

# Recomendaciones para la Gestión de Incidentes de TI

Verny Mora, Paulo Viales, Julio Córdoba

Escuela de Ingeniería,  
Universidad Latinoamericana de Ciencia y Tecnología,  
ULACIT, Urbanización Tournón, 10235-1000  
San José, Costa Rica  
vmor80@hotmail.com, pviales@gmail.com, jcordobar022@ulacit.ed.cr  
<http://www.ulacit.ac.cr>

**Abstract.** La gestión de incidentes es uno de los procesos más evidentes en el manejo de los servicios de TI, por el cual los usuarios interactúan con el departamento de TI. En este artículo se analizarán a fondo las actividades que proponen tres de los marcos metodológicos, más utilizados en las empresas y se recomendará una guía que asegure el éxito en la gestión de incidentes, basada en las mejores actividades que proponen los tres límites.

**Keywords:** Gestión de Incidencias, ITIL, COBIT, CMMi, buenas prácticas.

## 1 Introducción

La buena gestión de los servicios de TI se basa en cinco objetivos principales, [1] como lo son: proporcionar una adecuada gestión de la calidad, aumentar la eficiencia, alinear los procesos de negocio y la infraestructura de TI, reducir los riesgos y por último, generar negocio. Las buenas prácticas, marcos de trabajo, modelos de madurez y normas tales como: COBIT, ITIL, CMMi e ISO, brindan los lineamientos que fomentan las mejores prácticas necesarias para alcanzar dichos objetivos. El proceso de gestión de incidentes de servicios brindados por TI es uno de los puntos a tratar de mayor importancia para las organizaciones, su buena gestión conduce a la empresa a utilizar sus recursos de una forma más eficiente, carecer de esta, conlleva a la improvisación. El manejo de incidentes ayuda a mantener la calidad de servicio y a la disponibilidad, con lo que mejora la eficiencia y la duración de los procesos.

(Bauset-Carbonell & Rodenes-Adam, 2013) destacan que la experiencia ha demostrado que la calidad en el nivel de servicio, no se puede obtener únicamente, con fuertes inversiones en tecnología o personal altamente cualificado, sino que es el resultado de una buena gestión y planificación a nivel empresarial. Para ello, es necesario implantar un sistema de gestión de servicios de TI (SGSIT), potenciar la labor de los gestores y utilizar métricas para el seguimiento y control del progreso.

El manejo de incidentes es uno de los procesos más evidentes, en la dirección de los servicios de TI (Persse, 2013) no solamente por ser uno de los caminos por el cual, los usuarios interactúan más con el departamento de TI, sino también, debido a que va a ser un espejo de la calidad del departamento mismo.

Actualmente el negocio y la información van de la mano, sin la adecuada gestión de incidentes de servicios dentro de las empresas, puede materializarse riesgos que afectan de manera directa, tanto a clientes internos como externos de la empresa. En Costa Rica existe un vacío por parte de algunas empresas que han optado por la no aplicación de las mejores prácticas según sus necesidades, ya sea por desconocimiento o por decisión de no brindar la debida importancia al tema, pero la experiencia ha demostrado que la debida gestión de incidentes que detecte, clasifique, escale, solucione y cierre dichos incidentes mejora los procesos y la efectividad de la empresa.

Debido a la situación actual de las empresas y la problemática que tienen en cuanto a la gestión de incidentes, es por lo que se desea desarrollar un artículo que sirva de guía, para los procesos de gestión de incidentes de los servicios brindados por TI, en empresas costarricenses, y mejorar los porcentajes de efectividad, en resolución de incidentes, en un plazo no mayor a un año de la puesta en marcha.

Para lograr el cometido se realiza el estudio de las principales buenas prácticas como lo son ITIL V3 2011, COBIT 5 y CMMi, para servicios en lo que a materia de gestión de incidentes se refiere. Para lograr esto, será importante apoyarse en investigaciones a nivel nacional y acerca de casos de éxito que tengan que ver con este tema, con el fin de realizar su análisis y determinar qué se puede extraer de ellos. Basado en la información recolectada, se genera un proceso y una lista de recomendaciones que sirvan de guía, para realizar el proceso de gestión de incidentes en servicios de TI en la empresa.

Basados en el análisis profundo se brindarán recomendaciones para manejar los departamentos de TI en materia de gestión de incidentes para los servicios brindados, y lograr una mejora significativa en los porcentajes de resolución de incidentes.

## 2 Marco Teórico

En el marco teórico del estudio planteado, se tomarán como referencia primaria únicamente las buenas prácticas de gestión de incidentes contenidas en Cobit 5, ITIL v3 2011 y CMMI, para servicios.

El tema se inicia con el manual de buenas prácticas (IT Governance Institute, 2013) Cobit, en su área de Gestión y en el dominio llamado Entrega, Servicio y Soporte, posee su proceso llamado Gestionar Peticiones e Incidentes de Servicio, los cuales se describen como el proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de contratiempo. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes, además contiene una declaración del propósito del proceso, en el cual sí indica, que se debe lo-

gar una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

El proceso apoya la consecución de un conjunto de principales metas de TI, las cuales se subdividen en la parte de Riesgos de negocio relacionados con las TI gestionadas y a la entrega de servicios de TI, de acuerdo a los requisitos del negocio(O'Toole, 2015).

Además, entre sus objetivos y métricas se tienen los servicios relacionados con TI, los cuales están disponibles para ser utilizados, los incidentes y peticiones son resueltos, según los niveles de servicio acordados y la satisfacción del usuario

Como prácticas clave de gestión se tienen los subprocesos (Brand & Boonen, 2004), en los cuales se habla de definir esquemas de clasificación de incidentes y peticiones de servicio, registrar, clasificar y priorizar peticiones e incidentes, verificar, aprobar y resolver peticiones de servicio. Investigar, diagnosticar y localizar incidentes, resolver y recuperarse de incidentes, cerrar peticiones de servicio e incidentes y el seguir el estado y emitir informes.

Para el subproceso siguiente, se deben definir esquemas y modelos de clasificación de incidentes y peticiones de servicio y tiene como principales actividades, definir esquemas de clasificación y priorización de incidentes , reclamos y criterios de servicio, para el registro de problemas,y además, asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizar, análisis de tendencias. Definir modelos de incidentes para errores conocidos, con el fin de facilitar su resolución eficiente y efectiva, definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar, precisar reglas y procedimientos de escalado de incidentes, especialmente, para incidentes importantes e incidentes de seguridad y por último, fijar fuentes de conocimiento de incidentes e instancia y su uso.

Para el subproceso identificar, registrar y clasificar peticiones de servicio e incidentes o asignar una prioridad, según la criticidad del negocio y los acuerdos de servicio, esta a su vez tiene como actividades principales; registrar todos los riesgos y peticiones de servicio, toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo,que posibilite el análisis de tendencias, clasificar incidentes y peticiones de servicio e identifique el tipo y categoría,y priorizar peticiones de servicio e incidentes, según la definición de impacto en el negocio del ANS y la urgencia.

En este subproceso, se debe seleccionar los procedimientos adecuados para peticiones y verificar que estas cumplen los criterios de solicitud definidos, y como actividades, se tienen que verificar los derechos para realizar peticiones de servicio, con los cuales, se usen cuando sea posible un flujo de proceso predefinido y cambios estándares. Esto, para obtener aprobación financiera, funcional o firmada, si se requiere , que cambien los estándares acordados y completen las solicitudes. Para ello, se sigue el procedimiento del reclamo seleccionado y se utiliza, cuando sea posible, menús automáticos de autoayuda y modelos de diligencias predefinidas, para los elementos solicitados frecuentemente.

Terminado el paso anterior, se debe identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución, este posee actividades tales como el identificar y describir síntomas relevantes, para establecer las causas más probables de los incidentes. Hacer referencia a los recursos de conocimiento disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes), registrar un nuevo problema si está relacionado o error conocido, que aún no exista y si el incidente satisface los criterios acordados para registro de problemas, se debe asignarlas a funciones especialistas, si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado.

Por consiguiente, hay que Documentar, solicitar y probar las soluciones identificadas o temporales, asimismo, ejecutar acciones de recuperación para restaurar el servicio TI relacionado, el cual tiene como actividades, el seleccionar y aplicar las resoluciones de incidentes más apropiadas (soluciones provisionales y/o soluciones permanentes), registrar si se usaron soluciones temporales para resolver los incidentes, ejecutar acciones de recuperación, si se requieren, documentar la resolución del incidente y evaluar, si se pudiera usar como una fuente de conocimiento en el futuro.

A continuación, se verifica la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones; y cierre, las actividades de este apartado corresponden a tratar con los usuarios afectados (si lo han acordado) que la petición de servicio ha sido completada o el incidente ha sido resuelto de manera satisfactoria, cerrar peticiones de servicio e incidentes.

Por último, en el subproceso se debe hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua y las actividades de supervisar. Para lograrlo hay que hacer un seguimiento del escalado de incidentes, resoluciones y de los procedimientos de gestión de resoluciones; por lo que se encaminará hacia la resolución o cumplimentación, identificar la información para las partes interesadas y sus necesidades de datos o informes. Detallar la frecuencia y el medio para informarles, analizar incidentes y peticiones de servicio por categoría y tipo para establecer tendencias e registrar patrones de asuntos recurrentes, infracciones de ANSS o ineficiencias. Utilizar la información como entrada a la planificación de la mejora continua, de producir y distribuir informes de tiempo o proporcionar acceso controlado a datos en línea.

En lo que respecta a la colección de buenas prácticas CMMI para Servicios<sup>1</sup>, el cual proporciona guías para aplicar buenas prácticas en organizaciones proveedoras de servicios.

Las buenas prácticas del modelo se centran en las actividades para proveer servicios de calidad a clientes y usuarios finales. CMMI-SVC (Forrester, Buteau, & Shrum, 2011) integra conjuntos de conocimientos que son esenciales para proveedores de servicios. Estos modelos son desarrollados por equipos de producto con miembros procedentes de la industria, el gobierno, y el Instituto de Ingeniería de Software (SEI). En el apartado específico de incidentes, CMMi aclara

---

<sup>1</sup> Modelo de Capacidad y Madurez®

en su capítulo de resolución y prevención de incidencias el cómo se debería de realizar el proceso. Con este capítulo se busca asegurar que las incidencias en el servicio se resuelvan a tiempo y de forma eficaz y que las incidencias en el servicio se eviten según sea apropiado (Kenett & Baker, 2010). Primero que nada es importante definir que para CMMi: Las incidencias son eventos que, si no se tratan, pueden llegar a causar el incumplimiento de los compromisos de servicio adoptados por la organización proveedora. Por tanto, la empresa proveedora de servicios, debería tratar las incidencias de una manera oportuna y eficaz, conforme a los términos del acuerdo establecido. Es importante también identificar y tratar las causas subyacentes que son la condición o el evento, el cual contribuye a que una o más incidencias ocurran. No todas las causas subyacentes tienen como resultado incidencias de forma inmediata.

Las prácticas específicas que propone CMMI (Forrester et al., 2011) se categorizan en tres principales objetivos, la primera Preparar la resolución y prevención de incidencias, en esta se lleva a cabo la preparación de la resolución y prevención de incidencias. Se inicia por establecer un enfoque para la resolución y prevención de incidencias, en el cual se describen las funciones organizativas implicadas en la resolución y prevención de incidencias, los procedimientos empleados, las herramientas de soporte utilizadas, y la asignación de responsabilidades durante el ciclo de vida de las incidencias.

Entre las subprácticas asociadas a este proceso se encuentran: Definir criterios para determinar qué es una incidencia, Definir categorías para las incidencias así como criterios para determinar a qué categorías pertenece cada incidencia, Describir cómo se asigna y transfiere la responsabilidad del procesamiento de las incidencias, Identificar uno o más mecanismos para que los clientes y usuarios finales puedan reportar incidencias, Definir métodos y adquirir herramientas a utilizar para la gestión de incidencias, Describir el modo de notificar a todos los clientes y usuarios finales relevantes que puedan estar afectados por una incidencia reportada, Definir criterios para determinar los niveles de gravedad y prioridad, Identificar requisitos en el acuerdo de servicio acerca del tiempo disponible que está definido para resolver las incidencias y Documentar los criterios que definen cuándo deberían cerrarse las incidencias. Seguido a esto se sugiere Establecer un sistema de gestión de incidencias para procesar y seguir la información sobre las incidencias. El mismo debe incluir funcionalidades para procesar y seguir la información sobre las incidencias. Se debería disponer de una colección de datos históricos que cubran incidencias tratadas, causas subyacentes de incidencias, enfoques conocidos para tratar incidencias, y soluciones temporales con objeto de dar soporte a la gestión de incidencias. (Mutafelija & Stromberg, 2008)

El segundo objetivo es Identificar, controlar, y tratar cada incidencia, el cual se centra gestionar las incidencias individuales a medida que ocurren con objeto de restaurar el servicio o de resolver las incidencias tan rápido como sea posible. Tratar incidencias puede incluir recopilar y analizar datos para buscar incidencias potenciales, o simplemente esperar a que los usuarios finales o los clientes reporten incidencias. Dentro de este objetivo entonces, espera Identi-

ficar y registrar la incidencia e información sobre ella, Identificando, Registrando y Categorizando las incidencias.

Luego se deben analizar los datos de cada incidencia para determinar un curso de acción. Este se centra en resolver las incidencias a medida que ocurren por medio de un curso de acción que sea suficientemente oportuno y eficaz como para cubrir las necesidades inmediatas de la petición de servicio. Para este como subprácticas se sugiere Analizar los datos sobre la incidencia, Determinar qué grupo es el más adecuado para tratar la incidencia y Planificar las acciones a realizar.

Como siguiente práctica se deberá resolver las incidencias, siguiendo el curso de acción determinado por el análisis de cada incidencia. Las subprácticas recomendadas son Tratar la incidencia utilizando el mejor curso de acción, Gestionar las acciones hasta que el impacto de la incidencia llegue a un nivel aceptable, Registrar las acciones y el resultado y Revisar las acciones realizadas que dieron como resultado cambios.

La siguiente recomendación es monitorizar el estado de las incidencias hasta su cierre, a lo largo de toda la vida de la incidencia, su estado debería registrarse, seguirse, escalarse según se necesite, y cerrarse. Las subprácticas recomendadas son documentar las acciones y monitorizar, Escalar las incidencias según se necesite, Revisar la resolución y confirmar los resultados con las partes interesadas relevantes y Cerrar las incidencias que cumplen los criterios de cierre.

Como última práctica dentro de este objetivo es Comunicar el estado de las incidencias, la comunicación con la persona que reportó la incidencia, y posiblemente con quienes se vean afectados por ésta, debería tenerse en cuenta a lo largo de toda la vida del registro de la incidencia en el sistema de gestión de incidencias.

Como tercer objetivo en CMMI (Forrester et al., 2011) se encuentra analizar y tratar las causas e impactos de las incidencias seleccionadas y se busca la reducción de este o la ocurrencia de incidencias futuras. Aquí mismo se manejan los términos causa subyacente y causa raíz. La primera práctica que se sugiere es Analizar las incidencias seleccionadas y a su vez las causas subyacentes. El propósito de realizar el análisis causal de las incidencias es determinar el mejor curso de acción para tratar incidencias en el futuro, de forma que sus impactos se minimicen con la mayor eficacia. Como subprácticas se encuentran Identificar las causas subyacentes de las incidencias, Registrar información sobre las causas subyacentes de una incidencia, Realizar los análisis causales con las personas responsables de realizar las tareas relacionadas y Determinar el mejor enfoque global para abordar las incidencias seleccionadas en el futuro.

La siguiente práctica es Establecer soluciones para responder a futuras incidencias, las subprácticas recomendadas son: Determinar cuál es el grupo más adecuado para establecer y mantener una solución reutilizable, Planificar y documentar la medida útil, Verificar y validar la solución disponible, para asegurar que trata la incidencia de forma eficaz y Comunicar a las partes interesadas relevantes la salida aprovechable. Por último se tiene la práctica de establecer y aplicar resultados, para reducir la ocurrencia de incidencias. Después de que el

análisis determine las causas subyacentes de las incidencias, si existen acciones a realizar, éstas se planifican y ejecutan. Planificar incluye determinar quién actuará, cuándo, y cómo. Como subpráctica se deberá determinar qué grupo es el más adecuado para tratar la causa subyacente.

ITIL por su lado, en su proceso llamado Operación del servicio, en el subproceso 4.2 Gestión de Incidentes (ITILv3, 2011) da las recomendaciones o buenas practicas para que el manejo de las incidencias sea exitoso.

ITIL maneja la gestión de incidentes dentro del ciclo de vida de la operación de servicio, en el mismo que brinda recomendaciones para el manejo de problemas (Persse, 2013).

Es importante tomar en cuenta el marco de buenas prácticas ITIL, para fortalecer la investigación y formar mejores criterios. ITIL abarca la gestión de incidentes en su capítulo de Operación de servicio. En la terminología de ITIL, un "incidente" se define como una interrupción no planificada de un servicio de TI o reducción de la calidad de un servicio de TI o un fracaso de un CI que aún no ha impactado un servicio de TI (por ejemplo fallo de un disco de un conjunto de espejos).

Gestión de incidencias es el proceso responsable de la gestión del ciclo de vida de todos los incidentes. Los incidentes pueden ser detectados por el personal técnico, reportados por las herramientas de monitoreo de eventos, comunicaciones de los usuarios (por lo general a través de un teléfono llamando al mostrador de servicio), o informado por terceros proveedores y socios. El propósito de la gestión de incidentes es restaurar la operación normal de servicio tan pronto como sea posible y minimizar el impacto adverso en las operaciones del negocio. Los proceso recomendados por para una correcta gestión de incidentes inician por la identificación del incidente, se define como detectarlo, priorizarlo y categorizarlo.

Como segundo paso, se debe registrar el incidente, todos deben ser registrados con su completa información para mantener un histórico completo del mismo, la información debería de incluir: número único de referencia, categoría, urgencia, impacto, prioridad, hora y fecha, nombre y/o ID de la persona que registró el incidente, método de la notificación, forma de contactar de vuelta, descripción de los síntomas, estado, problemas relacionados, Actividades para resolver el incidente, fecha de resolución, categoría de cierre y fecha de cierre. Si el proceso se pasa a otro grupo como redes o soporte nocturno, el proceso debe registro debe ser igual de riguroso. El tercer proceso, es la categorización de los incidentes, todas las empresas son únicas y la definición de categorías puede presentar sus particularidades, sin embargo, se brindan una técnica que puede ser usada para ayudar a las organizaciones a definir un completo set de categorías, siempre y cuando se arranque desde cero.

El cuarto proceso, será darle prioridad a los incidentes, lo cual va a ser importante para determinar cuándo y cómo el incidente va a ser manejado por el departamento recomendado. Por lo general las prioridades son determinadas tomando en cuenta la urgencia del incidente y en nivel de impacto en el nego-

cio, otras pueden ser el número de servicios impactados, el nivel de pérdida en finanzas, el efecto de reputación del negocio y regulaciones del estado o locales.

Como quinto proceso, se va a realizar un diagnóstico inicial, si el incidente es reportado via el departamento de servicio, comúnmente mientras se tiene todavía a la persona en el teléfono se trata de brindar un primer diagnóstico y ver si es posible solucionarlo en la llamada. Si por lo contrario no se pudo resolver, entonces el agente deberá informar al interesado sobre el proceder y darle un número de incidencia para que este le pueda dar seguimiento, luego podrá buscar una solución para el incidente. En este paso también va a ser importante que la persona encargada del soporte busque dentro de la base de datos de incidentes si el reportado se encuentra ahí y ver posibles soluciones o bien, como este fue resuelto anteriormente. Esto va a ayudar a evitar un proceso de investigación redundante, tratando de encontrarle solución a un incidente que previamente había sido resuelto.

Para el sexto se habla sobre una posibilidad de escalamiento del incidente, esta puede ser de forma funcional (Se requiere el apoyo de un especialista de más alto nivel para resolver el problema) o jerárquico (Se debe acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico).

En seguida se recomiendan como paso número siete la investigación y análisis del incidente, todos los grupos envueltos en el manejo de incidentes van a investigar y diagnosticar que anduvo mal para que se diera el incidente y deberán documentar todo incluyendo detalles o cualquier acción tomada para resolver el incidente. La investigación deberá de incluir: que fue lo que anduvo mal o que hizo mal el usuario, entender el orden de las cosas que se hicieron, confirmar el impacto del incidente, identificar si hubieron eventos que pudieron dispararse debido al incidente y especificación de búsquedas detalladas de conocimiento en busca de ocurrencias anteriores mediante la búsqueda de incidentes.

Como octavo paso se encuentra la resolución y recuperación, cuando la solución es encontrada deberá aplicarse y probarse, las acciones que deben realizarse y las personas que van a participar en la toma de las acciones de recuperación puede variar, dependiendo de la naturaleza de la avería, pero podría involucrar: pedirle al usuario hacer alguna(s) actividades, solucionarlo desde el equipo de soporte, solicitarle la solución a un grupo de especialistas, o solicitarle el servicio a un proveedor.

Para finalizar el proceso y como noveno paso se requiere el cierre del incidente, en este se debe comprobar que el incidente está solucionado y se le debe verificar esto con los usuarios. También se deberán validar procesos como: categorización (validar si la inicial es la correcta), encuesta satisfacción al cliente, documentación del incidente y verificar si el incidente es recurrente.

### 3 Análisis de Resultados

Tras realizar un proceso de comparación exhaustiva entre los capítulos de gestión de incidencias en ITIL, COBIT y CMMi para servicios, se ha obtenido un proceso de recomendaciones, para la gestión de incidencias, las cuales engloba las mejores prácticas de los marcos de referencia, antes descritos en todos sus procesos, mientras establece un camino para asegurar el éxito cuando se gestionan las incidencias en los servicios de las empresas.

Las mejores prácticas seleccionadas de ITIL, COBIT y CMMi; han sido clasificadas dentro de cuatro procesos, con nombres explicativos y concisos en su forma de operar, tal y como se especifica en la figura 1. Se inicia con un proceso de Definición de Políticas, que definirán los pasos iniciales y parámetros, que deberán estar establecidos antes de empezar con el proceso de gestión de incidentes, aquí será importante definir los procesos, tal y como se recomendarán en la guía. El segundo paso es el Registro de Incidentes, en el cual se nombran todas las actividades para registrar los incidentes. En seguida se explicará a fondo, el tercer proceso conocido como Resolución, en el mismo, se incluyen todos los pasos relacionados al aseguramiento de la resolución de las incidencias y para concluir con la fase final definida como Cierre, la que incluye todos los procedimientos relacionados. con el fin del incidente y las mejores prácticas para un exitoso cierre. Los procesos se explican en la figura descripción de procesos.

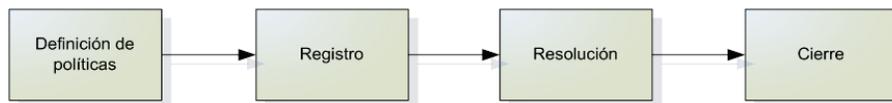


Fig. 1. Descripción de procesos

En el primer proceso, definido como planificación, se recomienda iniciar con la definición de los criterios para definir incidencias, actividad especificada tanto en ITIL como en CMMi. Parte importante en esta actividad es diferenciar entre un incidente y una solicitud de servicio, cada empresa debería de tener estos conceptos bien especificados. ITIL (ITILv3, 2011) recomienda señalar como incidente una interrupción no planificada de un servicio de TI o reducción de la calidad de un servicio de TI. Si bien las solicitudes de servicio serán reportadas al igual que las incidencias a la mesa de servicio, la diferencia es que estas no van a representar una interrupción sobre un servicio.

Como parte de la planificación misma, se tendrá como actividad el definir las categorías a utilizar para así luego, cuando un incidente llegue, este pueda ser categorizado. Tanto ITIL como CMMi brindan recomendaciones para realizar un catálogo de categorías, se recomienda utilizar los pasos sugeridos por ITIL (ITILv3, 2011) debido a la facilidad con la cual se va a lograr como resultado no solamente un buen catálogo de categorías, sino que también y más importante,

algo que se acople a las necesidades de la empresa en la cual se quiere implementar el proceso de gestión de incidentes. Para lograr esto se debe de crear una lluvia de ideas entre las personas involucradas en el soporte, supervisores de manejo de incidentes y administradores de problemas internos en la empresa. Esta reunión deberá dejar como resultado una lista preliminar de categorías que idealmente se pondrán a prueba por un periodo corto de tiempo. Dentro de la técnica se sugiere también hacer un análisis de incidencias reportadas durante un periodo de tiempo, esto permitirá analizar a fondo si el catalogo definido inicialmente cuenta o no con las categorías necesarias en la empresa. Después del periodo de prueba se tendrá un catálogo con las categorías de alto nivel o más usadas. En base a estas se pueden crear las categorías de bajo nivel, siempre y cuando estas vayan a ser necesarias. El catalogo definido debería pasar a análisis cada 3 o 5 meses, para así lograr tenerlas actualizadas a las necesidades del negocio.

En seguida se debe describir como se asigna la responsabilidad de una incidencia a un grupo de soporte, actividad que está bien especificada tanto en COBIT como en CMMi (Forrester et al., 2011), sin embargo, en la segunda se especifican las actividades que deben ser asignadas, lo que ayuda a agilizar la solución de la incidencia. La descripción debería incluir al menos: quién es responsable de monitorizar y seguir el estado de las incidencias, escalado y como se asigna y se transfiere la responsabilidad de todos los elementos. Si bien, CMMi (Forrester et al., 2011) menciona el definir como se asignan las tareas subyacentes, en este artículo se omite debido a que estas deben ser tratadas en un capítulo aparte de gestión de problemas. Los incidentes pueden presentarse en forma paralela y será aquí donde las prioridades tienen que tomar relevancia. Para esto se tienen que definir las prioridades y gravedad de los incidentes. Esta es una práctica que se encuentra en los tres manuales estudiados. En este caso específico la recomendación se basa en tomar lo mejor de los tres y crear una actividad que ayude a clasificar los incidentes. CMMi recomienda usar escalas numéricas al de 1-5, bastante similar a lo que propone ITIL, en este caso es importante usar números que nos indiquen la prioridad y gravedad debido a que esta va a ser una escala bastante fácil de entender por todas las personas implicadas. La priorización va a ser determinada tomando en cuenta la urgencia del incidente (que tan rápido el negocio ocupa que le solucionen) y el nivel de impacto que esto está causando, tal y como se especifica en la figura 2. Para utilizar números como se recomienda utilizar como patrón de impacto el número de usuarios afectados.

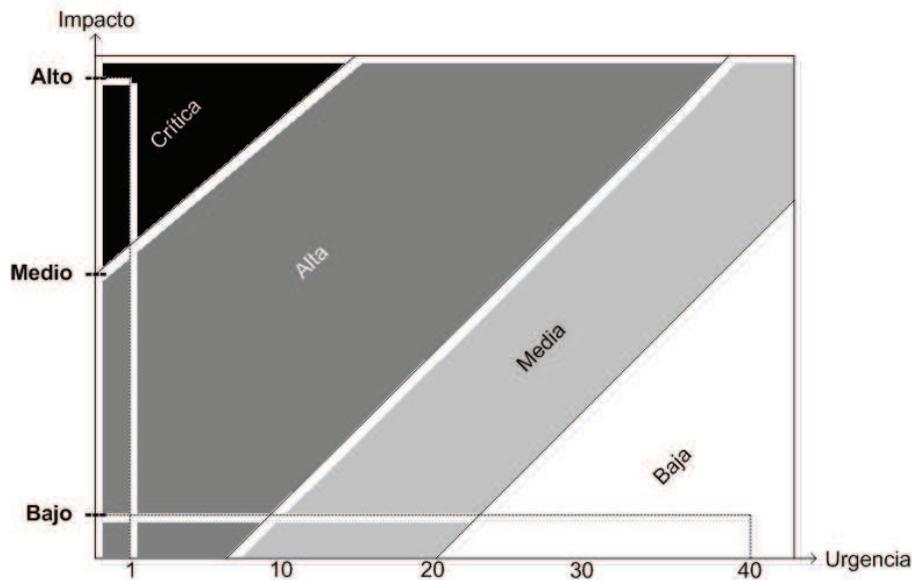


Fig. 2. Descripción de cálculo de prioridad.

Es importante también tener bien definidos los mecanismos para el reporte de los incidentes, práctica que se recomienda hacer en los tres manuales estudiados. La recomendación toma en cuenta lo positivo de todas. Para reportar incidencias CMMi (Forrester et al., 2011) recomienda tener un sistema encargado específicamente de esta labor, sin embargo se busca tener una guía que sirva para cualquier empresa sin importar si se tiene o no el software o recursos para adquirirlo, la recomendación es tener un sistema que se encargue de esto sin importar si es en papel o automatizado, siempre y cuando, los usuarios puedan de forma ágil hacer llegar su incidencia al departamento pertinente. Se debe de asegurar que el sistema de gestión de incidencias permite almacenar, actualizar, recuperar, y reportar información de incidencias que sea útil para resolver y prevenir las incidencias. Para darle seguimiento a los incidentes a través de su ciclo de vida se deberían definir estados los cuales pueden incluir: abierto, en progreso, resuelto y cerrado. Estos son los sugeridos en ITIL (ITILv3, 2011).

Si bien los incidentes se tratarán de manejar de la mejor forma y siempre buscando la mejor solución, pueden existir situaciones en las cuales un incidente pueda ser reabierto. En este mismo proceso se tiene entonces que tener reglas para reabrir un incidente, situación mencionada en ITIL, estas van a variar dependiendo la organización y las necesidades de la misma. La recomendación es definir las reglas utilizando franjas horarias, como por ejemplo, reabrir los tickets del mismo día o que fueron cerrados con un tiempo predeterminado de anterioridad.

Como segundo proceso se define la identificación de incidentes, de esto se habla tanto en ITIL como en CMMi, la recomendación toma ambas y define una actividad más completa. Se recomienda siempre tratar la incidencia antes de que esta ocurra, esto se logra con monitoreo constante sobre los servicios críticos de la empresa. La identificación de incidentes se puede realizar por medio monitoreo, análisis de anomalías en datos recogidos, detecciones por medio de un sistema automático, reportes por formulario web o llamadas telefónicas. Si ya se tiene planeado la forma o medio por el cual las incidencias van a llegar, se necesitará establecer un registro de incidencias que recolecte información suficiente para dar soporte a las actividades de análisis y solución que están por venir. ITIL (ITILv3, 2011) recomienda recolectar esta información y almacenarla para así tener un registro total de la incidencia y así, si esta tiene que ser enviada en un futuro a otro grupo o proceso se contará con la información necesaria para agilizar el proceso y evitar reprocesos. La información necesaria para el incidente es: número de referencia, categoría, urgencia, impacto, prioridad, día y hora, nombre de quien recibió el incidente, método de notificación, forma de contacto, descripción detallada de síntomas, estado del incidente, incidentes relacionados a este, actividades que se hicieron para resolver el incidente, fecha de resolución y categoría de cierre. Como parte de la actividad se realiza una categorización del incidente, basado en las categorías previamente definidas y en base a lo recolectado para el registro del mismo, se le asignará una categoría, la cual en el ciclo de vida de la incidencia podrá ser modificada.

Teniendo el incidente debidamente registrado se procede a realizar un diagnóstico inicial del mismo según recomienda ITIL. La mayoría de estos van a llegar vía teléfono, de ser así, se debe tratar de solucionar el incidente aun teniendo al cliente en la línea telefónica, si esto no es posible entonces se informará al usuario sobre el proceso para resolver el incidente y se proporcionará un número de referencia.

En el tercer proceso definido como Resolución, se recomienda iniciar con una verificación de los derechos para realizar peticiones de servicio, usando cuando sea posible, un flujo de proceso predefinido, actividad especificada en COBIT (IT Governance Institute, 2013), acá se trata de definir por medio de perfiles de usuarios los roles de usuario, que garanticen poder contar con una mejor administración de la mesa de servicio. Por otro lado es recomendable incluir lo que dice CMMI (Forrester et al., 2011) respecto al trato de la incidencia mediante el uso del mejor curso de acción, lo que nos indica que para esta actividad el personal de la mesa de trabajo deberá contar con todas las herramientas necesarias para determinar el mejor camino para la resolución del incidente. También agregar lo que COBIT recomienda acerca de obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados, actividad de suma importancia ya que para la resolución de cierto tipo de incidentes se tendrá la necesidad de realizar, por ejemplo, el reemplazo de algún dispositivo, que dependerá de la ejecución presupuestaria de la empresa para su final resolución, esto también va a agilizar los procesos, lo que va dar como resultado la mejora en la prontitud de la resolución de incidentes.

Además CMMI (Forrester et al., 2011) menciona a un nivel muy básico de detalle, que se deben gestionar y registrar las acciones hasta que el impacto de la incidencia llegue a un nivel aceptable, pero para esta propuesta lo que se va a tomar en cuenta es lo que ITIL(ITILv3, 2011) especifica muy a detalle, que dependiendo de la naturaleza de la falla pueden variar las acciones específicas necesarias así como el personal a cargo, por lo que se recomienda tomar en cuenta el listado de acciones del cómo llevar a cabo ese soporte en la mesa de servicio para la resolución final del incidente. Igualmente se recomienda que en caso de que la incidencia no pueda ser resuelta por la mesa de servicio y ésta deba realizar un proceso de escalado, si bien es cierto que tanto COBIT como CMMI hacen mención a esta actividad, ésta no está bien especificada, el presente artículo tomará como base la buena práctica recomendada por ITIL, en el cual se definen dos niveles de escalado, el Funcional y el Jerárquico. En el caso del primero y tomando en consideración que la organización cuenta con grupos de soporte funcionales con mayor experiencia, la mesa de servicio puede escalar estas incidencias al nivel funcional apropiado. Si el incidente requiere de un nivel de conocimiento más profundo, o un grupo de soporte no ha podido resolver el incidente dentro de los tiempos acordados (lo que ocurra primero), el incidente debe ser escalado inmediatamente al siguiente grupo de apoyo adecuado en el nivel funcional. Es importante saber que las reglas de escalado y manejo de incidentes deben ser acordados en las OLA y UC con cada grupo de soporte respectivamente. Algunos incidentes pueden requerir múltiples grupos de soporte para ser resueltos. Los grupos de apoyo pueden ser internos, pero también pueden ser terceros, como proveedores de software o fabricantes de hardware o personal de mantenimiento. Las reglas para el manejo de incidentes a través de grupos de apoyo y entre los proveedores de soporte de terceros, deben ser acordados en OLA y UC con cada grupo de apoyo, respectivamente. Es importante tener en cuenta que el incidente permanece en la mesa de soporte, sin importar donde haya sido referido para su resolución, la mesa de soporte sigue siendo la responsable del incidente en todo momento, además de dar seguimiento a su progreso, mantener a los usuarios informados y en última instancia hacer el cierre del incidente.

Para el segundo caso, si hay incidentes que sean muy serios (por ejemplo, incidentes de alta prioridad) los administradores apropiados de TI (Redes, aplicaciones, infraestructura) deben ser notificados, al menos para propósitos informativos. El escalado Jerárquico se da cuando la mesa de servicio no puede resolver el incidente (ya sea porque no poseen los conocimientos o por tiempo de respuesta), por lo que el incidente se traslada hacia los niveles de mando superiores para que estén enterados y puedan tomar acciones de ser necesarias, como buscar recursos adicionales o buscar proveedores o personal de mantenimiento. En la imagen 3 se especifica la actividad.

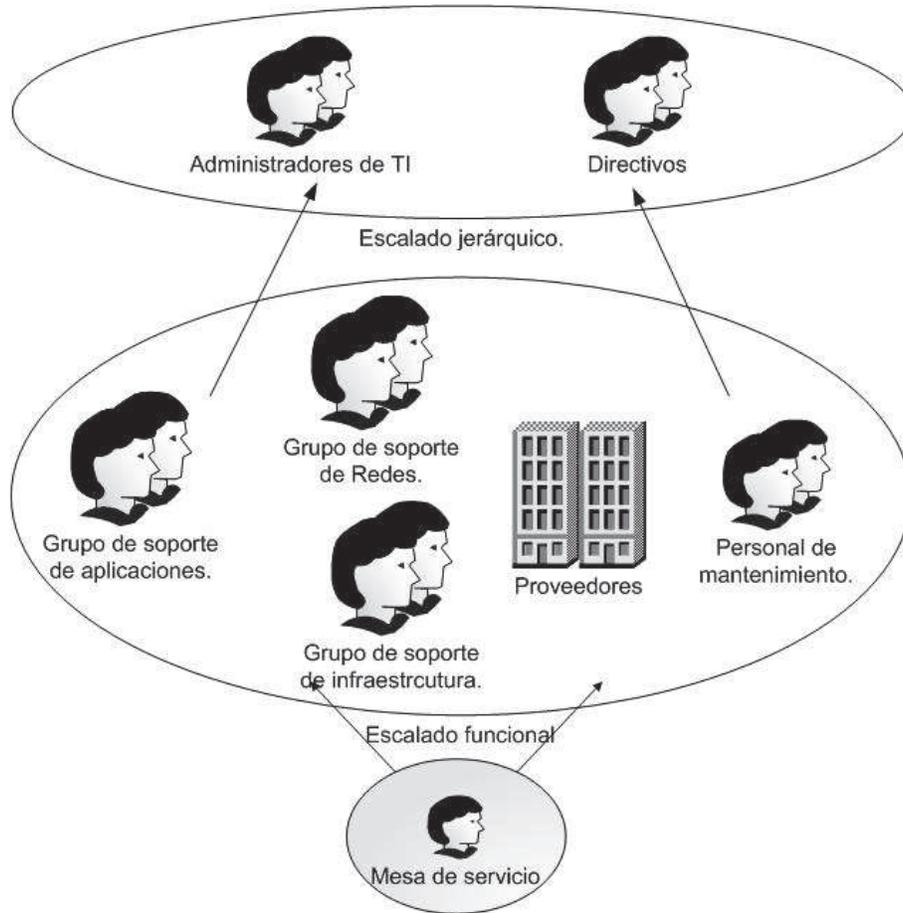


Fig. 3. Descripción de escalado.

Continuando con el proceso Resolución, se recomienda incluir también lo que nos dice COBIT (IT Governance Institute, 2013) en su siguiente actividad la cual hace mención a completar las peticiones siguiendo el procedimiento de petición seleccionado, utilizando, cuando sea posible, menús automáticos de auto ayuda y modelos de petición predefinidos para los elementos solicitados frecuentemente. Los formularios y menús de auto ayuda se podría implementar en un futuro, cuando la base de datos de conocimiento de la empresa posea el nivel de madurez aceptable, el cual cuando esté implementada será un tema de provecho para la rápida solución de incidencias conocidas, todo con el desarrollo de sistemas, formularios y menús, que permitan tanto al usuario como al personal de la mesa de servicio gestionar con mayor fluidez incidencias conocidas. Incluir además lo que recomienda CMMI, revisar las acciones realizadas que dieron como resultado cambios en el sistema de servicio con objeto de determinar si son necesarias

acciones adicionales que aseguren la trazabilidad a los requisitos, esto con la finalidad de que se mantenga actualizada la base de datos de conocimiento, por último y para cerrar el proceso de Resolución se recomienda la última actividad propuesta por ITIL(ITILv3, 2011), en donde se menciona que en caso de que la resolución del incidente haya sido resuelta por otro grupo de soporte de la empresa, éste deberá pasar de nuevo el incidente a la mesa de servicio para que se proceda con la acción de cierre del incidente.

Para el último proceso llamado Cierre, la recomendación es utilizar las actividades de ITIL, COBIT las menciona pero no con el nivel de detalle deseado para la presente propuesta, sino que, simplemente lo cita.

Primeramente ITIL (ITILv3, 2011) nos indica que la mesa de servicio debe realizar la comprobación de que el incidente está totalmente resuelto y que los usuarios estén satisfechos y dispuestos a aceptar el cierre del incidente, actividad que debe envolver a todos los involucrados en el incidente, además se tendrán que realizar las revisiones y comprobaciones acerca de las decisiones tomadas en la mesa de servicio respecto a la categorización de incidentes, indicar los pasos a seguir en caso de que esa categorización del incidente haya sido incorrecta, seguidamente se deben realizar encuestas para verificar la satisfacción del cliente, por medio de una llamada telefónica o correo electrónico, verificar también que la documentación de incidentes esté completamente documentada, se recomienda también que el caso de los problemas constantes o recurrentes estudiar en conjunto con los grupos de soporte si el incidente se resolvió sin determinar la causa raíz ya que esta situación provocará que el incidente pueda volver a ocurrir, lo que generará más medidas preventivas para evitar esto, en todos estos casos, determinar si ya se ha planteado un expediente de problema relacionado con el incidente, si no, levantar un nuevo registro de problemas en relación con el proceso de administración de problemas para que se reinicie la acción preventiva.

Por último se da la clausura oficial, en donde formalmente se cierra el registro de incidentes. Otro punto que las organizaciones pueden optar es por la utilización de un período de cierre automático del incidente, claro está, esta acción deberá ser discutida, acordada y publicada con los usuarios, de tal forma que todos estén conscientes de ello. La última actividad acá recomendada y presentada únicamente por ITIL son las reglas para reabrir incidentes. Hay ocasiones en las cuales los incidentes por más cuidado que se tenga se repiten, a pesar de que han sido cerrados oficialmente. Si se da el caso, se debe recolectar toda la información concerniente al trabajo realizado para la resolución del incidente.

Es recomendable tener las reglas claras, predefinidas y documentadas sobre cuando un incidente puede ser reabierto. Por último, es de suma importancia es que una vez definidas esas reglas se brinde la orientación debida a todo el personal de la mesa de servicio.

La guía completa se especifica en el modelado propuesto en la figura 4.

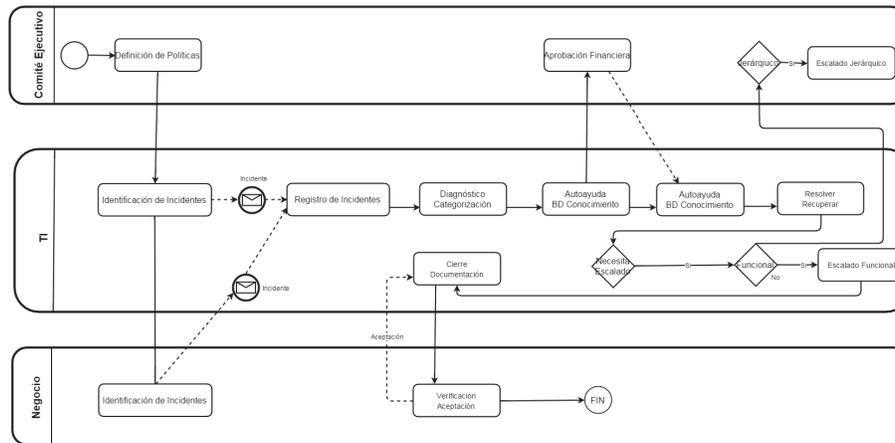


Fig. 4. Modelado BPMN3.

## 4 Conclusiones

Las empresas hoy en día buscan caminos seguros para tener éxito e incursionar en un mercado tan exigente como el actual. Trabajar bajo un estándar de buenas prácticas resulta ser vital y más aún cuando se trata del control de incidentes, el cual resulta ser la cara de TI, debido a ser este el proceso más expuesto ante los usuarios. Es aquí donde la importancia de una buena gestión de incidentes se vuelve vital en la concepción de buen servicio por parte de los usuarios, si bien actualmente, se invierte gran cantidad de recursos no solamente económicos sino también en tiempo, las empresas no siempre obtienen los réditos deseados. Dentro de los caminos a seguir hay varios marcos de referencia y buenas prácticas como las que se analizaron en este artículo, sin embargo siempre va a ser recomendable basarse no solamente en lo que podemos leer en un manual sino también en la forma de operar, crecimiento proyectado y recursos que tiene la empresa en la cual se quieren seguir las buenas prácticas. Situación a tomar en cuenta es establecer una gestión de incidencias que se adapte entonces a nuestra empresa, para esto, el estudio de posibilidades y formas de gestión se vuelve imprescindible, no es solamente seguir un manual, sino crear el nuestro, que se adapte a la empresa y que nos garantice el éxito en la operación. Hacer uso de lo recomendado en las buenas prácticas respecto a la resolución de incidentes pero de forma adaptada para cada necesidad, asegurará que la empresa esté siempre preparada para evitar la interrupción del servicio en los departamentos estratégicos que ayudan a cumplir con los objetivos de la organización.

Las buenas prácticas van a generar un modelo de referencia ampliamente reconocido en la empresa, debido a que llegará a constituir un éxito comprobado y un valor agregado para el servicio proporcionado. (Quesnel, 2012)

Implementar satisfactoriamente un conjunto de buenas prácticas, eliminará el trabajo redundante mientras mejora en tiempos, ayudando de forma sustan-

cial los procesos de TI. También se logrará un departamento de TI claramente estructurado, más eficiente y mejor enfocado en los objetivos de la empresa. (Realtimepublishers.com & Herold, 2007)

Usando buenas prácticas para la gestión de incidentes se generará una mejora importante en los indicadores creados y usados para dar soporte al negocio. Los resultados, entonces serán medibles con números, lo que produce un control total de procesos y evidenciará aspectos a mejorar.

Una implementación de buenas prácticas, sin embargo no es una tarea fácil para una empresa, mucho menos cuando la misma está empezando y quizás no desean invertir los recursos en algo diferente al negocio directo que les va a generar producción. El proceso puede tomar tiempo y recursos, mismos que en poco tiempo van a resultar retroactivos a los ingresos y producción de la empresa, a razón costo beneficio la implementación es sumamente positiva y los resultados serán evidenciados en poco tiempo.

Concluimos que las empresas con un nivel de madurez bajo o que apenas están en sus inicios, deben basarse en ITIL, debido al grado de detalle que este presenta, además no se basa en dar recomendaciones para empresas pequeñas, medianas o grandes, sino que las guías son generales y siempre buscan que cuando se implementen se hagan tomando en cuenta los factores internos de la empresa.

Concluimos que todos los marcos de referencia, si bien son similares en lo que buscan, sugieren cosas diferentes y sobre todo en el orden en el cual las actividades se deben manejar. Un ejemplo claro es los hipervínculos de autoayuda que lo mencionan tanto ITIL como CMMi pero en secciones diferentes.

Concluimos que CMMi es excelente para una empresa más madura, que tenga experiencia en el tema y ya tenga tiempo utilizando una guía de buenas prácticas. Esto es debido a ciertas recomendaciones que no se adaptan para empresas que están iniciando, tales como implementar un software de gestión de incidentes.

Un buen manejo de la gestión de incidentes es sumamente importante, sin embargo a la hora de elegir un marco, se deben analizar los servicios brindados, una empresa que brinde pocos servicios o que estos sean básicos, puede usar ITIL adaptando lo que ellos crean son las actividades que los van a llevar al éxito. Pocos servicios o que no sean complejos, no necesitan seguir un catálogo de actividades complejo o que incluya softwares y bases de datos. COBIT es bastante usado en empresas financieras y es debido a que sus actividades quedan muy adaptables a las empresas, dicen que hacer pero no lo especifican. Actividad importante que cita COBIT es la obtención de aprobaciones financieras que pueden retrasar los procesos o servicios.

Para implementar exitosa y eficientemente una guía de prácticas en la organización, se tiene que primero claramente entender los procesos de negocio y la forma en la que se soportan o funcionan los servicios de TI. En base a esto se definirán las prácticas idóneas para el éxito y siguiéndolas al pie de la letra los resultados serán mucho mejor que los esperados.

## Referencias

- Bauset-Carbonell, m., María-Carmen1, & Rodenes-Adam, m., Manuel2. (2013). Gestión de los servicios de tecnologías de la información: Modelo de aporte de valor basado en itil e iso/iec 20000. (spanish). *El Profesional de la Información*, 22. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=92774922&lang=es&site=ehost-live> pages 1
- Brand, K., & Boonen, H. (2004). *It governance: A pocket guide based on cobit*. Van Haren Publishing. Retrieved from <https://books.google.co.cr/books?id=LH77ZNT-MmEC> pages 3
- Forrester, E., Buteau, B., & Shrum, S. (2011). *Cmmi for services: Guidelines for superior service*. Pearson Education. Retrieved from <https://books.google.co.cr/books?id=ywvSVLmQmjoC> pages 4, 5, 6, 10, 11, 12, 13
- IT Governance Institute, I. (2013). *Cobit 5*. Rolling Meadows. pages 2, 12, 14
- ITILv3, F. (2011, Jul). *Itil v3 2011*. Retrieved from <http://itilv3.osiatis.es/> pages 7, 9, 11, 12, 13, 15
- Kenett, R., & Baker, E. (2010). *Process improvement and cmmi® for systems and software*. CRC Press. Retrieved from <https://books.google.co.cr/books?id=a7XS1GmuhWYC> pages 5
- Mutafelija, B., & Stromberg, H. (2008). *Process improvement with cmmi® v1.2 and iso standards*. CRC Press. Retrieved from <https://books.google.co.cr/books?id=ErVuWU\UOSwC> pages 5
- O'Toole, D. (2015). *Incident management for i.t. departments*. On Demand Publishing, LLC-Create Space. Retrieved from <https://books.google.co.cr/books?id=M2RargEACAAJ> pages 3
- Persse, J. (2013). *The it service management process manual*. van Haren Publishing. Retrieved from <https://books.google.co.cr/books?id=0FZeAgAAQBAJ> pages 2, 7
- Quesnel, J. (2012). *Entender itil 2011: Normas y mejores prácticas para avanzar hacia iso 20000*. Éd. ENI. Retrieved from <https://books.google.com/books?id=Tn2vJvQ3bwwC> pages 16
- Realtimepublishers.com, & Herold, R. (2007). *The shortcut guide to improving it service support through itil*. Realtimepublishers.com. Retrieved from <https://books.google.com/books?id=BT2bNZOqYjAC> pages 17