORME DE CALIDAD DE SERVICIO

1. Introducción

El presente documento detalla la situación del servicio mediante información e indicadores agrupados en los diferentes procesos del servicio.

Este informe abarca el periodo 01/03/2018 – 31/03/2018

2. Gestión de incidencias

En los siguientes apartados se reflejan diferentes aspectos del proceso de Gestión de Incidencias. Se considera una incidencia cualquier evento que no forma parte de la operación estándar del servicio y que causa, o puede causar una interrupción o una reducción de la calidad del servicio.

a. Resumen

A continuación, se muestra una tabla con los valores más relevantes en cuanto a calidad de servicio en la gestión de incidencias.

Número de incidencias	Tiempo medio de respuesta	ANS tiempo de respuesta correcto	ANS tiempo de resolución correcto	Masivas
7	3 min	7 (100%)	6 (85,7%)	3

b. Detalle de las incidencias

En la siguiente tabla se muestra el detalle de todas las incidencias registradas en el periodo 01/03/2018 – 31/03/2018

ID	Fecha de apertura	Fecha de respuesta	Fecha de resolución	Descripción	Solución	ANS
TIC0000101	05/03/2018 09:00	05/03/2018 09:02	05/03/2018 11:15	La pantalla situada en la zona NE no enciende.	Tras comprobaciones en remoto, el usuario observa que la toma de corriente no hace buen contacto. Ajusta el cable de alimentación y vuelve a encender la pantalla.	OK

ID	Fecha de apertura	Fecha de respuesta	Fecha de resolución	Descripción	Solución	ANS
TIC0000102	06/03/2018 10:11	06/03/2018 10:14	08/03/2018 09:30	Una parte de la pantalla situada en la zona NO no se ilumina quedándose en negro	Se sustituye la pantalla y se deja funcionando.	NO OK
TIC0000103	09/03/2018 10:30	09/03/2018 10:34	12/03/2018 09:30	En el servidor aparecen continuos pantallazos azules.	Se sustituye el servidor y se deja funcionando.	OK
TIC0000104	14/03/2018 12:00	14/03/2018 12:03	15/03/2018 09:45	El servidor se queda bloqueado continuamente.	Se sustituye el servidor y se deja funcionando. Se procede a apertura ticket de tipo problema por reiteración de incidencias similares	OK
TIC0000106	21/03/2018 10:33	21/03/2018 10:35	26/03/2018 09:14	La pantalla situada en la parte superior izquierda de Secretaría no enciende.	Se sustituye la pantalla y se deja funcionando.	OK
TIC0000107	21/03/2018 10:40	21/03/2018 10:43	26/03/2018 10:18	La pantalla situada en la parte superior central de Secretaría no enciende.	Se sustituye la pantalla y se deja funcionando.	OK
TIC0000108	21/03/2018 10:45	21/03/2018 10:47	26/03/2018 11:11	La pantalla situada en la parte superior derecha de Secretaría no enciende.	Se sustituye la pantalla y se deja funcionando.	OK

c. Incidencias Masivas

Se indican las incidencias marcadas cómo masivas, agrupándolas según las fechas y las causas:

ID	FECHA	CAUSA
TIC0000106	**21/03/2018**	**Fallo generalizado en fuentes de alimentación debido a un pico de tensión.**
TIC0000107		
TIC0000108		

3. Gestión de Problemas

En los siguientes apartados se reflejan diferentes aspectos del proceso de Gestión de Problemas. Se considera un problema cualquier situación no deseada que provoca una o más incidencias existentes o potenciales en el servicio. El problema puede tener una causa desconocida o un error conocido.

a. Indicadores de Gestión del Problema

Se indican los valores de los indicadores más representativos para el periodo en estudio:

Problemas registrados	Problemas abiertos (sin solución)	Problemas resueltos correcto	Tiempo medio de resolución	Incidencias causadas
1	0	1	10 días	2

b. Detalle de los problemas

En la siguiente tabla se muestra el detalle de todos los problemas registrados en el periodo 01/03/2018 – 31/03/2018.

ID	Fecha de apertura	Fecha de respuesta	Fecha de resolución	Descripción	Solución
TIC0000105	15/03/2018 09:50	15/03/2018 09:54	25/03/2018 09:00	El servidor se bloquea continuamente, generando errores del tipo “blue screen”	Ver texto anexo

Solución: Se realizan pruebas con el servidor de respaldo. Se instala el último parche de actualización del sistema operativo y se deja el servidor en observación 2 días. Tras comprobar la estabilidad se solicita a la ETSI que instale el parche en el servidor en producción. Tras la instalación del parche la ETSI no observa bloqueos en 3 días consecutivos por lo que se procede al cierre del problema.

4. Gestión de Peticiones

En los siguientes apartados se refleja la información sobre las peticiones registradas durante el periodo 01/03/2018 – 31/03/2018.

a. Resumen

A continuación, se muestra una tabla con los valores más relevantes en cuanto a calidad de servicio en la gestión de peticiones:

Número de peticiones	Tiempo medio de respuesta	ANS tiempo de respuesta correcto	ANS tiempo de resolución correcto
2	**3 min**	**2 (100%)**	**2 (100%)**

b. Detalle de las peticiones

En la siguiente tabla se muestra el detalle de todas las peticiones registradas en el periodo 01/03/2018 – 31/03/2018

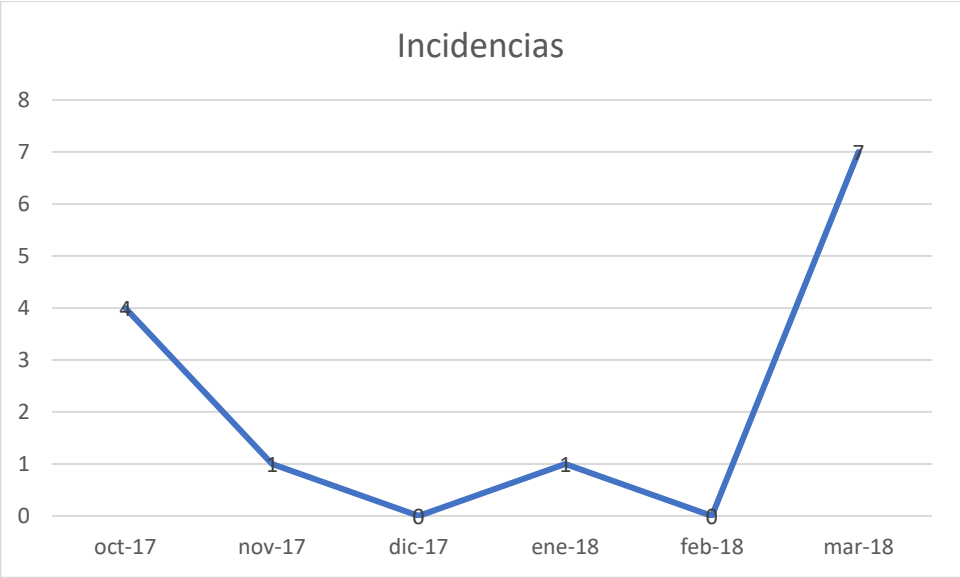
ID	Fecha de apertura	Fecha de respuesta	Fecha de resolución	Descripción	Solución	ANS
TIC0000109	25/03/2018 09:12	25/03/2018 09:15	25/03/2018 09:51	Se solicita se modifique la imagen del servidor de respaldo con los cambios realizados para subsanar el problema TIC0000105	Se actualiza imagen	OK
TIC0000110	26/03/2018 11:13	26/03/2018 11:16	27/03/2018 09:32	Se solicita informe sobre la incidencia TIC0000108	Se entrega informe	OK

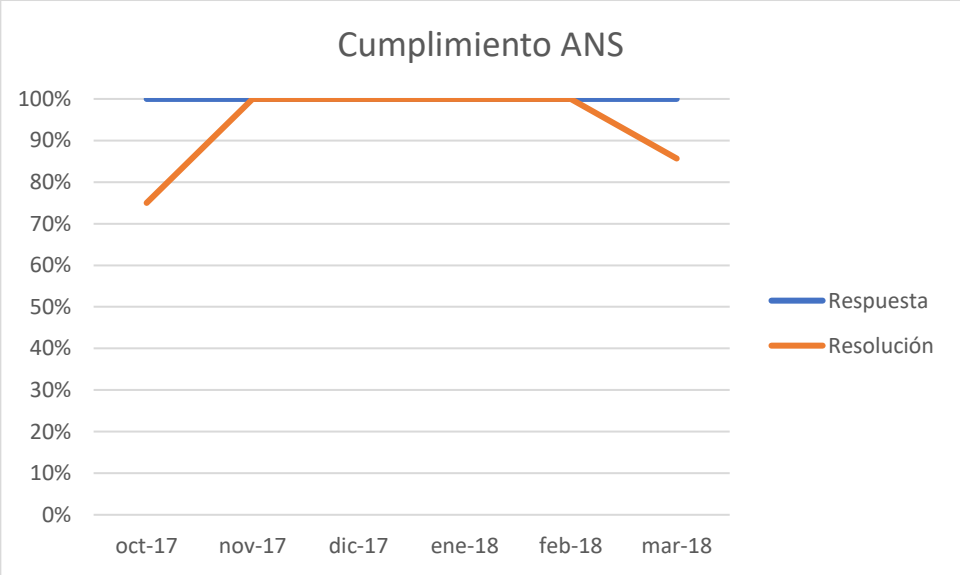
5. Tendencias sobre datos históricos

En este apartado se describen los datos sobre tendencias por periodos en aquellos procesos de los que se disponga datos históricos:

a. Gestión de incidencias

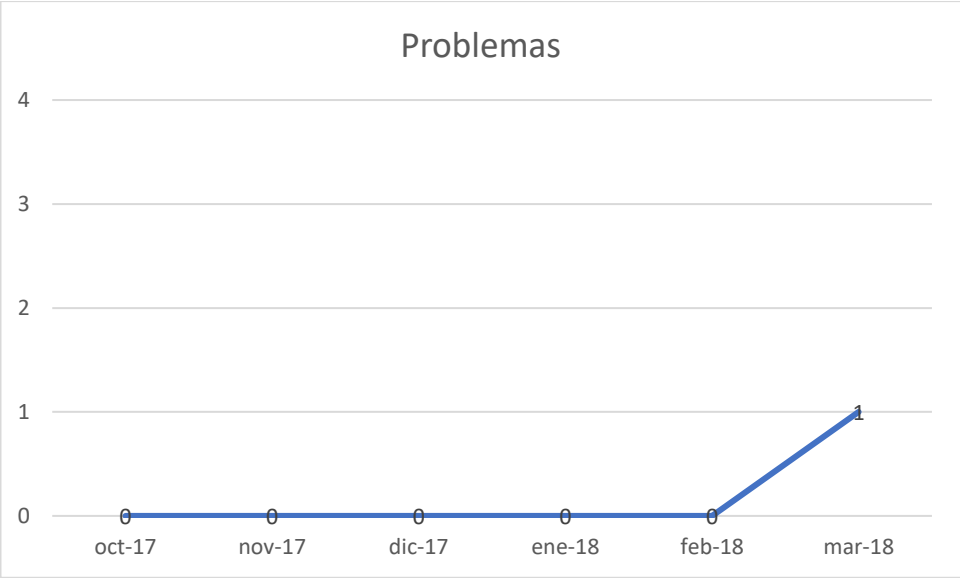
Parámetro	oct-17	nov-17	dic-17	ene-18	feb-18	mar-18
Incidencias resueltas	4	1	0	1	0	7
Cumplimiento tiempo de respuesta	100%	100%	100%	100%	100%	100%
Cumplimiento tiempo de resolución	75%	100%	100%	100%	100%	85,70%





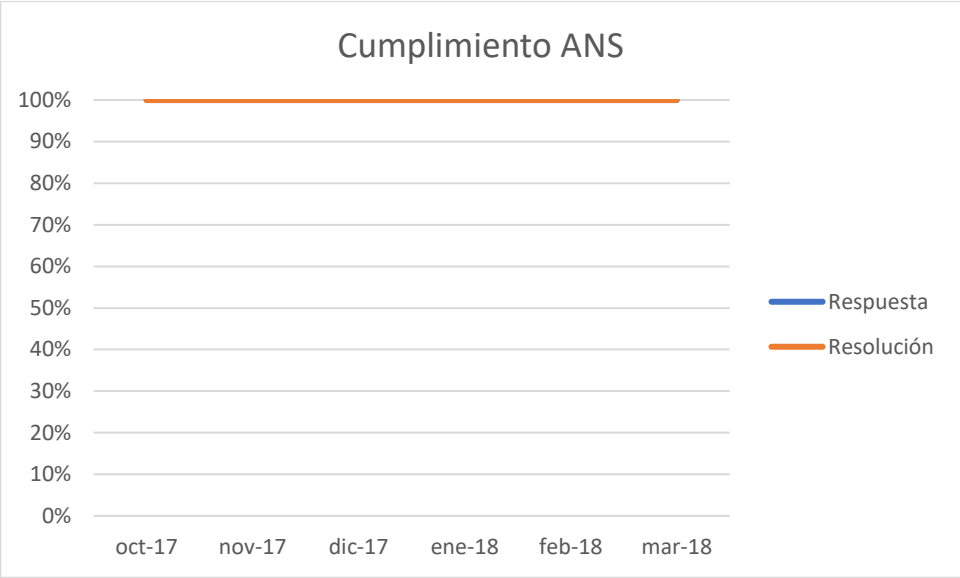
b. Gestión de problemas

Parámetro	oct-17	nov-17	dic-17	ene-18	feb-18	mar-18
Problemas resueltos	0	0	0	0	0	1



c. Gestión de Peticiones

Parámetro	oct-17	nov-17	dic-17	ene-18	feb-18	mar-18
Peticiones resueltas	1	0	0	0	0	2
Cumplimiento tiempo de respuesta	100%	100%	100%	100%	100%	100%
Cumplimiento tiempo de resolución	100%	100%	100%	100%	100%	100%



ANEXO B: INFORME DE MANTENIMIENTO PREVENTIVO

1. Introducción

En este documento se muestra el resultado de las actuaciones y revisiones realizadas por los técnicos in-situ realizada el pasado 15 de enero de 2018 en el marco del mantenimiento preventivo de los puntos de información de la Escuela Técnica Superior de Ingenieros de Sevilla.

2. Puntos de información

Cada equipo perteneciente a los puntos de información se revisa de forma independiente, realizando las siguientes verificaciones.

a. Verificación del estado físico

i. Procedimiento

En esta prueba se comprueba el estado físico del dispositivo mediante inspección visual encaminada a descubrir defectos externos provocados por:

- **Manipulación indebida.**
- **Derramamiento de líquidos.**
- **Golpes.**
- **Fuego.**

Si el dispositivo revisado no presenta síntomas externos de haber sufrido daños, se considerará como "físicamente óptimo", en caso contrario, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

El resultado de la inspección física de todos los dispositivos determinó que no habían sufrido daño alguno, considerándose su **estado como óptimo**.

b. Verificación del cableado

i. Procedimiento

Esta revisión pretende determinar el correcto estado de todos los cables que llegan al dispositivo a revisar, comprobando físicamente los siguientes aspectos:

- **Correcto anclaje de los cables de alimentación eléctrica.**
- **Correcto anclaje de los cables de enlace de datos.**
- **Estado físico de los cables de datos y de alimentación eléctrica.**
- ✓ **No existen torceduras en los cables.**
- ✓ **No existe aplastamiento en los cables.**
- ✓ **No existe falta de aislamiento en los cables.**
- ✓ **No existen enredos entre los cables.**

En el caso de existir alguna discrepancia con alguno de los aspectos referidos al cableado, se procede a su anotación y corrección inmediata. Si no fuera posible realizar la adecuación del cableado durante la visita Preventiva, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

Esta inspección determinó que el estado de los cables de alimentación eléctrica y de datos están correctamente anclados y libres de daños, siendo su **estado óptimo para el funcionamiento.**

c. Verificación de los indicadores de fallo y encendido.

i. Procedimiento

Esta prueba requiere la desconexión del equipo, quedando el mismo fuera de servicio durante el tiempo de duración de la misma, por lo que se deberá de convenir con los responsables adecuados del cliente, la fecha y hora más adecuadas para esta actuación, advirtiendo que puede existir el riesgo de que el equipo no arranque

correctamente o que se den situaciones de anomalía que impliquen la sustitución del equipo y una parada de los servicios que presta, superior a la prevista.

Esta verificación pretende determinar si los indicadores o Leds del equipo están en perfecto estado y si su función es idónea. Así mismo, esta prueba pretende comprobar que los diagnósticos de arranque progresan correctamente, sin detectar anomalías internas en el dispositivo.

La prueba se realiza apagando o "reseteando" el equipo y siguiendo la secuencia de arranque del mismo, según se especifica en el manual o guía de operaciones del mismo.

Cuando un dispositivo es conectado y su secuencia coincide con la descrita en la guía de operaciones y queda en estado preparado, indicado por los Leds e indicadores adecuados, o por los mensajes que presenta en su Consola de Gestión fuera de banda, se entiende que ha pasado todos los tests internos de arranque y que éstos han sido satisfactorios.

En el caso de que el dispositivo no realice la función de arranque de acuerdo con las indicaciones de la guía de operaciones o su estado final no sea el óptimo o bien sus indicadores muestren un síntoma de error, se anotará dicha circunstancia, en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

Todas las pantallas se encendieron con normalidad, no se observó ninguna anomalía por lo que se considera que su **estado es óptimo.**

d. Verificación de la temperatura

i. Procedimiento

Esta prueba está destinada a comprobar si la temperatura ambiente en la sala o armario en el que se esté ubicado el dispositivo se encuentra entre los rangos, establecidos como válidos, por el fabricante y reflejados en la guía de operaciones del equipo.

Esta comprobación de la temperatura se realiza mediante un termómetro digital. Con el resultado de la medición se comprueba si la temperatura, se encuentra en el rango válido, indicado por el fabricante para el correcto funcionamiento de los equipos.

En función de los valores obtenidos en la medición de la temperatura, se harán, las recomendaciones adecuadas para reducir o aumentar la misma, hasta un valor intermedio en el rango válido. En caso de que la temperatura quede fuera de los rangos establecidos por el fabricante, se indicará al cliente, que tome las medidas oportunas para corregir la situación, mediante la incorporación de la ventilación, calefacción o refrigeración adecuadas, para subsanar el defecto ambiental detectado.

ii. Resultado

Las temperaturas tomadas en las ubicaciones han estado dentro de los márgenes recomendables.

3. Servidor

Sobre el servidor se realizaron las siguientes verificaciones,

a. Verificación del estado físico

i. Procedimiento

En esta prueba se comprueba el estado físico del dispositivo mediante inspección visual encaminada a descubrir defectos externos provocados por:

- **Manipulación indebida.**
- **Derramamiento de líquidos.**
- **Golpes.**
- **Fuego.**

Si el dispositivo revisado no presenta síntomas externos de haber sufrido daños, se considerará como "físicamente óptimo", en caso contrario, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

El resultado de la inspección física del dispositivo determinó que no había sufrido daño alguno, considerándose su **estado como óptimo**.

b. Verificación del cableado

i. Procedimiento

Esta revisión pretende determinar el correcto estado de todos los cables que llegan al dispositivo a revisar, comprobando físicamente los siguientes aspectos:

- **Correcto anclaje de los cables de alimentación eléctrica.**
- **Correcto anclaje de los cables de enlace de datos.**
- **Estado físico de los cables de datos y de alimentación eléctrica.**
- ✓ **No existen torceduras en los cables.**
- ✓ **No existe aplastamiento en los cables.**
- ✓ **No existe falta de aislamiento en los cables.**
- ✓ **No existen enredos entre los cables.**

En el caso de existir alguna discrepancia con alguno de los aspectos referidos al cableado, se procede a su anotación y corrección inmediata. Si no fuera posible realizar la adecuación del cableado durante la visita Preventiva, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

Esta inspección determinó que el estado de los cables de alimentación eléctrica y de datos están correctamente anclados y libres de daños, siendo su **estado óptimo para el funcionamiento.**

c. Verificación de los indicadores de fallo y encendido.

i. Procedimiento

Esta prueba requiere la desconexión del equipo, quedando el mismo fuera de servicio durante el tiempo de duración de la misma, por lo que se deberá de convenir con los responsables adecuados del cliente, la fecha y hora más adecuadas para esta actuación, advirtiendo que puede existir el riesgo de que el equipo no arranque correctamente o que se den situaciones de anomalía que impliquen la sustitución del equipo y una parada de

los servicios que presta, superior a la prevista.

Esta verificación pretende determinar si los indicadores o Leds del equipo están en perfecto estado y si su función es idónea. Así mismo, esta prueba pretende comprobar que los diagnósticos de arranque progresan correctamente, sin detectar anomalías internas en el dispositivo.

La prueba se realiza apagando o "reseteando" el equipo y siguiendo la secuencia de arranque del mismo, según se especifica en el manual o guía de operaciones del mismo.

Cuando un dispositivo es conectado y su secuencia coincide con la descrita en la guía de operaciones y queda en estado preparado, indicado por los Leds e indicadores adecuados, o por los mensajes que presenta en su Consola de Gestión fuera de banda, se entiende que ha pasado todos los tests internos de arranque y que éstos han sido satisfactorios.

En el caso de que el dispositivo no realice la función de arranque de acuerdo con las indicaciones de la guía de operaciones o su estado final no sea el óptimo o bien sus indicadores muestren un síntoma de error, se anotará dicha circunstancia, en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

El servidor se reinició con normalidad así cómo todo el software que tiene instalado, no se observó ninguna anomalía por lo que se considera que su **estado es óptimo.**

d. Verificación de la temperatura externa

i. Procedimiento

Esta prueba está destinada a comprobar si la temperatura ambiente en la sala o armario en el que se esté ubicado el dispositivo se encuentra entre los rangos, establecidos como válidos, por el fabricante y reflejados en la guía de operaciones del equipo.

Esta comprobación de la temperatura se realiza mediante un termómetro digital. Con el resultado de la medición se comprueba si la temperatura, se encuentra en el rango válido, indicado por el fabricante para el correcto funcionamiento de los equipos.

En función de los valores obtenidos en la medición de la temperatura, se harán, las recomendaciones adecuadas para reducir o aumentar la misma, hasta un valor intermedio en el rango válido. En caso de que la temperatura quede fuera de los rangos establecidos por el fabricante, se indicará al cliente, que tome las medidas oportunas para corregir la situación, mediante la incorporación de la ventilación, calefacción o refrigeración adecuadas, para subsanar el defecto ambiental detectado.

ii. Resultado

Las temperaturas tomadas en los distintos armarios de comunicaciones y salas han estado dentro de los márgenes recomendables

e. Verificación del procesador

i. Procedimiento

Esta prueba requiere el uso total de procesador y el cierre de todos los programas activos exceptuando el de la prueba, lo cual hará que no se pueda transmitir las imágenes a los puntos de información, por lo que se deberá de convenir con los responsables adecuados del cliente, la fecha y hora más adecuadas para esta actuación.

Esta prueba está destinada a verificar la estabilidad del procesador del servidor.

Esta prueba consiste en ejecutar el programa *Prime95* con la opción "Blend" durante al menos dos horas.

Durante la comprobación se monitorizará la temperatura de los núcleos del procesador mediante el programa *Open Hardware Monitor*.

En el caso de que se produzcan fallos, paradas, temperaturas superiores al umbral marcado por el fabricante o situaciones de anomalía, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

Esta prueba se llevó a cabo durante unas 3 horas sin observarse ninguna anomalía y manteniéndose todos los núcleos del procesador con una temperatura dentro de los umbrales marcados por el fabricante. Se considera que el procesador se encuentra en un **estado óptimo**.

f. Verificación de los discos duros.

i. Procedimiento

En esta prueba se verifica el estado de los discos duros mediante el uso del programa CrystalDisk Info. Este programa emite un diagnóstico rápido del estado de cada uno de los discos. Los posibles diagnósticos pueden ser:

- Good
- Caution
- Bad
- Unknown

En el caso de que el diagnóstico no sea *Good*, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

El diagnóstico emitido para ambos discos duros fue *Good*, por lo se considera que su **estado es óptimo.**

g. Verificación de la memoria RAM.

i. Procedimiento

Esta prueba requiere que el servidor sólo ejecute el programa de prueba, lo cual hará que no se pueda transmitir las imágenes a los puntos de información, por lo que se deberá de convenir con los responsables adecuados del cliente, la fecha y hora más adecuadas para esta actuación.

Esta prueba consiste en ejecutar el programa *Memtest86* durante al menos dos horas.

En el caso de que se observe errores, paradas o situaciones de anomalía, se anotará dicha circunstancia en este informe y se procederá a la apertura de la incidencia correspondiente y a su resolución, conforme a las condiciones establecidas en el contrato.

ii. Resultado

Tras ejecutar la prueba durante algo más de 3 horas no se observó ningún error. Se considera que el **estado de la memoria es óptimo**.

h. Imagen actual del sistema.

i. Procedimiento

Este proceso consiste en obtener una imagen completa de los discos del servidor, para poder tenerla cargada en el servidor de repuesto y facilitar su reemplazo. Dicha imagen se generará con las herramientas del propio sistema operativo y será guardada en un dispositivo de almacenamiento externo que aportará el técnico in-situ.

ii. Resultado

Se realiza y guarda la imagen en un disco duro externo sin observar ningún error o anomalía.

ANEXO C: INFORME DE INCIDENCIA

1. Introducción

El presente documento responde al Informe sobre la incidencia TIC0000108 solicitado por parte de la ETSI mediante la petición con código TIC0000110.

2. Resumen del ticket

a. Ticket registrado

El Ticket registrado por el personal de la Escuela Técnica Superior de Ingenieros es el siguiente:

- **Código**: TIC0000108
- **Fecha y hora de registro**: 21/03/2018 a las 10:45
- **Fecha y hora de respuesta**: 21/03/2018 a las 10:47
- **Fecha y hora de resolución**: 26/03/2018 a las 11:11
- **Impacto**: Medio.
- **Urgencia**: Media.
- **Descripción reportada**: La pantalla situada en la parte superior derecha de Secretaría no enciende.
- **Diagnóstico**: Fallo en la fuente de alimentación, debido a un pico de tensión eléctrica en la sede.
- **Resolución**: Sustitución de pantalla.

b. Evolución del ticket

El pasado **día 21 de marzo a las 10:45** el personal de la Escuela Técnica Superior de Ingenieros registra en la Web de Gestión de Tickets el ticket con código TIC0000108 de tipo incidencia informando que la pantalla situada en la parte superior derecha de Secretaría no enciende.

El **día 21 de marzo a las 10:47** se envía a la ETSI la confirmación de la recepción del ticket.

El **día 21 de marzo a las 11:12** el personal del CAU contacta el contacto indicado en el ticket y le solicita que compruebe si la pantalla está correctamente conectada a la corriente y que vuelva a pulsar el botón de encendido de la pantalla. El usuario verifica que la pantalla está correctamente conectada a la corriente eléctrica y pulsa el botón varias veces sin que la pantalla responda. Informa de que no se ve ningún piloto iluminado.

El CAU pregunta al usuario si ha habido algún problema con el suministro eléctrico en la sede. El usuario contesta que a primera hora no había electricidad en Secretaría, en el resto de la sede no se observaba ninguna anomalía.

Ante esta respuesta el CAU informa al usuario de que será necesaria realizar una intervención in-situ. Le informa también de que dado que ese mismo día ya se han registrado otras dos incidencias sobre pantallas se marcarán esas dos incidencias y esta cómo masivas.

El **día 21 de marzo a las 11:40** se marca la incidencia cómo masiva.

El **día 21 de marzo a las 11:45** el CAU transfiere a los técnicos in-situ el ticket solicitando fecha de intervención.

El **día 21 de marzo a las 12:02** el grupo de técnicos in-situ transfiere el ticket al grupo de Garantías y Repuestos solicitando fecha de disponibilidad de una nueva pantalla.

El **día 21 de marzo a las 13:16** el grupo de Garantías y Repuestos devuelve el ticket al grupo de Técnicos In-situ indicando de la disponibilidad de la pantalla para el día 23 de marzo.

El **día 21 de marzo a las 13:30** transfiere el ticket al CAU proponiendo el 26 de marzo a primera hora cómo fecha para la intervención.

El **día 21 de marzo a las 13:40** el CAU contacta con el usuario para informarle de la fecha de la intervención. El usuario indica su disponibilidad para la fecha propuesta.

El **día 21 de marzo a las 13:49** el CAU transfiere el ticket a los técnicos in-situ confirmando el 26 de marzo a primera hora cómo fecha de la intervención.

El **día 26 de marzo a las 08:30** se personan en la sede y comienzan con los trabajos de sustitución. Dado que hay otras dos pantallas averiadas, se retrasará algo más la intervención, ya que se sustituirán primero las otras pantallas.

El **día 26 de marzo a las 11:11** se finaliza la instalación de la nueva pantalla y se verifica con el usuario de la ETSI presente su correcto funcionamiento. Los técnicos pasan el ticket al estado "Resuelto" describiendo la solución aportada ("sustitución de pantalla") y la transfieren al CAU informando de los datos de la nueva pantalla, así como los de la pantalla sustituida, para que actualice los datos del elemento en la CMDB.

El **día 26 de marzo a las 11:34** el CAU actualiza la CMDB con los datos de la nueva pantalla

El **día 27 de marzo a las 11:11** se pasa el ticket al estado "Cerrado".

3. Conclusiones

a. Causas

Según la información facilitada por el usuario y dado que fallaron las tres pantallas de forma simultánea las 3 pantallas que se ubicaban en la misma zona de la sede, todo hace indicar a que las averías fueron causadas por un pico de tensión.

En una evaluación preliminar de una de las pantallas averiadas realizada en la sede tras sustituirla los técnicos comprobaron que la fuente de alimentación no funcionaba correctamente.

b. Estado de la resolución

La incidencia ha sido resuelta.

c. Acciones correctivas

Se ha procedido a sustituir la pantalla