



**UNIVERSIDAD DEL BIOBIO
FACULTAD DE CIENCIAS EMPRESARIALES
DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN**

**GENERACIÓN DE UN MODELO DE GESTIÓN DE CALIDAD PARA EL
DEPARTAMENTO DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN
(TSI) DE LA COMPAÑÍA SIDERÚRGICA HUACHIPATO.**

PROYECTO DE TÍTULO PARA OPTAR AL TÍTULO DE INGENIERO
CIVIL EN INFORMÁTICA.

AUTOR: GUIDOTTI MORENO, RAFFAELLO GIANPAOLO VITTORIO.

PROFESOR GUÍA: SOTO CHICO, MARÍA ANTONIETA.

CONCEPCIÓN, 2012



**UNIVERSIDAD DEL BIOBIO
FACULTAD DE CIENCIAS EMPRESARIALES
DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN**

**GENERACIÓN DE UN MODELO DE GESTIÓN DE CALIDAD PARA EL
DEPARTAMENTO DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN
(TSI) DE LA COMPAÑÍA SIDERÚRGICA HUACHIPATO.**

PROYECTO DE TÍTULO PARA OPTAR AL TÍTULO DE INGENIERO
CIVIL EN INFORMÁTICA.

AUTOR: GUIDOTTI MORENO, RAFFAELLO GIANPAOLO VITTORIO.

PROFESOR GUÍA: SOTO CHICO, MARÍA ANTONIETA.

CONCEPCIÓN, 2012

“So many assholes, so few bullets!”

HARLIN, Renny. The Adventures of Ford Fairlane.[Película]. Estados Unidos: Silver Pictures.1990.

RESUMEN

Debido al acelerado avance de las tecnologías, se exige a las empresas contar con procesos cada vez más eficaces y eficientes. Es así, que muchas metodologías han surgido para avanzar con ellas en este aspecto. En el área de las Tecnologías de la información, específicamente, han surgido como alternativas varios modelos a implementar, de ellos tres son los más importantes y usados son: ISO/IEC 20.000, ITIL y CMMI.

Este proyecto de título tiene como objetivo la elaboración de un marco de trabajo, que se efectuará mediante una revisión de procesos, herramientas y metodologías que actualmente se utilizan en la organización. Al finalizar se pretende que la Unidad de Tecnologías y Sistemas de Información de CAP Acero agilice y mejore el uso de sus recursos tanto económicos como de horas de trabajo. Esto se realizará en base a la implementación de objetivos y prácticas de modelos de gestión de calidad.

TABLA DE CONTENIDO.

RESUMEN	- 3 -
TABLA DE CONTENIDO.	- 4 -
INTRODUCCIÓN	- 7 -
• OBJETIVO GENERAL.....	- 7 -
• OBJETIVOS ESPECÍFICOS.....	- 7 -
• ALCANCES.....	- 7 -
• LIMITACIONES	- 7 -
• METODOLOGÍA A UTILIZAR.....	- 8 -
1. MARCO TEÓRICO.....	- 10 -
1.1. Norma ISO/IEC 20000 Service Management	- 12 -
1.2. Information Technology Infrastructure Library (ITIL)	- 18 -
1.3. Capability Maturity Model Integration (CMMI)	- 25 -
1.3.1. Costos y beneficios de la implementación de CMMI	- 27 -
1.3.2. CMMI for Services (CMMI-SVC) v.1.2.....	- 29 -
2. RELACIONES ENTRE LOS MODELOS	- 31 -
2.1. Diferencia entre norma y mejores prácticas.....	- 31 -
2.2. Principios básicos de CMMI	- 31 -
2.3. Principios básicos de ITIL.....	- 31 -
2.4. Principios básicos de ISO 20000.....	- 33 -
2.4.1. Cómo se relacionan ITIL e ISO 20000	- 34 -
2.5. ¿Cuál es la mejor forma de implementar ITIL, CMMI e ISO/IEC 20000?.....	- 38 -
2.5.1. Elaboración.....	- 38 -
2.5.2. Priorización.....	- 38 -
2.5.3. Planificación	- 38 -
3. GRUPO CAP S.A. Y COMPAÑÍA SIDEGÚRGICA HUACHIPATO.	- 40 -
3.1. Grupo CAP S.A.	- 40 -
3.2. La Compañía Siderúrgica Huachipato S.A.	- 42 -
3.2.1. Estructura Organizativa.....	- 42 -
4. Unidad de Tecnologías y Sistemas de Información.....	- 45 -

5.	ANÁLISIS DE LAS ÁREAS A LAS QUE SE LE APLICARÁ EL MODELO	- 48 -
5.1.	Área de Plataforma	- 48 -
5.2.	Área de Operaciones	- 54 -
5.3.	Modelo de trabajo actual de la unidad de Tecnologías y Sistemas de Información (TSI). -	58 -
6.	ASPECTOS A CONSIDERAR PARA LA ELABORACIÓN DEL MODELO A UTILIZAR EN LA UNIDAD DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.	- 62 -
7.	MODELO PARA LA UNIDAD DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN	- 68 -
7.1.	Control de Incidentes.	- 69 -
7.1.1.	Resolución del Incidente	- 70 -
7.1.2.	Instancias dentro del Control de Incidentes	- 70 -
7.2.	Manejo de Problemas.	- 73 -
7.3.	Control de Versiones.	- 77 -
7.3.1.	Versiones	- 77 -
7.3.2.	DSL.....	- 78 -
7.3.3.	DHS	- 78 -
7.3.4.	Procesos del Control de Versiones.....	- 78 -
7.3.5.	Validación e Implementación.....	- 79 -
7.3.6.	Comunicación y Control del Proceso.....	- 79 -
7.4.	Control de Acuerdos de Niveles de Servicio	- 81 -
7.4.1.	Planificación	- 82 -
7.4.2.	Implementación y Monitoreo	- 83 -
7.4.3.	Revisión y Control.....	- 83 -
7.5.	Manejo de Cambios.....	- 85 -
7.5.1.	Alcance del Manejo de Cambios	- 87 -
7.5.2.	Actividades del Manejo de Cambios	- 87 -
7.5.3.	Control del Proceso	- 91 -
7.5.4.	Cambios de Emergencia	- 91 -
7.6.	Gestión de Capacidad.....	- 93 -
7.6.1.	Planificación.	- 95 -
7.6.2.	Supervisión del Proceso	- 96 -
7.6.3.	Gestión de la Demanda	- 97 -
7.7.	Gestión de Disponibilidad.	- 99 -

7.8.	Gestión de Peticiones.....	- 101 -
7.8.1.	El proceso de la Gestión de Peticiones	- 101 -
7.8.2.	Control del Proceso	- 102 -
7.9.	Continuidad del Servicio y Contingencias Mayores.	- 103 -
7.9.1.	Actividades contempladas en la Continuidad del Servicio.....	- 103 -
7.9.2.	Control.....	- 107 -
7.10.	Control de la Seguridad.	- 108 -
7.10.1.	Aplicación de las medidas de Seguridad.	- 109 -
7.10.2.	Responsabilidades.....	- 109 -
7.11.	Control de Acceso.	- 110 -
7.11.1.	Procedimiento.....	- 110 -
7.11.2.	Control.....	- 113 -
7.12.	Validación, Verificación y Pruebas.	- 114 -
7.12.1.	Proceso.....	- 114 -
7.13.	Planificación y Soporte para la Transición.	- 117 -
7.13.1.	Proceso.....	- 117 -
7.14.	Gestión Financiera.....	- 120 -
7.14.1.	Proceso.....	- 120 -
7.14.2.	Control del Proceso	- 122 -
7.15.	Gestión de Informes de Servicio.	- 123 -
7.15.1.	Proceso.....	- 123 -
7.16.	Mesa de Ayuda.....	- 125 -
7.16.1.	Actividades	- 126 -
7.16.2.	Control.....	- 127 -
8.	CONCLUSIONES	- 130 -
8.1.	Problemas encontrados en la implementación	- 131 -
8.2.	Beneficios encontrados.....	- 131 -
	BIBLIOGRAFÍA.....	- 133 -

INTRODUCCIÓN

Hoy con mayor frecuencia los negocios dependen de sus servicios de tecnologías y sistemas de información. Las organizaciones de Tecnologías de Información han evolucionado para funcionar como un proveedor de servicios de TI, enfrentando el desafío de crear, desarrollar, mantener y mejorar su gestión de los servicios, es desde aquí que nace el IT Service Management, con un enfoque de calidad y costo, ya que sólo de esta forma los servicios de Tecnologías de Información brindarán su completo valor y posibilidades al negocio, adaptándose a un entorno versátil tanto de la perspectiva del negocio como de su contexto.

En este trabajo se estudiarán estándares de gestión de los servicios de Tecnologías de Información, siendo las más relevantes o utilizadas la norma ISO/IEC 20000, el conjunto de buenas prácticas ITIL y el modelo CMMI, aplicables para cualquier proveedor de servicios de Tecnologías de Información y, en este caso, se analizarán con el fin de crear un estándar para la unidad de Tecnologías y Sistemas de Información de la Compañía Siderúrgica Huachipato. Dado que la adopción de una norma en el ámbito de la gestión de servicios de Tecnologías de Información permite mejorar la calidad de los servicios, un mayor alineamiento con el negocio y una reducción de costos operacionales para la empresa.

- **OBJETIVO GENERAL**

Generar un modelo de gestión de la calidad de los servicios de TI que se adecúe a las características propias de la unidad de Tecnologías y Sistemas de Información de la Compañía Siderúrgica Huachipato, a partir de los modelos, estándares o conjunto de prácticas de gestión existentes.

- **OBJETIVOS ESPECÍFICOS**

1. Mostrar las características de los modelos de gestión existentes para el área informática y determinar las características más relevantes de cada uno.
2. Dar a conocer los beneficios y mejoras de la implementación de un modelo de gestión de la calidad a fin de que este sea aceptado en la organización.
3. Definir un modelo de gestión de la calidad que se pueda implementar y esté acorde con las actividades que se desarrollan en la unidad.

- **ALCANCES**

- El Sistema de gestión de calidad aplicará a la unidad de tecnologías y sistemas de información de la Compañía Siderúrgica Huachipato.
- Se aplicarán las características de los diferentes modelos para generar un modelo de gestión apropiado para las características de la organización.

- **LIMITACIONES**

- La implementación del modelo de gestión de calidad será específico para la empresa objeto de este trabajo.

- Se generarán los documentos necesarios para el modelo de gestión, pero no se implementarán hasta que sean autorizados por la empresa.
- Este trabajo no será en pro de la obtención de un certificado de calidad.
- Los procedimientos, flujos de trabajo, ni material anexo creados no serán publicados, ya que estos pertenecerán a CAP Acero.

- **METODOLOGÍA A UTILIZAR**

“La investigación – acción se presenta como una metodología de investigación orientada hacia el cambio y se caracteriza, entre otras cosas, por ser un proceso que: (i) Se construye desde y para la práctica, (ii) pretende mejorar la práctica a través de su transformación, al mismo tiempo que procura comprenderla, (iii) demanda la participación de los sujetos en la mejora de sus propias prácticas, (iv) exige una actuación grupal por la que los sujetos implicados colaboran coordinadamente en todas las fases del proceso de investigación, (v) implica la realización de análisis crítico de las situaciones y (vi) se configura como una espiral de ciclos de planificación, acción, observación y reflexión.

Entre los puntos clave de la investigación – acción, Kemmis y McTaggart (1988) destacan la mejora de la educación mediante su cambio, y aprender a partir de la consecuencias de los cambios y la planificación, acción, reflexión nos permite dar una justificación razonada ante otras personas.

La investigación – acción no se limita a someter a prueba determinadas hipótesis o a utilizar datos para llegar a conclusiones. La investigación – acción es un proceso, que sigue una evolución sistemática, y cambia tanto al investigador como las situaciones en las que éste actúa. Pérez Serrano (1997) esquematiza los rasgos que definen la investigación acción, presentados en la siguiente figura:”.¹

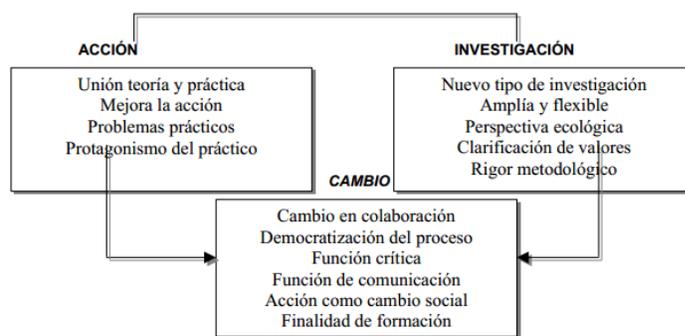


Figura 1: Rasgos que definen la investigación – acción (Pérez Serrano, 1997: 75).

Kurt Lewin, establece que ésta se constituye con tres momentos:

¹Bausela Herreras E., 1992.

1. Planificación.
2. Concreción de hechos.
3. Ejecución.

Igualmente, las condiciones elementales para calificar propiamente a la investigación-acción, son tres:

1. Existencia de un proyecto correspondiente a una práctica social que resulte susceptible de mejoramiento.
2. La interrelación sistemática y autocrítica de las fases de planeación, observación, reflexión y acción correspondientes al proyecto.
3. La inclusión de todos los responsables del proyecto en cada uno de los momentos investigativos, y la posibilidad abierta y permanente de incorporar a otros sujetos afectados por la práctica social que se está sometiendo al proceso de investigación-acción.

De lo anterior se puede observar que el método de investigación descrito se adecúa al que se utilizará en este trabajo, pues, como establece Lewin, se hará una planificación de las tareas a realizar, las cuales se cumplirán paso a paso dando como resultado un modelo de gestión, el que finalmente y cumpliendo los objetivos trazados, se implementará en la unidad de Tecnologías y Sistemas de Información.

Así se tiene que el aseguramiento de la calidad de la unidad de Tecnologías y Sistemas de Información puede ser mejorado, o implementado en base a la documentación existente en la unidad. Con esta información se realizará un proceso de análisis, investigación y acción con el fin de elaborar el modelo de gestión de calidad, en el que se considerará a todos los integrantes de la unidad que intervengan en los procesos tratados por el modelo, ya que ellos serán una fuente de información importante en cuanto a los procesos que se desarrollan actualmente, los cuales se verán afectados directamente con la implementación de este modelo. Es por estas razones que esta es la metodología elegida para desarrollar el proyecto, ya que si bien, la implementación completa de documentos y actividades debe ser autorizada por la empresa, puesto que ellos utilizarán el modelo, este se creará con la participación de la empresa, y con el fin de ser implementado.

1. MARCO TEÓRICO

La gestión de servicios de Tecnologías de Información es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, cuyo fin es generar valor para los clientes en forma de servicios.

“Este enfoque propone cambiar el paradigma con que se gestionan las Tecnologías de Información, por un conjunto de componentes enfocados en servicios de punta a cabo usando distintos marcos de trabajo como son las "mejores prácticas". Los proveedores de los servicios de TI no pueden seguir manteniendo su enfoque en la tecnología y sus propias organizaciones, ahora se deben considerar la calidad de los servicios que proveen y enfocarse en sus relaciones con los clientes. Eso se logra mediante la entrega de un servicio que vela por dar un valor a los clientes, facilitando los resultados que se quieren conseguir sin asumir costos o riesgos específicos”². En la Figura 2 podemos ver la evolución de los modelos de gestión de la calidad de TI a lo largo del tiempo.

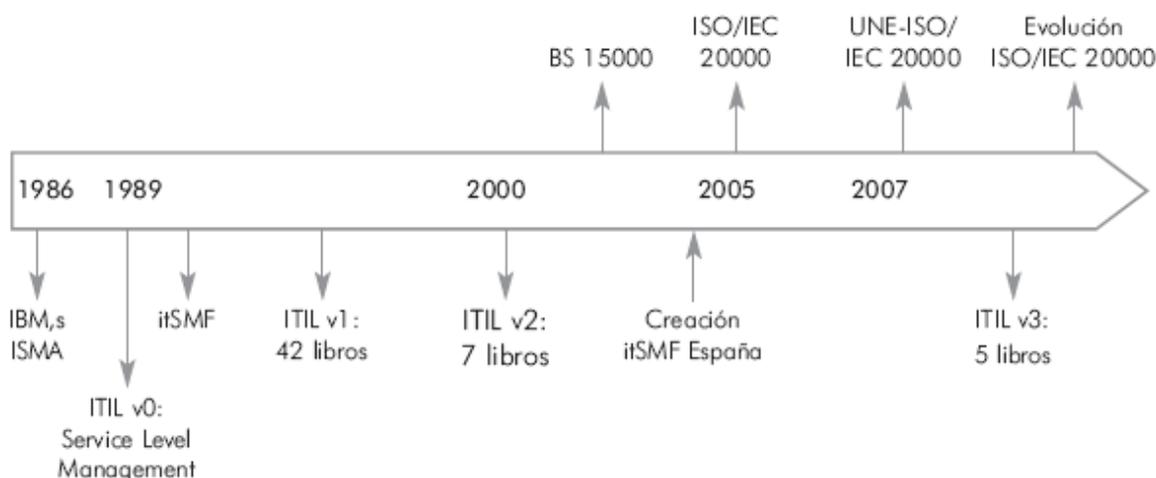


Figura 2. Evolución de los modelos de gestión de TI. Fuente: UNE-ISO/IEC

“El gobierno de TI, es un conjunto de mejores prácticas establecidas como Information Technology Service Management (ITSM) que nace a partir de la creación e implantación de los principios y fundamentos ingleses promovidos en el conjunto de prácticas documentadas en Information Technology Infrastructure Library (ITIL), normados en el código British Standard 15000 (BS15000) y que actualmente se ha internacionalizado y estandarizado a nivel global por la extensión en la norma ISO/IEC 20000, es hoy un nuevo y vigoroso enfoque de prácticas a seguir y base de certificación en esquemas de negocio, de mejoramiento continuo en el uso y aprovechamiento de Tecnologías de Información en apoyo al logro de los objetivos de negocio”³.

² Lobos A., Daniela, Baquinzay, Manuel, Bustos A., María Soledad, 2008.

³ Eder. E, 2010.

El ITSM está centrado en los procesos y, en este sentido, tiene lazos e intereses comunes con la mejora de procesos, por ejemplo, gestión de procesos empresariales o CMMI, marcos y metodologías. La disciplina no se ocupa de los detalles de cómo utilizar el producto de un fabricante concreto, ni necesariamente de los detalles técnicos de los sistemas bajo su administración. En cambio, se centra en proporcionar un marco para estructurar las actividades relacionadas con las Tecnologías de Información y las interacciones del personal técnico con los clientes de negocios y éstos a su vez con los usuarios.

No existe un único compendio de procedimientos o buenas prácticas, en el área de las Tecnologías de Información, aunque sí, unos más que otros, se centran en gestión de TI. Así existen posibilidades como son: ISO9000, BS15000, ITIL, CMM con CMMI, Six Sigma, y Cobit, por nombrar algunos. Además existen requerimientos de control corporativo que pueden afectar estas normas. El nivel de adopción de las normas de gestión de calidad se muestra en la Figura 3, según un estudio realizado por Forrester Research, Inc.

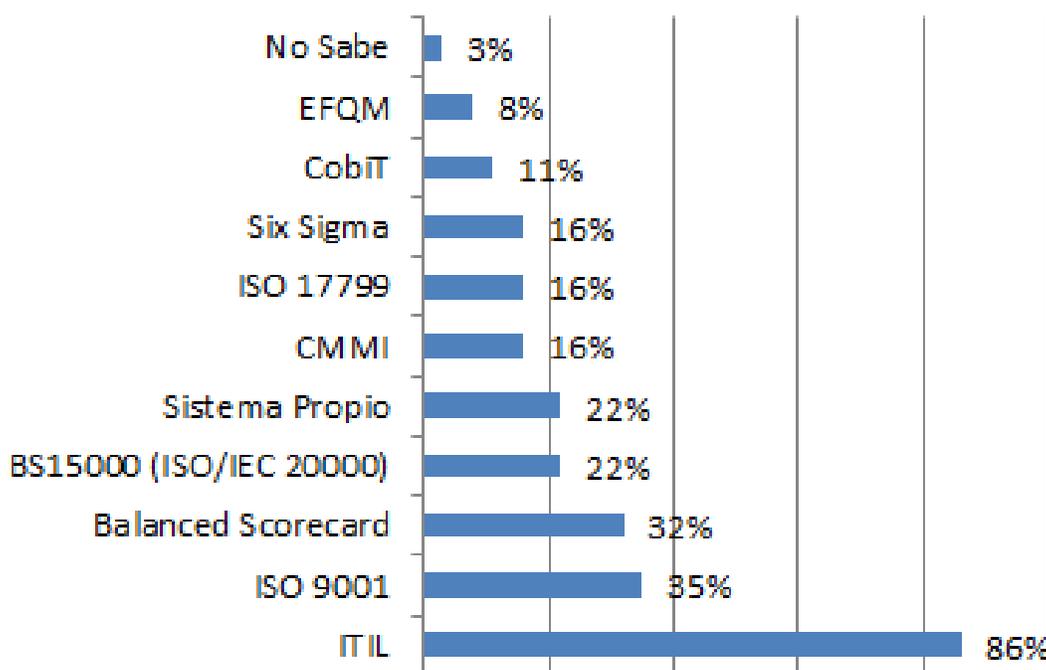


Figura 3. Nivel de adopción de normas de gestión de calidad. Fuente: Forrester Research, Inc.

Todas las normas presentes en la figura 3 fueron analizadas y estudiadas en busca de aquellas que se acomodaran a las necesidades de la unidad de TSI, luego de este análisis se determinó que sólo tres normas cumplían con este requisito, éstas eran ISO/IEC 20000, CMMI e ITIL, las que se detallan a continuación.

1.1. Norma ISO/IEC 20000 Service Management

Fue normalizada y publicada por la International Standard Organization y el International Electrotechnical Commission (IEC) el 14 de diciembre de 2005.

Tanto esta norma como IT Infrastructure Library (ITIL) se han convertido en estándares “de facto” para organizaciones de servicios TI en cualquier organización, independiente de su tamaño o área industrial. Hoy son considerados parte de las “mejores prácticas” relacionadas con TI, en tanto que ambas proveen referencias generales para administrar servicios de TI que deben ser ajustados a la organización.

Tomando como referencia fundamental ITIL, el Instituto Británico de Estándares (BSI), definió BS 15000, un estándar sobre los servicios TI. Posteriormente, a partir de BS 15000, publicada por primera vez en 2000, se definió ISO/IEC 20000:2005, en diciembre de 2005.

ISO 20000 es considerado el primer estándar internacional para la administración de servicios de TI, y al igual que los otros estándares ISO tiene dos partes centrales: la primera que es obligatoria, y la segunda que es un conjunto de sugerencias sobre la primera parte⁴.

Esta versión de la norma plantea a las organizaciones de todo el mundo que centren su estrategia en una mejora continua de su gestión en servicios TI, ya que así se beneficiarán del cumplimiento de esta. Este modelo promueve la adopción de un modelo de procesos integrados destinados a mejorar la eficiencia en la prestación de los servicios tecnológicos y establece directrices para una gestión de servicios de TI de calidad.

“La documentación donde se definen las especificaciones de la norma se publicó en 2005 y los procesos de certificación se iniciaron en 2007. La ISO 20000 es un código que proporciona bases para medir y validar el éxito de una organización a la hora de implementar las buenas prácticas definidas por ITIL. Las compañías que cumplan o estén esperando para implementar ITIL habrán recorrido ya gran parte del camino para conseguir la certificación ISO 20000”.

Para decidir solicitar o no la certificación ISO 20000 se debe tener en cuenta que esta norma es particularmente útil en organizaciones de sectores industriales en los que la calidad de los servicios de TI es fundamental para el éxito del negocio. Esto incluye al sector financiero, los servicios públicos, entre otros. La certificación le permite a las organizaciones que pertenecen a estas organizaciones demostrar que disponen de una infraestructura tecnológica bien gestionada.

Así mismo, es importante para organizaciones que prestan servicios gestionados internamente o mediante subcontratación. Los proveedores de servicios deben probar que han documentado las cinco áreas fundamentales previstas por la ISO y que cumplen todos los requisitos que la norma les exige. La documentación debe incluir las políticas y los planes de gestión de servicios, los acuerdos de nivel de servicio, los procesos y procedimientos exigidos por la norma y sus registros de datos correspondientes.

⁴ RIVERA, Luis, 2008.

La certificación ISO 20000 sólo se otorga a organizaciones que realicen operaciones de gestión de servicios TI y sólo certifica el buen funcionamiento de esas operaciones. Su objetivo no es certificar productos ni servicios de consultoría relativos a la aplicación de buenas prácticas.

Aunque inicialmente no quieran solicitar la certificación, la documentación proporciona una valiosa fuente de referencia para aquellas organizaciones que hayan adoptado el modelo ITIL y estén implementando o vayan a implementar procesos de gestión de servicios TI basados en las directrices de ese modelo, puesto que proporciona una forma normalizada de medir sus procesos en el proyecto de implementación.

Todas las organizaciones deben tener presente que uno de los objetivos fundamentales del modelo ITIL y, por tanto, de la ISO 20000 es validar la continua mejora de la calidad de la gestión de los servicios.

Un factor importante para lograr esta mejora continua es realizar comprobaciones periódicas de la calidad de la gestión de los servicios TI. La ISO 20000 proporciona una forma de verificar cómo se está comportando una organización en su objetivo de seguir mejorando la calidad de los servicios. La organización puede utilizar la ISO 20000 para definir y medir sus avances en la consecución de los nuevos niveles de mejora a medida que la gestión de los servicios gana madurez.

Uno de los tres grandes objetivos de la ISO 20000 es alinear los servicios tecnológicos con las necesidades del negocio. Para lograr esto, el departamento de TI debe gestionar los servicios desde una perspectiva empresarial, es decir, adoptar una filosofía de Gestión de Servicios de Negocio (BSM).

La norma ISO 20000 consta de cinco partes:

- **ISO/IEC 20000:1** Especificación. Contiene los 148 requerimientos necesarios para realizar una entrega de servicios TI alineados con las necesidades del negocio.
- **ISO/IEC 20000:2** Código de Prácticas. Representa el conjunto de buenas prácticas adoptadas y aceptadas por la industria en materia de Gestión de Servicios TI (ITIL).
- **ISO/IEC TR 20000:3** Es una guía en la que se define el alcance y la aplicabilidad de la norma (informe técnico): Proporciona orientación sobre la definición del alcance, la aplicabilidad y la demostración de la conformidad de los proveedores de servicios, orientados a satisfacer los requisitos de la norma ISO / IEC 20000-1.
- **ISO/IEC DTR 20000:4** Modelo de referencia de procesos (informe técnico): Consiste en una representación lógica de los elementos de los procesos de gestión de servicio, los que pueden ser llevados a cabo en un nivel básico. Este modelo de procesos de referencia describe de una manera abstracta los procesos, incluyendo también los procesos generales del sistema de gestión del servicio que implica ISO/IEC 20000-1.
- **ISO/IEC TR 20000:5** Ejemplo de implementación (informe técnico): Documento que contiene un ejemplo de plan de implementación que sirve como guía para

proveedores de servicios ayudándolos en “el cómo” poder cumplir los requisitos del ISO/IEC 20000-1.

Entre los objetivos que plantea la norma ISO 20000 se cuenta el regular la operación del soporte TI adoptando un conjunto de buenas prácticas probadas, adoptadas y reconocidas internacionalmente, pudiendo demostrar la calidad de la gestión en la provisión de servicios TI mediante el cumplimiento de normas internacionales de gestión, asimismo permite garantizar una mejora continua de la gestión de los servicios TI mediante el plan de “Plan-Do-Check-Act” reduciendo los riesgos, costos y optimizar el uso de los recursos. La norma ISO 20000 consta de cinco partes⁵:

- **ISO/IEC 20000:1** Especificación. Contiene los 148 requerimientos necesarios para realizar una entrega de servicios TI alineados con las necesidades del negocio.
- **ISO/IEC 20000:2** Código de Prácticas. Representa el conjunto de buenas prácticas adoptadas y aceptadas por la industria en materia de Gestión de Servicios TI (ITIL).
- **ISO/IEC TR 20000:3** Es una guía en la que se define el alcance y la aplicabilidad de la norma (informe técnico): Proporciona orientación sobre la definición del alcance, la aplicabilidad y la demostración de la conformidad de los proveedores de servicios, orientados a satisfacer los requisitos de la norma ISO / IEC 20000-1.
- **ISO/IEC DTR 20000:4** Modelo de referencia de procesos (informe técnico): Consiste en una representación lógica de los elementos de los procesos de gestión de servicio, los que pueden ser llevados a cabo en un nivel básico. Este modelo de procesos de referencia describe de una manera abstracta los procesos, incluyendo también los procesos generales del sistema de gestión del servicio que implica ISO/IEC 20000-1.
- **ISO/IEC TR 20000:5** Ejemplo de implementación (informe técnico): Documento que contiene un ejemplo de plan de implementación que sirve como guía para proveedores de servicios ayudándolos en “el cómo” poder cumplir los requisitos del ISO/IEC 20000-1.

Entre los objetivos que plantea la norma ISO 20000 se cuenta el regular la operación del soporte TI adoptando un conjunto de buenas prácticas probadas, adoptadas y reconocidas internacionalmente, pudiendo demostrar la calidad de la gestión en la provisión de servicios TI mediante el cumplimiento de normas internacionales de gestión, asimismo permite garantizar una mejora continua de la gestión de los servicios TI mediante el plan de “Plan-Do-Check-Act” reduciendo los riesgos, costos y optimizar el uso de los recursos. El que podemos observar en la Figura 4.

⁵ GUINDEL S., 2009.

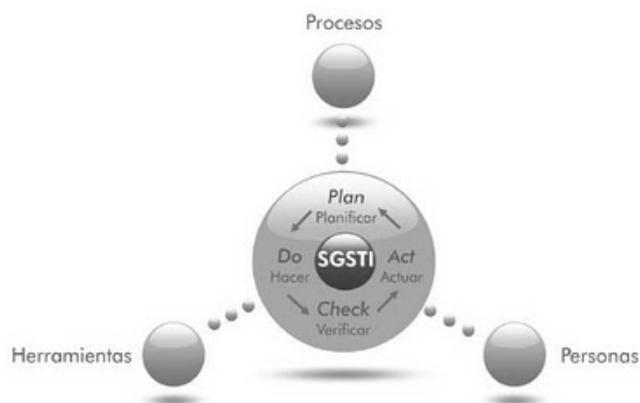


Figura 4. Áreas para la implementación de ISO 20000. Fuente: UNE-ISO/IEC

En Tabla 1 podemos observar una referencia cruzada de procesos ISO 20000 e ITIL v3, donde se muestran los procesos presentes en cada una y su equivalente:

REFERENCIA CRUZADA DE PROCESOS ISO 20000 E ITIL V3			
Procesos en ISO/IEC 20000	Procesos en ITIL	Procesos en ISO/IEC 20000	Procesos en ITIL
Administración de la Configuración	Administración de la Configuración	Reporte de Servicio	-
Administración de Cambios	Administración de Cambios	Administración de la Seguridad de la Información	Administración de la Seguridad
Administración de Liberaciones	Administración de Liberaciones	Presupuestos y Contabilidad de los Servicios de TI	Administración financiera
Administración de Incidentes	Administración de Incidentes	Administración de la Relación con el negocio	Las series de la Perspectiva del negocio y un volumen de conexión con el cliente
Administración de Problemas	Administración de Problemas	Administración de los Proveedores	Versión uno de los libros de ITIL y algo de contenido en el libro de Perspectivas del Negocio
Administración de Capacidad	Administración de Capacidad	-	Administración de la Infraestructura de TI
Administración de la Continuidad del Servicio y Administración de la Disponibilidad	Administración de la Continuidad del Servicio y Administración de la Disponibilidad	-	Administración de la aplicación
Administración de Niveles de Servicio	Administración de Niveles de Servicio	-	Planeación para la implementar Administración de Servicios

Tabla 1. Referencia cruzada de procesos ISO 20000 e ITIL v3 Fuente: BS15000 a Pocket Guide, itSMF

“Las compañías que han implementado un estándar ISO, cualquiera que éste sea, se verán mayormente beneficiadas al implementar ISO 20000 en lugar de ITIL, puesto que, todo el marco de administración del estándar que cubre los aspectos del negocio se puede aprovechar sin ningún esfuerzo adicional con la norma ISO 20000”.

Así mismo las compañías que han optado por implementar ITIL o ISO 20000 se han beneficiado de los aspectos indicados en la Tabla 2.

BENEFICIOS DE LA IMPLEMENTACION DE ITIL O ISO 20000	
<ul style="list-style-type: none"> • Mejora la satisfacción de los usuarios. 	<ul style="list-style-type: none"> • Se industrializan los procesos de soporte TI.
<ul style="list-style-type: none"> • Orientación hacia el cumplimiento con los requerimientos del negocio de parte de los servicios de TI. 	<ul style="list-style-type: none"> • Los riesgos inherentes a los servicios se gestionan de una forma segura y responsable.
<ul style="list-style-type: none"> • Establecimiento de un proceso de mejora continua de la calidad en la gestión de TI. 	<ul style="list-style-type: none"> • Identificación de los niveles de servicio (ANS) que requiere el negocio de parte de TI.
<ul style="list-style-type: none"> • Aprovechamiento de referencias de aplicación internacional. 	<ul style="list-style-type: none"> • Se refuerza la credibilidad y facilita el cambio cultural.
<ul style="list-style-type: none"> • Reducción de curvas de aprendizaje. 	<ul style="list-style-type: none"> • Se optimiza el consumo de los recursos.

Tabla 2. Beneficios de la implementación de ITIL o ISO 20000. Fuente: Elaboración propia.

Si bien los procesos de implementación de un estándar de TI son bastante similares, y todos ellos deben considerar etapas de capacitación, diagnóstico, implementación y opcionalmente certificación, el momento para iniciar el proyecto de implementación de una norma dependerá exclusivamente de la organización, ya que si bien, épocas de turbulencia económica generalmente involucran procesos de recortes presupuestarios, esta ocasión puede ser un momento ideal para implementar estándares como ISO 20000 e ITIL, principalmente si se considera que además de las ventajas mencionadas, un proyecto de este tipo puede convertirse en la base para definir un esquema de medición de costos de los servicios y productos que genera TI hacia los clientes internos.

La aparición de la serie ISO/IEC 20000 ha planteado el primer sistema de gestión en servicios de TI certificable bajo norma reconocida a nivel mundial. Hoy en día, las organizaciones podrían optar por aplicar un conjunto de mejores prácticas dictadas por ITIL (completadas por otros estándares como CoBIT o CMMI para el área de desarrollo) o certificar su gestión contra el estándar local británico BS 15000.

En la Figura 5 se muestran los procesos de la norma ISO/IEC 20000 enmarcados en su ámbito de acción.

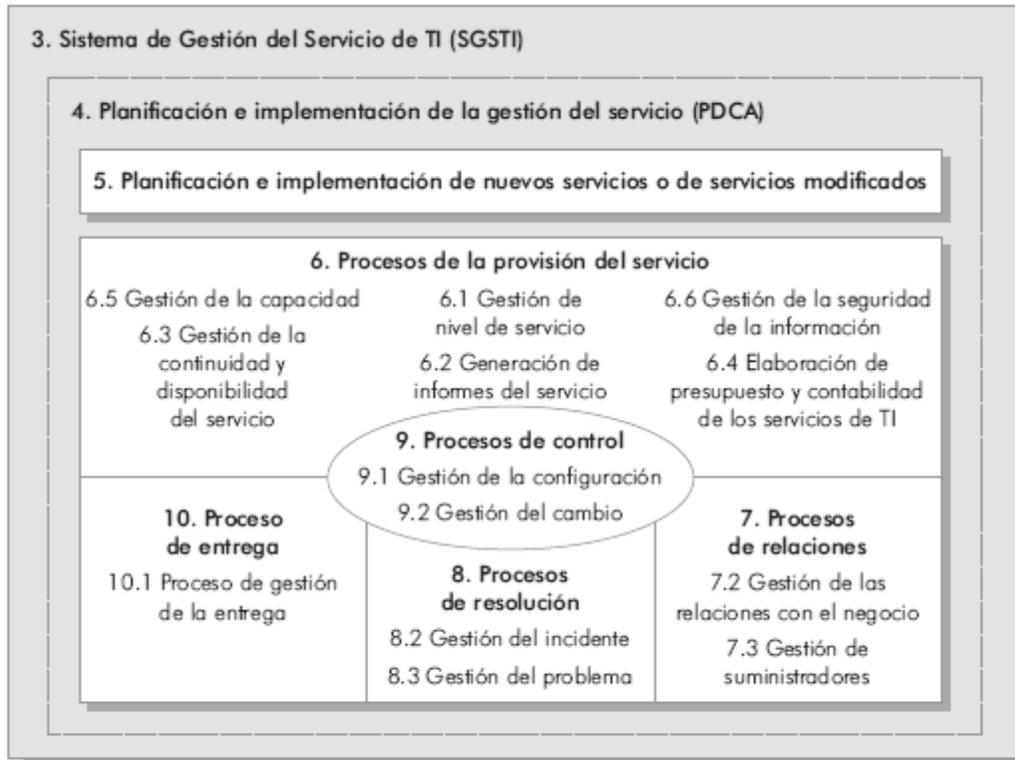


Figura 5. Procesos ISO/IEC 20000. Fuente: UNE-ISO/IEC

1.2. Information Technology Infrastructure Library (ITIL)

El modelo ITIL, fue desarrollado por primera vez en los años 80 por la Office of Government Commerce (OGC) del gobierno británico, aunque no fue publicado sino hasta 1995 por Central Computer and Telecommunications Agency (CCTA), una unidad del gobierno británico actualmente anexada a la Office of Government Commerce, convirtiéndose en el estándar adoptado a la hora de definir las prácticas que deben regir la gestión de los servicios TI. Muchas organizaciones han optado por este modelo como marco para establecer las mejores prácticas en sus procesos de gestión de los servicios informáticos.

ITIL tiene como objetivos fundamentales alinear las tecnologías de la información con los objetivos del negocio. Enfatizando en la importancia de que la gestión de la infraestructura de TI cumpla con los requerimientos económicos de las compañías integrando los procesos de gestión a través de todas las disciplinas de TI.

Cumplir estos objetivos exige a los departamentos de informática, o sistemas de información, dar un importante salto en el grado de madurez con el que administran sus sistemas, ya que deben pasar de la simple gestión de máquinas a la gestión de los servicios de negocio. Así los departamentos deben trabajar de una forma más integrada, reduciendo la distancia que separa las distintas disciplinas de las TI.

Aunque las especificaciones ITIL cubren diversas áreas, su principal foco de atención son, como se dijo, los procesos de gestión de los servicios de TI. Se centra en prestar y dar soporte a servicios que sean apropiados para las necesidades del negocio u organización. Para conseguirlo, ITIL proporciona un conjunto completo, homogéneo y coherente de buenas prácticas de gestión de servicios de TI, y sus procesos relacionados que promueven un modelo destinado a conseguir la eficiencia y efectividad de las empresas en el uso de los sistemas de información.

ITIL divide los procesos de gestión de servicios de TI en dos áreas, con sus respectivas sub áreas:

- El Área de Soporte de los servicios, que se compone de las siguientes sub áreas:
 - Gestión de Incidentes.
 - Gestión de Problemas
 - Gestión de Cambios.
 - Gestión de la Configuración.
 - Gestión del envío a entornos de producción.
 - Servicios de Asistencia.
- Área de Soporte de los servicios, con las sub áreas de:
 - Gestión del Nivel de Servicio.
 - Gestión de la Capacidad.
 - Gestión de la Disponibilidad.
 - Gestión Financiera de los Servicios de TI
 - Gestión de Continuidad del Servicio.

La implantación del modelo ITIL exige a las organizaciones capacidad para manejar altos niveles de complejidad, tanto en la infraestructura de TI como de los procesos de ITIL necesarios para gestionar esa infraestructura. También requiere formar a las personas para asumir y adoptar esos procesos, funciones y responsabilidades⁶.

ITIL debe implementarse como parte de una metodología empresarial versátil que abarque todos los procesos y que, al mismo tiempo, permita perfeccionar los procesos y la eficacia de la gestión de servicios. Al momento de la implementación de ITIL se deben fijar objetivos realistas, y no intentar conseguirlo todo de una vez. También la búsqueda de un producto de gestión de servicio adaptable juega un papel importante en la implementación de ITIL como norma flexible, mientras que al mismo tiempo permite a los departamentos de TI canalizar sus recursos humanos, sus procesos y su tecnología hacia el perfeccionamiento de la organización.

ITIL fue diseñado pensando en las grandes empresas. No obstante, incluso las grandes organizaciones que disponen de recursos dedicados para los procesos indicados anteriormente no siempre implementan las buenas prácticas de ITIL de manera exhaustiva en todas sus áreas⁷.

La división de los procesos de ITIL y su relación con el centro de servicios se muestra en la Figura 6.



Figura 6. Procesos ITIL y el centro de servicios. Fuente: BCM

ITIL define sus procesos y para ello no utiliza la asignación existente de tareas, ni utiliza la división actual de los departamentos, tampoco se establecen sus objetivos. Cada proceso deberá ser monitorizado para conocer su estado cuando sea necesario.

Si las actividades como resultado de la monitorización se desarrollan con el mínimo esfuerzo y costos necesarios, el proceso se considerará eficiente.

⁶ BMC Software, 2006.

⁷ ITNEWS, 2008.

El propósito de la gestión del proceso es utilizar la planificación y el control para garantizar que los procesos sean eficientes y eficaces.

ITIL cuenta con tres versiones. Su Versión 1 fue producida originalmente a fines de 1980, y en su versión 2 las publicaciones propias son diferentes y se trata de siete grupos distintos, los que se presentan en la Figura 7.



Figura 7. Procesos definidos en ITIL v.2. Fuente: ITIL Soporte de Servicio de la OCG.

Posteriormente, fue sustituida por la versión 3, entrando en vigencia, el 30 de mayo de 2007, tras un largo período de rehabilitación denominado ITIL refresh⁸.

Actualmente, la versión más reciente de ITIL, ITIL v3, comprende un conjunto de textos fundamentales con el apoyo de otros complementos y materiales web.

Los servicios de TI se dividen en 12 tipos, clasificados en dos grupos:

- Servicios orientados al Soporte de la infraestructura TI para administración de:
 - Asistencia (Service Desk)

⁸ Osiatis., 2006

- Configuración
- Incidentes
- Problemas
- Versiones
- Cambios
- Servicios orientados a las entregas al cliente para la administración de:
 - Niveles de servicios (ANS)
 - Finanzas
 - Capacidad
 - Disponibilidad
 - Continuidad de TI
 - Seguridad

El incremento del Rol de la función de IT a lo largo del tiempo y las incorporaciones realizadas por cada versión de ITIL se muestran en la Figura 8.

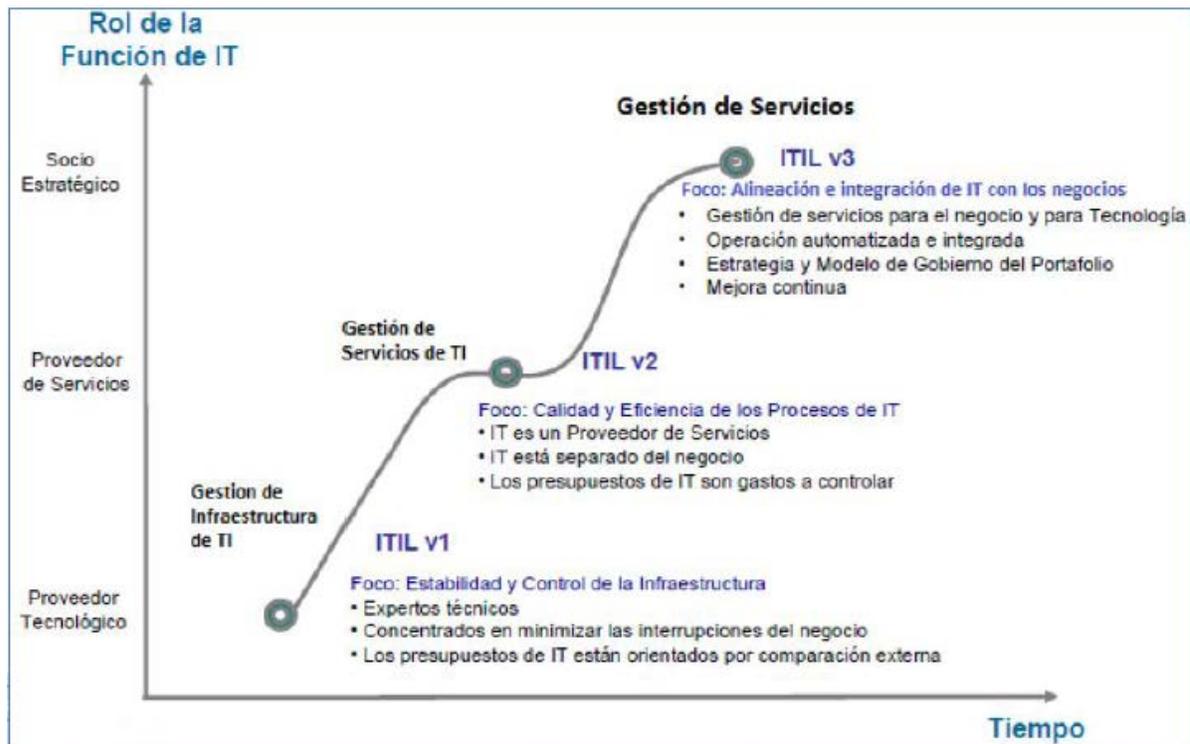


Figura 8. Diferencias entre ITIL v2 e ITIL v3. Fuente: TCM

Para la implementación de ITIL al interior de una organización se debe tener en cuenta que todas las actividades apuntan al objetivo de la empresa, y tienen dos administradores, el del proyecto en sí y el del cambio o cambios que se proponen con la realimentación del sistema.

Teniendo estos puntos ya aclarados se debe identificar la forma cómo trabaja la organización, considerando las funciones, roles, actividades y/o procesos. En esta etapa se

mapean las estructuras jerárquico-funcionales y los problemas operativos actuales; con esto se identifican las oportunidades de mejora.

Los pasos para la implementación de ITIL se muestran en la Figura 9 y se detallan luego de esta.

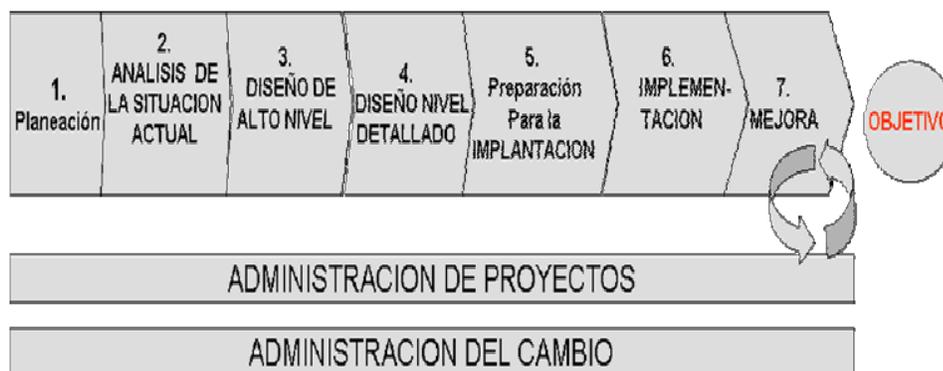


Figura 9. Fases de implementación de procesos ITIL Fuente: BCM.

En el diseño de alto nivel se determina el marco de referencia de mejores prácticas para el modelo a desarrollar. Se construye un modelo ideal considerando los principales procesos, con lo que se hace un análisis de brechas contra la situación actual para diseñar el modelo de gobierno futuro.

En una cuarta etapa se debe proveer un nivel detallado, que contenga la información necesaria para la operación del modelo.

Para la preparación de la implementación existen una serie de reglas y actividades previas que se deben realizar antes de ejecutar la implementación, como la adquisición de herramientas, la realización de cambios organizacionales, cambios a los reglamentos internos, preparación de infraestructura, etc.

Con estos pasos completados se da inicio a la implementación la que consiste en poner en marcha los nuevos procesos, tecnología de información y organización. Una vez terminada la implementación se inicia un proceso de mejora que establece mecanismos para asegurar la mejora continua a lo largo del tiempo y de esta manera identificar las nuevas áreas de oportunidad⁹.

Entre los principales beneficios que la metodología ITIL puede brindar a la organización se pueden nombrar los siguientes:

- Contiene procesos probados.
- Provee procesos simples y listos que pueden ser usados inmediatamente.

⁹ OCAMPO S., Carlos, MORENO Laverde, Ricardo y MILENA Caicedo, Sandra.,2009.

- Contiene las plantillas, listas de comprobación y descargas que pueden ser utilizados tal y como están o de forma personalizada.
- Separa las tareas administrativas y tareas técnicas que ayudarán a asignar los recursos más adecuados.
- Ayuda a medir el rendimiento de apoyo técnico.

Entre los errores más comunes al momento de la implementación de ITIL se conocen los siguientes:

- Mantener la información del proyecto a nivel ejecutivo sin permearlo a la organización.
- Permitir que la comunicación informal supere a la difusión institucional del proyecto, creando incertidumbre en los empleados.
- Asignar a personas con grandes cargas de trabajo.
- Desorden en la implementación de procesos o estrategia demasiado agresiva (un gran número de procesos simultáneamente).
- Confundir áreas con procesos.

Al momento de implementar este modelo se debe considerar:

- Participación y difusión de la iniciativa a toda la organización.
- Establecer un plazo adecuado para la ejecución del proyecto.
- Seleccionar dueños de procesos con el perfil y jerarquía suficientes para coordinar la implantación de cada proceso.

Las categorías de la versión 3 de ITIL y sus sub divisiones se muestran en la Figura 10.

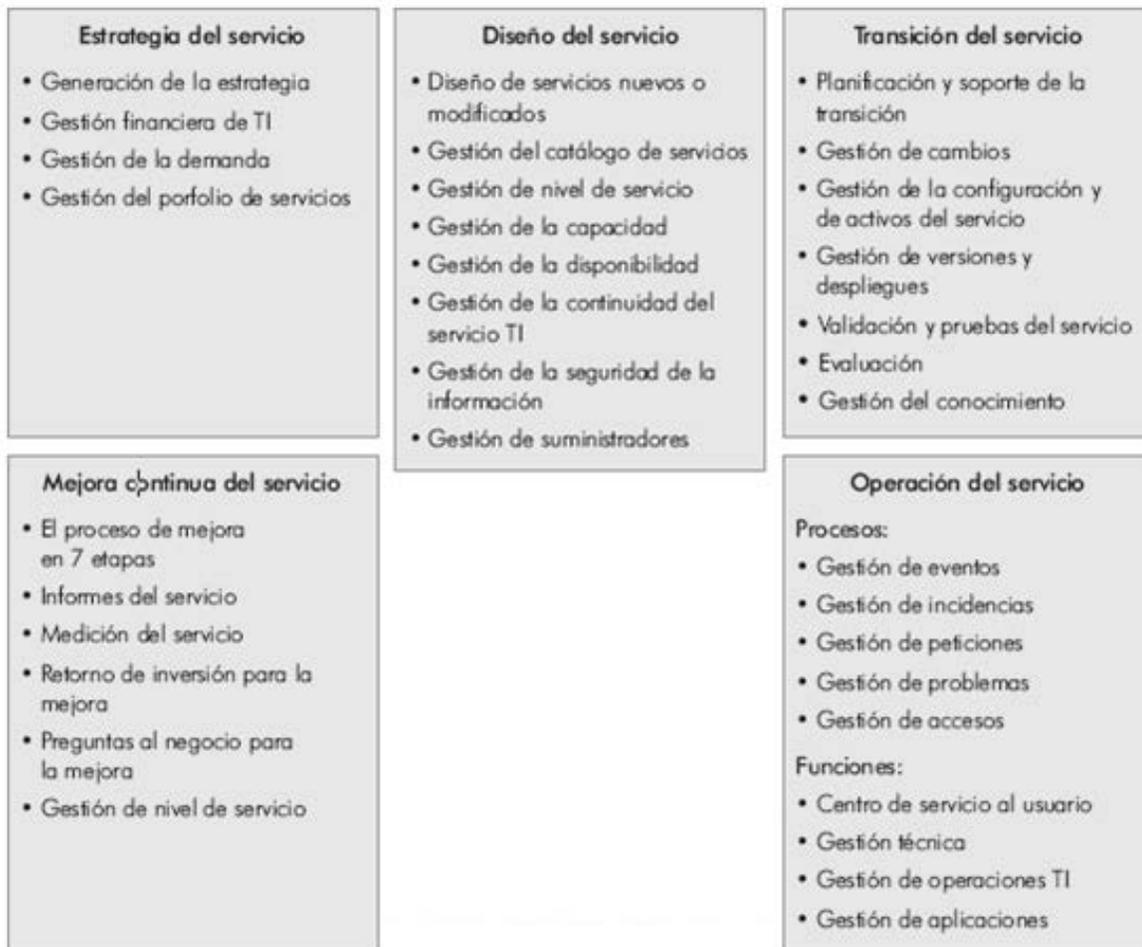


Figura 10. Etapas del modelo ITIL v3. Fuente: Libro ITIL v.3 publicado por la OGC.

1.3. Capability Maturity Model Integration (CMMI)

CMMI significa “Capability Maturity Model Integration” y se puede definir como: “un modelo de procesos que provee a una organización los elementos esenciales para el perfeccionamiento de sus procesos”. Actualmente CMMI abarca el desarrollo y adquisición de productos y servicios en general, sin embargo el origen del CMMI está en el modelo Software CMM, desarrollado por el Software Engineering Institute de la Universidad de Carnegie Mellon – SEI. La elaboración de CMMI fue encargada por la fuerza aérea estadounidense, con el objetivo de disponer de un modelo de evaluación para subcontratistas de software. Este modelo ha sufrido constantes mejoras a lo largo de su existencia, estas modificaciones se detallan en la Figura 11.

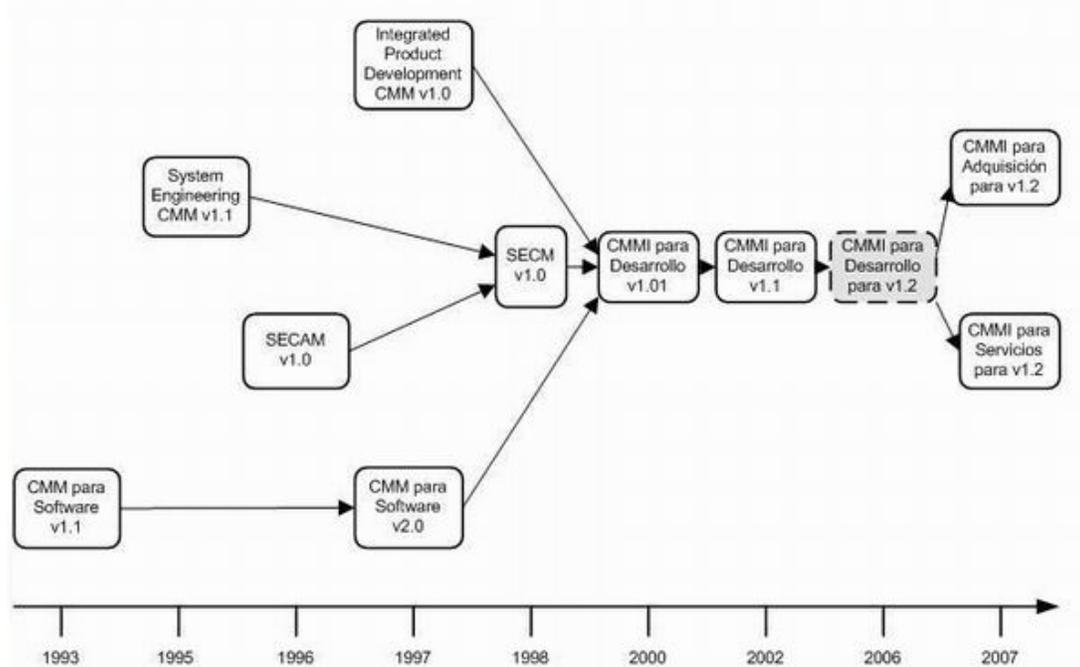


Figura 11. Evolución de los modelos CMM y CMMI. Fuente: SEI

Dentro del modelo CMMI, existen tres sub modelos principales, o constelaciones, que solucionan necesidades específicas de un área de interés, así se definen, en este modelo, tres constelaciones: CMMI for Acquisition (CMMI-ACQ) y CMMI for Development (CMMI-DEV) y CMMI for Services (CMMI-SVC), el cual posee objetivos similares a los de ITIL. Dentro de cada categoría, las áreas de procesos tienen ciertas interacciones y relaciones de dependencia que es importante conocer al momento de seleccionar las áreas de procesos que se desean implementar. Estas tres constelaciones y la relación entre ellas es posible observarlas en la Figura 12.

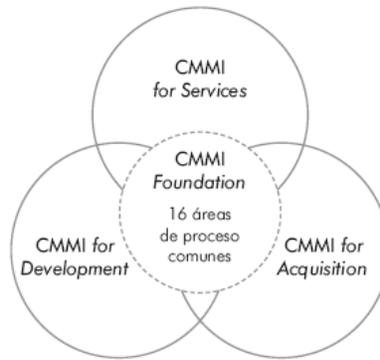


Figura 12. Áreas de CMMI. Fuente Elaboración propia.

Cada área de procesos incluye objetivos específicos requeridos, cuya implementación se puede lograr a través de prácticas específicas y otros elementos informativos que el mismo modelo recomienda. Esto se observa en la Figura 13.

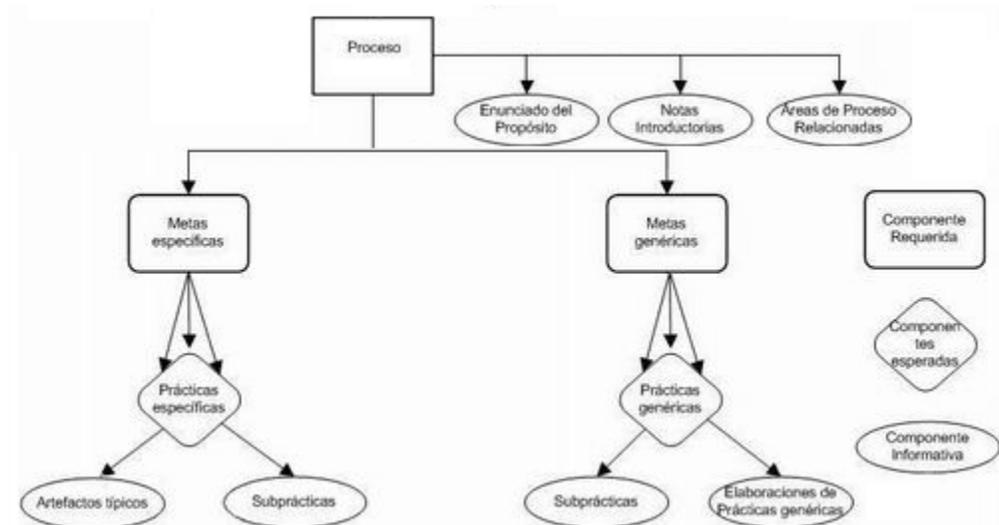


Figura 13. Elementos de un área de procesos en el modelo CMMI. Fuente: SEI.

Existe además un grupo de objetivos y prácticas genéricas, que son comunes a todas las áreas de procesos. Estas prácticas genéricas están orientadas a lograr la institucionalización de los procesos de la organización. Esto implica que “el proceso está arraigado en las formas de trabajo y que existe compromiso y consistencia en las prácticas del proceso”.

Entre los objetivos genéricos y las áreas de procesos también existen dependencias que se deben conocer, ya que la implementación de un área de procesos puede facilitar el cumplimiento de algunos objetivos genéricos para otras áreas y que, por tanto, deberían implementarse antes.

Junto con lo anterior, el modelo está organizado en distintos niveles incrementales, donde cada área de proceso corresponde a un nivel de madurez de CMMI. Por ejemplo, el área Configuration Management corresponde al nivel 2, el área Risk Management al nivel 3, el área Quantitative Project Management al nivel 4 y el área Casual Analysis an Resolution al nivel 5.

Estos niveles describen un camino predefinido y sistemático para realizar una mejora general a los procesos de la organización. La implementación a través de los niveles de madurez corresponde a la representación escalonada del modelo. Lo que se muestra en la Figura 14.

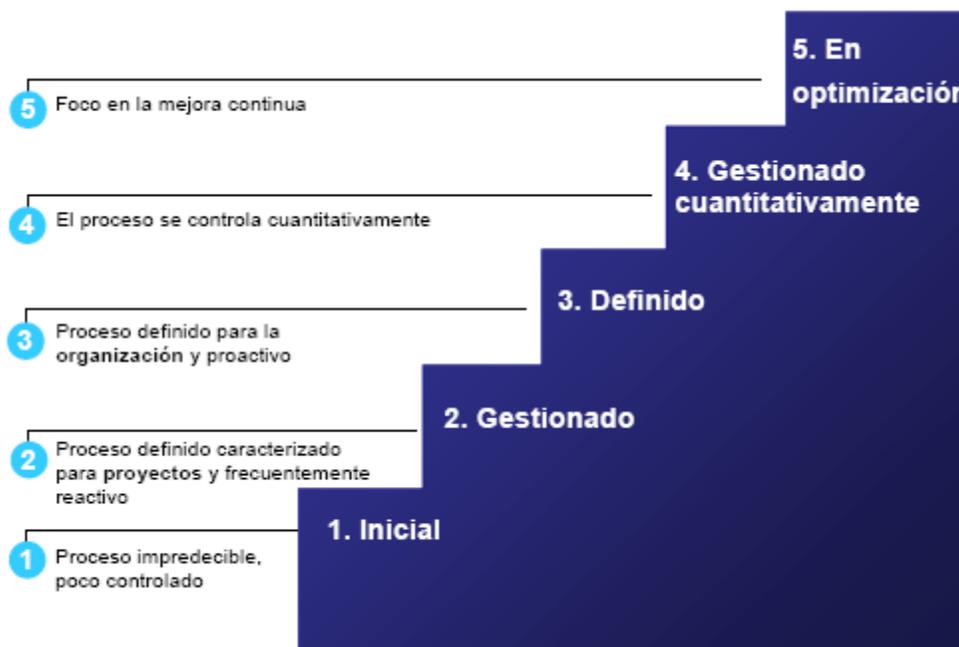


Figura 14. Niveles definidos en CMMI para medir la capacidad de los procesos. Fuente: SEI.

El nivel inicial corresponde a un nivel base, en el cual se encuentra cualquier organización, previo a la implementación de CMMI. El nivel administrado, corresponde a una organización donde los proyectos son planificados, ejecutados y monitoreados para cumplir con los objetivos planteados. En el nivel definido, las actividades de planificación, ejecución y monitoreo de proyectos se realizan en base a un conjunto de procesos estándares de la organización. En el nivel cuantitativamente administrado, la organización establece objetivos y criterios cuantitativos en base a los cuales se administran los proyectos. Finalmente, en el nivel optimizado, los procesos de la organización son constantemente perfeccionados en base a parámetros cuantitativos y a los objetivos de negocio de la organización.

1.3.1. Costos y beneficios de la implementación de CMMI

Las bases del modelo CMM se establecen a fines de los años 80 por W. Humphrey, *“el que define cómo va a ser el modelo de capacidad y madurez”*. Desde ese momento, hay una ramificación de modelos tanto para software como para ingeniería de sistemas y sus distintas aplicaciones, y según va avanzando la década de los 90 el modelo CMM sienta las bases de la mejora de la calidad del software en las organizaciones.

SW-CMM es un modelo de madurez de capacidades desarrollado para los procesos relativos a la producción y mantenimiento de sistemas software. Ya en los años 2000 se publica CMMI, intentando integrar gran parte de las versiones que CMM estaba proponiendo hasta entonces.

Sin embargo, hasta el año 2007, el modelo CMMI proponía buenas prácticas para un desarrollador de software. Dentro del desarrollo de software, existía un área de proceso donde el modelo presentaba especial atención al hecho de que si el software se subcontrata a un tercero, debían establecerse una serie de controles. Es el modelo CMMI-DEV v.1.2.

Normalmente cuando un consultor o un auditor evaluaban los procesos de un cliente, interpretaba el modelo CMMI desde el punto de vista del control que el cliente establecía en las actividades realizadas por el proveedor.

A fines de 2007, el SEI publica el modelo CMMI for Acquisition, que es el resultado de un grupo de trabajo entre General Motors y el SEI.

“No resulta fácil realizar un análisis concreto de los costos en los que incurría una organización cualquiera para implementar CMMI, sin embargo, a groso modo, es posible indicar que estos costos corresponden a las horas-hombre invertidas en el análisis de la organización y posterior implementación y adaptación de los nuevos procesos o mejoras en procesos existentes”.

En cuanto a los beneficios, un estudio del SEI presenta una serie de casos de adopción de modelos CMMI o software CMM, que proveen evidencia acerca de que un perfeccionamiento de procesos basado en estos modelos puede tener como resultado un mejor rendimiento en proyectos y una mejor calidad en los productos finales.

El despliegue, del modelo CMMI, en el mundo se presenta en la Figura 15.

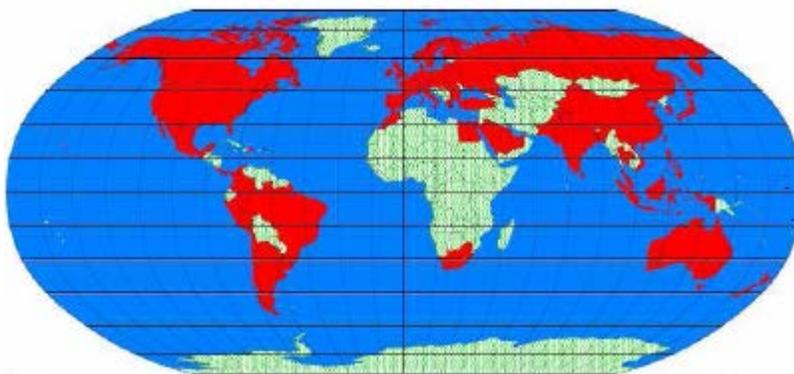


Figura 15. Despliegue del modelo CMMI en el mundo. Fuente: SEI, Process Maturity Profiles CMMI-DEV, September 2009.

1.3.2. CMMI for Services (CMMI-SVC) v.1.2

Este modelo fue publicado en febrero de 2009. Es usado en empresas que se dedican a establecer, gestionar y entregar todo tipo de servicios, enfatizando en la institucionalización de los procesos de manera incremental, a partir de niveles de madurez que posean los procesos. Consta de 24 áreas de proceso. De ellas 16 son áreas de proceso del modelo CMMI Foundation (CMF); 7 son áreas de proceso, específicas de servicios; y una es adicional de soporte. Y es la respuesta del SEI frente a modelos y estándares enfocados a los servicios de TI como ITIL, BS15000 e ISO 20000. Estas áreas de procesos son expuestas en la Figura 16.

CMMI para el desarrollo incorpora el desarrollo de los servicios, incluida la combinación de componentes, consumibles, y las personas destinadas a satisfacer las necesidades del servicio, esto difiere de la constelación prevista para servicios de CMMI-SVC que se centra en la prestación de servicios.

Esta sección de la norma abarca las actividades necesarias para establecer, entregar y administrar servicios. Tal como se define en el contexto de CMMI, un servicio es un intangible, un producto no almacenable. El modelo CMMI-SVC ha sido desarrollado para ser compatible con esta amplia definición. Las metas y prácticas de CMMI-SVC son, por lo tanto, potencialmente relevantes para cualquier organización interesada en la prestación de servicios, incluidas las empresas en sectores como: defensa, salud, TI, finanzas y transportes. Los primeros usuarios de CMMI-SVC durante su desarrollo y la experimentación reportan la prestación de servicios tan variados como capacitación, logística, mantenimiento y servicios TI. Además contiene prácticas que cubren la gestión de proyectos, gestión de procesos, establecimiento del servicio, entrega y soporte del servicio y soporte de los procesos. Todos los modelos CMMI-SVC comparten una gran cantidad de material con los modelos de CMMI, en otras materias.

Aproximaciones de CMMI-SVC v.1.2 permiten la mejora de procesos y consecuente valoración utilizando dos representaciones: escalonada y continua.

La representación continua permite a una organización seleccionar un proceso/área de proceso (o grupo de áreas de proceso) y mejorar individualmente los procesos relacionados. Esta representación utiliza niveles de capacidad para caracterizar una mejora con respecto a un área de proceso individual.

La representación escalonada usa conjuntos predefinidos de áreas de proceso para definir un camino de mejora de una organización. El camino de mejora se caracteriza por niveles de madurez.

Por ejemplo las ocho áreas de proceso del nivel dos son las siguientes:

- Gestión de requerimientos.
- Planificación de proyectos.

- Monitoreo y control de proyectos.
- Acuerdo de gestión de proveedores.
- Medición y análisis.
- Procesos y productos de calidad.
- Gestión de la calidad.
- Entrega del servicio.



Figura 16. Procesos definidos en CMMI-SVC v.1.2. Fuente: SEI

2. RELACIONES ENTRE LOS MODELOS

2.1. Diferencia entre norma y mejores prácticas.

Según la Asociación Española de Normalización y Certificación una norma es: “Un documento de aplicación voluntaria que contiene especificaciones técnicas basadas en los resultados de la experiencia y del desarrollo tecnológico. Las normas son el fruto del consenso entre todas las partes interesadas e involucradas en la actividad objeto de la misma. Además, debe aprobarse por un organismo de normalización reconocido”.

De acuerdo a las características que señala la definición, se puede implementar y certificar la conformidad con una norma.

En cuanto al término “mejores prácticas” no hay un consenso claro sobre lo que significa. En este sentido se podría decir que las “mejores prácticas” son: *“aquellas técnicas o métodos que han demostrado ofrecer resultados más eficientes y efectivos que el resto de las técnicas o métodos a la hora de aplicarse en un determinado ámbito”*.

Las mejores prácticas al igual que las normas deben ser publicadas por organismos que las recogen y elaboran, de aquí que exista una variada gama de ellas, que en el ámbito de los Sistemas de Gestión de Servicios de TI existen variadas aplicaciones, como son ITIL, CMMI, ISO 20000, ISO 27000, etcétera.

A modo de conclusión se puede señalar que la mayor diferencia entre una norma y las mejores prácticas es que en estas últimas no se puede hablar de conformidad, sino de alineamiento con sus recomendaciones.

2.2. Principios básicos de CMMI

El modelo CMMI es una fusión de modelos de mejora de procesos para ingeniería de sistemas, ingeniería del software, desarrollo de productos integrados y adquisición de software. La gran ventaja de CMMI es que ha demostrado ser una metodología de gran eficacia, que ha permitido mejoras de gran impacto en ***procesos de desarrollo de productos software***, tales como reducción del costo de desarrollo, localización y resolución de defectos, entre otras. El gran problema de CMMI es su falta de adecuación al enfoque a servicio que está experimentando el sector de las TI en todas sus líneas de actividad, así como el alto esfuerzo que exige su implementación.

2.3. Principios básicos de ITIL

La metodología ITIL es la norma más ampliamente conocida para la gestión de los servicios TI, se basa en recopilar una serie de mejores prácticas en diferentes sectores de actividad a nivel mundial, que se publican de forma habitual y sistemática, con el objetivo de lograr una gestión

eficiente de la infraestructura y los servicios de TI, permitiendo un alto nivel de disponibilidad de dichos servicios y un alto nivel de satisfacción de clientes y empleados de la compañía.

La principal ventaja de ITIL es que ha demostrado su eficacia con su enfoque a la gestión de servicios de TI. El gran problema de ITIL es que ***no cubre adecuadamente las fases de desarrollo de software ni la gestión de proyectos asociada a esa fase de construcción de activos de software.***

Los procesos, en este modelo, están alineados con el estándar de calidad ISO 9000 y se encuentran vinculados con el Modelo de Excelencia de la EFQM (European Foundation for Quality Management), el cual es utilizado por empresas en todo el mundo.

ITIL se centra en brindar servicios de alta calidad para lograr la máxima satisfacción del cliente a un costo manejable. Para ello, parte de un enfoque estratégico basado en tres pilares:

- Los procesos.
- Las personas.
- La tecnología.

En otras palabras: determina la forma de ejecutar procesos estándar ayudados de la tecnología para lograr la satisfacción de las personas, usuarios de los servicios de TI.

Por otro lado, la gestión de servicios con ITIL tiene su columna vertebral en la función de Service Desk, la cual es el punto único de contacto entre la organización y el usuario o cliente del servicio. Lo que se puede observar en la Figura 12 de este proyecto de título.

Tener un sistema de gestión de servicios basado en ITIL permitirá a la compañía lograr:

- Mayor alineamiento de TI con el negocio: Los procesos ITIL están dirigidos a maximizar la disponibilidad de los servicios TI con el propósito de lograr la satisfacción de los clientes y cumplir con los acuerdos de nivel de servicio (SLA) acordados.
- Resolución de incidencias y problemas más rápido y eficiente: Al tener una posición proactiva hacia la resolución rápida y eficaz de incidentes y a la vez hacia la prevención de los mismos, se logra también la satisfacción de los clientes.
- Reducción del número de llamadas a Mesa de Ayuda: Las mejores prácticas de ITIL establecen los procesos necesarios no solo para resolver incidentes, sino para aprender de ellos y lograr tener una base con la que la organización pueda tener una mejora continua minimizando cada vez el número de incidentes y la carga de trabajo de la Mesa de Ayuda.
- Aumento del nivel de resolución de incidencias en primera instancia: Organizando adecuadamente los niveles de escalamiento de incidentes en Mesa de Ayuda, se logra maximizar el tiempo de respuesta y resolución desde que se comunica el incidente en el servicio TI hasta su resolución.

- Implantación de cambios más rápido / mejor control de cambios: Gracias al proceso de gestión de cambios de ITIL, se pueden administrar los cambios requeridos en la infraestructura TI que se generan a raíz de algún incidente determinado. El correcto manejo de los cambios garantiza la calidad y estabilidad de los servicios TI.
- Reducción del número de cambios que necesiten ser revocados: Con una correcta gestión de cambios, que cuente con revisiones de la Junta de cambios y el cliente, se minimizarán los posibles problemas que puedan surgir, respecto a dichos cambios, entre la organización y el cliente.

2.4. Principios básicos de ISO 20000.

Se definió en diciembre de 2005, y es considerado el primer estándar internacional para la administración de servicios de TI. ISO 20000 toma como base fundamental ITIL, pero además ha considerado otras referencias relevantes del sector tecnológico. En cuanto a la efectividad de la implementación de la ISO 20000, esta puede ser certificada por terceros independientes.

Por otro lado, las compañías que han implementado un estándar ISO, se beneficiarán de implementar ISO 20000 puesto que todo el marco de administración del estándar que cubre los aspectos del negocio se puede aprovechar sin ningún esfuerzo adicional, y al igual que los otros estándares ISO tiene dos partes:

- ISO/IEC20000-1 - requisitos , lo que se hará.
- ISO/IEC20000-2 - código de prácticas, una orientación en cuanto a cómo se debe hacer con más detalle

Como ya se dijo, primera, es obligatoria y es sobre la cual se puede certificar el cumplimiento con el estándar, y la segunda que es un conjunto de sugerencias sobre la parte 1. ISO 20000-1 indica textualmente que “promueve la adopción de un enfoque integrado para administrar de manera efectiva la entrega de servicios para satisfacer los requerimientos del cliente y el negocio”.

Complementariamente, ISO 20000-2 (la parte 2) corresponde con las “mejores prácticas” sugeridas para satisfacer la parte 1. En general los procesos de implementación de un estándar de TI son bastante similares, y todos ellos deben considerar etapas de capacitación, diagnóstico, implementación y opcionalmente certificación. Aunque las épocas de turbulencia económica generalmente involucran procesos de recortes presupuestarios para este tipo de proyectos, algunos autores sugieren que son momentos ideales para implementar estándares antes mencionados.

2.4.1. Cómo se relacionan ITIL e ISO 20000

Como ya se ha mencionado anteriormente la norma ISO 20000 se encuentra profundamente relacionada con ITIL, esto se observa en la siguiente figura que muestra la relación entre ISO/IEC 20000, ITIL y los procesos In-house:

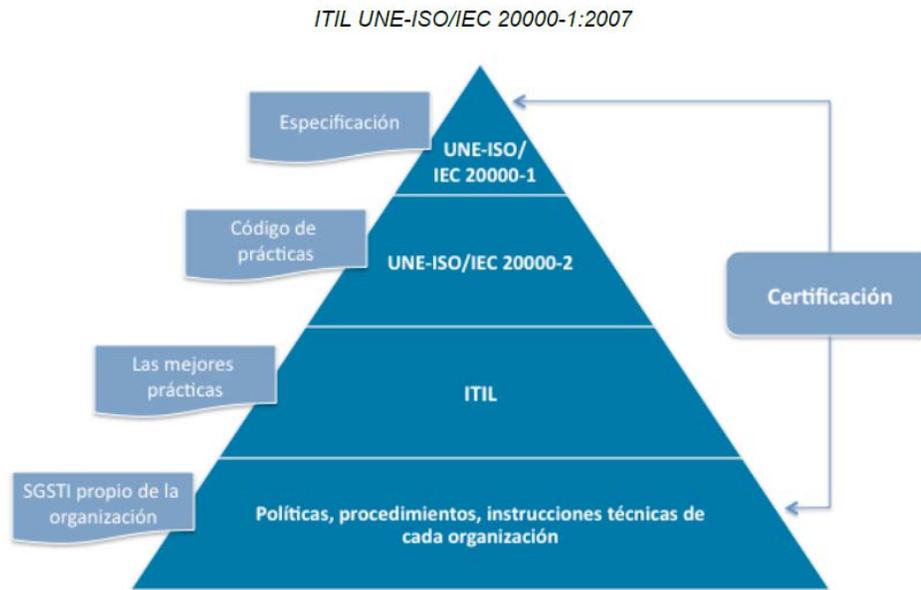


Figura 17. Relación Entre ISO/IEC 20000, ITIL y Procesos In-house. Fuente: ITSM.

Como se indica en la figura, la parte superior de la pirámide equivale a la parte 1 de la norma ISO/IEC 20000 que presenta la Especificación de esta, es decir, objetivos a alcanzar con el Sistema de Gestión de Servicios TI (SGSTI) para que sea certificable. En este caso y utilizando el símil de la construcción de un vehículo podemos considerar que en esta parte se recogen las características que deberá tener un SGSTI para ser considerado vehículo por gobierno.

La segunda capa de la pirámide representa la parte 2 de la norma, es aquí donde se define un código de buenas prácticas y es una guía que trata de aclarar los requerimientos especificados de la parte uno. Siguiendo con el símil del vehículo, representaría el “manual” para construir el vehículo, independientemente de los recursos que se tengan pero en línea con las directrices del gobierno.

La tercera capa, que representa la capa ITIL, contiene las mejores prácticas recogidas en el sector para la implementación de un SGSTI. En el símil automovilístico, representaría la opinión y metodologías empleadas por los grandes fabricantes del mundo del automóvil donde se reflejan los procedimientos que les han permitido construir los mejores coches.

La cuarta capa es la aplicación práctica de todos los elementos o capas anteriormente señaladas. Es decir, se mantienen como principal referencia las especificaciones de la parte 1, teniendo en cuenta que es la norma certificable, se considera la parte 2, buenas prácticas y las mejores prácticas propuestas por ITIL, pero se acomodan a un entorno más limitado en cuanto a

recursos humanos y materiales como es la PYME. Siguiendo con la analogía para la construcción de un vehículo, se mantienen las especificaciones a cumplir, definidas por quien posteriormente verificará que el coche pueda circular por las carreteras. Se sabe y considera la experiencia y maneras de construir que han resultado exitosas a lo largo del tiempo, pero se construye el vehículo en un taller ubicado en cualquier ciudad del país y no en un centro de producción de una multinacional.

Una comparación entre ITIL, CMMI y la norma ISO 20000 se muestra en la Tabla 3, que se presenta a continuación.

Modelo	ITIL	ISO/IEC 20000	CMMI
Creador	Office of Government Commerce (OGC)	International Organization for Standardization (ISO)	Software Engineering Institute de la Universidad de Carnegie Mellon
Certificación	Personas	Organizaciones-Empresas	Organizaciones-Empresas
Enfoque	<ul style="list-style-type: none"> • Se enfoca en el Cómo hacer. • Establece las mejores prácticas para la gestión de servicios, proporcionando lineamientos de gestión para adoptar roles, responsabilidades y actividades que deben realizar los diferentes procesos descritos para entregar servicios con eficiencia y calidad. 	<ul style="list-style-type: none"> • Enfoque en el Qué • Indica los requisitos mínimos que deben cumplir las empresas para tener un Sistema de Gestión de Servicios de TI, estos requerimientos sirven como base para realizar auditorías de certificación. 	<ul style="list-style-type: none"> • Se Centra en el Qué. • Es una fusión de modelos de mejora de procesos para ingeniería de sistemas, ingeniería del software, desarrollo de productos integrados y adquisición del software. Constituye una forma de medir el grado de madurez de las organizaciones, con el objetivo de establecer una guía que les permita mejorar sus procesos y su habilidad para organizar, desarrollar, adquirir y mantener productos y servicios informáticos.

Cumplimiento	<ul style="list-style-type: none"> • Voluntario. • Las organizaciones pueden adoptar las prácticas establecidas en ITIL para seguirlas dentro de su organización, pudiendo seleccionar las que le brinde mayor valor y que cumplan con los objetivos estratégicos de la organización. 	<ul style="list-style-type: none"> • Voluntario/Vinculante • Si bien puede ser usado como modelo de referencia sin fines de certificación principalmente es utilizado para fines de obtención de un certificado de cumplimiento, para lo cual es obligatorio cumplir con todos los requisitos definidos. • La certificación contempla vigilancias que aseguran se mantiene el cumplimiento a través del tiempo. 	<ul style="list-style-type: none"> • Vinculante • Se deben cumplir con los puntos que serán evaluados para obtener la certificación. • Si bien no existe una duración de la certificación, las empresas sólo parecerán durante 3 años en los registros de CMMI.
	Ventajas	<ul style="list-style-type: none"> • Puede ser adoptado de manera parcial. • Sugiere la mejora continua. 	<ul style="list-style-type: none"> • Establece un sistema de gestión. • Se vigila su cumplimiento. • Asegura la mejora continua. • Proporciona certidumbre y confianza a clientes.

Desventajas	<ul style="list-style-type: none"> • No contempla un esquema de cumplimiento ni seguimiento. • No se puede garantizar su cumplimiento 	<ul style="list-style-type: none"> • No define en sí mismo los ¿cómo?, aunque existen las partes 2-5 para ello. • Tiene un alcance limitado sobre la gestión de activos y conocimiento. 	<ul style="list-style-type: none"> • Falta de adecuación al enfoque a servicio que está experimentando el sector de las TI (procesos de desarrollo de productos de software) en todas sus líneas de actividad, así como el alto esfuerzo de implantación que exige. • El proceso de evaluación es muy costoso (tiempo y esfuerzo).
--------------------	---	---	--

Tabla 3. Relación ITIL, ISO/20000 y CMMI. Fuente: Elaboración propia.

2.5. ¿Cuál es la mejor forma de implementar ITIL, CMMI e ISO/IEC 20000?

Como ya se ha mencionado la adopción de estándares y mejores prácticas facilita la rápida aplicación de buenos procedimientos y evita retrasos en la creación innecesaria de nuevos enfoques en los que hay que ponerse de acuerdo. Esto sin dejar de ser compatibles con un marco de gestión de riesgos y de control apropiado para la organización e integrándose con otros métodos y prácticas que se estén utilizando. Para realizar esta integración es que se sugiere tener en consideración cuatro puntos:

2.5.1. Elaboración

Todas las empresas pueden adaptar por el uso de al menos uno de los estándares y prácticas presentados en este documento, los que se deberán ajustar sus requisitos individuales. Los tres documentos mencionados en este punto pueden desempeñar un papel muy útil al utilizarse juntos. CMMI e ISO/IEC 20000 para ayudar a definir qué debería hacerse e ITIL muestra el cómo para los aspectos de la gestión de servicios. Las aplicaciones típicas para este tipo de estándares y prácticas son las siguientes:

- Para definir los requisitos del servicio y las definiciones del proyecto, tanto internamente como con los proveedores de servicios.
- Para facilitar la mejora continua.
- Como marco para la auditoría, evaluación y una visión externa.

2.5.2. Priorización

Es necesario que el estándar escogido sea adecuado para la organización, además de que este sea posible de implementar y no implique gastos excesivos o innecesarios para la compañía. Para esto la empresa necesita un plan de acción eficaz que se adapte a sus circunstancias y necesidades particulares. Es muy importante que se asuma el liderazgo TI real que permita establecer la dirección que la gestión debe seguir.

2.5.3. Planificación

Una vez que se ha decidido implementar un estándar y que se ha escogido a los líderes del proyecto se debe planificar la forma en la que se implementará este estándar. Un ejemplo que ayuda a esta tarea se encuentra en la guía IT Governance Implementation Guide del ITGI, el que propone los siguientes pasos:

1. Establecer un marco organizativo, idealmente como parte de una iniciativa global de gobierno de TI, con objetivos y responsabilidades claras, la participación de todas las partes involucradas, quienes impulsarán la implementación y la asumirán como una iniciativa propia.
2. Alinear la estrategia de TI con los objetivos del negocio. ¿En cuáles de los objetivos de negocio actuales, TI contribuye de forma significativa a ellos?.

3. Entender y definir los riesgos. Dados los objetivos de negocio, ¿cuáles son los riesgos relativos a la capacidad de TI para cumplirlos?
4. Definir las áreas objetivo y determinar las áreas de proceso de TI que son críticos para la entrega de valor y gestionar estas áreas de riesgo.
5. Analizar la capacidad vigente e identificar las brechas. Realizar una evaluación de la capacidad de madurez para saber dónde es que más se necesitan mejoras.
6. Desarrollar estrategias de mejora y decidir cuáles son los proyectos de mayor prioridad que ayudarán a mejorar la gestión y el gobierno de estas áreas importantes.
7. Medir los resultados, estableciendo un mecanismo de puntuación para medir el desempeño actual y monitorear los resultados de nuevas mejoras.
8. Repetir los pasos 2 a 7 con una frecuencia regular.

3. GRUPO CAP S.A. Y COMPAÑÍA SIDERGÚRGICA HUACHIPATO.

3.1. Grupo CAP S.A.

El grupo CAP, creado en 1946 bajo el mandato del presidente Juan Antonio Ríos con el nombre de Compañía de Acero del Pacífico S.A. centra sus actividades en las distintas etapas (3) de la producción ferrífera. La primera etapa se realiza a través de la Compañía Minera del Pacífico S.A. (CMP), creada en 1981, y consiste en la extracción y concentración de mineral de hierro, desde sus yacimientos en el Norte de Chile. Esta producción se vende como materia prima entre productores siderúrgicos, principalmente en el mercado asiático (China, Japón, e Indonesia).

La segunda etapa se realiza a través de Compañía Siderurgia Huachipato S.A. (CSH), inaugurada en 1950, con el nombre de Planta Siderúrgica Huachipato, y consiste en la utilización en Chile de parte de la producción de CMP, de minerales de hierro, para producir aceros planos y largos, para las más variadas industrias nacionales.

La tercera y última etapa, la que utiliza también parte de la producción de acero, consiste en el desarrollo de productos de valor agregado en acero, procesados por empresas filiales en Chile, Perú y Argentina, para su uso en la construcción, industria e infraestructura. Esta etapa se desarrolla a través de Cintac S.A. e Intasa S.A. y sus respectivas filiales.

La misión del Grupo CAP S.A. es liderar los negocios en que participa, creando valor sustentable tanto en la minería del hierro como la siderurgia y el procesamiento de acero, ofreciendo productos y soluciones innovadoras a sus clientes. Buscando la excelencia operacional y ambiental, privilegiando el desarrollo de las personas como factor determinante del éxito.

Así mismo como visión busca ser un actor relevante a nivel regional, capaz de crecer para responder oportunamente a la evolución de los requerimientos de los mercados en que están presentes. Continuar contribuyendo al desarrollo de las comunidades donde se ubican sus operaciones y al progreso de Chile.

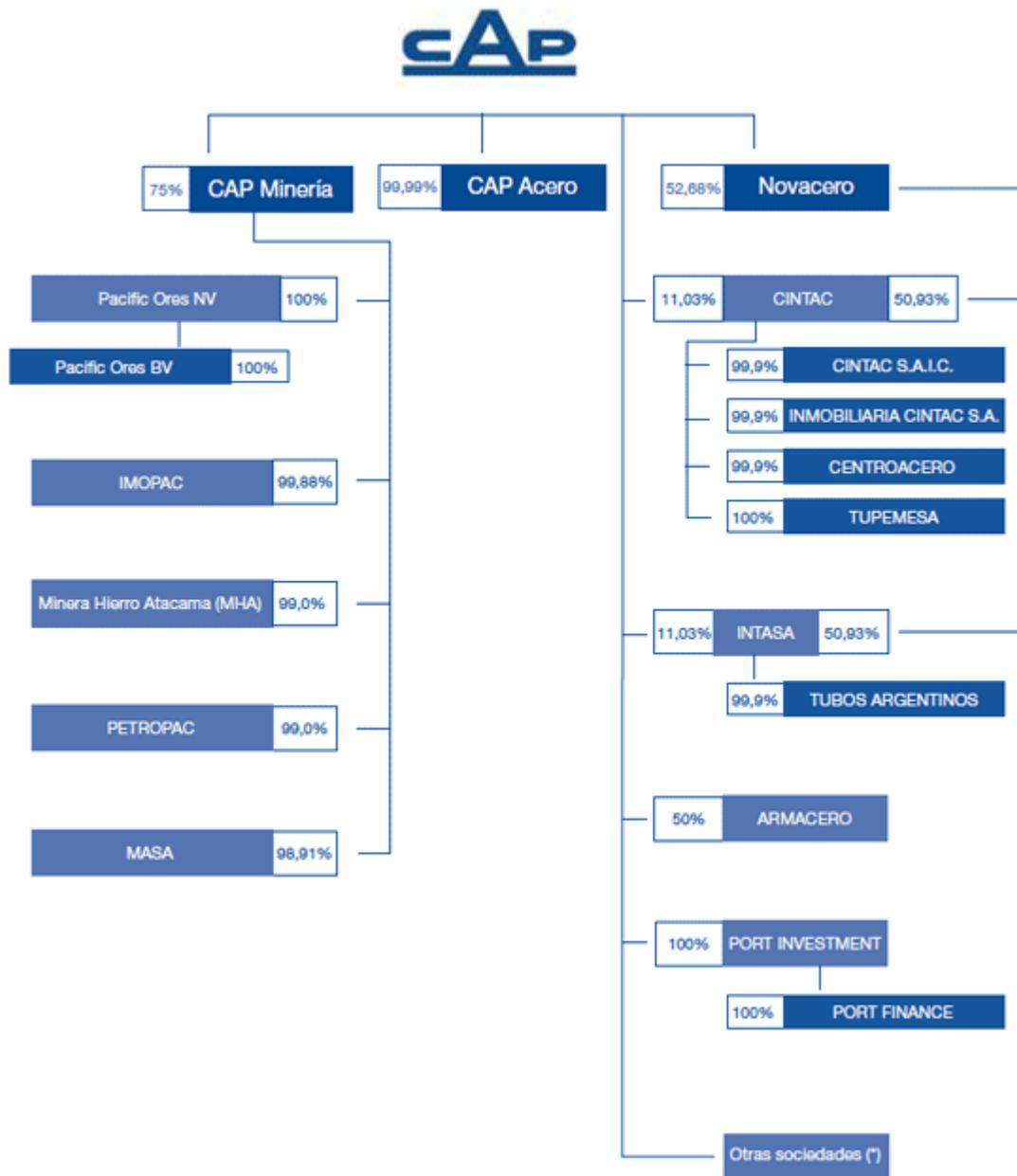


Figura 18: Holding Corporativo Grupo CAP con porcentaje de participación. Fuente: CAP.

3.2. La Compañía Siderúrgica Huachipato S.A.

Es una empresa siderúrgica integrada que obtiene arrabio por reducción de pellets y granza de mineral de hierro en sus Altos Hornos. El acero producido en la Acería de Convertidores al oxígeno es colado a planchones y palanquillas, los que posteriormente, por laminación, se transforman en diversos productos destinados al mercado nacional e internacional.

La Compañía, se ubica en la Bahía de San Vicente, 14 Km. al noroeste de la ciudad de Concepción, capital de la Octava Región, Chile, y comenzó a ser construida a comienzos de 1947 siendo oficialmente inaugurada el 25 de noviembre de 1950.

En el año 1981 la Compañía de Acero del Pacífico S.A., a través de sus organismos estatutarios, se transformó en una Sociedad de Inversiones con empresas subsidiarias. Como consecuencia de lo anterior, con fecha 15 de diciembre de 1981 se constituyó la Compañía Siderúrgica Huachipato S.A., que inició su giro el 1 de enero de 1982.

Desde su fundación en 1950, la capacidad de producción de la Compañía ha aumentado en más de ocho veces, llegando hoy a 1.450.000 toneladas de acero líquido, con lo cual consolida su liderazgo en el mercado nacional. Actualmente CAP Acero, cuya razón social es Compañía Siderúrgica Huachipato S.A. cubre las necesidades de importantes sectores de la economía del país: minería, industria metalmeccánica, construcción y elaboración de envases de hojalata. Además, los productos CAP están presentes en exigentes mercados internacionales.

Cerca de 2000 personas trabajan hoy directamente en la Compañía, la que a su vez, ofrece un importante espacio de desarrollo a muchísimas pequeñas y medianas empresas que la proveen de insumos y servicios.

Su Misión es producir y proveer productos y soluciones en acero de excelente calidad y servicio que superen las expectativas de sus clientes, privilegiando el desarrollo del recurso humano como factor determinante del éxito. Desarrollar ventajas competitivas, que generen rentabilidad, a través de la innovación de sus procesos mediante el uso de tecnologías sustentables.

La Visión de CAP Acero es liderar en Chile el negocio del acero en todas sus formas y desarrollar nuevas oportunidades en el área de tecnologías siderúrgicas.

3.2.1. Estructura Organizativa

La estructura de la organización de CAP Acero está conformada básicamente por gerencias, divisiones y unidades. Son cinco gerencias (De Administración y Desarrollo Humano, De Operaciones, De Ingeniería, De Medio Ambiente y Seguridad, y Gerencia Comercial) encabezadas por la Gerencia General que da cuentas al Directorio de la empresa.

De ellas, la que agrupa la mayor cantidad de personal es la Gerencia de Operaciones que está dividida en cuatro divisiones (Hierro y Acero; Productos Planos; Productos Largos; y Servicios).

Existen tres divisiones asesoras de la Gerencia General (la División Finanzas, la División Calidad, Ambiente y Seguridad y la División Planificación y Gestión Estratégica). A su vez, la División Ventas depende de la Gerencia Comercial y la División Ingeniería, de la Gerencia de Ingeniería.

Las unidades tienen carácter tanto de organismos asesores como de dependientes de las distintas gerencias o divisiones.



Figura 19: Organigrama Compañía Siderúrgica Huachipato al 17 de Abril de 2011. Fuente: CSH.

4. Unidad de Tecnologías y Sistemas de Información

La Unidad de Tecnologías y Sistemas de Información (TSI) es la unidad encargada del soporte informático de la Compañía Siderúrgica Huachipato. Está subordinada a la División de Planificación y Gestión Estratégica, que a su vez depende directamente de la Gerencia General. Por su ubicación dentro del organigrama de la compañía, la unidad de TSI tiene una mirada transversal de esta.

Su estructura interna se encuentra dada de la siguiente manera: a la cabeza está el jefe de la unidad, de este depende el encargado de seguridad y calidad y las áreas de gestión de procesos de negocio, operaciones y el área de plataforma. Esta estructura se detalla en el organigrama de la unidad, que se muestra en la Figura 20.

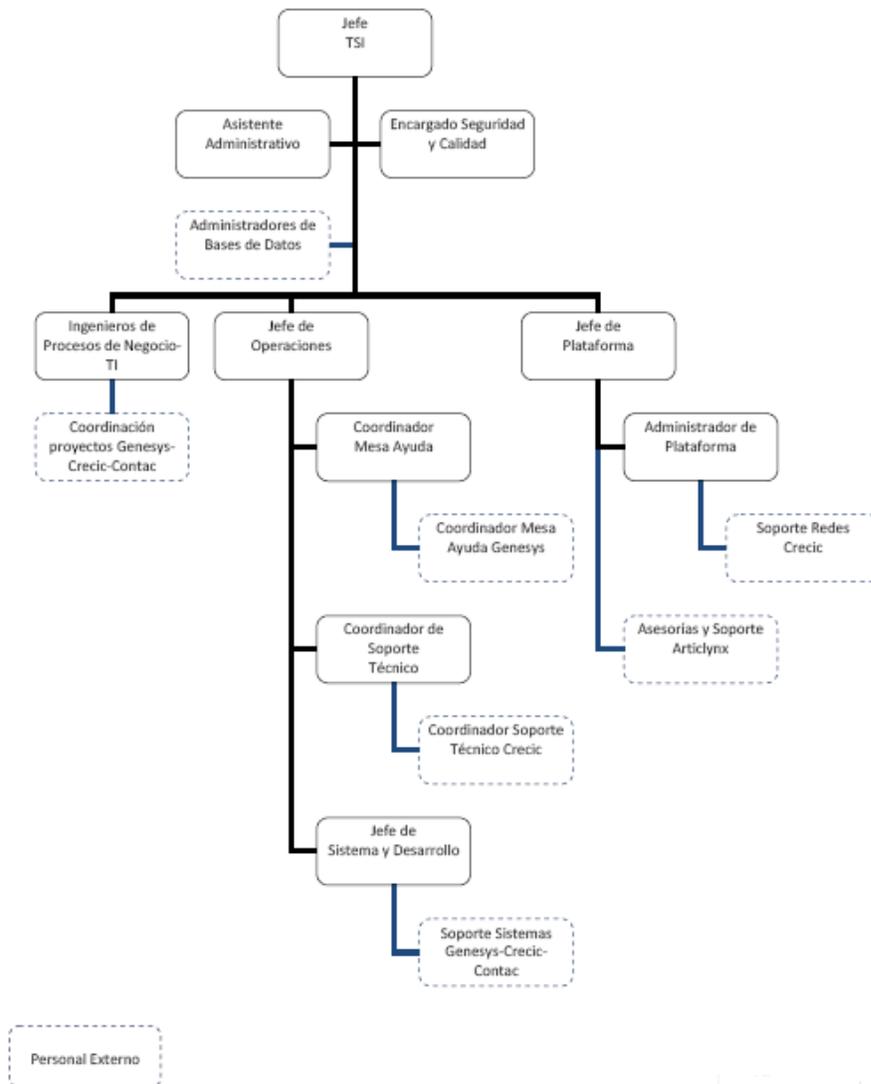


Figura 20: Organigrama de la unidad de Tecnologías y Sistemas de Información de la Compañía Siderúrgica Huachipato. Fuente: CSH.

Las responsabilidades se detallan a continuación:

- En el área de Gestión de Procesos de Negocio, los ingenieros de procesos de negocio (IPN) planifican, organizan, evalúan y controlan los recursos que tengan incidencia en los procesos, que están bajo su responsabilidad, por medio del desarrollo de soluciones de negocio con componentes tecnológicas, acorde a las demandas de la Compañía.
- En el área de Operaciones, su jefe de área, el coordinador de mesa de ayuda, el coordinador de soporte técnico y el jefe de sistemas y desarrollo gestionan y controlan las actividades de apoyo y mantención asociadas a la explotación diaria de las soluciones tecnológicas y las tecnologías de Información de escritorio que posee la compañía.
- En el área de Plataforma, su jefe y los administradores de plataforma tienen como objetivo gestionar y controlar las actividades de incorporación, soporte y mantención de las tecnologías de Información, de comunicaciones, redes y servidores que posee la compañía.
- Por último, el área de Seguridad y Control de Calidad tiene como objetivo definir, gestionar y administrar las políticas de seguridad de la unidad que permitan garantizar la continuidad del negocio, desde la perspectiva de apoyo de las TI, ante incidentes o amenazas.

Las funciones que deben desarrollar las personas en los distintos cargos son las siguientes:

- Ingeniero de Procesos de Negocio:
 - Velar por el mejoramiento continuo de los procesos de negocio bajo su cargo, por medio del desarrollo de soluciones de negocio con componentes tecnológicas y la continuidad operacional, controlando el fiel cumplimiento de las políticas y reglas de negocio.
 - Gestionar y administrar los proyectos de desarrollo o mantenciones de soluciones de negocio, velando por la optimización de los recursos internos y la utilización eficiente de la metodología de desarrollo de proyectos de la unidad de TSI.
- Jefe De Operaciones:
 - Gestionar la continuidad operacional de las soluciones de negocio desarrolladas en el área de Gestión de Procesos de Negocio.
 - Gestionar la continuidad operacional de las tecnologías de hardware y software de escritorio utilizado en las operaciones de la compañía.
- Jefe de Sistemas y Desarrollo:

- Administrar la continuidad operacional y apoyar el mejoramiento continuo de las soluciones de negocio desarrolladas en el área de Gestión de Procesos de Negocio.
- Gestionar el control de calidad de las soluciones desarrolladas por las empresas contratistas.
- Coordinador Soporte:
 - Mantener la continuidad operacional de los equipos y sistemas de escritorio, generando y supervisando planes, procedimientos de mantención y soporte. Todo lo anterior se debe realizar optimizando los recursos de la empresa.
 - Coordinar y supervisar a los coordinadores de las empresas prestadoras de servicio y áreas de la unidad a la solución de fallas o requerimientos relacionados con software y hardware de escritorio.
 - Administrar y controlar la asignación de equipos, junto a lo anterior mantener el inventario de los equipos y software licenciado de estos. Generar y dar cumplimiento al plan de mantención diario.
- Coordinador Mesas de Ayuda:
 - Administrar la resolución de los incidentes declarados en mesa de ayuda.
- Jefe de Plataforma:
 - Gestionar la continuidad operacional de las plataformas de servidores y comunicaciones que garanticen la disponibilidad de tecnologías y soluciones de negocio desarrolladas por la unidad de TSI.
- Administrador de Plataforma:
 - Administrar y ejecutar las actividades que aseguren disponibilidad y continuidad operacional de las plataformas de servidores y comunicaciones y de las tecnologías.
- Encargado de Seguridad y Control de Calidad:
 - Gestionar y administrar el plan de continuidad del negocio.

5. ANÁLISIS DE LAS ÁREAS A LAS QUE SE LE APLICARÁ EL MODELO

El análisis se centrará en dos sub áreas dentro de la unidad: Plataforma, que como se dijo tiene como objetivo gestionar y controlar las actividades de incorporación, soporte y mantención de las tecnologías de Información, de comunicaciones, redes y servidores que posee la compañía. Además de Operaciones donde se gestionan y controlan las actividades de apoyo y mantención asociadas a la explotación diaria de las soluciones tecnológicas y las tecnologías de Información de escritorio que posee la compañía. Se analizarán sólo estas dos sub áreas ya que en estas se enfocará el modelo.

5.1. Área de Plataforma

Esta área es la encargada de velar por el cuidado y mantención del ambiente de servidores, la conectividad lógica y física de estos y de las máquinas y estaciones de trabajo, así mismo es la encargada del almacenamiento centralizado de la información y del acceso a los recursos, como acceso remoto a estaciones de trabajo y servidores. Todas estas actividades se centran en dos grandes aspectos que son:

- Dar soporte a la continuidad operacional del negocio.
- La innovación.

Esta área trabaja con un esquema donde los servicios que se desarrollan dan lugar a procesos que se ejecutan en el área mediante los procedimientos establecidos para cada uno. Así, un servicio consta de procesos asociados a él, y este a su vez requiere de procedimientos establecidos para su funcionamiento. Esto se detalla en la Figura 21.

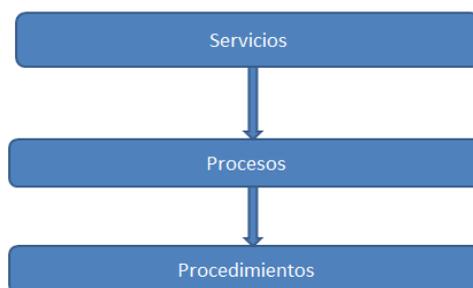


Figura 21. Funcionamiento Área de Plataforma unidad de TSI. Fuente: CSH.

Dentro de lo que corresponde a la continuidad operacional del negocio se destacan actividades como el monitoreo de servidores y el control de servicios, el respaldo y restauración de la información de la compañía, almacenada en las estaciones de trabajo y servidores, el manejo de contingencias, la seguridad de la información, que se garantiza mediante la encriptación de datos. También esta área es la encargada del soporte y mantención del hardware y software. Además, dentro de las actividades que desarrolla está la de someter a una evaluación la infraestructura informática de la organización.

En cuanto a la innovación, esta área se encarga de analizar requerimientos y plantear soluciones a las problemáticas que se generan de la operación de la unidad.

Los servicios que entrega plataforma se centran en cinco sectores, los que se subdividen en procesos. Estos sectores y procesos son los que se muestran en la siguiente tabla:

Conectividad física	Conectividad lógica	Acceso a recursos
<ul style="list-style-type: none"> • Manejo de equipos (NPI). • Instalaciones. • Cableado. 	<ul style="list-style-type: none"> • Autenticación en red RADA. • Autenticación en red AD. • Manejo de DNS y DHCP. 	<ul style="list-style-type: none"> • Acceso a internet. • Accesos remotos (VPN). • Control de correo electrónico. • Telefonía IP.
Ambiente de servidores	Almacenamiento centralizado	
<ul style="list-style-type: none"> • Datacenter. • Servidores. • Comunicación. 	<ul style="list-style-type: none"> • Almacenamiento personal. • Almacenamiento compartido. 	

Tabla 4. Sectores y procesos del área de Plataforma de la unidad de TSI. Fuente: CSH.

Todo lo anterior queda explicado en la Figura 22 que muestra el modelo de trabajo de Plataforma.

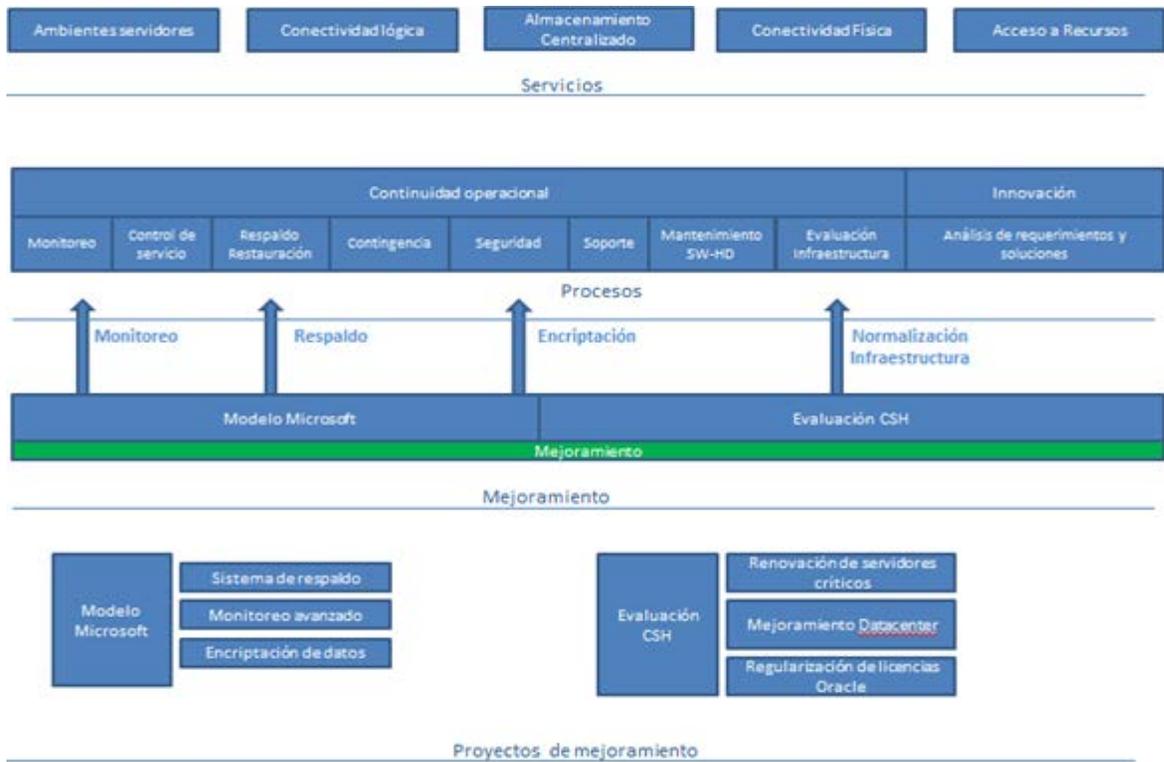


Figura 22. Modelo Área de Plataforma unidad de TSI. Fuente: CSH.

El área de plataforma cuenta con proyectos de mejoramiento, entre los que se cuentan:

- En la continuidad operacional:
 - **Respaldo y recuperación**, el estado actual de este proceso es básico, ya que el servidor de respaldo es un PC armado con una unidad de cintas anexada. El software es libre sin soporte. Lo que se quiere lograr es una estandarización con el objetivo de mejorar el sistema de respaldo lo que involucra la adquisición del hardware y software necesarios, con esto se espera garantizar la continuidad operacional, asegurando la disponibilidad de información en caso de catástrofe, disminuyendo la probabilidad de pérdidas irrecuperables de información. Además, esto permitirá una administración centralizada de respaldos, que hará posible verificar y programar eficientemente la manera y el período en que se realizarán estos. Ello se pretende implementar debido a la imposibilidad de realizar un monitoreo y control efectivo de los respaldos, además de disminuir la probabilidad de pérdida por falla del hardware debido al uso de infraestructura que no es apropiada.
 - **Monitoreo**, el estado actual de este proceso también es básico, ya que consiste en la detección de fallas, no está la opción de auditar eventos de seguridad o de monitorear servicios en servidores. Lo que se quiere lograr es la implementación de un monitoreo avanzado, permitiendo mejorar la continuidad operacional, puesto que se podrán realizar detecciones tempranas de posibles caídas de servicio, mejora en la auditoría de acceso a la información, permitiendo el seguimiento de eventos. Esto otorgará un monitoreo proactivo de servidores determinando condiciones de falla de manera oportuna, mejorando la detección de anomalías, revisión de logs de servidores y auditando los eventos de seguridad.
 - **Encriptación de datos**, en la actualidad no hay una encriptación de los datos real. Al estandarizar este proceso se puede asegurar que la información sea accedida únicamente por su propietario o quienes tengan acceso a ella. La situación actual permite que se pueda acceder a información no autorizada.

En el área de mejora continua se tienen proyectos de mejora como:

- **Renovación de servidores**, este proyecto pretende renovar servidores de sistemas críticos, MES, BD y PI, que no tienen garantía y soporte, permitiendo contar con servidores al comienzo de su vida útil, con garantía y soporte. Además, permite mejorar la continuidad operacional de los sistemas críticos de CSH, eliminando o disminuyendo la probabilidad de pérdida de servicio por falla irrecuperable de hardware.

- **Modernización de infraestructura de respaldos**, esta pretende renovar el servidor de respaldos, almacenamiento de respaldos y unidad de cintas. A su vez, contar con una infraestructura con garantía y de equipos de misión crítica, lo que permite dar mayor protección al momento de recuperar la información cuando ello sea necesario. Hasta el momento el respaldando se realiza en equipos no calificados para esto (un PC) y en una unidad de cinta de baja capacidad. Lo que se traduce en una falla del sistema de respaldo y la imposibilidad de la recuperación de los datos.

En relación a los datacenter, se encuentran proyectos de mejora que proporcionarán una optimización de las UPS, el sistema de enfriamiento y el sistema de extinción de fuego. Así también del mejoramiento del cableado de las redes, esto ya que las UPS están al borde de su capacidad de funcionamiento, sin poder reponerlas ante una falla, además los equipos son antiguos y no cuentan con regulación de humedad.

En cuanto a la mejora del sistema de extinción de incendios en la sala de servidores, se cuenta con extintores estándares, lo que no permite una correcta extinción del fuego sin dañar el equipamiento, para evitar esto se debe ocupar un sistema especializado en base a gases.

En cuanto al cableado la situación actual es la misma que cuando se creó la sala de servidores, donde se contempló el cableado de redes para un número limitado de servidores. Hoy la unidad cuenta con nuevos servidores los que se instalaron con cableado provisorio, por lo que se hace necesaria una optimización del cableado. El mejoramiento de estas condiciones traerá beneficios como:

- Evitar un colapso del datacenter por problemas de alimentación eléctrica contando con UPS redundante ante fallas y con la capacidad de carga disponible.
- Mantener controlado el clima dentro del datacenter y asegurar la continuidad del servicio.
- Tener la garantía de una extinción de incendios oportuna y sin daños para los equipos.
- Contar con una estructura de redes solida a Gb/s que favorezca la continuidad operacional y la rápida identificación de fallas.

Estas implementaciones vienen a mejorar la situación actual en la cual se mantiene el riesgo de falla de datacenter por problemas de UPS y la imposibilidad de aumentar los equipos conectados. En caso de un siniestro, la capacidad de apagado dependerá del uso de los extintores arriesgando los equipos de la sala. Y en cuanto a la mejora del cableado si se mantiene la situación actual habrá problemas para la conexión de nuevos servidores y la imposibilidad de detectar fallas de estos.

En cuanto a los servicios que se prestan en plataforma y el estado o procedimientos que se desarrollan en estos, son los que se detallan en la Tabla 5, donde por un lado se tienen los procesos y por el otro los servicios que se desarrollan en estos por parte de plataforma:

Proceso/ Servicio	Ambiente Servidores	Conectividad lógica	Almacenamiento centralizado	Conectividad física	Acceso a Recursos
Monitoreo	SI	SI	SI	SI	SI
Respaldo/ Restauración	SI	-	SI	SI	SI
Mantenimiento	SI	-	-	SI	-
Soporte	SI	SI	SI	SI	SI
Contingencia	SI	SI	SI	SI	SI
Requerimientos	SI	SI	SI	SI	SI
Evaluación de Infraestruct.	SI	-	-	SI	-
Control de servicio	SI	SI	SI	SI	SI
Seguridad	SI	SI	SI	SI	SI
Nuevos requerimientos y soluciones	SI	SI	SI	SI	SI

Tabla 5. Relación entre procesos y servicios del área de plataforma. Fuente: CSH.

El área de plataforma, en pro de mejorar sus procesos y procedimientos se ha fijado objetivos para procesos como datacenter, la instalación de equipos, el mantenimiento, operación y requerimiento de redes, procedimientos de monitoreo y manejo de incidentes, renovación de equipos y trabajo y manejo de servidores, cada uno de los cuales contempla una herramienta de control y una medida, además de una meta que es lo que se desea lograr, la que puede ser semanal, semestral o anual.

En general, la herramienta de medición será Sharepoint, que es la herramienta utilizada por la unidad para el manejo de solicitudes y trabajos.

Nombre	Objetivos	Herramienta de Control	Medida	Meta	Medición
Acceso a Datacenter	Establecer el protocolo a seguir para la entrada y salida del datacenter.	Bitácora de eventos	Cantidad de registros	100%	Semanal
Instalación de Equipamiento	Establece de forma general la seguridad y las consideraciones generales de la instalación de nuevo equipamiento.	Checklist de Instalación	Checklist completado	100%	Mensual
Mantenimiento de redes	Establece un plan de mantenimiento de equipos e instalaciones de redes.	SharePoint	Ejecución del plan según programación	80%	Mensual
Procedimientos de Contingencia	Establecer que cada componente de	SharePoint	Procedimiento creado y validado	80%	Mensual

	infraestructura requiere un plan de contingencia actualizado y probado.		en ambiente de pruebas		
Procedimiento de monitoreo	Establecer qué y cuándo se debe monitorear un elemento de infraestructura.	SharePoint	Ejecución de monitoreo	90%	Semanal
Procedimiento de respaldo restauración	Procedimiento que rige la forma de hacer los respaldos y restauración de información.	SharePoint	Ejecución de respaldos	100%	Semanal
Procedimiento de soporte	Normar las actividades de soporte plataforma.	SharePoint	Cumplimiento de estándares y tiempo	90%	
Equipos e instalaciones críticas	Tener identificado los equipos críticos de la unidad.	SharePoint	Procedimiento incluye todos los equipos críticos	100%	Semestral
Renovación de equipamiento	Realizar periódicamente una revisión del equipamiento definiendo el plan de acción para garantizar la continuidad operacional.	SharePoint	Ejecución de proceso	100%	Anual

Tabla 6. Procedimientos y objetivos de plataforma. Fuente: CSH.

5.2. Área de Operaciones

Esta área es la encargada de dar soporte a los sistemas que se encuentren en el ambiente productivo, realizar los trasposos desde ambientes de prueba a productivo, como también de brindar soporte técnico a todo el hardware y software de escritorio de la compañía. Para esto cuenta con una mesa de ayuda que es la encargada de coordinar el soporte a los incidentes ocurridos en estos dos sectores, así como también de manejar los cambios que ocurran en ellos, con el fin de mantener la continuidad operacional del negocio. Esto se detalla en la Figura 23, donde se muestra el modelo de Operaciones y sus relaciones.

Para lograr los objetivos antes mencionados, el área de Operaciones interactúa con cuatro sectores:

1. Soporte de Sistemas.
2. Soporte Técnico.
3. Desarrollo y Mantenimiento de Sistemas.
4. Área de Plataforma

La interacción de los sectores comienza con el manejo de las solicitudes de Cambio de Sistemas, que vienen desde Desarrollo y Mantenimiento, poniendo en el ambiente productivo y luego monitoreando el funcionamiento de los sistemas desarrollados o las modificaciones realizadas. Soporte de Sistemas es el encargado de controlar los incidentes que se presenten en los sistemas, y su resolución, generando informes de dichos incidentes y el grado de resolución de éstos. Soporte Técnico gestiona y mide la respuesta de los problemas presentados en las estaciones de trabajo que se encuentran en la planta, generando informes de los mismos, como es el caso de virus o problemas de licencias. Además, el área de Operaciones es la encargada de realizar las compras de equipamiento que sea necesario para dar continuidad operacional a la compañía, efectuando las cotizaciones y encargándose de las compras con los proveedores.

Para la solución de Incidentes esta área cuenta con dos líneas de acción:

- **Mesa de Ayuda:** Brindando soporte telefónico a los usuarios.
- **Soporte Terreno:** Enviando a un técnico al equipo con problemas.

Estas soluciones se gestionan de dos formas, dependiendo del tipo de problema detectado, los que pueden ser:

- Problemas en Sistemas.
- Problemas en Plataforma.

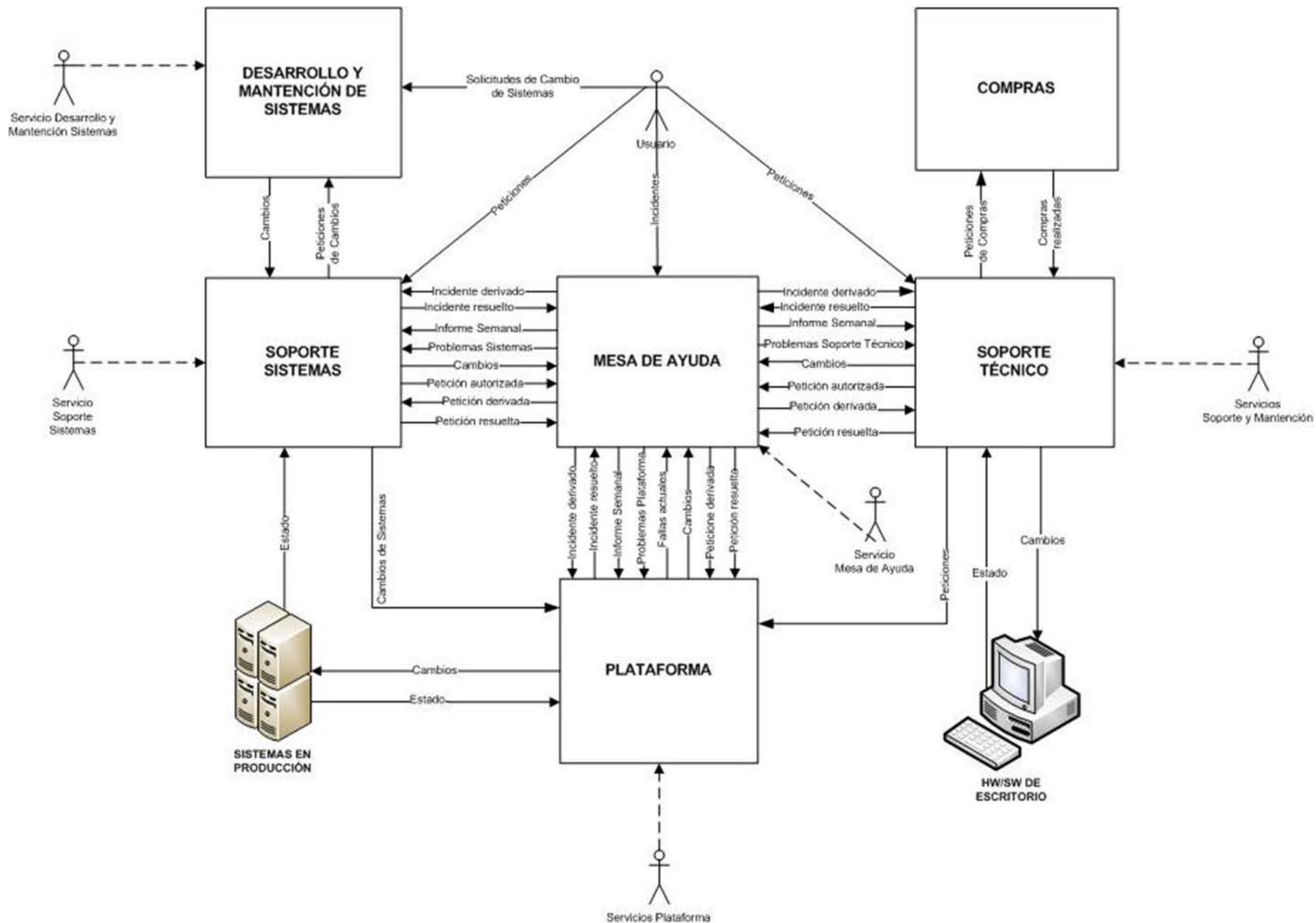


Figura 23. Modelo Área de Operaciones unidad de TSI. Fuente: CSH.

Dentro de los procedimientos de soporte que realiza el área de operaciones, se pueden distinguir las siguientes clasificaciones:

- Petición de nuevo equipo o componente
- Petición de nuevo punto de red
- Petición de cuenta :
 - Correo institucional
 - Internet corporativa
 - Cuenta de dominio
- Petición de cuenta o privilegio en un sistema
- Petición de instalación de software
- Peticiones de traspaso
- Mantención de equipos

Cada una de las peticiones que se reciben por esta área se manejan de acuerdo a un flujo-grama estándar que se muestra a continuación:

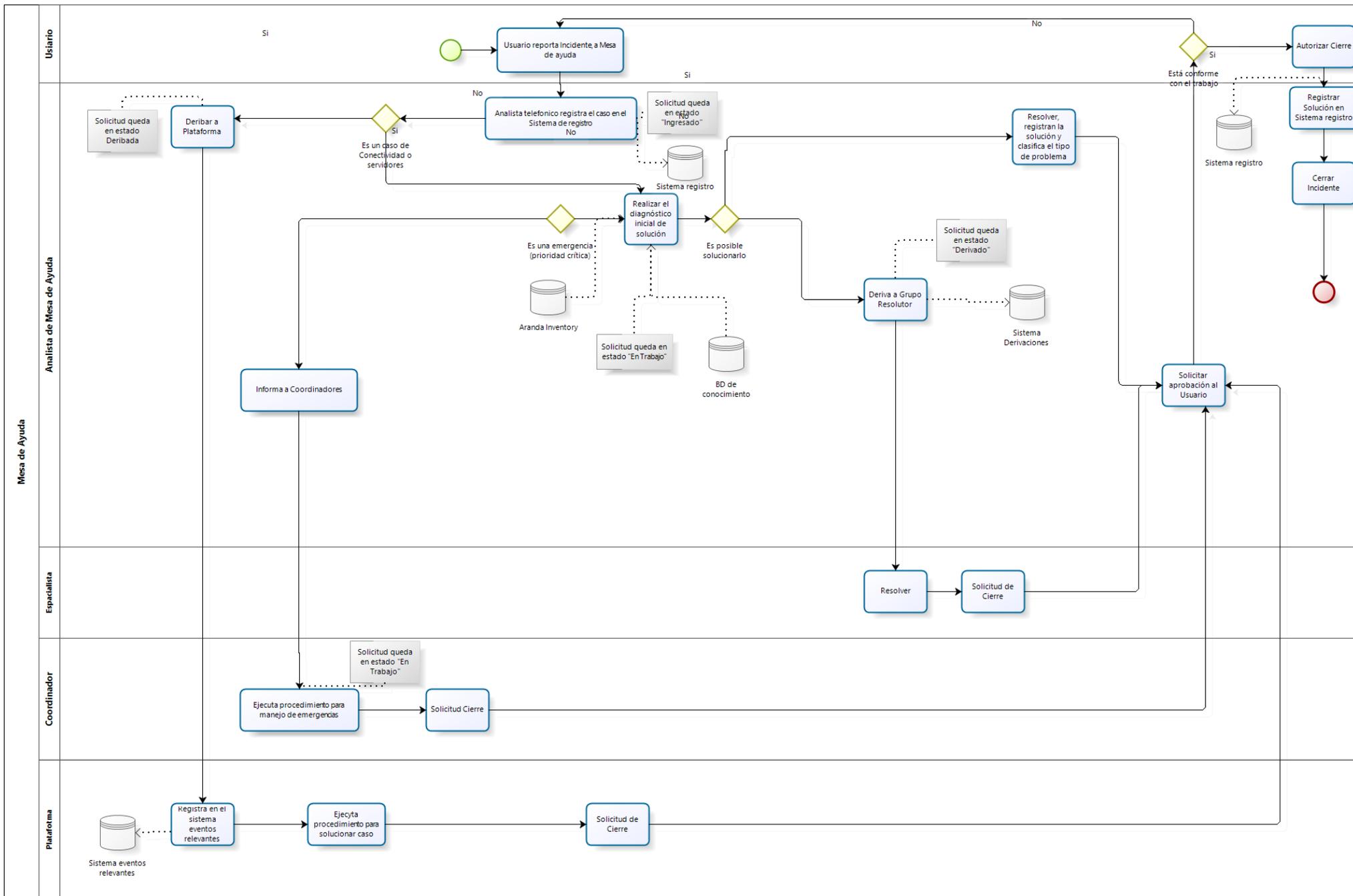


Figura 24. Flujograma resolución área de Operaciones unidad de TSI. Fuente: CSH.

5.3. Modelo de trabajo actual de la unidad de Tecnologías y Sistemas de Información (TSI).

La Unidad de Tecnologías y Sistemas de Información (TSI) de la Compañía Siderúrgica Huachipato, se encuentra estructurada jerárquicamente, como se observa en el organigrama de la unidad presente en la Figura 20 de este proyecto de título, donde claramente se pueden apreciar cuatro áreas de trabajo, de las cuales las últimas dos, como ya se dijo, serán objeto de análisis para los fines de este trabajo:

- Ingenieros de procesos de Negocio,
- Seguridad y Calidad,
- Operaciones y
- Plataforma

Operaciones y Plataforma se subdividen de acuerdo a los diferentes servicios que presta la unidad a la compañía:

- Área de Operaciones:
 - Coordinador Mesa de Ayuda.
 - Coordinador de Soporte Técnico.
 - Jefe de Sistema y Desarrollo.
- Área de Plataforma:
 - Administradores de Plataforma

En la Figura 21 se muestra que estas áreas ofrecen servicios tanto al resto de la Compañía como a la propia unidad de TSI a través de procesos regidos por procedimientos, los que se encuentran debidamente estructurados y normados.

Existe una interrelación entre las áreas que conforman la Unidad de Tecnologías y Sistemas de Información (TSI) y los Usuarios de sus servicios, al mirar la Figura 23 queda claro que para ingresar una solicitud de desarrollo o mantención de un sistema, los usuarios solicitan al área de Desarrollo y Mantención de Sistemas, compuesta por los Ingenieros de Procesos de Negocio TI y el Jefe de Sistema y Desarrollo, la creación o modificación de un sistema, para que sean estos quienes entreguen a Soporte, encabezado por el Coordinador de Soporte Técnico, los requerimientos de cambio o requerimientos del nuevo sistema, los cuales son obtenidos por el Ingeniero de Procesos de Negocio TI.

El Jefe de Sistema y Desarrollo es el encargado de monitorear el estado de los sistemas en los Servidores del ambiente Productivo y de mantener los ambientes de prueba.

El hardware, software y conexiones de red de estos servidores, son mantenidos y monitoreados por el área de Plataforma, que además es el encargado de realizar los cambios que sean necesarios en estos. El encargado de solicitar estos cambios a Plataforma es el área de Soporte Técnico que entrega las peticiones de cambio o modificación de uso sobre los servidores, así mismo Soporte Técnico es el encargado de mantener el hardware de escritorio de la planta,

verificar que funciona correctamente, realizarle mantenciones y hacer cambios cuando se considera oportuno, por lo que se coordina con Compras, función a cargo del Coordinador de Soporte Técnico, con supervisión del Jefe de Operaciones, cuando requiere la adquisición de suministros.

Desde el punto de vista del usuario, además de comunicarse con Desarrollo y Mantenimiento de Sistemas debe contactarse con Soporte Técnico para solicitar cambios o errores en el hardware y con Soporte de Sistemas para solucionar problemas presentes en el funcionamiento de los sistemas. Cabe señalar que una parte importante de las relaciones y comunicaciones se realizan en la Mesa de Ayuda. Esta importancia se evidencia en la figura 20 donde es posible observar que Mesa de ayuda cuenta con un Coordinador propio y además se sitúa en el centro del Modelo de Operaciones, se relaciona con gran parte de las funciones de la Unidad de Tecnologías y Sistemas de Información (TSI), y se encarga de coordinar la comunicación entre el usuario y los demás organismos de la unidad de TSI, según se muestra claramente en la figura 23. Dentro de sus muchas funciones se destacan:

- Gestión de Incidentes.
- Gestión de Peticiones.
- Generación de Informes Semanales de Soluciones.
- Gestión de Cambios.
- Solicitudes de Autorización.
- Gestión de Fallas.

Para ejemplificar el funcionamiento interno del área de Operaciones, se tomará la función Gestión de Incidentes, cuyo flujograma se muestra en la Figura 37, donde se observa cómo Operaciones reacciona frente a un Incidente o solicitud de algún usuario y que se detalla a continuación:

Frente a uno o más incidentes es el mismo usuario quien debe reportar mediante una llamada telefónica a la Mesa de Ayuda donde se le registra asignándole un ticket de servicio, para, en primera instancia, tratar de resolverlo y cerrarlo, y el usuario proceda con la aprobación del trabajo realizado y, si no es posible, se pase a la segunda instancia en donde Mesa de ayuda derivará el ticket al especialista o encargado mediante un sistema de derivación. Una vez resuelto el problema, se devolverá el ticket con la solución a Mesa de Ayuda para que proceda al cierre del caso y solicite la aprobación al usuario.

Cabe mencionar que existe otra forma de dar respuesta a un ticket, en donde no interviene Mesa de Ayuda, esto se da cuando:

- El usuario solicita directamente al Coordinador de Soporte o Mesa de Ayuda la solución de un problema, y será este quien coordine con el especialista la solución, siguiendo luego el curso normal del ticket, que es el cierre y la aprobación del Usuario. Este caso se presenta en la siguiente Figura:

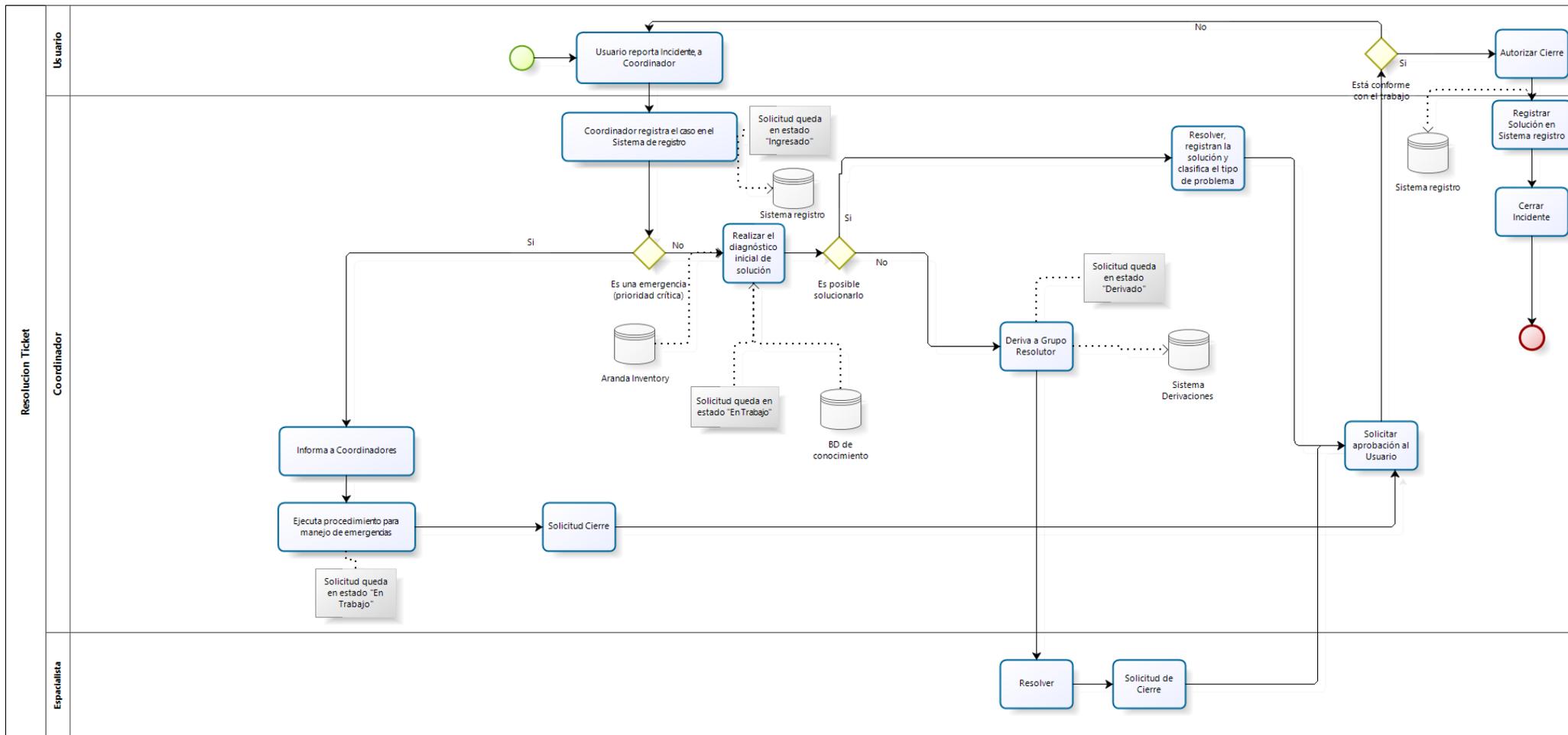


Figura 25: Flujo de respuesta de un ticket reportado a Coordinador. Fuente: CSH.

Una excepción a este flujo se da cuando el Coordinador debe comunicarse con el área de Plataforma para dar respuesta a un ticket, siendo esta área la responsable de dar solución y aviso al Coordinador para el cierre del ticket, este caso se presenta cuando el usuario solicita acceso a un servidor o un servicio, ya que es Plataforma el encargado de los servidores y de las políticas de seguridad de estos, como se puede ver en la siguiente Figura:

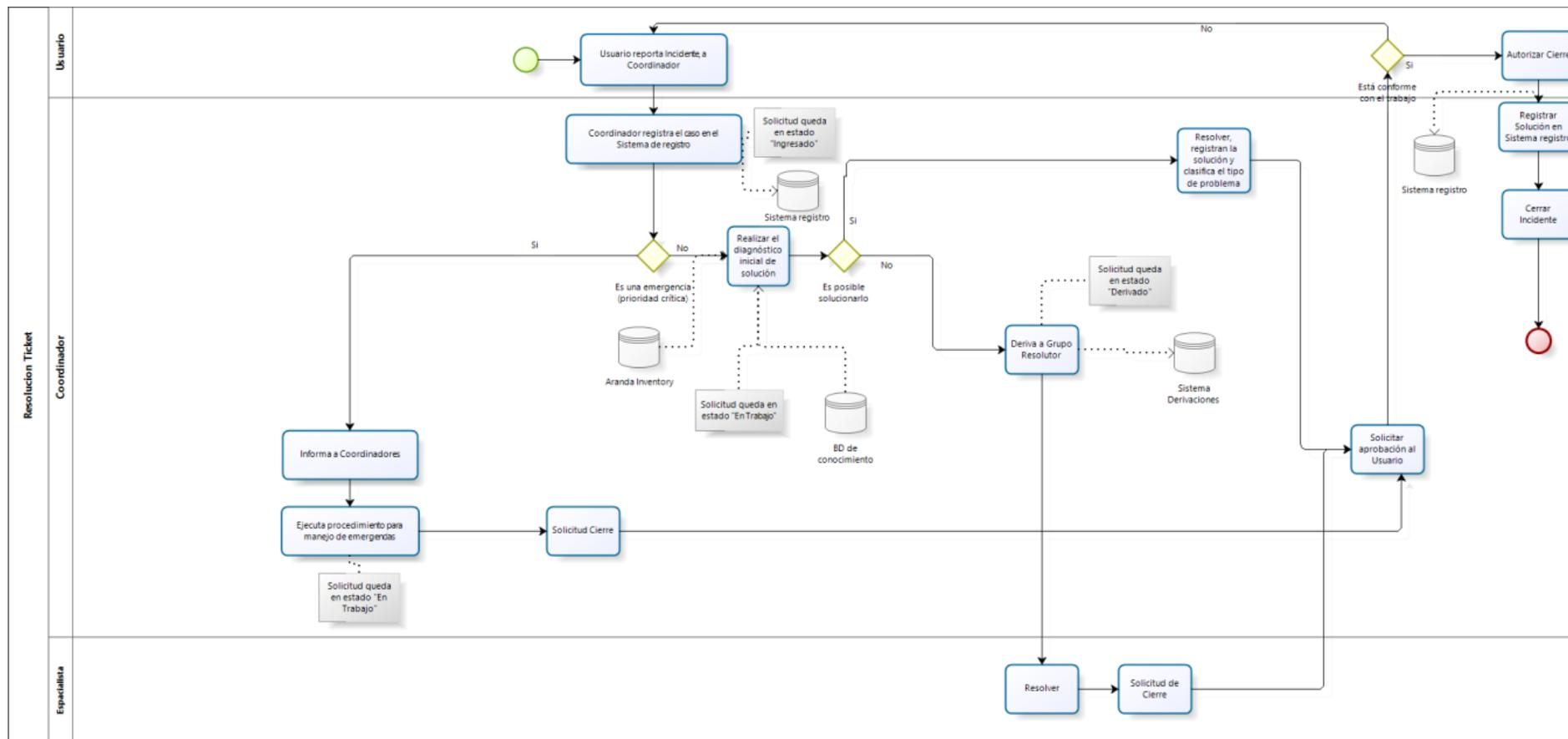


Figura 26: Flujograma de respuesta de un ticket reportado a Coordinador y resuelto por Plataforma. Fuente: CSH.

6. ASPECTOS A CONSIDERAR PARA LA ELABORACIÓN DEL MODELO A UTILIZAR EN LA UNIDAD DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN.

Este capítulo tiene como objetivo describir los aspectos que se tuvieron en consideración al momento de elaborar el modelo para la unidad de Tecnologías y Sistemas de Información (TSI). El que se ajusta a la cultura de la organización y está determinado por el impacto de los cambios y el nivel en que se ven afectadas las personas y procesos, para lo cual se realizó un diagnóstico de la cultura organizacional con el objetivo de conocer cómo se comporta la unidad de TSI, cuál es su organización y cuáles son sus procesos, resultados que se encuentran detallados en el Capítulo 5.

Unido a lo anterior, tanto en el Capítulo 4 como en el 5 se muestra cómo está estructurada la unidad, cuáles son las funciones de los miembros y cuáles son los procedimientos que se desarrollan en esta para poder entenderla e intervenirla, ya que se prevé que el desarrollo y la implementación de un modelo de gestión de la calidad para la unidad TSI producirá cambios que llevará consigo el desafío de gestionar con las personas que trabajan en la unidad para que se adapten a ellos y los acepten, para lo cual al elegir este modelo se consideran factores que pudiesen estar en estas personas como los miedos, la incertidumbre, la pérdida de control, la ruptura de la rutina.

En cuanto a los motivos que se pueden encontrar para argumentar que existe una necesidad de cambio organizacional en esta unidad, se encuentran los reactivos, la organización ha de dar respuesta a presiones internas o externas, o bien los proactivos, con los que da respuesta a demandas futuras. Para el caso de este estudio la necesidad de la implementación de, a lo menos, un marco de trabajo organizado y normado de los procesos de la unidad, facilita dar respuesta a las necesidades internas al saber cuáles son los procesos internos de la unidad y cómo se organizan, normándolos y dejándolos documentados para poder ser consultados por cualquier persona, tanto interna como externa a la organización o por la gerencia o una auditoría que los solicite.

Una vez realizado el análisis de la situación actual de la empresa, de ver cómo funciona y cuáles son sus procesos, hay que centrarse en la situación en la que se encontrará la unidad luego del cambio, o durante el periodo de implementación de éste. Es aquí donde se debe considerar:

- La resistencia al cambio que pueda presentar el personal a la implementación del modelo, pudiendo rescatar elementos del sistema de trabajo, que se tiene actualmente, dentro de la unidad para aminorar esta resistencia.

En resumen, para la elaboración de este modelo se utilizaron los siguientes criterios:

En primer lugar saber que cambiar la estructura y la forma de trabajar de una organización, en especial de una tan grande como CAP Acero en su división Huachipato, es un trabajo difícil de realizar y, de hacerse, debe ser llevada a cabo por un equipo especializado, lo que presenta una limitación que se ha de considerar al momento de implementar este proyecto de título, ya que es un factor importante el no alterar la organización de la unidad, ni su

funcionamiento interno. Es aquí donde toma importancia el Capítulo 5, en él se observa que esta unidad funciona con patrones semejantes a los de ITIL, en especial el Área de Operaciones, con la Mesa de Ayuda como punto central de su funcionamiento, otro aspecto importante que lleva a optar por un modelo sobre otro.

Además lo que a primera vista puede ser el gran problema de ITIL en relación a no cubrir las fases de desarrollo de software, ni la gestión de proyectos asociada a esa fase de construcción de activos de software, para efectos de este proyecto es una ventaja, dado que la unidad de Tecnologías y Sistemas de Información de CSH no desarrolla software, sino que subcontrata estos servicios a empresas externas, por lo que al no abarcar de forma completa este punto ITIL posee una ventaja comparativa respecto a los demás modelos de gestión.

Otro punto a considerar es la escalabilidad. En la Figura 17 se muestra una pirámide de escalabilidad en la que ITIL se encuentra en el primer escalón luego de los procesos in-house, esto permite que luego de ser implementada se pueda escalar a una norma con mayor alcance, como lo es la norma ISO/IEC 20000, dependiendo de los requerimientos futuros de la unidad o de su crecimiento, esto se transforma en una ventaja ya que no se debe retroceder si se desea cambiar de norma en el futuro.

En base a los puntos antes mencionados y al alcance de cada norma, ISO/IEC 20000, ITIL y CMMI en su versión para servicios CMMI-SVC, es que se construye una tabla comparativa, Tabla 7, en la que se describen las diferencias o similitudes existentes entre estos modelos. Esta Tabla se muestra a continuación y considera los 12 aspectos más importantes:

Aspecto / Norma	CMMI-SVC	ITIL	ISO/IEC 20000
Modelo para empresas Informáticas.	No	No	No
Se adecúa al modelo de trabajo actual de TSI.	No	Sí	No
No es estricta (admite cambios).	No	Sí	No
Es certificable.	Organización	Personas	Organización
Es escalable.	No	Si	No
Cumplimiento de sus puntos.	Obligatorio	Voluntario	Obligatorio
Es auditable.	Sí	Sí	Sí
Asegura una mejora continua.	Sí	Sí	Sí
En el ciclo de vida del Servicio TI se centra en:	Desarrollo e Infraestructura TI	Procesos Operacionales	Procesos e Infraestructura TI
Considera a mesa de ayuda como un punto.	No	Sí	No
Considera Control de versiones.	No, presente en un nivel 2 de CMMI-SW	Sí, es un punto.	No
Considera gestión de incidentes.	Lo abarca desde la perspectiva de los proyectos	Es un punto en la norma	Sí

Considera acuerdos de nivel de servicio (SLA).	Sí	Sí	Sí
Asegura una continuidad de los servicios TI.	Sí	Sí	Sí

Tabla 7. Tabla comparativa entre CMMI-SVC, ITIL e ISO/IEC 20000. Fuente: Elaboración propia.

La propuesta del modelo que se presenta a la Unidad de Tecnologías y Sistemas de Información considera los aspectos mencionados en la Tabla 7. La Tabla 8, por su parte, refleja el grado de intervención y su aporte, y la descripción de cómo se vieron afectadas las tareas que realiza la Unidad. El grado de intervención se clasifica en tres tipos:

- **Incorporado:** Esto sucede cuando el aspecto no era considerado por la unidad y ha sido definido en el modelo propuesto, o si se genera a partir de la división de un procedimiento o servicio que realiza la unidad, o se realizaron cambios mayores en él.
- **Modificado:** La unidad posee una función que realiza este procedimiento, pero se realizan algunos cambios, los que pueden incluir la subdivisión del punto.
- **Sin Cambios:** El procedimiento que realiza la unidad se deja de la misma forma y es traspasado como un punto al modelo, esto debido a que son servicios o procedimientos comunes, que tienen cierta robustez adquirido mediante la ejecución.

N°	ASPECTO	GRADO DE INTERVENCIÓN	DESCRIPCIÓN
1	Control de Incidentes	Modificado	Este punto fue modificado, ya que se realizan cambios en la forma de tratar los problemas. El modelo propone una nueva forma de asignar las prioridades a los incidentes ocurridos y su documentación.
2	Manejo de Problemas	Incorporado	Este punto se incorpora debido que hasta este momento los problemas se tratan igual que los incidentes, y este modelo propone separar los errores más comunes y tratarlos en un punto diferente.
3	Control de Versiones	Modificado	Actualmente la compañía posee un sistema de almacenaje de las versiones de los sistemas desarrollados, pero esta forma utiliza mucho espacio en disco, por lo que se habilita un servidor con un software que permite almacenar el sistema y tener un mejor control de las versiones.
4	Control de Acuerdos de Niveles de Servicio	Modificado	Las métricas utilizadas para medir a las empresas externas en la actualidad, no son completas debido a que no abarcaban todos los procedimientos, por lo que se agregaron métricas a estos procesos y se modificaron las métricas de algunas de las prestaciones.
5	Manejo de Cambios	Modificado	Si bien se mantiene casi en su totalidad la forma en que los cambios, tanto de software o hardware son aplicados, se realizaron modificaciones sobre cuáles son los conductos que hay que seguir antes de la instalación, en especial en lo que tiene que ver con el inventario del hardware y software que se instala. También se realizan mejoras pequeñas en los RFC donde se incluye una descripción más completa del por qué se realiza el cambio y de su seguimiento.
6	Gestión de Capacidad	Incorporado	Se trabaja en la implementación de un plan de control de los niveles de servicio, además de la forma de medir la respuesta de la unidad frente a peticiones de los usuarios. También se propone conocer cuál es el uso que los usuarios dan a los

			recursos TI.
7	Gestión de Disponibilidad	Modificado	En este punto se mejoraron las métricas de cumplimiento de servicios que tenía la unidad en pos de poder asegurar servicios 27/7, minimizando las caídas o fallas de sistemas y mejorando los planes de recuperación. En la misma línea se propone la disminución progresiva de los incidentes presentados por algunos sistemas.
8	Gestión de Peticiones	Modificado	Mesa de ayuda es la encargada de recibir las peticiones de los usuarios, tanto de acceso, de utilización o mal funcionamiento de la infraestructura TI, es así que se trabaja en el control de las peticiones de los usuarios al mejorar la herramienta computacional que se posee en la actualidad, permitiendo con esto conocer en tiempo real el estado de las solicitudes, su tiempo de cierre y la trazabilidad de los encargados de la solución.
9	Continuidad del Servicio y Contingencias Mayores	Modificado	Se genera el plan completo de Contingencias para la unidad, realizando una recopilación de la documentación existente, de un levantamiento de información de los procedimientos de los sistemas.
10	Control de la Seguridad	Sin Cambios	Dado que las políticas de seguridad, tanto de la unidad como de la empresa, son claras, no fue necesario realizar modificaciones ni alteraciones en este punto.
11	Control de Acceso	Sin Cambios	Este punto no se modificó, ya que las políticas de acceso no merecían ser objeto de cambios de acuerdo a lo expresado por el jefe de la unidad.
12	Validación, Verificación y Pruebas	Sin Cambios	En relación a este punto, se puede señalar que no se realizaron modificaciones, aunque sí sugerencias de cómo realizar los informes finales de aprobación de los sistemas realizados para su implementación. En la actualidad el sistema de VyV funciona correctamente.
13	Planificación y Soporte	Incorporado	Este punto se incorpora, a pesar de que existe un manejo de cambios, pero este no estaba regulado, por lo que se incorporan los cronogramas de trabajo, con las

	para la Transición		fechas en las que se deben iniciar y terminar los trabajos, además se incorpora al usuario en el proceso.
14	Gestión Financiera	Modificado	Si bien la unidad tiene un sistema de manejo financiero que es robusto y funciona, se trabajó fue en darle un marco y estructurar los procesos.
15	Gestión de Informes de Servicio	Modificado	Se mejora el sistema de información, en especial del estado de los servicios, permitiendo un mejor acceso a los informes de estado y funcionamiento.
16	Mesa de Ayuda	Sin Cambios	Se puede decir que este es un punto fundamental en el funcionamiento de la unidad, ya que a través de este se recibe la mayor cantidad de información de los usuarios, es un punto que funciona con normalidad, que cumple los objetivos por lo que no se le realizarán cambios, salvo, como se dijo anteriormente, la posible implementación de un nuevo sistema informático.

Tabla 8. Tabla Aporte realizado por cada punto del modelo. Fuente: Elaboracion propia.

7. MODELO PARA LA UNIDAD DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

El modelo generado para la unidad de Tecnologías y Sistemas de Información, se desarrolló considerando los modelos preentados en el punto 1 de este Proyecto de Título, principalmente en base a las mejores prácticas de ITIL los cuales fueron presentados en el punto 1.2 de este documento. De los modelos presentados en el punto 1 no fue necesaria la implementación de la totalidad de sus aspectos de trabajo, sino que sólo fueron adoptados aquellos conocimientos que eran útiles para este estudio en concreto.

La integración de cada punto y su aporte fue presentado en el Capítulo 6 mediante la Tabla 8 de este proyecto de título. Así solamente se procedió a efectuar un compendio de los puntos o factores que eran necesarios trabajar para mejorar el modelo de esta unidad, los que han sido adecuados a los procesos y metodologías de trabajo que se realizan en ella durante su funcionamiento diario.

De la misma forma, para la realización de este modelo de trabajo, se tuvo en cuenta los procedimientos que se desarrollan actualmente al interior de la unidad, como por ejemplo, la resolución de tickets de incidentes, las solicitudes de cambio, el manejo de SLA y planes de contingencia.

Todo lo anterior fue expuesto y acordado en conjunto con el personal encargado de la modificación y/o sustitución de la unidad de Tecnologías y Sistemas de Información de la empresa, así como también se contó con la venia de quienes tienen la administración directa de dicha unidad. De esta forma, para el caso específico de este proyecto, sólo fue necesaria la integración de mejoras a la unidad que permitieran el funcionamiento más expedito y eficaz que el que hasta ahora existe, pero dejando siempre en resguardo los elementos medulares y esenciales que integran de forma completa el proceso de la unidad.

Es así como finalmente el modelo a implementar queda formado por dieciséis (16) procesos, a saber:

- | | |
|---|---|
| 1. Control de Incidentes | 9. Continuidad del Servicio y Contingencias Mayores |
| 2. Manejo de Problemas | 10. Control de la Seguridad |
| 3. Control de Versiones | 11. Control de Acceso |
| 4. Control de Acuerdos de Niveles de Servicio | 12. Validación, Verificación y Pruebas |
| 5. Manejo de Cambios | 13. Planificación y Soporte para la Transición |
| 6. Gestión de Capacidad | 14. Gestión Financiera |
| 7. Gestión de Disponibilidad | 15. Gestión de Informes de Servicio |
| 8. Gestión de Peticiones | 16. Mesa de Ayuda |

7.1. Control de Incidentes.

Es el encargado de tratar, de forma rápida y eficaz, la restauración de los servicios. Aquí no se examinan las causas de los incidentes, sino que se intenta dar una rápida solución a los incidentes para que el servicio pueda estar disponible en el menor tiempo posible. Entre los principales objetivos se pueden encontrar los siguientes:

- Permite detectar cualquier alteración de los servicios, registrándolas, clasificándolas y asignando el personal encargado de restaurar el servicio.
- Resolver dicha alteración en el servicio tan pronto como sea posible, manteniendo información sobre el estado del servicio y su solución.
- Evaluar la posibilidad de una nueva ocurrencia en la alteración del servicio.

En este sentido se entiende un incidente como: *“Un evento que causa o puede causar una interrupción temporal o una reducción de la calidad del servicio, generada en una aplicación”*. Este será gestionado por el responsable directo de la aplicación, es decir, serán estos los primeros en brindar soporte. Esta interrupción se registrará y se le asignará una prioridad, calculada como **impacto * urgencia** y dependiendo de este factor se le asignará un tipo y número de personas para su solución.

- **Impacto:** Es el nivel de importancia del incidente, directamente relacionado con cuánto afecta a los procesos del negocio, pudiendo incluirse el número de usuarios a los que afecta el incidente.
- **Urgencia:** Es el tiempo máximo definido para la resolución del incidente.

Con todo esto se espera mejorar el funcionamiento de la unidad. Los objetivos básicos son:

- Mejorar la productividad de los usuarios, debido a las menores interrupciones en el servicio.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.
- Menor tiempo en la respuesta y resolución para agilizar el proceso.
- Debido a la menor ocurrencia o la disminución del tiempo de respuesta ante un incidente aumentan los niveles de disponibilidad de los servicios TI.
- Obtención de información precisa de gestión sobre la calidad del servicio.

7.1.1. Resolución del Incidente

Para resolver el incidente se deberá revisar primero si esta incidencia ha ocurrido anteriormente, si fue solucionada y de qué forma, así, de existir una solución conocida será ésta la que se aplicará en primera instancia, asignando los recursos necesarios para ello. De lo contrario, esta incidencia se analizará por los responsables primarios quienes intentarán generar una solución. Si ellos no pueden dar una solución se ascenderá en la organización para encontrar una solución incorporando personas y recursos para este efecto. Esta escalada podrá ser de dos formas:

- Una funcional, en la que se recurrirá a personal técnico más calificado.
- Una jerárquica, donde se incorporarán al equipo los responsables jerárquicos de la organización.

Este proceso debe ser monitoreado o controlado mediante la generación de documentos que contengan la solución, los responsables y los resultados de la implementación de la misma.

Una vez resuelto el incidente, éste se registrará junto a su solución, así como también el tiempo y recursos invertidos, todo para tener conocimiento de ello en caso de una nueva ocurrencia. Cualquier cambio que sea necesario realizar a causa de este incidente será manejado por los encargados.

Una adecuada interrelación entre el control de incidentes y los procesos de la unidad permite mejorar los servicios, conocer la capacidad y disponibilidad de la infraestructura de TI, lo que permite hacer cambios que admitan una optimización y desarrollo de los servicios de TI.

Para establecer las prioridades de atención, como se dijo anteriormente, se utilizará la fórmula de impacto por urgencia, para esto definiremos el impacto como: *“la importancia del incidente”*, eso se hará viendo cómo éste afecta a los procesos del negocio. Y la urgencia será: *“el tiempo máximo definido para la solución del problema”*, que dependerá directamente del tiempo que podrá estar desactivado o sin funcionar el servicio. Mediante esta fórmula se asignarán los recursos para resolver los incidentes.

7.1.2. Instancias dentro del Control de Incidentes

7.1.2.1. Registro

Un incidente puede ser generado o registrado por un usuario, mesa de ayuda o soporte técnico, entre otros. Este registro puede realizarse durante la aparición del incidente, debiendo considerarse el costo que implicará solucionarlo, indicando la fecha y hora de la ocurrencia, como también cualquier información relevante para la resolución del incidente. Además se deberá revisar la existencia anterior del incidente para evitar una duplicidad en su atención. Posterior al

registro del incidente se deberá notificar de él a quienes puedan verse afectados por el mal funcionamiento o no funcionamiento del servicio y cómo afectará esto su trabajo.

7.1.2.2. Monitoreo

Todos los incidentes deben tener asociados a ellos un estado, que es aquel en el que se encuentren. Estos pueden ser:

- **Registrado:** Es el primer paso, y se define como un incidente del que se tiene conocimiento pero que no ha comenzado a ser tratado aún.
- **Activo:** Se modificará a activo el estado de un incidente cuando comience a ser solucionado, registrándose las actividades que se realizan o la etapa de avance de éste.
- **Resuelto:** Un Incidente estará resuelto cuando se haya implementado una solución a dicho incidente, y esta solución se encuentre completamente funcionando, es decir cuando el incidente haya sido resuelto.
- **Suspendido:** Indica una interrupción temporal en el tratamiento del incidente. Esto puede producirse por varias causas como la aparición de un incidente de mayor prioridad que implique más asignación de recursos.
- **Cerrado:** Un Incidente será marcado como cerrado si es que no fue posible encontrar una solución a él.

7.1.2.3. Análisis y cierre

En este punto se deberá examinar el incidente y buscar ocurrencias previas para descubrir soluciones ya probadas para éste, de no encontrarse se deberá analizar el incidente y buscar posibles soluciones, analizarlas y aplicarlas con el fin de dar una definitiva solución a la anomalía.

Durante todo este proceso se debe actualizar la información del incidente, con el fin de contar con un estado actualizado de éste.

Para el cierre de un incidente se debe considerar una solución satisfactoria del mismo, o la imposibilidad de solucionar el problema. Registrar la nueva solución encontrada con el fin de que sea posible utilizarla nuevamente si se llegara a generar el incidente.

En resumen, la resolución de los incidentes se realizará de la siguiente forma:

Como primer paso se deberá registrar el incidente, para esto se deberá verificar que el incidente no esté registrado, además se deberá verificar las ocurrencias anteriores del incidente, de ser así, se aplicará la solución conocida. Si éste no es el caso, si el incidente no ha ocurrido o la solución no es aplicable o no funciona de manera correcta, se deberá remitir el incidente a los expertos correspondientes, escalando en la organización hasta llegar a la solución del incidente.

La actualización del estado y vida del incidente se deberá registrar durante toda ocurrencia, generándose una solicitud a Manejo de Problemas cuando el incidente se torne demasiado común o irreparable, es aquí donde se realizará un estudio de las causas y se deberá dar una solución definitiva.

Cuando se haya solucionado el incidente se deberá confirmar a los usuarios afectados la solución satisfactoria de éste, incorporación del proceso de solución al registro del incidente. De ser necesario se deberá reclasificar el incidente, finalmente se marcará el incidente como cerrado.

Durante el Control de Incidentes, el registro de ellos debe ser actualizado, con el fin de conocer el número de incidentes detectados, la demora en su resolución, su impacto y urgencia, y así se podrá manejar u obtener información de los costos asociados a la resolución de problemas, los recursos utilizados y disponibles, el porcentaje de incidentes de acuerdo a las prioridades y estado de los mismos, además del número de ocurrencias.

7.2. Manejo de Problemas.

El Manejo de Problemas tiene como objetivo identificar las causas subyacentes de los fallos y recomendar cambios de ser necesarios. Además de minimizar el impacto adverso de incidencias y problemas en el negocio causados por errores en la infraestructura de TI. El manejo de problemas también se encarga de prevenir la recurrencia de incidencias relacionadas con estos errores.

Un problema podrá ser manejado de dos formas, la primera es al analizar los incidentes ocurridos, intentando descubrir sus causas y proponiendo posibles soluciones para eliminarlos, esta será un manejo reactivo, pues reacciona luego de presentarse un incidente. La segunda forma de manejar problemas es la preventiva, que surge del monitoreo de los sistemas, de la infraestructura de la unidad, y de analizar su funcionamiento con el objetivo de prevenir futuros incidentes, incluso antes de que ocurran.

Para lograr su objetivo se debe tener en cuenta la investigación de las causas subyacentes o basales a los cambios potenciales o reales de los servicios de la unidad, así como determinar las posibles soluciones a estos problemas. Teniendo estos aspectos claros se podrán proponer o generar las peticiones de cambios para restaurar el nivel y/o calidad del servicio.

También será necesario revisar los sistemas constantemente luego de su implementación para asegurar que los cambios que se generaron han hecho efecto y que a su vez se han obtenido los resultados esperados sin crear o generar problemas secundarios.

Ahondando un poco más se puede decir que el trabajo proactivo de los sistemas tiene por objetivo prevenir los incidentes antes que ocurran, estudiando y monitoreando los sistemas y la infraestructura de la unidad, analizando posibles amenazas y manteniendo informada a la unidad de los hallazgos encontrados. Esto en contraposición del trabajo reactivo, que es aquel que intenta dar solución a los problemas que se presentan con mayor frecuencia o que muestran una mayor amenaza para el funcionamiento de la unidad. En este sentido el manejo de problemas trabaja estrechamente relacionado con el Control de Incidentes, ya que de este tópico se pueden encontrar los incidentes más recurrentes, de los cuales se conoce o no su causa basal, aquellos incidentes aislados que pueden tener un gran impacto en la calidad del servicio que presta la unidad que no han podido ser asociados a algún error conocido.

Lo anterior se llevará a cabo siempre que, en primer lugar, se tenga un registro y clasificación de los problemas, lo que permitirá identificarlos y clasificarlos según su tipo, urgencia y prioridad. Con estos antecedentes es posible una adecuada asignación de recursos para su resolución y no una falta o exceso de estos, además se pueden determinar las causas de un problema, transformándolo en un error conocido, proporcionando soluciones temporales al Control de Incidentes y minimizar el impacto del problema hasta que se implementen los cambios necesarios para solucionarlo definitivamente.

La solución definitiva del problema debe considerar el posible impacto que ella tendrá en la organización y la infraestructura de esta, además de los costos de aplicar una u otra solución, teniendo en cuenta que los beneficios justifican los costos, y las consecuencias sobre los SLA. También es necesario tener en cuenta que las soluciones definitivas no deben demorar en su implementación, y así evitar una nueva ocurrencia del problema, puesto que las soluciones temporales no son suficientes. Esta solución definitiva deberá generar una petición de cambio para su implementación.

- **SLA:** Es un contrato escrito entre un proveedor de servicios y su cliente con objeto de fijar el nivel de la calidad de un servicio solicitado en aspectos tales como: tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Básicamente un SLA establece la relación entre ambas partes: proveedor y cliente. Un SLA identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa¹⁰.

En resumen, el manejo de problemas determinará las causas que pudieron o podrían provocar la ocurrencia o recurrencia de incidentes con el objetivo de buscar una solución definitiva. Transformando así un problema, que es una causa, no identificada, de una serie de incidentes o un incidente aislado de importancia, en un error conocido, debiendo pasar por una solución temporal con el fin de minimizar el impacto del problema o error en la prestación de servicios, mientras se tramita o ejecuta la petición de cambio que solucionará de forma definitiva el problema. De esta forma, al tener problemas y errores se tiene también un control de ellos. El control de problemas será el encargado de registrarlos, clasificar los problemas y determinar sus causas. Mientras que el control de errores registrará los errores conocidos, proponiendo soluciones y enviando peticiones de cambio, realizando revisiones posteriores a la implementación de estos cambios. Lo anterior sin olvidar el manejo proactivo de problemas que permitirá su posible identificación y así generar soluciones anticipadas, evitando su ocurrencia futura.

Para identificar los problemas potenciales se puede recurrir a la base de datos de incidentes, que como se dijo es donde el Control de Incidentes los almacena y registra, pues puede ocurrir que un potencial problema surja cuando un incidente es cerrado mediante una solución temporal, pero sin conocer sus causas, por lo que se debe establecer su impacto en la estructura de TI antes de elevarlos a la categoría de problema. Otra manera de identificar problemas potenciales es el análisis de la infraestructura de TI que se posee, esto puede permitir al Manejo de Problemas analizar los diferentes procesos y determinar en qué aspectos corresponde o es conveniente reforzar los sistemas y/o la infraestructura TI para evitar futuros inconvenientes.

Otra forma de determinar potenciales problemas es verificar el deterioro de los servicios, esto en relación a que el descenso del rendimiento puede ser una señal de la presencia de

¹⁰ The Service Level Agreement Zone, <http://www.sla-zone.co.uk/index.htm>

complicaciones que no se hayan manifestado aún. Esta verificación debe darse en todas las áreas de la infraestructura de TI para poder identificar y dar solución a problemas potenciales o no manifestados. El registro de este problema será similar al de un incidente, pero incorporando la naturaleza y el posible impacto del mismo sobre la infraestructura de la organización.

Con el fin de conseguir una adecuada solución del problema se deben establecer las áreas afectadas por éste, tanto el hardware, software y otros elementos involucrados. Se les asignará una urgencia y un impacto para poder conocer su prioridad de atención, la que puede variar durante la vida del problema, pudiendo convertirse en un problema de mayor o menor prioridad, determinando mayores o menores recursos dependiendo de la prioridad, y alcanzar así minimizar el impacto sobre la infraestructura de TI.

Cuando se analiza o diagnostica un problema para transformarlo en un error conocido se debe tener presente que lo que se busca es conocer las causas que producen este error, y no buscar una solución a éste. Mientras se realiza esta búsqueda, y como se dijo anteriormente, se deberá dar una solución temporal al error mediante el Control de Incidentes, esta solución deberá mantenerse hasta que se implementen los cambios que resolverán de forma definitiva este error. Generalmente los factores que originan los problemas pueden deberse a errores en el procedimiento, documentación o coordinación entre las áreas. Estos aspectos deben tenerse en cuenta durante la aplicación de esta etapa y así no caer en un ciclo de aplicaciones desarrolladas defectuosas.

Con estos antecedentes se puede decir, que la función del Manejo de Problemas es trabajar sobre un “error conocido” y a este aplicarle una solución, y no necesariamente al incidente que pudo generar este error.

Cuando el impacto del problema es alto, es una solución enviar un requerimiento a los IPN, con su respectiva solicitud de cambios, para esto es importante o recomendable realizarse las siguientes preguntas:

El problema ¿genera cambios significativos para su solución?, estos cambios significativos ¿justifican demorar la solución?, esta demora ¿genera un alto o bajo impacto en la infraestructura de TI?, ¿los beneficios esperados justifican los costos?. Ahora si el problema necesita una solución temporal se debe preguntar si esta solución ¿Logra mantener los niveles de calidad aceptables en el o los servicios?

Antes de cerrar el problema, o darlo por resuelto, es imprescindible revisar el resultado de la solución implementada, y ver los posibles efectos de los cambios realizados, lo que permitirá determinar si la solución es adecuada y sólo de serlo se deberá proceder a cerrar el caso.

Como ya se mencionó, el control continuo en esta etapa es fundamental para conseguir buenos resultados, y así asegurar una disminución en el número de incidentes y una rápida resolución de los mismos, logrando una mayor eficiencia en el proceso. Lo anterior está

estrechamente ligado a la búsqueda proactiva de posibles problemas y soluciones oportunas, evitando una baja en la calidad de los servicios.

En este sentido, la elaboración de informes periódicos brinda, a todos los involucrados en el procedimiento, información relevante en el proceso y evaluación del Manejo de Problemas y aporta información que puede resultar relevante a otras áreas o personas de la infraestructura de Tecnologías de Información. También es importante y de ayuda nombrar un responsable en cada etapa del proceso, que no necesariamente debe ser el jefe de la unidad, y a su vez puede no ser una sola persona, pero si debe ser un número limitado, esto dependerá del tamaño o envergadura del problema y teniendo en cuenta la disminución de los costos técnicos y humanos.

De la documentación obtenida es necesaria la elaboración de Informes que midan el rendimiento del Manejo de Problemas, que muestre los problemas tratados, cuántos de estos fueron resueltos, cuántos se encuentran en proceso de ser resueltos y cuantos no pudieron ser solucionados. Además se deberá conocerse los tiempos de respuesta, cuánto tiempo y recursos fueron empleados en la solución definitiva de los problemas, todo con el fin de calcular el impacto en la organización.

Otro informe que es posible generar es el de Gestiones Proactivas, el que contendrá cómo las medidas de mitigación de problemas han ayudado a la organización, cómo el prevenir los errores aporta a la reducción de costos y a la estabilidad del servicio. Aquí es importante saber cuáles han sido los problemas encontrados, cuáles se han analizado y cuántos han sido resueltos.

También es necesario generar informes de la Calidad de los Servicios prestados, donde se debe medir el impacto en la calidad del servicio, donde se muestre el comportamiento de los sistemas, su tiempo sin servicio, y los impactos que esto tiene en la organización. Ello con el fin de ayudar a la Gestión Proactiva a buscar posibles problemas y analizar áreas defectuosas.

7.3. Control de Versiones.

Control de Versiones es el encargado de la implementación y control de calidad del software y hardware del entorno productivo, para garantizar que la información de las nuevas versiones se adecue a los requerimientos y que esta implementación sea adecuada y brinde una imagen real de la configuración de la infraestructura de TI.

Asimismo, es el encargado de mantener una Biblioteca de Software Definitivo (BSD o DSL por sus siglas en inglés) y un Repositorio de Hardware Definitivo (RHD o DHS).

Para una buena operación de Control de Versiones debe existir una estrecha relación entre esta y otros procesos de TI con el fin de:

- Asegurar que las nuevas versiones satisfagan las expectativas.
- Controlar la calidad del entorno de producción.
- Preservar la integridad de las bases de datos asociadas.

El objetivo primordial del Control de Versiones es la protección de los ambientes de producción y los servicios que este presta a través de procedimientos formales y puntos de control, para así proteger el software, hardware e ítems relacionados con estos. Asimismo se asegura que sólo las versiones finales, aprobadas y autorizadas, sean las que se encuentran en uso. Entre los objetivos específicos del Control de Versiones se cuentan:

- Revisar y planificar la distribución exitosa del software y hardware relacionado.
- Asegurar que el software y hardware modificado sea trazable, seguro y que sólo se instalen las versiones correctas, autorizadas y probadas.
- Implementar las nuevas versiones de software y hardware dentro del entorno de producción.
- Asegurar que se registren copias finales de todo software en la Biblioteca de Software Definitiva, y que esta Biblioteca esté actualizada.
- Asegurar que se registre todo hardware en el Repositorio de Hardware Definitivo, y que este Repositorio esté actualizado.

7.3.1. Versiones

Una versión es un cúmulo de cambios generados y autorizados a un servicio de TI, la que puede resultar de solucionar problemas o de mejorar el servicio, esto mediante la modificación de un software o hardware existente o su implementación desde cero. Generalmente a una versión se le asignan, luego del nombre, dos números (major.minor) que se van incrementando conforme el desarrollo del software aumenta y se requiera la asignación de un nuevo nombre o número único. Aunque menos habituales, también puede indicarse otro número más, micro, y la fase de desarrollo en que se encuentra el software.

De esta forma las Versiones suelen dividirse según su impacto o envergadura dentro de la infraestructura de TI, de la siguiente forma:

- Versión mayor: Son aquellas que normalmente contienen una gran cantidad de funcionalidades nuevas, las que pueden reemplazar parches temporales a problemas que se hayan presentado. Para identificarlas se utilizará un único número luego del nombre de la versión, por ejemplo: Programa V1.
- Versión menor: Aquellas que contienen una funcionalidad mejorada o parches, los que pueden haber sido liberadas como parches de emergencia, por ejemplo: Programa V1.1.
- Versión de emergencia: Contienen correcciones a un pequeño número de errores conocidos, por ejemplo: Programa V1.1.1.

7.3.2. DSL

Es un depósito que contiene las versiones definitivas autorizadas de todo el software. Además del ciclo de vida de ellos, indicando todas las modificaciones, versiones, documentación y código fuente que se le han realizado desde que fue incorporado a la DSL. Por este motivo se deben realizar respaldos frecuentes de la DSL, puesto que ella no sólo contiene la versión actual, sino que un historial de versiones.

Antes de incorporar un software a la DSL se debe asegurar su calidad, esto con el fin de garantizar que:

- Todos los cambios han sido autorizados.
- El software pasó los controles de calidad respectivos durante su desarrollo.
- No se deben realizar cambios adicionales para su implementación.

7.3.3. DHS

El Repositorio de Hardware Definitivo contiene un inventario del hardware disponible, tanto aquel que está siendo utilizado como el que se encuentra para repuestos. El hardware disponible como repuestos debe ser similar al que posee la infraestructura de TI.

7.3.4. Procesos del Control de Versiones

El Control de Versiones es el encargado de generar políticas de planificación para la implementación de nuevas versiones, poniéndolas a prueba en entornos que simulen de mejor manera el entorno de producción, para luego validar estas versiones e implementarlas en el entorno de producción, e ingresándolas tanto al DHS como al DSL según corresponda. Informando a los usuarios sobre la nueva versión y sus formalidades.

También es el encargado de llevar a cabo los planes de backout, es decir, de retomar una versión anterior, si esto fuese necesario.

- **Backout:** Recuperación a la última configuración estable conocida anterior a un cambio o publicación fallida.

7.3.5. Validación e Implementación

Es necesario planificar de la mejor forma los protocolos de test, para ayudar a lanzar, con éxito, al medio de producción una nueva versión. Para ello se deben realizar pruebas funcionales con el fin de asegurar que la aplicación cumple con los requisitos establecidos y es útil.

También será indispensable, al momento de contemplar estas pruebas, tener planes de backout para asegurarse que se podrá regresar a la última versión estable de forma rápida, ordenada, segura y sin pérdidas de información. Para esto los usuarios y el personal de servicio deben contar con la documentación necesaria, además deben haberse realizado pruebas a los procedimientos o revisiones a los manuales de instalación. De encontrarse errores estos deben ser notificados en una lista de bugs.

Una vez realizadas las validaciones finales a las versiones se debe proceder a la implementación. Ésta se puede realizar de las siguientes formas:

- **Completa:** De manera simultánea en todos los lugares.
- **Fragmentada:** De manera parcializada o temporal, introduciendo la versión por grupos o áreas de trabajo e incrementando progresivamente la funcionalidad.

Luego de la implementación se deberá informar de esta para que la organización tenga conocimiento, así como a la Mesa de Ayuda para que reciba las quejas, incidentes o comentarios que produzca la nueva versión.

7.3.6. Comunicación y Control del Proceso

Los usuarios deben estar informados de la nueva versión y sus funcionalidades para que ellos puedan utilizar el sistema. Además en las pruebas funcionales se deben incorporar usuarios finales, y este proceso debe ser documentado para contar con un registro de los comentarios, sugerencias y/o dudas que hayan surgido durante el uso de la nueva versión.

Se debe tener en cuenta que la documentación de las versiones debe ser lo más clara e intuitiva posible para el usuario final, pudiéndose incorporar cursos o charlas en las que se le enseñará a los usuarios a utilizar las nuevas versiones.

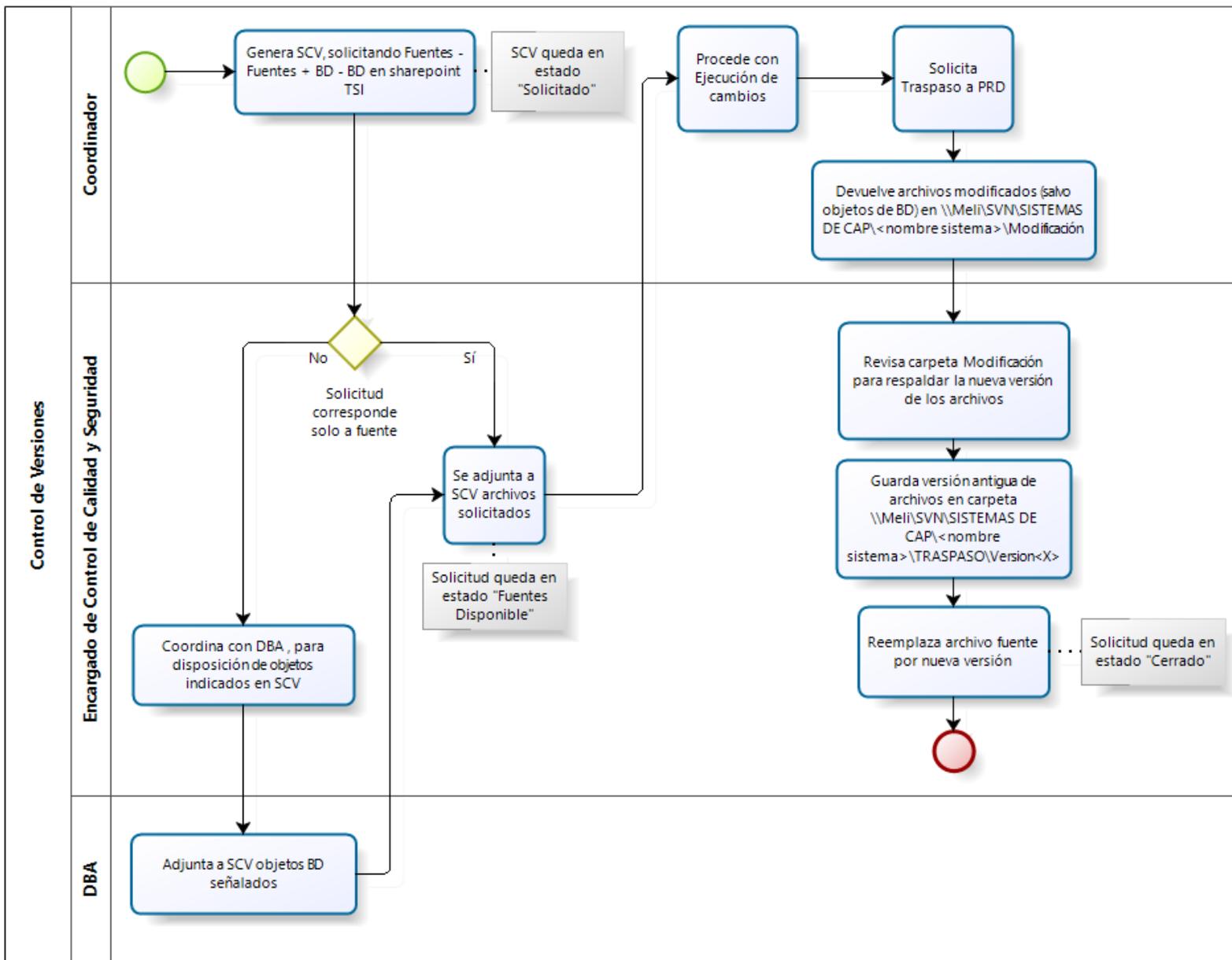


Figura 27. Diagrama BPMN del funcionamiento de Control de Versiones. Fuente: Elaboración Propia.

7.4. Control de Acuerdos de Niveles de Servicio

Tiene por objetivo primario conocer las necesidades de los clientes y de los usuarios, además de definir los servicios que se necesitan para aportar valor, mediante tecnologías alineadas a los procesos de negocios a bajos costos y altos niveles de calidad.

El Control de Acuerdos de Niveles de Servicio es el encargado de asegurar la calidad en la provisión y soporte de los servicios, alineándose de este modo con los procesos del negocio como también mejorando el rendimiento y rol del cliente, asegurando el cumplimiento de los acuerdos de nivel de servicios (SLAs), y elaborando informes de rendimiento y métricas para evaluar los SLAs.

Este control es el los encargado de llegar a acuerdos con los proveedores externos de servicios de TI, planificando los servicios ofrecidos, analizando las necesidades, elaborando las especificaciones de los servicios solicitados y estableciendo parámetros de rendimiento para verificar la calidad del servicio entregado.

Además debe controlar los SLAs, formalizando los acuerdos de nivel de operación y los contratos con proveedores externos, también debe monitorear sus servicios, elaborando informes de rendimiento de la calidad del servicio, modificando los SLAs de ser necesario de igual modo debe corregir problemas ocurridos por el incumplimiento de los SLAs, o generar los documentos de apoyo en caso de renovación de un SLA.

El Control de Acuerdos de Niveles de Servicio es el proceso mediante el cual se definen, negocian y supervisan la calidad de servicios. Es decir es el encargado de planificar, implementar, monitorear y revisar los SLAs. Teniendo como funciones principales:

- Documentar y preparar los servicios de TI para el usuario de forma que estos sean comprensibles para él.
- Establecer acuerdos con proveedores para ofrecer los servicios requeridos e indicadores del rendimiento del servicio TI.
- Monitorizar la calidad de los servicios acordados con el objetivo de mejorarlos a un costo aceptable.
- Elaborar informes sobre la calidad del servicio y planes de mejora de este (SIP)

Esto permite, siempre que se haya implementado correctamente, que se establezcan de forma clara y medible los objetivos que ayuden a determinar de una mejor forma las necesidades de los clientes, facilitando además, una mejor comunicación entre estos y los proveedores de los servicios, evitándose malentendidos sobre las características y calidad de los servicios ofrecidos, estableciéndose claramente las responsabilidades y obligaciones tanto de clientes como proveedores. Asimismo un monitoreo constante del servicio favorece la detección de falencias o puntos débiles, permitiendo su temprana mejora. Además los SLAs facultan a la Gestión de TI calcular los costos de las diferentes soluciones necesitadas.

7.4.1. Planificación

Se debe contar con la colaboración de todos o la mayor parte de los involucrados de la organización, ya sean usuarios o clientes y los proveedores del servicio, así esta colaboración será la base para la correcta planificación del Control de Acuerdos de Niveles de Servicio. De este modo se dará una mejor cobertura a las necesidades del cliente, mediante la definición, negociación y monitoreo de los acuerdos, buscando minimizar los niveles de insatisfacción por los servicios ofrecidos, si ello no es posible la organización deberá hacerse responsable de las consecuencias que deriven del no cumplimiento de la expectativa de los clientes o de su insatisfacción.

Para la planificación se debe tener en cuenta cuáles son las necesidades y qué servicios se deben solicitar para dar solución a estas. Para lo cual se debe tener en cuenta cual será la calidad esperada del servicio que se solicita, señalando los indicadores de rendimiento o satisfacción que se requerirán, y quienes serán los responsables de dar solución estos y de qué forma lo realizarán.

Todo este proceso deberá ser documentado, dicha documentación puede ser tanto interna como pública, dependiendo de quién se quiere que tenga acceso a la información. Todo con el objetivo de que la documentación sirva de guía a la hora de seleccionar un servicio que se adapte a las necesidades, así también para delimitar funciones y compromisos de la organización, evitando malentendidos entre los diferentes actores implicados en la prestación de servicios.

Los resultados de la planificación deben ser presentados, de manera formal, en un documento en el que se señalen los Requisitos de Nivel de Servicio (SLR), que debe mostrar las necesidades como las expectativas que se tienen respecto a:

- La funcionalidad, características y calidad del servicio.
- La disponibilidad y continuidad que debe tener el servicio.
- La interacción del servicio con la infraestructura TI o de otro tipo.
- Tiempos y procedimientos de implementación del servicio.
- La escalabilidad o no escalabilidad del servicio.

Este SLR servirá de base para elaborar la documentación interna de cómo se realizará el servicio y quién o quiénes serán los responsables de brindar este servicio, el documento de Especificación de Servicio deberá contener una descripción detallada de todos los factores técnicos necesarios sobre la prestación e implementación del servicio, así como cuáles serán los indicadores internos de rendimiento y calidad del servicio.

Se deberá generar un Programa de Calidad del Servicio o (SQP), que debe contener la información necesaria para que la organización conozca los procedimientos y procesos involucrados en el suministro de servicios que se prestará, asegurando que éstos se alinearán al negocio y se mantendrán los niveles de calidad óptimos. Indicando:

- Los objetivos del servicio.
- Un estimado de los recursos.

- Indicadores de rendimiento.
- Procedimientos de monitoreo de proveedores.

Este documento debe ser el principal para la gestión de los servicios contratados, ya que cuenta con toda la información de todos los procesos TI involucrados en la prestación de los servicios.

El Acuerdo de Nivel Operacional (OLA) será el documento donde se especificarán las responsabilidades y compromisos de los diferentes departamentos de la organización en la prestación de un determinado servicio.

El Programa de Mejora de Servicio (SIP) será el encargado de recoger las medidas correctivas a fallas detectadas en los niveles de servicio como propuestas de mejoras basadas en el avance de la tecnología. Será parte de la documentación base para la renovación de los SLAs y debe estar disponible para los gestores de otros procesos de TI.

7.4.2. Implementación y Monitoreo

La implementación será la que refleje la elaboración y aceptación de los acuerdos necesarios para la prestación de un servicio, entre estos se pueden mencionar los Acuerdos de Nivel de Servicio, los Niveles de Operación y los Contratos de Soporte, siendo estos últimos los documentos internos, propios de la organización, donde se detallará de manera clara los procesos, compromisos, que se acordará con las empresas externas, indicando sus responsabilidades, deberes y obligaciones.

El monitoreo hará un seguimiento de los niveles de servicio, para mejorar la calidad de los servicios ofrecidos, tanto en los parámetros y procedimientos internos, incorporando la precepción de los usuarios. Para realizar el monitoreo se debe tener en cuenta la información extraída desde la mesa de ayuda, pues por el trato que el tiene con los usuarios conoce la precepción de calidad de los servicios, el control de incidentes, que informa de los incidentes y tiempos de recuperación, los SLAs con información de incidentes, impactos y frecuencia de éstos, las quejas de los usuarios, la calidad del servicio prestado por los proveedores externos, etc.

7.4.3. Revisión y Control

La revisión continua de la calidad de los servicios prestados, en base a los objetivos y los SLAs vigentes son la base para una correcta implementación del Control de Acuerdos de Niveles de Servicio, con el objetivo de centrarse en el mejoramiento de la calidad de los servicios y no quedarse únicamente en los SLAs no cumplidos. Así, el Programa de Mejora del Servicio (SIP), es el resultado de la revisión, en la que se analizan los problemas relacionados con los servicios TI, las posibles causas de fallas o baja en la calidad de los mismos, así como también los nuevos requerimientos que ellos generen, la evaluación de los costos reales, SLAs, reasignación de recursos o petición de nuevos servicios.

Respecto a los SLAs se debe revisar la percepción de cumplimiento de los mismos, al igual que la demás documentación por parte de los clientes, usuarios y la organización en general. Evaluando el rendimiento y capacitación del personal, así como los usuarios de los servicios.

En base al SIP se negociará la renovación del SLA con los proveedores, así como también con los demás documentos de referencia.

Una adecuada revisión y control del Control de Acuerdos de Niveles de Servicio en que se deberá realizar un adecuado manejo de los procesos involucrados, siendo necesario disponer de objetivos y asignaciones de tareas y responsabilidades claras, además de indicadores de rendimiento específicos, como:

- Porcentaje de servicios amparados bajo SLAs.
- Porcentaje de incumplimiento en los SLAs, clasificándolos por su impacto en la calidad del servicio.
- SIPs elaborados e impacto de estos en la calidad del servicio.

La elaboración de Informes de gestión aportará información relevante a las áreas involucradas con el soporte y la entrega de servicios. Esta documentación será:

- **Informes de Rendimiento:** Donde se detallan los SLAs, OLAs, con su nivel de cumplimiento y los costos promedios asociados al promedio.
- **Informes de Seguimiento:** Donde se describan las acciones de monitoreo realizadas, sus resultados y el grado de cumplimiento con el servicio.
- **Planes de Mejora:** Donde se proponen acciones de mejora a los servicios y el impacto que éstas han tenido en la calidad del servicio.

7.5. Manejo de Cambios.

El proceso del Manejo de Cambios es el encargado de la evaluación y planificación de los cambios, con el fin de asegurar una implementación eficiente del proceso, siguiendo con los procedimientos establecidos, asegurando, en todo momento, la continuidad y calidad de los servicios. Lo anterior en relación a que toda mejora implica realizar cambios, por lo que es importante determinar las posibles consecuencias que traerán esta mejoras antes de proceder a su implementación. Por lo general las principales razones para la aplicar cambios en la infraestructura TI son:

- Solución de un error conocido.
- Implementación de un nuevo servicio.
- Mejora de un servicio existente.
- Implementación de una nueva normativa legal.

Por esta razón se debe asegurar que dichos cambios están debidamente justificados, y que se llevarán a cabo sin interferir en la calidad del servicio, que están clasificados y documentados, que han sido probados, en el entorno de pruebas, y se dispone de planes de backout en caso de un incorrecto funcionamiento tras su implementación.

Para llevar a cabo esta implementación debe existir una estrecha relación entre el Manejo de Cambios y los demás procesos TI, con el objetivo de asegurar que los cambios satisfacen las necesidades del servicio TI, preservando la calidad del servicio durante todo el proceso de cambio y la integridad de las bases de datos asociadas.

El registro de RFC es el primer paso del proceso de cambio. No siempre un cambio implica una RFC. Para cambios livianos o reiterativos se acuerdan procedimientos estándar que no requiera la aprobación de la Gestión de Cambios en cada caso.

- **RFC:** Una Solicitud de Cambio (RFC) es una propuesta formal para un cambio a realizar. Una RFC incluye detalles de la propuesta de cambio, pudiendo ser escrita en papel o electrónicamente. El término RFC es a menudo mal utilizado para referirse a un registro de cambio, o al cambio en sí.

La RFC debe ser correctamente registrada para poder efectuar un seguimiento durante todo el proceso de cambio. Este registro debe incluir:

- Fecha de recepción.
- Identificador único de la RFC.
- Identificador del error conocido si es necesario
- Descripción del cambio propuesto incluyendo motivación, propósito, CIs involucrados, estimación de recursos necesarios para la implementación, tiempo estimado, estatus: aceptado, aprobado, registrado, en curso. El estado inicial de una RFC será el de "registrado".

Una vez registrada la RFC, el cambio debe ser revisado para determinar si cumple con las características y requisitos para su aprobación y posterior implementación. El resultado de la revisión puede ser la aceptación, procediéndose a determinar su prioridad y categoría, o su denegación, devolviéndose la RFC al solicitante para su revisión y solución de problemas presentados. Si se decide la aprobación definitiva de un cambio es indispensable una correcta planificación, elaborándose una calendarización adecuada del cambio, monitorizando las incidencias secundarias derivadas del cambio, esto cumpliendo los objetivos previstos.

- **Prioridad:** Importancia relativa de una RFC, la que determina el calendario de cambio.
- **Categoría:** Impacto y dificultad del cambio, determinando la asignación de recursos y plazos previstos.

Los niveles de prioridad se clasifican en:

- **Baja:** Se puede realizar junto a otros, es decir sin urgencia, por ejemplo, durante la actualización de paquetes de software o inclusión de nuevo hardware, etc.
- **Normal:** Cuando es conveniente realizar el cambio, siempre que ello no entorpezca algún otro de más alta prioridad.
- **Alta:** Un cambio que debe realizarse de forma urgente ya que está relacionando errores conocidos que deterioran la calidad del servicio. Se evalúa este cambio en la siguiente reunión y se adoptan las medidas necesarias que permitan una solución rápida.
- **Urgente:** Es necesario resolver un problema que está provocando una interrupción o deterioro grave del servicio. Un cambio de prioridad urgente desencadena un proceso denominado “Cambio de Emergencia” y se trata de forma independiente.

Se debe tener en cuenta que en ocasiones surgen cambios que se deben implementar de forma urgente, estos pueden ser originados por interrupciones graves del servicio, debiendo aplicarse protocolos de emergencia, estos pueden ser una aprobación directa, procediéndose a su implementación, obviándose las etapas normales del proceso, las que deberán ser completadas con posterioridad a la implementación, para preservar la integridad de los sistemas y bases de datos.

Tras la implementación de un cambio es necesario evaluar si se cumplieron los objetivos para los cuales fue previsto dicho cambio, además se debe conocer la percepción de los usuarios y así conocer si el cambio fue aceptado por ellos. Si la valoración de estos aspectos interrogantes es positiva se deberá cerrar el cambio, en caso de no ser así se llevarán a cabo los planes de backout.

El Manejo de Cambios debe asegurar que los cambios:

- Son justificados.
- No perjudican la calidad de el/los servicio.
- Se encuentran correctamente registrados, clasificados y documentados.

- Han sido cuidadosamente testeados en un entorno de prueba.
- No producirán inconsistencias en las Bases de Datos
- Pueden deshacerse mediante planes de backouts en caso de un incorrecto funcionamiento tras su implementación.

7.5.1. Alcance del Manejo de Cambios

En una primera instancia se puede dar por sentado que el Manejo de Cambios podrá hacerse responsable de todo cambio no estándar, lo que en ocasiones no ocurre, es por esto que el alcance del Manejo de Cambios no debe entenderse como un ente aislado, sino que debe entenderse como interrelacionado con las demás partes del modelo.

La cuidadosa elaboración de protocolos estándar de cambio permite una gestión rápida y eficiente de los cambios menores o que representen un bajo impacto en la infraestructura, estos procedimientos servirán para la creación de adecuados “procesos de cambio”.

7.5.2. Actividades del Manejo de Cambios

Las actividades de las que se encarga el Manejo de Cambios se resumen en la dirección y monitoreo de todo proceso de cambio que se produzca en la infraestructura de TI, dichos cambios deberán ser registrados mediante las RFC correspondientes, las que deberán ser revisadas y evaluadas. El responsable de Manejo de Cambios será el responsable de la aceptación o rechazo de las RFC recibidas, salvo el caso en que los cambios sean menores, realizando la elaboración del FSC correspondiente.

- **Calendario de Cambios (FSC):** Un programa que contiene detalles de todos los cambios aprobados para la ejecución y las fechas de ejecución propuestas. Una vez acordado, el Centro de Servicio comunicará a los Usuarios el tiempo de inactividad planificado o adicional que surja de la aplicación de los cambios.

Dentro de las actividades está también el coordinar el desarrollo e implementación del cambio, evaluando los resultados de este, procediendo, finalmente, al cierre en el caso de éxito de la implementación.

7.5.2.1. Clasificación y Registro

Para un adecuado proceso de cambio se deben tener correctamente registradas las RFC, las que pueden ser provocadas por diversas causas, como:

- Propuestas de solución a errores conocidos, tal es el caso del Manejo de Problemas, estos errores pueden requerir cambios en la infraestructura TI, por lo que será necesario que se adjunte la mayor cantidad de información posible en la RFC.

- Aparición de nuevos servicios, de ocurrir esto se debe coordinar, con los responsables de estos nuevos servicios, para procurar que el impacto en la implementación de este sea el menor posible y con los mejores resultados.
- Una nueva estrategia de negocio puede implicar la aparición de cambios en procedimientos, hardware o sistemas de la organización.
- Las actualizaciones de software, con versiones antiguas, por pérdida del respaldo por parte de los proveedores podrían generar la necesidad de aplicar nuevas versiones de dichas aplicaciones.
- Un cambio en la legislación puede inducir a cambios dentro de la infraestructura TI.
- Así también la sugerencia de empleados, usuarios u otros para mejorar el servicio puede generar cambios en la infraestructura.

Como ya se mencionó no todos los cambios requieren una RFC, existen aquellos que por su pequeñez no requieren una, en este caso sólo se requerirá un procedimiento estándar para implementarlos. Si este no es el caso y se debe completar la RFC correspondiente, esta debe contener los siguientes campos:

- Fecha de recepción.
- Identificador de la RFC.
- Identificador del error conocido asociado (de existir).
- Descripción del cambio propuesto:
 - Motivación.
 - Propósito.
 - CIs involucrados.
- Estimación de recursos necesarios para la implementación.
 - Tiempo estimado.
- Estatus: que inicialmente será "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. El registro debe incluir al menos:

- Estatus actualizado: (aceptado, rechazado, implementado, registrado)
- Fecha de aceptación (denegación) del RFC.
- Evaluación preliminar de la Gestión del Cambio.
- Prioridad.
- Categoría.
- Plan(es) de "backout".
- Recursos asignados.
- Fecha de implementación.
- Plan de implementación.

- Cronograma.
- Revisión post-implementación.
- Evaluación final.
- Fecha de cierre.

Además todo cambio puede ser clasificado como Cambio Estándar, aquellos que afectan la calidad de peticiones de Servicio, o Cambio no Estándar.

7.5.2.2. Aceptación y Clasificación

Es indispensable hacer una evaluación preliminar de una RFC, lo que permite determinar si el cambio que se solicita está justificado, y por ende si debe ser aceptado o no. Una vez realizado esto, la RFC deberá ser devuelta a quien la solicitó, persona o área, para confirmar la respuesta de la evaluación, aceptación o rechazo de la RFC, pudiendo presentarse nuevos antecedentes en el caso de que ésta sea rechazada. Cabe destacar que una aprobación preliminar de la RFC no implica que ella será implementada, sólo indica que la RFC cuenta con la justificación suficiente para su procesamiento y análisis.

Al momento de manejar un cambio se debe tener en cuenta factores como la urgencia y el impacto del mismo, y con ello poder determinar la prioridad y la categoría del RFC, lo que se anotará en el calendario junto a los otros pendientes, asignándole plazos, recursos y si es necesario autorización para realizar el cambio. Esta categorización se hará de acuerdo a la escala dada anteriormente, donde se consideran cuatro posibles valores: baja, normal, alta y urgente. La categoría es el resultado del impacto sobre la organización y el esfuerzo requerido para su implementación, desde la modificación mínima del servicio con poca intervención del personal de TI, hasta grandes recursos y aprobación directa de la jefatura o gerencia.

Es posible con estos datos determinar la Categoría a la que pertenece el Cambio, pudiendo ser: Impacto Menor, Impacto Sustancial o Impacto Mayor

7.5.2.3. Aprobación y Planificación

Se deben realizar reuniones periódicas para la aprobación de RFC pendientes, consolidar los cambios, planear su implementación, asignación de los recursos necesarios, elaboración de FSC y seguimiento de ellos. Además se deben mantener planes de backout, cuando existan CIs interrelacionados y tener en cuenta que al momento de realizar un cambio se puedan producir resultados inesperados que impliquen volver a un estado de configuración anterior. Para la aprobación del cambio se debe evaluar minuciosamente las siguientes interrogantes:

- ¿Cuáles son los beneficios esperados del cambio propuesto?
- ¿Justifican esos beneficios los costos asociados al proceso de cambio?
- ¿Cuáles son los riesgos asociados?
- ¿Disponemos de los recursos necesarios para llevar a cabo el cambio con garantías de éxito?

- ¿Puede demorarse el cambio?
- ¿Cuál será el impacto general sobre la infraestructura y la calidad de los servicios TI?
- ¿Puede el cambio afectar 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 estratégico y de política general de la organización.

Una vez aprobado el cambio debe evaluarse si este 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 backout.

7.5.2.4. Implementación del Cambio

Si bien la función de la implementación del Cambio es responsabilidad de Control de Versiones, Manejo de Cambios es la encargada de supervisar y coordinar el proceso. Es aquí donde se debe monitorear el proceso para asegurar que tanto el software desarrollado, como el hardware cumplan con las especificaciones requeridas, y que su implementación cumpla con los plazos establecidos y los recursos asignados. Así mismo, se debe supervisar que el entorno de pruebas o simulación sea el más adecuado posible, y que simule de mejor manera el entorno productivo. Además, de ser necesario, se implementen los planes de backout pertinentes para permitir una rápida recuperación a la última configuración estable.

Idealmente se debería permitir un acceso restringido de usuarios al entorno de pruebas con el fin de realizar la valoración preliminar de el o los sistemas en las áreas de:

- 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, teniéndose en cuenta la resistencia habitual al cambio por parte de cierto tipo de usuarios. Debiendo mantenerse informado a usuarios y proveedores de cambios futuros por medio del Manejo de Cambios y la Mesa de Ayuda.

7.5.2.5. Evaluación

Se debe hacer una evaluación antes de proceder al cierre del cambio, que permita valorar realmente el impacto del mismo en la calidad del servicio y en la productividad de la organización.

Los aspectos fundamentales a tener en cuenta son:

- Si se cumplieron los objetivos previstos.
- En qué medida se apartó el proceso de las previsiones realizadas por la Gestión de Cambios.
- ¿Provocó el cambio problemas o interrupciones del servicio imprevistas?
- ¿Cuál ha sido la percepción de los usuarios respecto al cambio?
- ¿Se pusieron en marcha los planes de "backout" en alguna fase del proceso?¿Por qué?

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 Revisión Post Implementación (PIR) asociada.

7.5.3. Control del Proceso

Es necesaria la elaboración de informes que permitan evaluar el rendimiento de la Gestión de Cambios. Estos informes deben contener métricas de referencia que abarquen aspectos 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 backouts con una detallada explicación de los mismos.
- Evaluaciones post-implementación.
- Porcentajes de cambios cerrados sin incidencias ulteriores.
- Incidencias asociadas a cambios realizados.

7.5.4. Cambios de Emergencia

Habitualmente los cambios realizados mediante procedimientos de emergencia son resultado de una planificación deficiente y muchas veces resultan inevitables.

Cualquier interrupción del servicio de alto impacto, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios 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.

Como el objetivo prioritario en estos casos es restaurar el servicio es, frecuente que los procesos asociados sigan un orden inverso al usual, así por ejemplo tanto los registros como la documentación asociada al cambio se realicen a posteriori. Sin embargo, es esencial 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 se podrían provocar situaciones de cambios futuros incompatibles, configuraciones registradas incorrectas, etc. que serían fuente de nuevas incidencias y problemas.

7.6. Gestión de Capacidad.

La Gestión de la Capacidad es la encargada de que todos los servicios TI se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada.

Sin una correcta Gestión de la Capacidad los recursos no se aprovechan adecuadamente y se realizan inversiones innecesarias que acarrearán gastos adicionales de mantenimiento y administración. O aún peor, los recursos son insuficientes con la consecuente degradación de la calidad del servicio.

Entre las responsabilidades de la Gestión de la Capacidad se encuentran:

- Asegurar que se cubren las necesidades de capacidad TI tanto presentes como futuras.
- Controlar el rendimiento de la infraestructura TI.
- Desarrollar planes de capacidad asociados a los niveles de servicio acordados.
- Gestionar y racionalizar la demanda de servicios TI.

El objetivo primordial de la Gestión de la Capacidad es poner a disposición de usuarios y el propio departamento TI los recursos informáticos necesarios para desempeñar de una manera eficiente sus tareas, todo ello sin incurrir en costos desproporcionados. Para lograrlo la Gestión de la Capacidad debe:

- Conocer el estado actual de la tecnología y previsible 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 previsible.
- Dimensionar adecuadamente los servicios y aplicaciones alineándolos a los procesos de negocio y necesidades reales del cliente.
- Gestionar la demanda de servicios informáticos racionalizando su uso.

La Gestión de la Capacidad intenta evitar situaciones en las que se realizan inversiones innecesarias en tecnologías que no son adecuadas 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.

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

- Se optimiza el rendimiento de los recursos informáticos.

- 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 los gastos de mantenimiento y administración asociados a aplicaciones y equipos obsoletos o innecesarios.
- Se reducen posibles incompatibilidades y fallos en la infraestructura informática.

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

- Información insuficiente para una planificación realista de la capacidad.
- Expectativas injustificadas sobre el ahorro de costos y mejoras del rendimiento.
- Insuficiencia de recursos para la correcta monitorización del rendimiento.
- Infraestructuras informáticas distribuidas y excesivamente complejas en las que es difícil un correcto acceso a los datos.
- No existe el compromiso suficiente de la dirección por implementar rigurosamente los procesos asociados.
- La rápida evolución de las tecnologías puede obligar a una revisión permanente de los planes y escenarios contemplados.
- Un excesivo celo en el dimensionamiento de la propia Gestión de la Capacidad puede provocar costosos y/o 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.
- Modelado y simulación de diferentes escenarios de capacidad.
- Monitorización del uso y rendimiento de la infraestructura TI.
- Gestión de la demanda.

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: que centra su objeto de atención en las necesidades futuras de usuarios y clientes.
- Gestión de la Capacidad del Servicio: que analiza el rendimiento de los servicios TI con el objetivo de garantizar los niveles de servicio acordados.
- Gestión de la Capacidad de Recursos: 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.

7.6.1. Planificación.

7.6.1.1. Plan de Capacidad

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

El Plan de Capacidad debe incluir información sobre los costos 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.

7.6.1.2. Modelado y Benchmarking

Cuanto más compleja sea una infraestructura informática 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:

- Costos asociados al incremento de la capacidad.
- Costos inherentes al proceso mismo de modelado y simulación.
- Alcance de los incrementos de capacidad previstos.
- La "criticalidad" de los sistemas implicados.

Sopesando los anteriores factores podemos optar por:

- Un simple análisis de tendencias que permita evaluar la carga de proceso esperada en la infraestructura informática 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 informática.
- Realizar benchmarks con prototipos reales para asegurar la capacidad y el rendimiento de la futura infraestructura.

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 siguientes aspectos:

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

Es importante que la Gestión de la Capacidad participe en las primeras etapas de desarrollo de un producto, servicio o definición de un SLA para asegurar que se dispondrá de la capacidad necesaria para llevar el proyecto a buen término.

Es relativamente frecuente que se obvian aspectos relativos al correcto dimensionamiento de una aplicación, esto debido a expectativas injustificadas sobre la tecnología. Se puede caer en el equívoco de que los costos asociados a la capacidad se limitan por ejemplo a la compra de más servidores, o más espacio de almacenamiento, entre otros, olvidando que algunos sistemas más complejos implican mayores gastos de mantenimiento y administración, o ignorando quizás los problemas que pueden conllevar dichos cambios.

7.6.2. Supervisión del Proceso

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

Tanto la información obtenida en estas actividades como la generada a partir de ella por la Gestión de la Capacidad se almacenan y registran.

7.6.2.1. Monitorización

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

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

7.6.2.2. 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.

7.6.2.3. Optimización y cambios

Si se ha optado por solicitar un aumento de la capacidad se elevará una 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.

7.6.3. Gestión de la Demanda

El objetivo de la Gestión de la Demanda es el de optimizar y racionalizar el uso de los recursos TI.

Aunque la Gestión de la Demanda debe formar parte de las actividades rutinarias de la Gestión de la Capacidad ésta cobra especial relevancia cuando existen problemas de capacidad en la infraestructura TI.

El origen de los problemas que la Gestión de la Demanda debe subsanar a corto plazo incluyen:

- Degradación del servicio por aumentos no previstos de la demanda.
- Interrupciones parciales del servicio por errores de hardware o software.

La Gestión de la Demanda es la encargada en estos casos de redistribuir la capacidad para asegurar que los servicios críticos no se vean afectados o, cuando menos, lo sean en la menor medida posible. Para llevar a cabo esta tarea de forma eficiente es imprescindible que la Gestión de la Capacidad conozca las prioridades del negocio del cliente y pueda actuar en consecuencia.

Además, una tarea no menos importante es la Gestión de la Demanda a medio y largo plazo. Un aumento de la capacidad siempre conlleva costos que muchas veces resultan innecesarios. Una correcta monitorización de la capacidad permite reconocer puntos débiles de la infraestructura TI o “cuellos de botella” y así evaluar si es posible una redistribución a largo plazo de la carga de trabajo que permita dar un servicio de calidad sin aumento de la capacidad.

Por ejemplo, una incorrecta distribución de tareas puede provocar que el ancho de banda contratado por la organización se muestre insuficiente en horas punta porque se estén enviando miles de correos electrónicos asociados a procesos automáticos (tales como campañas de marketing promocional, informes de rendimiento para clientes, etcétera). En la mayoría de los casos esos procesos pueden desplazarse fuera de horas punta sin degradar la calidad del servicio, ahorrando a la organización una gravosa ampliación del ancho de banda.

Ahora bien, si el costo añadido por aumentar el ancho de banda es marginal, puede resultar más eficiente su contratación directa que invertir el precioso (y costoso) tiempo de personal altamente especializado en la optimización del sistema.

La Gestión de la Capacidad debe evaluar a priori, basándose en la experiencia y las tendencias del mercado, cuándo la solución "más potente, más grande" es económicamente más rentable (teniendo en cuenta los costos indirectos) que un análisis pormenorizado de la situación.

7.7. Gestión de Disponibilidad.

La Gestión de la Disponibilidad es responsable de optimizar y monitorizar los servicios TI para que éstos funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLAs y todo ello a un costo razonable. La satisfacción del cliente y la rentabilidad de los servicios TI dependen en gran medida de su éxito.

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 establecidos. 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.
- Monitorizar la disponibilidad de los sistemas TI.
- Proponer mejoras en la infraestructura y servicios TI con el objetivo de aumentar los niveles de disponibilidad.

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

- **Disponibilidad:** porcentaje de tiempo sobre el total acordado en que los servicios TI han sido accesibles al usuario y han funcionado correctamente.
- **Fiabilidad:** medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida.
- **Mantenibilidad:** capacidad de mantener el servicio operativo y recuperarlo en caso de interrupción.
- **Capacidad de Servicio:** determina la disponibilidad de los servicios internos y externos contratados y su adecuación a los OLAs y UCs en vigor. Cuando un servicio TI es subcontratado en su totalidad la disponibilidad y la capacidad de servicio son términos equivalentes.

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 correcta Gestión de la Disponibilidad son:

- Cumplimiento de los niveles de disponibilidad acordados.
- Reducción de los costos asociados a un alto nivel de disponibilidad.
- Percepción de parte del cliente de una mayor calidad de servicio.
- Aumento progresivo de los niveles de disponibilidad..
- Reducción del número de incidentes.

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

- No se monitoriza correctamente la disponibilidad real del servicio.
- No existe compromiso con el proceso dentro de la organización TI.
- 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.
- Los proveedores internos y externos no reconocen la autoridad del Gestor de la Disponibilidad por falta de apoyo de la dirección.

7.8. Gestión de Peticiones.

La Gestión de Peticiones es la encargada de atender las peticiones de los usuarios, solicitudes que los usuarios pueden plantear al departamento de TI, proporcionándoles información y acceso rápido a los servicios estándar de la organización TI, trabajando en conjunto con otros como lo es Mesa de Ayuda o Control de Cambios. Entre estas solicitudes podemos encontrar:

- Solicitudes de información o consejo.
- Peticiones de cambios estándar, correspondientes al punto de Control de Cambios, como problemas con el correo o de olvido de claves de acceso.
- Peticiones de acceso a servicios TI.

Entre los objetivos de la Gestión de Peticiones se encuentran el ser un canal de comunicación para que los usuarios soliciten y obtengan acceso a los servicios para los que se encuentren habilitados a acceder, además de proporcionar información sobre la disponibilidad de los servicios y los procedimientos para obtenerlos, ayudando en la resolución de quejas o recepción de comentarios, pudiendo además ofrecer información general sobre estos. Para ello la Gestión de Peticiones será la encargada de localizar y distribuir los componentes de servicio estándar solicitados por los usuarios.

7.8.1. El proceso de la Gestión de Peticiones

Las actividades de las que el proceso de Gestión de Peticiones es responsable se pueden dividir en cuatro grandes grupos:

- **Selección de peticiones:** Los usuarios, a través de las herramientas destinadas a tal fin por la Gestión de Peticiones, emiten sus peticiones conforme a una serie de tipologías predefinidas.
- **Aprobación de la petición:** Al ser recepcionada una petición, esta debe ser evaluada para revisar si cumple con los requisitos para su tramitación.
- **Tramitación:** La petición es cursada por la persona o personas adecuadas según cada caso.
- **Cierre:** Tras comprobar que el usuario ha quedado conforme con la gestión se procede a su cierre.

7.8.1.1. Selección de peticiones

La Gestión de Peticiones permite que los propios usuarios generen sus peticiones de servicio, ya sea:

- De manera telefónica, mediante la mesa de ayuda,
- De forma electrónica, por plataforma o correo electrónico.

En esta petición, el usuario deberá especificar qué es lo que solicita y por qué lo solicita.

7.8.1.2. Aprobación

La tramitación de las peticiones conlleva un gasto, por lo que se debe tratar de gestionar sólo aquellas peticiones que son viables, lo anterior porque en muchas ocasiones los usuarios no tendrán los privilegios para obtener lo que solicitan. Por eso, antes de autorizar una tramitación es principal determinar primero la viabilidad que esta acarreará.

Se pueden definir, para determinadas peticiones estándares fijos que ayuden a gestionar con rapidez aquellos casos más frecuentes.

7.8.1.3. Tramitación y Cierre

Esta actividad consiste en dar curso a la petición, por lo que las acciones a desempeñar dependerán de la naturaleza de la misma. Cabe hacer notar que por cada solicitud aceptada se generará un ticket de servicio, el que identificará la petición.

Mesa de Ayuda puede encargarse de las peticiones más simples, mientras que otras necesitarán de una intervención especializada o atención en terreno. Independientemente de la tramitación de la petición se deberá monitorear todo el proceso, indicando su estado de avance.

Una vez resuelta la petición, se debe notificar a quien corresponda para que compruebe si el usuario está satisfecho con el resultado y de ser así se proceda al cierre de la petición o ticket.

7.8.2. Control del Proceso

Para controlar el proceso de la Gestión de Peticiones se deberá tener un control del:

- Número total de peticiones de servicio ingresadas:
 - Número total de peticiones atendidas y solucionadas, como también el estado de las que se encuentran en tramitación.
- Tiempo medio que dura la gestión de cada tipo de petición de servicio.
- Número y porcentaje de peticiones de servicio completadas y tiempo de duración de la tramitación.
- Nivel de satisfacción del cliente con la gestión de las peticiones de servicio.

7.9. Continuidad del Servicio y Contingencias Mayores.

La Continuidad del Servicio y Contingencias Mayores, como su nombre lo indica, es la responsable de procurar la continuidad del negocio frente a incidentes que afecten a los servicios, causando en éstos una indisponibilidad o una interrupción mayor ya sea por desastres naturales o causas de fuerza mayor. Para el manejo de ellas se deben considerar todas las acciones predictivas, como las reactivas del proceso. Las predictivas serán aquellas que buscan impedir o aminorar las consecuencias de una interrupción grave del servicio, mientras que las reactivas serán las que se encarguen de reanudar el servicio tan rápido como sea posible luego de la ocurrencia del desastre.

Cabe destacar que los beneficios de la implementación de este punto sólo podrán ser visibles a largo plazo, y no se verán de forma directa en la organización.

Los principales objetivos de este punto son el garantizar la rápida recuperación de los servicios críticos tras un desastre y el establecer políticas y procedimientos para evitar las consecuencias de un desastre en la organización.

Este proceso se interrelaciona con otros puntos del modelo, por lo que se debe tener en cuenta los demás puntos y disponer de un plan de continuidad acorde a las capacidades del negocio.

7.9.1. Actividades contempladas en la Continuidad del Servicio

- Establecer las políticas y alcance del Manejo de Continuidad del Servicio.
- Evaluar el impacto en el negocio de una interrupción de el/los servicios TI.
- 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.

7.9.1.1. Alcance de la Continuidad del Servicio.

Se deben definir en este punto objetivos generales, incluyendo su alcance y el compromiso de la organización, es decir, que su política apoye esta iniciativa, involucrándola por completo en este proceso, que no le retornará beneficios visibles y se debe contar con los recursos necesarios, tanto en a nivel humano como técnico y el dimensionamiento depende del alcance. Gran parte de

la inversión que se debe realizar en este punto va en la formación del personal, para que este conozca los planes y como ponerlos en marcha.

El alcance de la continuidad es determinada por los planes generales de Continuidad del Negocio, los servicios TI estratégicos, los estándares de calidad adoptados, un análisis histórico de las interrupciones graves de los servicios, las expectativas de negocio y la disponibilidad de los recursos.

7.9.1.2. Análisis del Impacto.

Se debe determinar el impacto que una interrupción de los servicios tiene en el negocio. Esto dado que la empresa depende de la infraestructura de TI y el negocio directamente de la disponibilidad de ella.

Cuanto mayor sea el impacto derivado de una interrupción de servicio, mayor esfuerzo se deberá realizar para prevenirlo. Los servicios de TI se deben analizar en base a los siguientes factores, de los que se encontrará el equilibrio entre la prevención y la recuperación, teniendo en cuenta sus respectivos costos financieros:

- Consecuencias de la interrupción del servicio en el negocio (pérdida de rentabilidad, pérdida de cuota de mercado y mala imagen de marca).
- Tiempo aceptable antes de la restauración del servicio sin un alto impacto en los procesos de negocio.
- Compromisos adquiridos a través de los SLAs.

7.9.1.3. Evaluación de los riesgos.

Una adecuada Evaluación de riesgos previene la prevención y recuperación ante la ocurrencia de desastres de manera eficaz, considerando y evaluando los factores de riesgo en función de la probabilidad y el impacto de que el desastre tenga. Así mismo la evaluación permite conocer de manera más profunda la infraestructura TI y los elementos que la conforman, y además cuales están presentes en cada servicio.

De este análisis es posible obtener información confiable y necesaria para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales de la empresa.

7.9.1.4. Estrategias para lograr la continuidad.

La continuidad de los servicios se basa tanto en medidas preventivas como reactivas, es la responsable de diseñar actividades de prevención y recuperación que ofrezcan las garantías necesarias a unos costos razonables.

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. Los sistemas de protección habituales son los que ofrecen protección perimetral a la infraestructura TI.

Las actividades de recuperación se definen de forma diferente dependiendo de la opción escogida para la recuperación del servicio:

- **Cold standby:** que requiere un emplazamiento alternativo en el que se pueda reproducir en un plazo no superior a las 72 horas el 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.

7.9.1.5. Planificación.

Definido el alcance, analizados los riesgos y vulnerabilidades y definidas también las estrategias de prevención y recuperación, se procede a la asignación y organización de los recursos necesarios. Con ese objetivo 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.

7.9.1.5.1. El Plan de prevención de riesgos

Es el plan definido para evitar o minimizar el impacto de un desastre en la infraestructura TI. Entre las medidas habituales que se deben tomar se encuentran:

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

7.9.1.5.2. El Plan de gestión de emergencias

Es aquel en el que se definen claramente, en caso de una situación de emergencia, 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 de 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.

7.9.1.5.3. 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 que se pueda:

- 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 los siguientes aspectos:

- 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.

7.9.1.6. Supervisión.

Mantener en constante formación al personal involucrado y la continua monitorización y evaluación de los planes para que se adecuen a las necesidades reales del negocio, esto es básico para que los planes de continuidad sean efectivos.

Respecto a la formación, es imprescindible que la gestión de la continuidad promocióne dentro 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 y facilite el acceso permanente a toda la información necesaria.

Por otro lado, las políticas, estrategias y planes se deben actualizar 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.

7.9.2. Control

La Continuidad del Servicio deberá realizar informes para la dirección que incluyan el análisis sobre nuevos riesgos y evaluación de su impacto. Además de una evaluación de los simulacros de desastre realizados, actividades de prevención y recuperación realizadas, costos asociados a los planes de prevención y recuperación y preparación y capacitación del personal TI respecto a los planes y procedimientos de prevención y recuperación.

Se deberán llevar a cabo, de forma obligatoria, controles rigurosos que impidan que la inversión y compromiso inicial se diluyan y el control del proceso es importante en condiciones normales éste se vuelve crítico durante las situaciones de crisis, por lo que se debe asegurar que:

- 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.

7.10. Control de la Seguridad.

El Control de la Seguridad es la encargada de que la información sea transmitida de forma correcta e íntegra, además de estar siempre disponible y a disposición del negocio, para que sea utilizada por quienes tienen la autorización para hacerlo, es decir la información deberá estar disponible de manera confiable para aquellos autorizados a verla, esto basado principalmente en la:

- Confidencialidad: La información sólo será accedida por aquellos usuarios que tengan los privilegios para hacerlo.
- Integridad: La información que se proporcione deberá ser correcta y no poseer errores.
- Disponibilidad: La información debe poder obtenerse en el momento que se necesite, es decir, debe estar siempre disponible.

Los objetivos principales en los que se basa el Control de la Seguridad son diseñar una política de seguridad, correctamente alineada con las necesidades del negocio. Como también asegurar el cumplimiento de los estándares de seguridad y minimizando los riesgos de seguridad que amenacen la continuidad del servicio. Debe también establecer protocolos de seguridad que garanticen que la información esté accesible cuando se necesita por aquellos que tengan autorización para utilizarla.

Una vez comprendidos los requisitos de seguridad del negocio, se debe supervisar que éstos se encuentran documentados para garantizar su cumplimiento.

El Control 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 lo cual es necesario que se:

- 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, monitoreando y evaluando este plan.
- Realizar una supervisión proactiva de los niveles de seguridad, analizando tendencias, nuevos riesgos y vulnerabilidades.
- Realice periódicamente auditorías de seguridad.

La Política de Seguridad debe determinar:

- La relación con la política general del negocio.
- La coordinación con los otros procesos TI.
- 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.

7.10.1. 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. Será responsabilidad del Control de Seguridad coordinar la implementación de los protocolos y medidas de seguridad establecidas en la Política y el Plan de Seguridad. Se deberá verificar netonces 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 imparta la formación pertinente.

7.10.2. Responsabilidades.

Entre las responsabilidades de las que debe hacerse cargo el Control de Seguridad se pueden destacar las siguientes: asignar los recursos necesarios para cumplir con las normas de seguridad impuestas, además de generar la documentación de referencia necesaria para que estas normas sean aplicadas, proponiendo RFCs a Manejo de Cambios que aumenten los niveles de seguridad.

Cuando se detecten incidentes será su responsabilidad colaborar tanto con Mesa de Ayuda como con Control de Incidentes en el tratamiento y resolución de incidentes relacionados con la seguridad, además de colaborar con la Manejo de Cambios y Control de Versiones para asegurar que los nuevos sistemas que ingresen a los entornos de producción o de pruebas no generen nuevas vulnerabilidades.

Será también una de sus responsabilidades instalar y mantener las herramientas de hardware y software necesarias para garantizar el cumplimiento de las políticas de seguridad impuestas, estableciendo políticas y protocolos de acceso a la información.

Así mismo será de su responsabilidad el monitorear las redes y servicios en red para detectar intrusiones y ataques.

7.11. Control de Acceso.

El objetivo de la Gestión de Acceso es otorgar permisos de acceso a los Servicios TI a aquellos usuarios autorizados e impedirlos a los usuarios no autorizados. Es decir, es la aplicación de todas las políticas y acciones definidas en el Control de Seguridad y la Gestión de la Disponibilidad.

El Control de Acceso proporciona una serie de ventajas a la organización TI que justifican su implantación, estas con:

- 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, por ejemplo en el sector industrial, como es el caso de CAP Acero.

7.11.1. Procedimiento

Las actividades de la Gestión de Acceso son las que se detallan a continuación:

- **Petición de acceso:** Es la solicitud formal de un usuario para acceder a algún recurso, este puede ser presentado por distintas vías como el departamento de Recursos Humanos, en el caso de ingresar un nuevo trabajador, una solicitud de cambio, una instrucción autorizada, etc.
- **Verificación:** Tiene como función comprobar 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.
- **Monitoreo de identidad:** Los cambios en la asignación de permisos suelen estar asociados a un cambio de estatus dentro de la organización: ascensos, despidos, jubilaciones, contrataciones, por lo que se debe saber qué es lo que se solicita y si es correspondiente realizar el cambio.
- **Registro y monitoreo 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:** Los derechos de un usuario pueden ser eliminados por completo o de forma parcial de alguno de los servicios.

7.11.1.1. Petición de Acceso

La petición de acceso puede llegar a través de numerosas vías, como por ejemplo:

- 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 deberán estar siempre documentadas

7.11.1.2. 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 las 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, este es el caso de la solicitud de la tarjeta de identificación con chip al ingreso a la planta o a algunos sectores de esta, permitiendo con esto que sólo el personal autorizado tenga acceso a estos sectores.

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 jefe del departamento en el que fue contratado o directamente desde la Unidad de Organización y Personal.

7.11.1.3. Monitoreo 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 que 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, deben 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 servirá para automatizar el proceso y ahorrar tiempo.

7.11.1.4. Registro y monitoreo 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 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 a la Gestión de Accesos proporcionar evidencias de los datos, tiempos e incluso contenido al que el usuario tiene acceso en determinados servicios.

7.11.1.5. 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, son las siguientes :

- 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.

7.11.2. Control

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 incidentes que requirieron la revocación de los permisos de acceso.
- Número de incidentes causados por una configuración incorrecta de los accesos.

7.12. Validación, Verificación y Pruebas.

Se encarga de probar cada nueva versión en un entorno idéntico al real antes de proceder a su implantación en un ambiente productivo, con el fin de detectar y prevenir aquellos errores causados por incompatibilidades imprevistas, y verificar que se cumplen los niveles de utilidad y garantía establecido y así asegurar que las ediciones implementadas y los servicios resultantes cumplan las expectativas de los clientes, y verificar que las operaciones de TI sirvan de soporte a los servicios nuevos.

Para cumplir con esto Validación, Verificación 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.

7.12.1. Proceso

Las principales actividades de la Validación y Pruebas del Servicio se resumen en:

- Validación de paquetes de servicios, ofertas y contratos. Definición del modelo de pruebas, la planificación y los protocolos de testeo.
- Construcción del escenario de pruebas y acceso a los elementos a probar.
- Pruebas de las nuevas versiones en un entorno idéntico al entorno real de desarrollo del servicio nuevo o mejorado.
- Aceptación de los datos y elaboración de informes de resultados que registren los errores, de haberse producido.
- Limpieza del entorno de pruebas y cierre del proceso.

7.12.1.1. Validación, planificación y verificación de tests

Al lanzar al entorno de producción una nueva versión se debe tener razonables garantías de éxito, para esto es indispensable realizar un protocolo de test.

Es necesario procurar que las pruebas no sólo se limiten a la 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 razonable su uso. Estas pruebas deben incluir planes de backout para asegurar que se podrá volver a la última versión estable de una forma rápida, ordenada y sin pérdidas de valiosa información.

Se deberá supervisar las tareas contenidas en el Plan de Pruebas al final de todo el proceso, para posteriormente elaborar un registro de todas las tareas realizadas y 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. Esto con el fin de asegurar que el servicio a implementar cumple con la utilidad y garantía esperadas, y que se está preparado para poner en funcionamiento el nuevo servicio a partir de su despliegue.

También se deben repasar los diseños y planes de pruebas para verificar que todo está completo y que se ajusta a los perfiles de riesgo previstos y a todos los casos de uso.

7.12.1.2. Construcción de tests

Esta etapa es la responsable 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. Este entorno debe ser lo más similar posible al entorno final, para verificar que no se produzcan diferencias entre los resultados obtenidos de las pruebas y la ejecución del sistema en productivo. Se debe considerar que el entorno de pruebas debe tener:

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

7.12.1.3. Pruebas de Validación

Esta es la etapa donde son examinados uno por uno todos los componentes, herramientas y mecanismos que participan en el despliegue, la migración y el backout. El desarrollo de estas 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 backout.
- 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 grupo seleccionado 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.

7.12.1.4. Aceptación y reporte

Consiste en la comparación de los datos obtenidos en las pruebas con los resultados esperados de la ejecución del sistema. Si la versión no cumple los requisitos mínimos preestablecidos, es devuelta como “no aceptada” y se procederá a su reevaluación. Si el análisis es favorable y existen garantías de que la versión cumple las condiciones necesarias, 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.

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

7.12.1.5. Limpieza y cierre

Por último, se procede a la limpieza del entorno de pruebas, revirtiendo los cambios incorporados durante los test a 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 y plazos acordados. Pudiendo detectarse mejoras para perfeccionar el proceso.

7.13. Planificación y Soporte para la Transición.

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

Para ello, debe asegurarse 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 usuario final del sistema.

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

- 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.

Revisión Post-Implantación (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.

7.13.1. Proceso

Las principales actividades de la Planificación y Soporte a la Transición se resumen en las siguientes:

- Estrategia
 - Políticas generales.
 - Metodología.
 - Actores implicados (instituciones, proveedores, etc.).
 - Requisitos internos y externos a tener en cuenta.
 - Tipos de entregas.
- Preparación
 - Revisión de la documentación.
 - Comprobación de los elementos de configuración.
 - Identificación de los cambios de que consta la transición.
- Planificación
 - Definición de fases y plazos.
 - Asignación de recursos.

- Establecimiento de SACs.

7.13.1.1. 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 deben tenerse en cuenta (estándares, legislación vigente, acuerdos contractuales, etc.).
- Marco de trabajo a adoptar (políticas, protocolos de autorización, etc.).
- Roles y responsabilidades.
- Planificación de hitos y entregables.
- Convenios de nomenclatura que se han adoptado para denominar las entregas (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, grosso modo, 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.

7.13.1.2. 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.

7.13.1.3. Planificación de la transición

Esta es la actividad principal del proceso, y consiste en la descripción 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 implicados en la prestación del mismo, los requisitos específicos acordados con quien solicita el cambio en el sistema o la creación de una solución, 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 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 distinto.

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

7.14. Gestión Financiera.

El objetivo de la Gestión Financiera es evaluar y controlar los costos asociados a los servicios TI, de forma que se ofrezca un servicio de calidad a los clientes con un uso eficiente de los recursos TI necesarios, con el fin de no desperdiciar recursos tecnológicos y presupuestar correctamente los gastos asociados.

Al tener conciencia de los costos asociados a los servicios se puede evaluar el ROI y establecer planes de inversión tecnológica.

Mediante la Gestión Financiera es posible administrar de forma eficaz y rentable los servicios y la organización, los que se realizan según la evaluación de costos reales asociados a la prestación de servicios y proporcionando a la organización TI la información financiera necesaria para la toma de decisiones. De este modo se puede evaluar el retorno (ROI) de las inversiones TI y llevar la contabilidad de los gastos asociados a los servicios TI.

7.14.1. Proceso

Las principales actividades de la Gestión Financiera son la evaluación de presupuestos y la contabilidad, que tienen como aspectos más destacados la:

- Generación de presupuestos.
- Contabilidad de la unidad.
- Supervisión

7.14.1.1. Presupuestos.

La elaboración de presupuestos TI tiene como objetivos la planificación del gasto e inversión TI a largo plazo, asegurar que los servicios TI están suficientemente financiados y establecer objetivos claros que permitan evaluar el rendimiento de la organización TI.

Los presupuestos realizados pueden tener diferentes horizontes temporales; a corto plazo, o resultar de una proyección sobre la evolución prevista del negocio en dos o más años. Los métodos más utilizados para realizar un presupuesto se basan en la identificación inicial de todos los elementos de costo y son:

- **Presupuesto incremental:** El presupuesto se realiza en base al histórico de presupuestos anteriores, adaptándolos a las modificaciones en los costos y el desarrollo de nuevas tecnologías, y teniendo en consideración la aparición de nuevas líneas de servicios.
- **Presupuesto "desde cero":** Se replantea toda la estructura de costos e inversiones a partir de cero en base a los servicios prestados en la actualidad y las expectativas de crecimiento en el periodo presupuestado.

La estimación de los costos asociados a esos elementos no es siempre una tarea sencilla y a menudo influyen factores externos que no se hallan bajo el control directo de la organización TI.

7.14.1.2. Contabilidad

El proceso de contabilidad debe tener en consideración la complejidad del mismo y evitar un excesivo nivel de detalle que lo encarezca más allá de lo razonable. Las actividades contables deben permitir:

- Una correcta evaluación de los costos reales para su comparación con los presupuestados.
- Tomar decisiones de negocio basadas en los costos de los servicios.
- Evaluar la eficiencia financiera de cada uno de los servicios TI prestados.

Se podría considerar a la unidad como otra área de negocio, para lo que sería necesario conocer en detalle tanto sus costos como sus ingresos, aunque estos sólo serían nominales, pues el “cliente” es la propia organización.

Una de las actividades principales de la Gestión Financiera es identificar los denominados elementos de costo que se pueden clasificar de forma genérica en costos de hardware y software, costos de Personal y costos generales, asignando a cada servicio/cliente su parte proporcional.

7.14.1.3. Supervisión

No es tarea de la Gestión Financiera de los Servicios TI, sino de Control de Acuerdos de Niveles de Servicio quien elaborar el catálogo de servicios. Sin embargo, es recomendable que, en los aspectos económicos, su actividad sea supervisada por la Gestión Financiera.

Para ello es necesario que exista una comunicación fluida y convenientemente estructurada entre ambos procesos.

Por un lado Control de Acuerdos de Niveles de Servicio debe proveer información a la Gestión Financiera sobre:

- El tipo de servicios demandados por los clientes.
- Los SLAs contratados.
- Los contratos de soporte en vigor.
- Tendencias del mercado y Planes de Mejora del Servicio.

Mientras que por otro, la Gestión Financiera debe aportar información sobre:

- Los costos reales de los servicios.
- Desviaciones en las previsiones de costos respecto a los gastos reales.

Sin una estrecha colaboración entre ambos procesos será imposible llegar a acuerdos que sean rentables y a su vez satisfactorios.

7.14.2. Control del Proceso

Es imprescindible que el responsable del proceso de Gestión Financiera disponga de cierto conocimiento sobre los servicios TI y/o esté correctamente asesorado por especialistas en todo lo referente a la tecnología.

Para poder evaluar la función de la Gestión Financiera es necesario establecer tanto unos criterios claros para evaluar su éxito como unos indicadores de rendimiento específicos. Entre los primeros cabe destacar:

- Conocer los costos reales de los servicios TI de la organización.
- Los responsables de los otros procesos TI deben colaborar con la Gestión Financiera.
- Los gastos en servicios e infraestructuras TI deben estar alineados con los procesos de negocio.
- Gestionar la unidad de TSI como una unidad de negocio.

En lo que respecta a los indicadores de rendimiento, estos deben incluir métricas que permitan evaluar si:

- Los gastos están correctamente planificados y presupuestados.
- Se cumplen los objetivos de costos e ingresos.
- Se lleva a cabo una contabilidad precisa asociada a cada servicio.
- Se conoce el ROI de las inversiones TI.
- La organización TI funciona de manera "rentable".

La correcta elaboración de informes internos de gestión permite evaluar el rendimiento de la Gestión Financiera según los parámetros descritos y aporta información de vital importancia a la organización en su conjunto. Entre la documentación generada cabría destacar las siguientes:

- Resúmenes contables.
- Análisis de eficiencia de cada uno de los servicios TI.
- Planes de inversión TI basados en el histórico del negocio y en previsiones de evolución de la tecnología.
- Planes de reducción de costos por servicio.

7.15. Gestión de Informes de Servicio.

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 de 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 los siguientes:

- Ofrecer a la unidad de TSI, de forma periódica, un 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.

7.15.1. Proceso

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.

7.15.1.1. Recopilación de datos

Los sistemas TI deben ser capaces de registrar, manipular y procesar los datos. Es por ello imprescindible que desde el mismo inicio del proceso de recogida de datos para la elaboración de informes se seleccionen y filtren 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 se debe pensar que los datos sobran, es por ello que no será necesario hacer un registro de todos ellos ya que el costo de la recopilación y preparación de los datos para su posterior análisis y proceso puede ser extremadamente alto, además de ser una tarea que requiere una cantidad enorme de recursos, tanto tecnológicos como humanos.

7.15.1.2. Análisis de datos

Una vez recopilados los datos necesarios se precisa 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 realizar.

Durante el proceso y análisis de los datos se deben destacar aquellos que han tenido un impacto apreciable en el pasado y puedan también tener un impacto en el futuro. Los datos no son sólo una fuente necesaria para tomar acciones correctivas sino también pueden ser de utilidad para futuras decisiones estratégicas.

Durante el proceso de análisis se deben evaluar a su vez la calidad y cantidad de los datos corregidos y proponer así los cambios necesarios para asegurar que se dispone de la información esencial para evaluar la calidad y rendimiento de los servicios TI prestados.

7.15.1.3. Generar documentación

Después de procesar y analizar toda la información recopilada es momento de darle forma a través de informes y así proceder a su comunicación al 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 abstrusos 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 Factores Críticos de Éxito y Key Performance Indicators (KPI).
- **Personal técnico:** necesita información que les permita mejorar aspectos operativos en la prestación de servicio TI.

7.16. Mesa de Ayuda.

La Mesa de Ayuda, será el punto de contacto entre los usuarios que necesiten asistencia, y quienes les darán soporte en el uso de los servicios que se brinden. Además de monitorear estos servicios asegurándose de que se cumpla con los niveles de servicio acordados y ser la puerta de ingreso de las incidencias que ocurran durante la entrega de algún servicio. Está compuesta por personas que recogerán todo tipo de solicitudes e incidentes y que tienen la capacidad técnica para dar respuesta a cualquier pregunta o queja y derivarla a quien corresponda de ser necesario.

La Mesa de Ayuda es la encargada de recibir las solicitudes de los usuarios, y dar una respuesta inicial a problemas que se puedan presentar en los servicios de TI, además de coordinar a las empresas de apoyo externas en la resolución de las inquietudes de los usuarios. El Control de Acuerdos de Niveles de Servicio es un punto primordial para esta función. La Mesa de Ayuda proporciona valor a la organización dado que ella:

- Identifica y reduce los costos de mantener la infraestructura de soporte e informática.
- Soporta la integración y el Manejo de Cambios a lo largo de los límites del negocio, tecnología y procesos.
- Reduce costos con el uso eficiente de recursos y tecnología.
- Ayuda a asegurar la satisfacción del usuario.

Para un correcto desarrollo del negocio es primordial que los usuarios perciban que están recibiendo una atención personalizada y ágil que les proporcione a su vez:

- Resolución rápida de las incidencias en el servicio.
- Recepción de las peticiones de servicio.
- Información sobre el cumplimiento de los SLAs.

Cuando un servicio se ha interrumpido, el objetivo de algunos procesos es restaurar el servicio. La Mesa de Ayuda es responsable de un evento de servicio de principio a fin. Mientras que otras funciones, tal como soporte de segunda y tercera línea, asistirán en la resolución, la Mesa de Ayuda en tanto retiene el control “administrativo” de la incidencia. Además, como ya se mencionó, será el único punto de contacto entre los usuarios, servicios de TI y organizaciones de soporte externas para todas las necesidades, preguntas, quejas, comentarios y cambios relacionados con TI.

El objetivo principal de la Mesa de Ayuda es servir de punto de contacto entre los usuarios y la gestión de servicios TI. Es decir, debe funcionar como punto central de todos los procesos de soporte al servicio y para ello será la encargada de ir:

- Registrando y monitorizando incidentes, colaborando con Control de Incidentes.
- Aplicando soluciones temporales a errores conocidos en colaboración con el Manejo de Problemas.

- Colaborando para asegurar la actualización de las bases de datos correspondientes.
- Gestionando cambios solicitados por los clientes mediante peticiones de servicio en colaboración con Manejo de Cambios y Control de Versiones.
- Dando soporte al negocio identificando nuevas oportunidades en sus contactos con usuarios y clientes:
 - Comunicándose con los usuarios acerca de sus llamadas de servicio.
 - Generando informes de gestión.

7.16.1. Actividades

Las principales actividades que realiza la Mesa de Ayuda, con el fin de cumplir con los objetivos y responsabilidades de esta función se basan en:

- Centralizar todos los procesos asociados a la Gestión TI, mediante la recepción y control de peticiones de servicio, incidentes, consultas y solicitudes de cambio.
- Restaurar el servicio normal, reduciendo el impacto para el negocio, dentro de los niveles de servicio convenidos y desde la prioridad del negocio.
- Hacer informes, comunicar y promover, facilitando el intercambio de información.
- Ofrecer valor a la organización.
- Desenvolverse como una función de estrategia que ayude a la identificación y disminución de los costos de propiedad, relacionados con el soporte de la infraestructura TI.
- Colaborar para obtener la satisfacción de los clientes a largo plazo y dar asistencia en la identificación de oportunidades de negocio.

7.16.1.1. Funciones de Mesa de Ayuda

Las funciones que deberá tener implementada la Mesa de Ayuda son las siguientes:

- Recibir llamadas, siendo el primer nexo con los usuarios.
- Registrar y seguir los incidentes y las quejas.
- Mantener a los clientes informados sobre alguna solicitud y su evolución, haciendo una evaluación inicial de las solicitudes, intentando resolverlas o remitiéndolas a la persona responsable que puede atenderlas.
- Monitorear los procedimientos relativos a SLAs
- Administrar el ciclo de vida de la demanda, incluyendo el cierre y la verificación de incidentes y solicitudes.
- Identificar los problemas.
- Cerrar los incidentes y confirmación con los clientes
- Proporcionar confirmación a los usuarios de que su solicitud ha sido aceptada y de su progreso.

7.16.1.2. Perfil para el centro de servicio al usuario

El perfil del Service Desk debe cumplir los siguientes criterios:

- El servicio debe estar orientado al cliente.
- Tener la capacidad para entender los objetivos del negocio y poder tomar las decisiones más adecuadas para el logro de los mismos.
- Aspirar a dar un servicio de primera categoría, orientado a una mejora continua.
- Usar expresiones que el usuario comprenda, saber escuchar de manera activa y ofrecer aportaciones precisas y necesarias.
- Debe conocer las diferentes tecnologías sobre las que se da el servicio.

7.16.2. Control

La medida básica para el control de la Mesa de Ayuda es la satisfacción del cliente, aunque ésta no sea responsabilidad exclusiva de ella. Las métricas deben estar bien definidas para que midan el rendimiento de la Mesa de Ayuda y la apreciación que los usuarios tienen de ésta. En los informes de control se debe considerar:

- Tiempo medio de respuesta a peticiones e incidencias
- Porcentaje de incidentes cerrados en primera línea de soporte.
- Porcentaje de consultas atendidas en primera instancia.
- Análisis estadísticos de tiempos de resolución de incidentes clasificados por urgencia e impacto.
- Cumplimiento de los SLAs.
- Cantidad de llamadas gestionadas por cada persona de la Mesa de Ayuda.
- Grado de satisfacción del cliente mediante el uso de encuestas que evalúen la percepción del cliente respecto a los servicios prestados.

7.16.2.1. Informes de Control

Para el Control del funcionamiento de la Mesa de Ayuda, y para que ella sea un aporte real a la organización de su gestión se deberán generar informes con la frecuencia que se indica, de manera de que la gestión de ésta ayude a brindar un mejor servicio. Los informes son los que se detallan a continuación:

7.16.2.1.1. Informes semanales

- Disponibilidad del servicio.
- Áreas de los incidentes más significativos:
 - Donde ocurren con mayor frecuencia.
 - Exigen más tiempo de ocupación personal.
 - Tardan más tiempo en resolverse.
- Incidentes relacionados que generan la necesidad de crear registros de problemas.
- Errores conocidos y los cambios que sean necesarios.
- Pérdidas de servicio.
- Informes de satisfacción de usuario.
- Tendencias que afectan al servicio y/o negocio.
- Cargas de trabajo personal.

7.16.2.1.2. Informes mensuales

- Disponibilidad del servicio.
- Rendimiento general, logro de objetivos y análisis de tendencias
- Apreciaciones y niveles de satisfacción de clientes.
- Requerimientos de formación y entrenamiento de los usuarios.
- Rendimiento del personal de soporte y externo.

7.16.2.1.3. Análisis de satisfacción

- Si el centro de servicio al usuario está cumpliendo correctamente sus funciones, el usuario percibirá de forma positiva esta apreciación
- La encuesta de satisfacción permite monitorizar la percepción y las esperanzas del usuario, para ello es necesario:
 - Limitar el alcance de la encuesta
 - Concretar la muestra del público objetivo
 - Hacer las preguntas con claridad
 - Realizar una encuesta fácil de completar
 - Hacer la encuesta regularmente o cada vez que se crea necesario
 - Publicar los resultados para darlos a conocer
 - Seguir con fidelidad los resultados de la encuesta
 - Transformar los resultados de la encuesta en acciones.

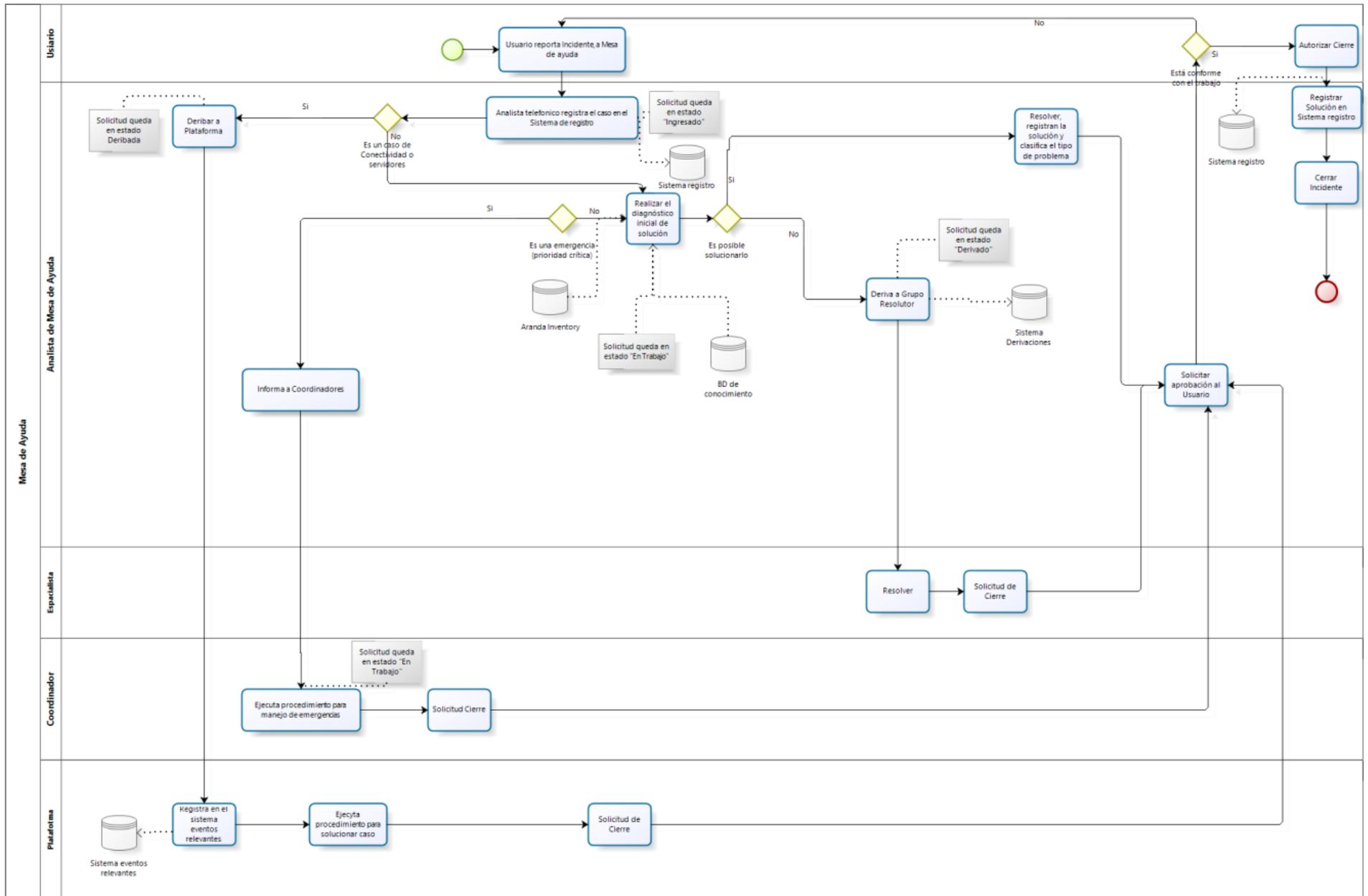


Figura 28. Diagrama BPMN del funcionamiento de Mesa de Ayuda. Fuente: Elaboración Propia.

8. CONCLUSIONES

Tras la realización de este proyecto de título tanto el objetivo general como los objetivos específicos se han logrado. Es así que se ha conseguido generar un modelo de gestión de la calidad que se adecúe a las características propias de la unidad de Tecnologías y Sistemas de Información de la Compañía Siderúrgica Huachipato, a partir de los modelos de gestión existentes para el área informática, de los que se muestran sus características y las comparaciones entre estos. El modelo generado es el que se describe en el capítulo 7 de este proyecto.

A lo largo del proyecto se ha analizado el estado de implementación de los procesos en la unidad de TSI, considerando los procesos y metodología de trabajo de la unidad. Es así que algunos de estos fueron modificados o creados, los que se adaptaron a la forma de trabajo de la unidad.

Con la implementación de este modelo se ha avanzado para que la unidad de TSI mejore hacia la gestión de calidad de sus procesos, y de los servicios que brinda a los demás departamentos de CAP Acero, de manera que los alinee con las necesidades y objetivos de la empresa. Además de reducir costos al mejorar la productividad, reduciendo trabajo innecesario o la utilización más eficiente de los recursos. Esto se puede notar en que con este proyecto se ha logrado:

- Formalizar y estandarizar, delimitando responsabilidades, los procesos de la unidad de TSI, facilitando así que el personal trabaje de forma conjunta en la entrega y el soporte de los servicios, alineando los servicios de TI con los objetivos y políticas de CAP Acero.
- Generar sistemas de trabajos metodológicos e integrados, para los procesos de la unidad de TSI, orientados a los usuarios, y teniendo siempre una alineación con el negocio.
- Avanzar en pos de la gestión de calidad.
- Mejorar la comunicación interna y externa, permitiendo un seguimiento continuo de resultados.
- Proporcionar información del funcionamiento de la unidad de TSI a la dirección de CAP Acero mediante los informes que surgen a consecuencia del control de los diferentes procesos, como es el caso de la gestión financiera.
- Mejorar la calidad y fiabilidad de los servicios que la unidad de TSI proporciona a los usuarios de los sistemas. Lo que conlleva una mayor satisfacción del usuario.
- Incremento de la productividad y eficacia, reduciendo riesgos y costos, ya que se cuenta con procedimientos estandarizados y de público conocimiento al interior de la unidad, donde cada empleado tiene un rol y responsabilidades debidamente asignadas.

La ejecución de este proyecto de título no debe considerarse como un proyecto meramente relativo a las tecnologías de información, sino como un proyecto donde se tienen varios factores críticos de éxito, como son:

- Los procesos serán definidos, para luego ser soportados por las herramientas. No se debe considerar que las herramientas que soportan la infraestructura de TI deben dar lugar a

los procedimientos, pues las herramientas deben ser una ayuda a los procesos, no una condicionante.

- Es importante que las implementaciones de procesos o cambios de estos sean de forma gradual y realista.
- El análisis e investigación de los procesos y como gestionarlos. Para esto es imprescindible:
 - Realizar un diagnóstico de la situación actual.
 - Definir un objetivo y estrategia para lograrlo.
 - Realizar un plan de trabajo y seguimiento.
- La definición, monitoreo y control de los SLAs es un punto clave para garantizar la medición de resultados y realizar una mejora continua de los servicios.
- Las personas que intervienen en los procesos deben verse implicadas y encontrarse en conocimiento de los procesos de la implementación del modelo. Esto es vital para evitar fracasos durante la implementación. La Formación del personal debe acompañar o, más aún, preceder a la implantación de cualquier cambio que se quiera implementar. La Comunicación de los logros alcanzados es esencial.

Como conclusión final de este proyecto de título se mencionarán algunos de los problemas encontrados para la implantación de los procesos del modelo y los beneficios que se derivan de la implantación de cada uno de estos.

8.1. Problemas encontrados en la implementación

Las principales dificultades que se encuentran en la implantación de un proyecto de TI es el poco compromiso de la dirección. Esta es una dificultad común para la implantación de todos los procesos de TI. En el caso concreto de CAP Acero, esto no ha sido un inconveniente considerable, ya que la dirección, tanto de CAP Acero como de TSI, estaban muy involucradas y conocían los beneficios de implantar un modelo de gestión de calidad.

Otra dificultad común es la resistencia al cambio del personal. Esta reticencia al cambio y/o a las modificaciones es intrínseca al ser humano, lo que dificulta la implantación de mejoras. Ya que los usuarios tienden a continuar realizando las tareas como lo hacían antes de implementar el cambio o, ante un incidente o duda, intentan solucionarlos por su cuenta o buscar alternativas.

8.2. Beneficios encontrados

Se han obtenido los siguientes beneficios:

- Mejorar la utilización de recursos.
- Reducir las tareas repetitivas y eliminar tareas redundadas.
- Mejorar los plazos de entrega y el tiempo en el desarrollo de un proyecto.
- Mejorar la disponibilidad, confianza y seguridad de los servicios TI de misión crítica
- Justificar el costo de la calidad de servicio.
- Proporcionar servicios que se adecuen a las necesidades del negocio del cliente o usuario.
- Integrar procesos centrales.

- Documentar y comunicar roles y responsabilidades en el suministro del servicio.
- Aprender de la experiencia previa.
- Proporcionar indicadores de rendimiento demostrables.

BIBLIOGRAFÍA.

1. ALVAREZ, Raul. ISO 20000: ¿Qué deben hacer las organizaciones?. Revista a+. 8:140-143. Marzo, 2007.
2. ALVAREZ, Raul. ISO 20000: ¿Qué es?. Revista a+. 7:142-144. Febrero, 2007.
3. Avila, J. Normas internacionales ISO 9000, 14000, 18000 [en línea] <www.itescam.edu.mx/principal/syllabus/fpdb/recursos/r82797> [Consultado: 06 de julio de 2012].
4. BAUSELA HERRERAS E., La Docencia a través de la Investigación-Acción, [En línea] <http://www.une.edu.ve/uneweb2005/servicio_comunitario/investigacion-accion.pdf> Consulta: 03 de abril de 2012].
5. BLANCO Ariza, Ana. Gestión aplicada a la tecnología informática. Revista Desarrollo Gerencial. 2(2):58-69. Mayo, 2010.
6. BMC Software. Gestión de Eventos e Impacto en el Servicio: un paso fundamental para la implementación del modelo ITIL [en línea] <apps.bmc.com/products/documents/49/63/64963/64963.pdf> [Consultado: 06 de Junio de 2012].
7. CEÑIZALES Sales, Ricardo. ITIL & ISO 20000. Revista a+ (27): 58-59, Noviembre, 2008.
8. COMPAÑÍA SIDERÚRGICA HUACHIPATO. Memoria Anual 2011. 2011.
9. CONSOLIDACIÓN DE LA POLÍTICA NACIONAL DE INFORMACIÓN GEOGRÁFICA Y LA INFRAESTRUCTURA COLOMBIANA DE DATOS ESPACIALES – ICDE, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION [en línea] <http://www.icde.org.co/web/guest/enlaces?p_p_id=101_INSTANCE_1kUv&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_101_INSTANCE_1kUv_advancedSearch=false&_101_INSTANCE_1kUv_andOperator=true&cur=4> [Consultado 06 de Julio de 2012].
10. CORLETTI, Alejandro y DE ALBA, Carmen. ¿ISO 20000 o ISO 27000?. Revista a+. 16:158-161. Noviembre, 2007.
11. DATATI. CMMI ACQ: CMMI for Acquisition [en línea] <<http://www.datati.es/?p=852>> [Consultado: 06 de Junio de 2012].
12. DUGMORE, Jenny y TAYLOR, Sharon. ITIL V3 and ISO/IEC 20000. 2008.
13. E TURBITT, KEN. ISO 20000:¿qué deben hacer las organizaciones? [en línea] <documents.bmc.com/products/documents/49/67/64967/64967.pdf> [Consultado: 06 de Junio de 2012].
14. EDER, E, Gestión de Servicios de Tecnologías de la Información [en línea] <<http://ensayos.com/imprimir/Gesti%C3%B3n-De-Servicios-De-Tecnolog%C3%ADas/34744.html>> [Consultado: 06 de Junio de 2012].

15. EDUTEKA. EstandaresTIC [en línea]
<http://www.eduteka.org/directorio/index.php?t=sub_pages&cat=231>. Fundación Gabriel Piedrahita Uribe, Cali, Colombia. [Consultado: 06 de Junio de 2012].
16. FLORES Barrios, Leonardo, “et al”. Evaluación del impacto de los sistemas de gestión de seguridad de la información bajo la serie ISO/IEC 27001 en empresas de la ciudad de Tuxpan, Veracruz. Revista de Alta Tecnología y la Sociedad. 5(1): 44-49, 2011.
17. Gobierno de La Rioja. Modelo de Excelencia EFQM. La Rioja, Argentina.
18. GONZÁLEZ, Héctor. Gestión de Servicios de TI ITIL e ISO/IEC 20000. EN: Cómo lograr una implementación exitosa de ITIL/ISO 20000. Bogotá, Colombia. Mayo, 2011
19. HARDLY Gary, HESCHL Jimmy. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, Estados Unidos, 2008. p. 23-129.
20. HRABINSKY, Sergio. 2006. De las mejores prácticas de Gestión de IT a la certificación. EN: EXPOCOMM: Octubre de 2006. La Rural de Palermo, Buenos Aires, Argentina.
21. IBEROSYS. SM.ITILV3 Fundamentos de la Gestión del Servicio de TI con ITIL Versión 3. [en línea] <www.iberosys.net> [Consultado: 06 de Junio de 2012].
22. International Organization for Standardization. Information technology - Security techniques - Code of practice for information security management. ISO/IEC 17799. 2005.
23. ITNEWS. ITIL para pymes. [en línea] <http://itnews.ec/documentos/doc_itolpyme.pdf> [Consultado: 06 de Junio de 2012].
24. Laboratorio Nacional de Calidad del Software, Guía de Gestión de Servicios en ISO/IEC 20000 y Relación entre CMMI e ITIL. España. Marzo, 2010.
25. Lobos A., Daniela, Baquinzay, Manuel, Bustos A., María Soledad Gestión de Servicios TIC (Tecnología de la información y las comunicaciones) – ITIL (Biblioteca de Infraestructura de Tecnologías de Información). REVISTA DE DIVULGACIÓN CIENTÍFICA DE CIENCIA Y TECNOLOGÍA DE LA UNCa. 1(1) 13-26, Diciembre 2008
26. LOBOS Anfuso, Daniela, BAQUINZAY, Daniel y BUSTOS Aguilar, María. Gestión de servicios TIC (Tecnologías de la información y las comunicaciones)- ITIL (Biblioteca de Infraestructura de Tecnologías de Información). Revista de divulgación científica de ciencia y tecnología de la UNCa. 1(1):13-26. Diciembre, 2008.
27. López Neira, Agustín, Ruiz Spohr, Javier. Norma ISO 27000. España 2005.
28. MOREY, Enrique. Evolución de los modelos CMMI. [en línea] <www.euskadinnova.net/documentos/1086.aspx> [Consultado: 06 de Junio de 2012].
29. MUÑOZ Perrián Ingrid y GÓMEZ Arenas Liliana. Vista ampliada para Gerencia de Proyectos usando mejores prácticas del PMBok cuarta edición y CMMI-SVC V.1.2 nivel de capacidad o madurez 2. Revista Sistemas y Telemática. 9(16): 73-90, 2011.
30. OCAMPO S., Carlos, MORENO Laverde, Ricardo y MILENA Caicedo, Sandra. Implementación de modelo de procesos de gestión de servicios con ITIL (Information Technology Infrastructure Library). Revista Scientia et Technica. 15(41): 215-220, Mayo de 2009.
31. OSORIO, Jorge. ISO/IEC 20000: de las mejores prácticas TI a la norma. EN: Sociedad de la Información en Aragón. Zaragoza, España. Noviembre, 2009.

32. Ramírez Bravo, Pía y Donoso Jaurés Felipe. Metodología ITIL Descripción, Funcionamiento y Aplicaciones. Seminario de título. Santiago, Chile. Universidad de Chile, Facultad de Ciencias Económicas y Administrativas, Julio de 2006. 99h.
33. RIVERA, Luis. ITIL & ISO 20000. Revista a+ (27): 72-74, Noviembre, 2008.
34. SUAREZ, Bismark. Norma ISO/IEC 20000 para la gestión de servicios de TI. [en línea] <http://www.inteli.com.mx/articulos%20I-News/09_BS_QueeslaISO20kv2.pdf > [Consultado: 06 de Junio de 2012].
35. TAYLOR, Sharon y TURBITT, Ken. ITIL versión 3: un modelo adaptado a la creciente importancia de la gestión de servicios de negocio. [en línea] <documents.bmc.com/products/documents/74/14/87414/87414.pdf > [Consultado: 06 de Junio de 2012].
36. TURBITT, Ken. ISO 20000:¿qué deben hacer las organizaciones? [en línea] <documents.bmc.com/products/documents/49/67/64967/64967.pdf> [Consultado: 06 de Junio de 2012].
37. TUYA Dextre, Jesús. Implementación de ITIL. [en línea] <<http://itilunfv.net16.net/implementacion.php>> [Consultado: 06 de Junio de 2012].
38. Unidad de Tecnología y Sistemas de información CSH. Roles y Funciones por Cargo TSI. Talcahuano, Chile. Mayo 2012.
39. VALDÉS GÓMEZ, daniel. Balanced Scorecard.
40. RIVERA, Luis. ITIL & ISO 20000. Revista a+ (27): 72-74, Noviembre, 2008.
41. GUINDEL S., Esmeralda CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA. Tesis para optar al grado de INGENIERO TÉCNICO DE INFORMÁTICA DE GESTIÓN. Madrid, España: UNIVERSIDAD CARLOS III DE MADRID, 2009. 239 p.
42. Garzas Javier. ¿ISO/IEC 9000, 12207,27001 o 20000?[en línea] <<http://www.javiergarzas.com/2010/05/iso9000-iso15504-iso12207-iso27001-iso20000.html>> [Consultado: 06 de Junio de 2012].
43. Oocities. ISO 9000 Norma mexicana de control de calidad. [En línea] <<http://www.oocities.org/iaqtmx/ISO9000.htm>> [Consultado: 06 de Junio de 2012].
44. HUERTA José. Administración y Seguridad en Redes Unidad III.[En línea] <<http://huertahernandez.wikispaces.com/Administracion+y+Seguridad+en+Redes+Unidad+III>> [Consultado: 06 de Junio de 2012].
45. LÓPEZ, Agustín y RUIZ, JAVIER. [en línea] <ISO 27000 <http://www.iso27000.es/iso27000.html>> [Consultado: 06 de Junio de 2012]
46. BMC Software. Gestión de Eventos e Impacto en el Servicio: un paso fundamental para la implementación del modelo ITIL [en línea] <apps.bmc.com/products/documents/49/63/64963/64963.pdf > [Consultado: 06 de Junio de 2012].
47. ITNEWS. ITIL para pymes. [en línea] <http://itnews.ec/documentos/doc_itilpyme.pdf> [Consultado: 06 de Junio de 2012].
48. Osiatis. ¿Qué es ITIL? [En línea] <http://www.osiatis.es/formacion/formacion_itil.php>. [Consultado: 06 de Junio de 2012].

49. OCAMPO S., Carlos, MORENO Laverde, Ricardo y MILENA Caicedo, Sandra.
Implementación de modelo de procesos de gestión de servicios con ITIL (Information Technology Infrastructure Library). Revista Scientia et Technica. 15(41): 215-220, Mayo de 2009.