INSTITUTO TECNOLÓGICO DE COSTA RICA
ESCUELA DE COMPUTACIÓN
PROGRAMA DE MAESTRÍA

Propuesta de implementación del proceso de soporte de aplicaciones de seguridad de la información para que sea brindado por InfoSec de Intel Costa Rica

Proyecto para optar por el grado de Maestría Profesional
con énfasis en Sistemas de Información

Estudiante

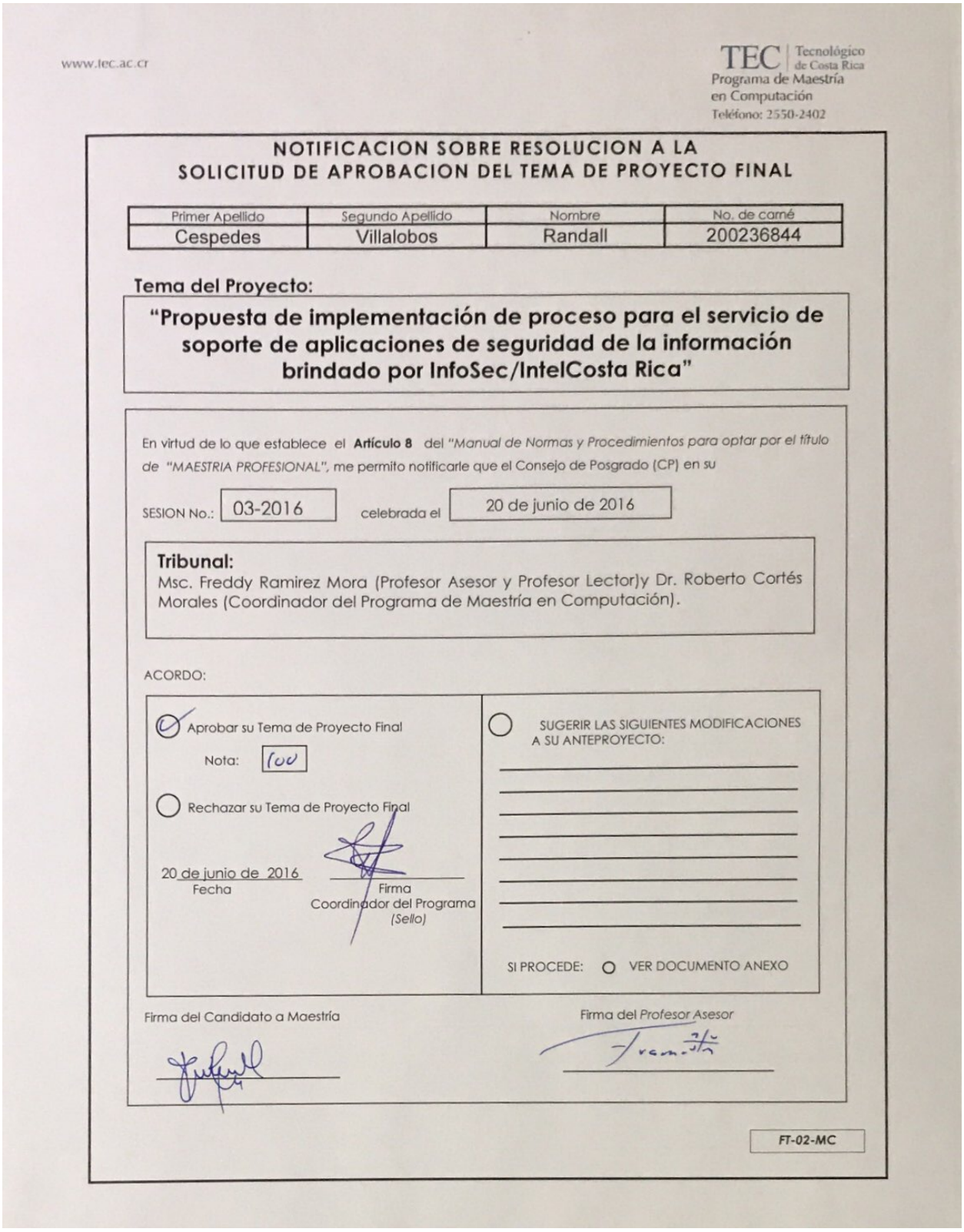
Randall Céspedes Villalobos

Profesor Asesor

Ronald Monge

Cartago, Costa Rica
Junio 2017

Hoja de Aprobación



www.tec.ac.cr

TEC | Tecnológico de Costa Rica
Programa de Maestría en Computación
Teléfono: 2550-2402

NOTIFICACION SOBRE RESOLUCION A LA SOLICITUD DE APROBACION DEL TEMA DE PROYECTO FINAL

Primer Apellido	Segundo Apellido	Nombre	No. de carné
Cespedes	Villalobos	Randall	200236844

Tema del Proyecto:

"Propuesta de implementación de proceso para el servicio de soporte de aplicaciones de seguridad de la información brindado por InfoSec/IntelCosta Rica"

En virtud de lo que establece el **Artículo 8** del *"Manual de Normas y Procedimientos para optar por el título de "MAESTRIA PROFESIONAL"*, me permito notificarle que el Consejo de Posgrado (CP) en su

SESION No.: 03-2016 celebrada el 20 de junio de 2016

Tribunal:
Msc. Freddy Ramirez Mora (Profesor Asesor y Profesor Lector)y Dr. Roberto Cortés Morales (Coordinador del Programa de Maestría en Computación).

ACORDO:

☑ Aprobar su Tema de Proyecto Final

Nota: 100

☐ Rechazar su Tema de Proyecto Final

20 de junio de 2016
Fecha

Firma
Coordinador del Programa
(Sello)

☐ SUGERIR LAS SIGUIENTES MODIFICACIONES A SU ANTEPROYECTO:

SI PROCEDE: ☐ VER DOCUMENTO ANEXO

Firma del Candidato a Maestría

Firma del *Profesor Asesor*

FT-02-MC

Dedicatoria

A mi madre, quien desde niño me animó
y apoyó incondicionalmente
para que alcanzara mis metas.

A mi esposa, por la paciencia, los consejos
y el apoyo que me brindó durante todo este tiempo.

Agradecimientos

Deseo agradecer al profesor Ronald por el apoyo que me brindó a lo largo de todo este proceso.

Epígrafe

“Una locura es hacer la misma cosa una y otra vez esperando obtener resultados diferentes. Si buscas resultados distintos, no hagas siempre lo mismo”.

Albert Einstein

Resumen

En el presente proyecto se plantea una propuesta para el servicio de soporte de aplicaciones relacionadas con seguridad de la información en Intel Cota Rica. El proyecto se basa en la aplicación de buenas prácticas para la gestión y operación de servicios de Tecnología de Información como ITIL y DevOps, así como los principios del Manifiesto Ágil, todo lo anterior con el fin de establecer una serie de procesos eficientes y ágiles que se adapten rápidamente a las necesidades del negocio.

Los servicios de tecnologías de información se han convertido en un elemento fundamental en la operación y éxito de las empresas actuales, por lo que su disponibilidad y adecuada gestión adquieren más relevancia cada día. Uno de estos servicios es el soporte de aplicaciones, que tiene como objetivo asegurar el buen funcionamiento de las aplicaciones y mantener vigente su capacidad de adaptarse a los cambios que se dan en la empresa.

La propuesta planteada se desarrolla a través de una metodología que consta de cinco fases, a saber: análisis de la situación actual, conocimiento del marco de referencia organizacional para la operación del servicio en Intel, identificación del nivel de conocimiento de elementos de ITIL, DevOps y Agile, diseño de procesos y hoja de ruta de implementación y, por último, evaluación y mejoras.

Mediante esta metodología se proponen cinco procesos para el soporte de las aplicaciones de seguridad de la información. Estos se basan en los procesos de la fase de operación del servicio de ITIL que son los siguientes: gestión de eventos, gestión de incidentes, resolución de solicitudes, gestión de problemas y gestión de acceso, además, como se indicó antes, se incorporan elementos de DevOps y Agile.

Como resultado, se obtienen procesos que combinan elementos de estos marcos de referencia en búsqueda de eficiencia y agilidad a través del aprovechamiento de los beneficios que cada uno de ellos ofrece.

Palabras clave: ITIL, DevOps, Agile, servicios de TI, operación del servicio, gestión de incidentes, gestión de eventos, gestión de problemas, gestión de acceso, resolución de solicitudes, seguridad de la información, Scrum, procesos, soporte de aplicaciones, BPMN.

www.tec.ac.cr

TEC | Tecnológico de Costa Rica

Programa de Maestría
en Computación
Teléfono: 2550-2402

APROBACIÓN DE PROYECTO FINAL

"Propuesta de implementación del proceso de soporte de aplicaciones de seguridad de la información para que sea brindado por InfoSec de Intel Costa Rica"

TRIBUNAL EXAMINADOR

M.B.A Ronald Monge Monge.
Profesor Asesor

Dr. José Helo Guzmán
Profesor Lector

Máster Carlos Núñez Ramírez
Profesor Externo

Dr. Roberto Cortés Morales
Coordinador del Programa
de Maestría en Computación

TEC | Tecnológico de Costa Rica
Maestría en Computación

Junio, 2017

Índice General

Índice de Figuras

Índice de Tablas

1. Capítulo I: Introducción

1.1. Descripción General

En la actualidad, las empresas necesitan de los recursos de tecnologías de información (TI) para operar y mantenerse competitivas en los mercados donde tienen presencia o pretenden incursionar. Sin embargo, los mecanismos ofrecidos para acceder a esos recursos de TI, así como la calidad del servicio entregado pueden no satisfacer las expectativas de los usuarios o consumidores.

Los servicios que permiten el acceso a los recursos de TI deberían estar disponibles en todo momento, ya sean aplicaciones, canales de comunicación, infraestructura, entre otros., con el fin de que estos recursos estén aportando valor a la empresa constantemente. Sin embargo, debido a múltiples factores, por ejemplo: aplicaciones fuera de servicio, fallas en el software, fallas en el hardware, deficiencias en el conocimiento técnico, cambios en las reglas del negocio y otros, estos servicios pueden no estar disponibles para ser utilizados por los usuarios, lo que genera un impacto en los negocios.

Con el objetivo de estandarizar los procesos de gestión de los recursos de TI, mediante un marco de referencia que reúna las mejores prácticas en la gestión de los servicios de TI, se creó la Biblioteca de Infraestructura de Tecnologías de Información (ITIL por sus siglas en inglés), que es una referencia para la gobernanza de TI, la gestión y el control de sus servicios. Se concentra en el monitoreo y mejora continua de la calidad de los servicios que provee, tanto desde la perspectiva del cliente como del negocio. (Axelos, 2016b).

El presente proyecto se concentrará en la fase de operación del servicio de ITIL 2011, que en adelante se menciona solamente como ITIL, con el objetivo de proponer una implementación del proceso de soporte de aplicaciones de seguridad de información que son de gran importancia para Intel, por lo que se busca garantizar, no solo el funcionamiento de estas aplicaciones, sino también su disponibilidad para los usuarios en la compañía.

El proceso será definido de acuerdo con los requerimientos establecidos en la compañía para la prestación de servicios de soporte a través del seguimiento de las buenas prácticas propuestas por ITIL, así como de la utilización de herramientas tecnológicas con que cuenta la empresa para este fin.

1.2. Antecedentes

1.2.1. Descripción de la empresa

Intel es el líder mundial en fabricación de componentes de computación, redes y comunicaciones. Fundado en 1968 por Gordon Moore y Robert Noyce, tiene su sede en Santa Clara, California. Cuenta con más de 107.000 empleados distribuidos en 170 oficinas y fábricas en más de 70 países alrededor del mundo. Su ingreso anual es de 56.000 millones de dólares estadounidenses. Es la catorceava marca más valiosa del mundo según Interbrand (2015) y

ocupa la undécima posición en la lista de compañías de mejor reputación en el mundo según Strauss (2016). Es el mayor comprador de energía verde en los Estados Unidos desde 2008. Ha invertido más de 1.000 millones de dólares estadounidenses en más de 100 países durante la última década (Intel, 2016).

Intel Costa Rica inició operaciones en 1997 como una planta de prueba y ensamble, donde los productos eran sometidos a pruebas de calidad antes de ser enviados a los clientes. La sede en suelo nacional se mantuvo realizando esa labor hasta 2005, cuando la corporación decidió trasladar a Costa Rica negocios basados en servicios tales como finanzas y soporte de operaciones de tecnologías de información.

En los años siguientes, la compañía decidió continuar con el traslado de más negocios hacia Costa Rica, entre los que están funciones del departamento de Seguridad de la Información (Information Security - InfoSec), como por ejemplo desarrollo de software para autenticación y autorización de usuarios, de productos y de servicios; el monitoreo de posibles ataques hacia los sistemas de la compañía; y la evaluación de los mecanismos de seguridad implementados para la protección de la información de la empresa.

Como se puede observar en la figura 1.1, InfoSec pertenece al Departamento de Seguridad de la Información, está ubicado dentro de la Unidad de Negocios Tecnologías de Información y se encarga de velar por la protección de los datos, así como de la infraestructura y activos de TI de Intel. Para este fin, se cuenta con herramientas que se han desarrollado internamente y también se han adquirido productos de terceros.

Entre las aplicaciones existentes en InfoSec están las relacionadas con Authentication & Authorization (autenticación y autorización), Controls & Compliance (controles y auditoría seguridad de información), Risk & Security Management (administración de riesgo y seguridad), Data Protección (protección de datos) y Threat Management (administración de amenazas).

Figura 1.1 Organigrama de Intel. Fuente: Intel Corporation

1.3. Descripción del problema

Como se mencionó en la descripción de la empresa, Intel cuenta con aplicaciones que desempeñan funciones relacionadas con seguridad de la información, tales como autenticación y autorización de usuarios, controles y auditoría, protección de datos o administración de amenazas, entre otras. Estas aplicaciones son utilizadas tanto a lo interno de InfoSec como en otros departamentos de tecnologías de la información. La mayor parte de ellas fueron desarrolladas internamente y eran soportadas por equipos de trabajo en la sede de Intel en Guadalajara, México.

Sin embargo, la compañía decidió reubicar el personal en Guadalajara en un nuevo departamento y asignarle nuevas funciones, por lo que el servicio de soporte que brindaban a las aplicaciones antes mencionadas dejó de existir como tal y solamente se realizó una transición parcial del conocimiento técnico a un equipo de trabajo en Folsom a modo de recargo de funciones, de tal manera que este personal en Folsom fuera capaz de brindar un soporte básico a las aplicaciones.

Posteriormente, la compañía toma la decisión de trasladar las funciones de soporte de estas aplicaciones a Costa Rica, para lo cual se crea un equipo de trabajo y se le asigna la responsabilidad de brindar el soporte y también de definir la forma en que se dará el servicio.

Por tanto, resulta necesario contar con un proceso de soporte de aplicación, es decir, un proceso cuyas actividades tienen como objetivo mantener a las aplicaciones funcionando sin interrupciones el mayor tiempo posible, que brinde soporte integral a las aplicaciones antes descritas de tal manera que, por una parte, permita que estas se encuentren disponibles siempre que los usuarios las requieran y también que, ante cambios en las reglas del negocio, se cuente con la posibilidad de hacer los ajustes necesarios en la funcionalidad del software.

1.4. Trabajos similares

Tema: "Propuesta de implementación de los procesos de Gestión de Incidentes y Gestión de Cambios, para el Centro de Gestión Informática del Hospital Dr. Maximiliano Peralta Jiménez, aplicando como base el marco de referencia ITIL v3s".
Año: 2013
Autor: Monge Jiménez Milena
Asesor: MBA Ronald Monge Monge
Profesor lector: Máster Freddy Ramírez Mora
Profesional externo: Máster Roberto Masís Fonseca
Director del Programa: M.Sc. Edwin Aguilar Sánchez

1.5. Definición del problema

La inexistencia de un proceso formal de soporte genera que la atención y la resolución de incidentes no se esté llevando a cabo de acuerdo con las expectativas de los usuarios de las aplicaciones, ya que al no haber un canal definido para que los usuarios puedan reportar incidentes, se ven forzados a enviar correos electrónicos esperando que lleguen a la persona correcta, lo cual no siempre ocurre de manera oportuna para evitar un impacto negativo en la aplicación.

De igual manera, las solicitudes de usuario que pueden ser de acceso o de otro tipo no son atendidas oportunamente, porque tampoco existe un canal de comunicación que los usuarios puedan utilizar. Al igual que ocurre con los incidentes, las solicitudes de usuarios llegan al equipo de soporte a través de correos electrónicos que deben viajar a través de múltiples destinatarios antes de llegar a su destino. Esto ha provocado que un dato incorrecto no pueda ser corregido forma rápida, como ha ocurrido con información sobre actualizaciones del sistema operativo de servidores que han sufrido demoras en la autorización para que sean aplicadas en los sistemas.

También, existe el riesgo potencial de que un nuevo usuario de una aplicación deba esperar varios días para poder hacer uso de la herramienta, o más grave aún que un usuario haya sido removido de sus funciones y todavía cuente con acceso a las aplicaciones.

No existe ningún tipo de monitoreo de eventos ni gestión de estos, por lo que ante una situación inesperada que se presente con las aplicaciones o la infraestructura que la soporta, será el

usuario el primero en enterarse del problema con el consiguiente impacto negativo en la calidad del servicio. Esta situación dificulta que se puedan realizar acciones preventivas por parte del equipo de soporte para extender los períodos de disponibilidad de las aplicaciones.

En Intel, la gestión de los servicios de tecnologías de información está basada en ITIL 2011 (Axelos, 2016a) que es el conjunto de buenas prácticas destinadas a mejorar la gestión y prestación de servicios de TI. Su objetivo es mejorar la calidad de los servicios de TI ofrecidos, evitar los problemas asociados a ellos y, en caso de que estos ocurran, ofrecer un marco de acción para que se resuelvan con el menor impacto en el negocio y a la mayor brevedad posible. Se cuenta con una herramienta de apoyo para la gestión de estas buenas prácticas, que es ServiceNow (ServiceNow, 2016).

1.6. Justificación del proyecto

1.6.1. Impacto

Las aplicaciones de seguridad de la información son de gran importancia para Intel. Permiten, entre otras cosas, validar la identidad de los usuarios que interactúan con ellas; identificar elementos de software o hardware que representan un riesgo, es decir, son un punto vulnerable a ataques maliciosos; proteger los datos de la empresa, por mencionar dos ejemplos. Sin embargo, actualmente existe un grupo de este tipo de aplicaciones que no cuenta con servicio de soporte, lo que representa un alto riesgo de que dichas aplicaciones queden fuera de servicio debido a incidentes que no se atienden oportunamente o, por ejemplo, solicitudes de usuarios que no se logran satisfacer ante, por ejemplo, cambios en las reglas del negocio.

Ante la decisión de Intel de brindar el servicio de soporte para las aplicaciones de seguridad de la información desde Costa Rica, resulta necesario diseñar un proceso que permita brindar el servicio de soporte de aplicaciones en el corto plazo, con lo cual se podrá garantizar el funcionamiento continuo de estas aplicaciones. Pero no solamente eso, sino que también se podrán realizar los ajustes necesarios ante el surgimiento de nuevas reglas de negocio a partir de eventos como adquisiciones de otras compañías, reorganizaciones internas, entre otros.

El diseño del nuevo proceso espera lograr un ordenamiento de los procesos internos, la documentación, el conocimiento, entre otros beneficios, mediante la implementación de las mejores prácticas que propone ITIL® y, con ello, ofrecer un servicio de soporte de alta calidad que logre, no solamente la satisfacción de los usuarios que utilizan el servicio, sino garantizar la protección de los datos de Intel.

1.7. Objetivos

1.7.1. Objetivo general

Diseñar una propuesta de implementación del servicio de soporte de aplicaciones basada en la fase de operación del servicio de ITIL® 2011, DevOps y Agile en el equipo de trabajo InfoSec de Intel Costa Rica.

1.7.2. Objetivos específicos

1. Analizar el estado actual del servicio de soporte de aplicaciones de seguridad de la información.
2. Evaluar las características de implementación de la fase de operación del servicio de ITIL en los procesos de soporte de aplicaciones en Intel.
3. Formular una propuesta de implementación de los procesos de la fase de operación del servicio de ITIL tomando en consideración conceptos DevOps y Agile.
4. Proponer acciones de evaluación y mejor continua del proceso de soporte.

1.7.3. Alcance

El proyecto aquí planteado contempla la propuesta de implementación del proceso que permitirá brindar el servicio de soporte para las aplicaciones de seguridad de la información que se utilizan en Intel, siguiendo las recomendaciones planteadas en el marco de referencia ITIL® 2011, específicamente la fase operación de servicio.

1.7.4. Entregables

Los entregables del proyecto serán los siguientes:

- Un análisis de la situación actual del proceso de soporte de aplicaciones de seguridad de la información.
- Una evaluación de las características de la fase de operación del servicio de ITIL presentes en otros procesos de soporte en Intel.
- Una hoja de ruta de implementación de los procesos definidos en la fase de operación del servicio de ITIL.
- Una propuesta con una lista de acciones para evaluar el proceso de soporte una vez implementado con el fin de incorporar mejoras.

2. Capítulo II: Marco teórico

De acuerdo con ITIL un servicio es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados (ClydeBank Technology, 2015).

Con respecto al significado de valor, ITIL lo considera el elemento sobre el cual gira el concepto de servicio. Desde la perspectiva del cliente, el valor consiste de dos componentes, a saber: utilidad y garantía. La utilidad puede satisfacerse si se tiene el rendimiento esperado o si se reducen las limitaciones. Sin embargo, la garantía busca disponibilidad, capacidad, continuidad y seguridad suficientes. Se podrá decir que un servicio es valioso si cumple alguna condición de utilidad y satisface todas las condiciones de garantía (De Jong, et al., 2008).

Por otra parte, para ITIL los servicios de TI deben ser útiles para que la empresa logre sus objetivos estratégicos; deben estar disponibles para ser consumidos en todo momento en que se requieran; deben contar con la capacidad suficiente para satisfacer la demanda, ya sea de clientes externos o internos; deben ser capaces de seguir funcionando a pesar de que se presenten interrupciones, debido a factores externos al negocio como desastres naturales y deben ser seguros, tanto para la empresa como para el cliente que los consuma.

Los servicios de TI para las empresas se relacionan más con la estrategia que con las tecnologías, esto porque los recursos de tecnológicos deben existir y ser utilizados para entregar a las áreas de negocio dentro de la empresa las herramientas necesarias para la consecución de los objetivos estratégicos, más allá de ser adquiridos porque son modernos, creyendo que con ello la empresa será más competitiva y eficiente de forma automática.

Lo anterior lleva a pensar que los servicios de TI no aportarán valor solamente porque existen, sino que deben ser gestionados adecuadamente para que aporten el máximo beneficio a la empresa.

2.1. Gestión de servicios de TI

La gestión de los servicios de TI (ITSM por sus siglas en inglés) se refiere a la implementación y gestión de la calidad de los servicios de TI que satisfacen los requerimientos del negocio (ClydeBank Technology, 2015). El enfoque es siempre brindar apoyo al negocio para que se alcancen los objetivos estratégicos de la empresa.

Es importante mencionar que desde el punto de vista de ITSM, los sistemas de TI no son sinónimo de servicios de TI. Los primeros se refieren a una colección de componentes que trabajan en combinación unos con otros para lograr un objetivo. Un sistema de TI o una colección de estos brinda soporte a cada servicio de TI. Los sistemas pueden ser intercambiados con otros, o bien, entremezclados con el fin de procurar mejoras en un servicio existente. Los componentes de un sistema de TI pueden incluir software, servidores, aplicaciones, elementos de intermediación y otros (ClydeBank Technology, 2015).

Los recursos tecnológicos no aportan valor a los negocios de la empresa por el simple hecho de ser adquiridos e incorporados a los procesos existentes o a los nuevos procesos que se quieran implementar sobre la base de una nueva herramienta tecnológica recientemente adquirida. El aporte de valor dependerá en gran medida de la gestión que se haga de esos recursos y de qué tan alineada esté con respecto a los objetivos estratégicos de la empresa.

En la actualidad, las empresas dedican grandes esfuerzos en la gestión de los servicios de TI, porque todas las áreas de negocio se apoyan en recursos tecnológicos, por lo que una buena gestión resulta en un factor de éxito. Para ello, buscan apoyo en marcos de referencia de buenas prácticas en la industria que ofrecen recomendaciones comprobadas acerca de cómo gestionar los servicios de TI.

Existen varios marcos de referencia para la gestión de servicios de TI. Ejemplos de ellos son ITIL, COBIT y CMMI. El primero se utilizará en el desarrollo del presente documento, específicamente, la fase de operación de servicio. COBIT y CMMI serán descritos brevemente con el fin de ofrecer al lector una pequeña noción de cómo enfocan la gestión de servicios de TI estas colecciones de buenas prácticas.

2.1.1. COBIT

El término COBIT es un acrónimo que proviene del inglés *Control Objectives for Information and related Technology* que se puede traducir como los Objetivos de Control para Información y Tecnologías Relacionadas. Fue publicado por primera vez en 1996 y su edición más reciente es la del 2012 llamada COBIT 5. Es una guía de mejores prácticas dirigida al control y supervisión de las tecnologías de información en las empresas. Su mantenimiento está a cargo de ISACA, organización cuyo nombre tiene origen en el acrónimo del inglés *Information Systems Audit and Control Association*.

COBIT ayuda a las empresas a obtener el valor óptimo de los recursos de TI, manteniendo un balance entre obtención de beneficios, optimización de los niveles de riesgo y uso de recursos. COBIT logra que los recursos de TI sean gobernados y gestionados de una manera holística para toda la empresa. Incorpora todos los aspectos del negocio y las áreas funcionales tomando en cuenta los intereses de todas las partes involucradas, ya sean internas o externas. COBIT es un marco de referencia de uso genérico que puede ser utilizado en organizaciones de todos los tamaños, ya sean comerciales, sin fines de lucro o del sector público (ISACA, 2012).

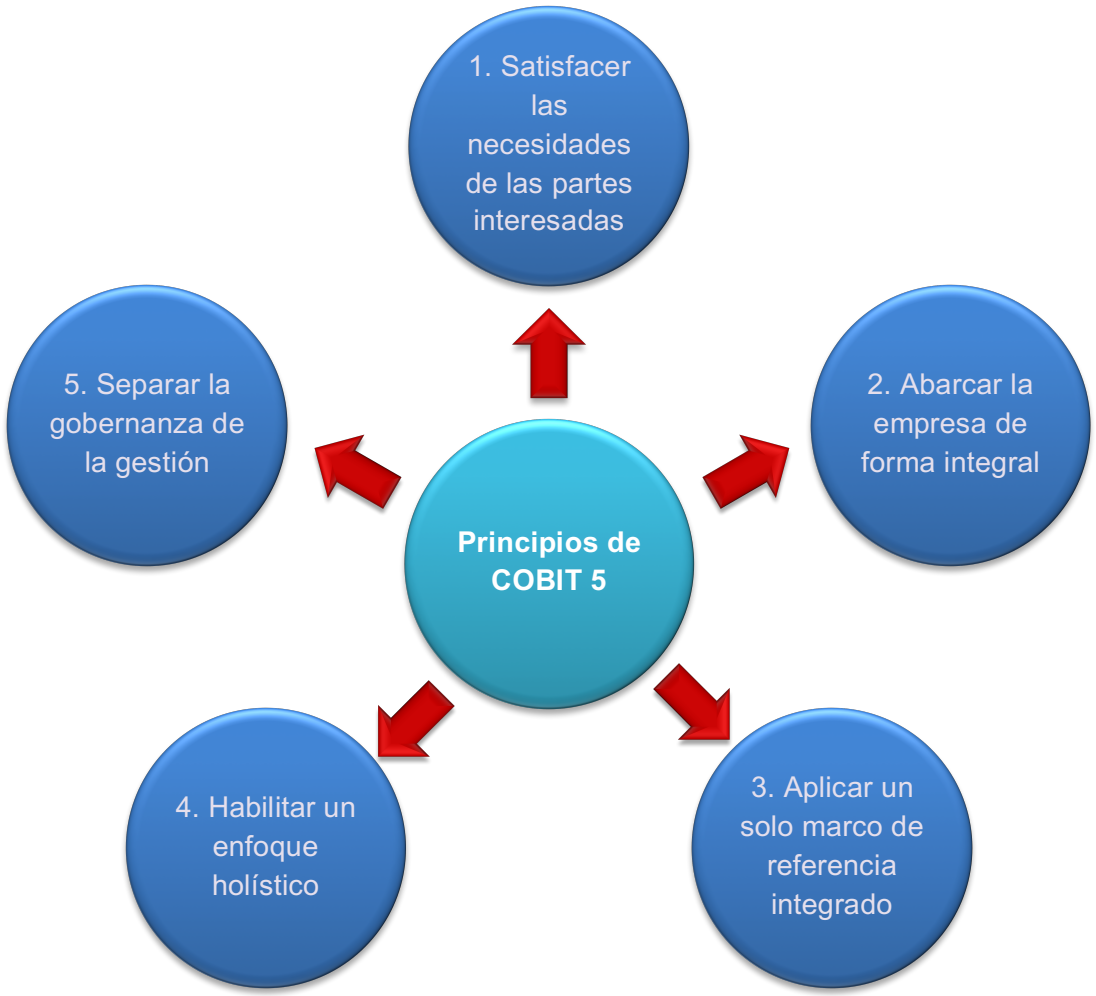


Figura 2.1 Principios de COBIT 5. Fuente: COBIT® 5, © 2012 ISACA®

COBIT se basa en cinco principios para la gobernanza y gestión de las tecnologías de información en la empresa, que se pueden observar en la figura 2.1. A continuación, se describen brevemente los cinco principios de COBIT.

Principio 1: Satisfacer las necesidades de las partes interesadas

Las empresas existen para crear valor a todas las partes interesadas, ya sean dueños, clientes, socios comerciales, entre otras, y lo consiguen manteniendo un balance entre la obtención de beneficios y la optimización del riesgo y uso de recursos. COBIT provee los procesos y otros mecanismos necesarios para la creación de valor a través del uso de recursos de TI.

Principio 2: Abarcar la empresa de forma integral

COBIT integra la gobernanza de TI en la de toda la empresa, es decir, abarca todos los procesos y funciones y no se enfoca únicamente en los recursos de TI, sino que trata la información y otras tecnologías como cualquier otro recurso que debe ser gestionado.

Principio 3: Aplicar un solo marco de referencia integrado

Debido a que existen otros marcos de referencia y guías de buenas prácticas que se enfocan en actividades específicas de TI, COBIT procura alinearse con ellos en un nivel general para la gobernanza y gestión de los recursos de TI de tal manera que se puedan obtener los beneficios que cada uno de ellos ofrece de manera integral.

Principio 4: Habilitar un enfoque holístico

Una gobernanza y una gestión de los recursos de TI eficientes y efectivas requieren un enfoque holístico, que tome en consideración varios componentes que interactúan entre sí. COBIT proporciona un conjunto de habilitadores que brindan apoyo a la implementación de un sistema comprensivo de gobernanza y gestión de los recursos de TI en la empresa. Estos habilitadores se definen como cualquier elemento que pueda ayudar a la consecución de los objetivos de la empresa. Los siete habilitadores se pueden apreciar en la figura 2.2.

Figura 2.2 Habilitadores de COBIT 5. Fuente: COBIT® 5, © 2012 ISACA®

Principio 5: Separar la gobernanza de la gestión

COBIT establece una clara distinción entre gobernanza y gestión de los recursos de TI. Ambas disciplinas incluyen diferentes tipos de actividades y requieren estructuras organizacionales diferentes, porque sirven propósitos distintos. Para COBIT, la gobernanza se relaciona con el aseguramiento de que las necesidades, condiciones y opciones de las partes interesadas. Estas

son analizadas y evaluadas para determinar los objetivos a alcanzar; además, establece la dirección a seguir a través de la definición de prioridades y toma de decisiones. También, monitorea el desempeño y cumplimiento de los objetivos y dirección definidos.

Por otra parte, la gestión está relacionada con la planificación, ejecución y monitoreo de las actividades que están alineadas con la dirección con el fin de lograr los objetivos estratégicos que fueron definidos.

2.1.2. CMMI

La integración del modelo de madurez de capacidades o *Capability Maturity Model Integration* (CMMI) es un modelo de capacidad y madurez (*Capability Maturity Model*, CMM) que se centra en mejorar los procesos en una organización. Contiene elementos esenciales para la eficacia de los procesos en una o más disciplinas y describe un camino evolutivo de mejora desde procesos ad hoc e inmaduros a procesos disciplinados y maduros con calidad y eficacia mejoradas (CMMI Institute, 2013).

Los modelos CMMI proporcionan una guía de uso, una referencia de buenas prácticas para el desarrollo de procesos, pero no son procesos en sí mismos, ni los describen. Los procesos reales en una organización dependen de diversos factores entre los que se incluyen dominios de aplicación e infraestructura, así como el tamaño de ella. Es habitual que no haya una correspondencia directa entre las áreas de proceso de un modelo CMMI y los procesos que se utilizan en una organización que lo haya empleado.

En la actualidad, existen tres modelos CMMI que cubren igual cantidad de áreas de interés, a saber: desarrollo, adquisiciones y servicios. En la tabla 1, se describen brevemente cada uno de los modelos CMMI.

2.1.3. BPM

Business Process Management (BPM) o gestión de los procesos de negocio es el arte y ciencia de supervisar la forma en que se realiza el trabajo en una organización para asegurar resultados consistentes y para sacar provecho de oportunidades de mejora. En este contexto, el término “mejora” puede adquirir diversos significados dependiendo de los objetivos de la organización. Ejemplos típicos de objetivos de mejora pueden ser reducción de costos, reducción de tiempos de ejecución y reducción de errores. Es importante resaltar que BPM no se enfoca en mejorar la forma en que se realizan las actividades individuales, sino que busca gestionar cadenas completas de eventos, actividades y decisiones que combinados aportan valor a la empresa y sus clientes. Según Dumas, La Rosa, Mendling, & Reijers (2013), a estas cadenas de eventos, actividades y decisiones se les llama procesos.

Modelos CMMI	
CMMI® for Development (CMMI-DEV), Version 1.3	El modelo CMMI-Dev es una guía para la mejora de las capacidades de la organización para desarrollar productos y servicios de calidad que satisfagan las necesidades de los clientes y usuarios finales, a través del mejoramiento de la eficiencia, velocidad y calidad apoyado en una reducción de los defectos.
CMMI® for Services (CMMI-SVC), Version 1.3	El modelo CMMI-SVC es una guía para la mejora de las capacidades de la organización para ofrecer servicios de calidad a los clientes y usuarios finales, a través del fortalecimiento de los puntos de contacto con el cliente y mejorando su experiencia al consumir los servicios.
CMMI® for Acquisition (CMMI-ACQ), Version 1.3	El modelo CMMI-ACQ es una guía para la mejora de las capacidades de la organización para iniciar y gestionar la adquisición de productos y servicios que satisfagan las necesidades de los clientes y usuarios finales, a través de la definición de requerimientos para identificar proveedores capaces de ayudar en la reducción de costos, la gestión de la calidad, el incremento de la eficiencia y la mitigación de demoras.

Tabla 2.1 Modelos CMMI. Fuente: http://cmmiinstitute.com/cmmi-models

BPM propone una serie de herramientas para analizar la situación actual de un proceso o una serie procesos de negocio, a través del descubrimiento o identificación de los distintos elementos que lo conforman, así como de los actores que toman parte en su ejecución. Esto permite conocer y documentar la forma en que el proceso se realiza actualmente en la empresa y definir ajustes o nuevas formas de realizarlo, que puedan aportar más valor a la organización y sus clientes.

Identificar los roles

Durante la etapa de descubrimiento o identificación de un proceso, debe tenerse en cuenta que existen dos perfiles o tipos de actores, a saber: el analista de proceso y el experto. El primero es la persona que cuentan con el conocimiento y las destrezas necesarias para documentar y modelar el proceso, manteniendo un enfoque objetivo, aunque no necesariamente está familiarizado con el proceso en sí. Por su parte, el experto −que puede ser una o más personas− es quien conoce con gran nivel de detalle la forma en que se ejecuta el proceso. Sin embargo, usualmente no son buenos creando o interpretando modelos de procesos.

Las diferencias entre estos dos roles ofrecen tres retos que deben ser manejados y superados adecuadamente. El primero de ellos trata de la fragmentación del conocimiento del proceso por parte de los expertos. Esto se debe a que usualmente distintos expertos conocen solamente una parte del proceso, la parte en que ellos participan de forma directa. Por tanto, es importante identificar a todos los expertos que de una u otra forma participan en el proceso para conocer todos los detalles de este.

El segundo reto consiste en el pensamiento basado en casos. La razón de esto es que los expertos tienden a pensar en términos de casos de uso y se les dificulta visualizar un proceso en forma general. Aquí, el analista debe interpretar la información aportada por el experto y abstraer los datos generales del proceso.

Por último, está el reto que se refiere al escaso conocimiento que los expertos tienen del modelado de procesos, lo que lleva al analista de proceso a que deba guiarlos en la lectura e interpretación de los modelos para que puedan brindar retroalimentación y con ello se hagan las correcciones necesarias.

Recopilar la información

Para conocer la forma en que se ejecuta un proceso, es necesario revisar toda la información que esté al alcance y, para ello, Dumas, et al. (2013) plantean usar las siguientes técnicas: recopilación de información basada en evidencias y entrevistas a los expertos.

1. Recopilación de información basada en evidencias

Esta técnica permite formar la visión más objetiva acerca de la manera en que se ejecuta el proceso; sin embargo, es importante tener presente que la retroalimentación tiende a ser lenta y que el nivel de detalle de la visión puede ser limitado.

La información se obtiene mediante la lectura y análisis de documentos oficiales del proceso, tales como acuerdos de condiciones del servicio, políticas de seguridad, descripción técnica de los productos o servicios brindados, por ejemplo.

Se utiliza, también, la observación del proceso para comprender la forma en que cada rol participa, tanto desde el punto de vista del cliente como desde el de los miembros de la organización que ejecutan el proceso. En este punto se debe tener presente que los expertos pueden modificar su comportamiento al saber que están siendo observados. De ser necesario acceder a algún sistema de información que se utilice en el proceso, se debe gestionar la debida autorización por parte de quien corresponda.

2. Entrevistas

Las entrevistas son una gran herramienta para obtener información acerca del proceso de forma inmediata y con gran nivel de detalle, aunque pueden reflejar la opinión del entrevistado y esto debe tomarse en cuenta. También, debido a la retroalimentación inmediata ofrecen la posibilidad de aclarar dudas con el entrevistado; esta característica puede ser de gran utilidad.

Las entrevistas deben ser abiertas para que los expertos sientan la libertad de bridar todos los detalles del proceso que consideren pertinentes. Si se utilizan listas de verificación en cada una de las entrevistas, los expertos pueden considerar reservarse detalles que no son consultados y esto puede ser contraproducente con el objetivo de obtener toda la información acerca de la forma en que el proceso se ejecuta.

Asimismo, el analista de proceso debe estar atento a realizar consultas sobre casos excepcionales en los que los expertos tuvieron que resolver situaciones fuera de lo normal, con el fin de conocer detalles adicionales sobre el proceso y no solamente mantenerse en un contexto de casos exitosos, que son los que los entrevistados tienden a mencionar y describir con mayor frecuencia.

Modelar el proceso

Con la información recopilada que describe en detalle la forma en que el proceso se ejecuta, se elabora un modelo utilizando alguna notación, preferiblemente estándar, que permita representar el proceso. Tal es el caso del lenguaje BPMN (*Business Process Model and Notation*, www.bpmn.org) que es una notación estándar ampliamente utilizada y que consta de una serie de pasos que se describen a continuación.

1. Identificar los límites del proceso. Este paso es esencial para comprender los límites del proceso. Consiste en identificar los eventos que marcan el inicio y el fin del proceso de soporte.

2. Identificar las actividades y eventos esenciales del proceso. El objetivo de este segundo paso es identificar aquellas actividades y eventos más importantes dentro del proceso de soporte. Actividades y eventos adicionales se podrán agregar posteriormente.

3. Identificar los recursos y las transiciones. Una vez que se identifiquen las actividades y eventos principales se puede plantear la pregunta de quién es responsable de ellos, que ayuda a descubrir las transiciones entre recursos, las cuales pueden darse entre personas o entre departamentos. La información reunida en este paso establece las bases para definir los contenedores (*swimlanes*) y compartimentos (*pools* y *lanes*) (Berliner BPM-Offensive, 2015).

4. Identificar el flujo de control. Los puntos de transición definen la estructura inicial del flujo de control. En esencia, el flujo de control se relaciona con las preguntas cuándo y por qué se ejecutan las actividades. Se requiere identificar el orden de las dependencias, los puntos de decisión, la ejecución concurrente de actividades y eventos, así como potenciales repeticiones y retrabajo.

5. Identificar elementos adicionales. En el último paso se puede extender el modelo agregando elementos adicionales como datos de entrada o salida, objetos de datos o almacenes de datos. Asimismo, para los casos de excepción es necesario identificar los límites del alcance, los flujos de excepción y manejadores de compensación. Estos elementos adicionales van a ir de la mano con el enfoque utilizado en la elaboración del modelo. Así, por ejemplo, si se pretende automatizar el proceso, es importante destacar elementos de datos y aspectos relacionados con casos de excepción. Por otra parte, si el modelo se usa para un análisis de riesgos o estimación de costos, los elementos a incorporar serán aquellos que tengan que ver con riesgos y costos.

Asegurar la calidad del modelo

Una vez que se ha obtenido la información del proceso y se ha representado en un modelo, resulta necesario asegurar la calidad de dicha modelo. Esto se puede lograr siguiendo tres pasos que asegurarán la calidad sintáctica, semántica y pragmática.

La calidad sintáctica se logra mediante la verificación de que en su elaboración se hayan seguido las reglas y guías que establece el lenguaje de modelado utilizado. La calidad semántica se logra por medio de la validación de que el proceso representado refleja aspectos del mundo real, basado en dos aspectos: uno la validez, que se refiere a que todos los elementos deben ser correctos y relevantes al problema y dos la completitud, que trata de que todos los elementos del proceso están presentes en el modelo.

Por último, la calidad pragmática del modelo se logra mediante la certificación de que el modelo cuenta con un alto nivel de usabilidad, es decir, que puede ser interpretado con facilidad, que puede ser fácilmente modificado para aplicar cambios y que puede ser empleado para mostrar la forma en que el proceso modelado se ejecuta.

2.2. ITIL 2011

El nombre ITIL es un acrónimo que proviene del inglés *Information Technology Infrastructure Library* o Biblioteca de Infraestructura de Tecnologías de Información y que de forma sencilla se puede definir como un conjunto de buenas prácticas y métodos para la gestión de los servicios de TI, que se centra en la continua medición y mejora de la calidad con que se proveen dichos servicios, tanto desde el punto de vista del negocio y como del cliente (ClydeBank Technology, 2015).

Best Management Practice (2011) deja claro que “ITIL no es un estándar que debe seguirse, es una guía que debe ser leida, comprendida y utilizada para crear valor al proveedor del servicio y a sus clientes” (p. 3).

ITIL propone que los servicios presentan un ciclo de vida organizado en las fases que podemos apreciar en la Figura 2.3 y que se listan a continuación:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

Estrategia del servicio

Aquí se da la comprensión de los objetivos estratégicos de la organización. Cada activo incluyendo personas, procesos y productos debe brindar soporte a la estrategia. Entre los temas tratados en esta fase del ciclo de vida están el desarrollo de mercados, características de tipos de proveedores internos y externos, activos de servicios, portafolio de servicios, gestión de las

relaciones de negocios, gestión de demanda, gestión financiera, desarrollo organizacional, estrategia de riesgos, entre otros (Best Management Practice, 2011).

Diseño del servicio

En esta fase es donde la estrategia definida en la fase previa se convierte en un plan para alcanzar los objetivos estratégicos del negocio. Comprende servicios nuevos y ajustes a los existentes. Contempla también la continuidad de los servicios, el logro de niveles de servicio, conformidad con estándares y regulaciones, coordinación de diseños, gestión del catálogo de servicios, gestión de los niveles de servicio, gestión de la disponibilidad, capacidad y continuidad de los servicios, gestión de la seguridad de la información, gestión de los proveedores y otros (Best Management Practice, 2011).

Transición del servicio

Aquí se incorporan servicios nuevos y renovados en el ambiente de producción. En términos generales, garantiza que el valor identificado en la fase de estrategia del servicio y codificado en la fase de diseño del servicio atraviese una transición efectiva para que pueda ser llevado a la realidad en la fase de operación del servicio.

Los temas tratados son la planificación de la transición y soporte, gestión de cambios, gestión de activos y configuración, gestión de versiones y despliegues, validación y prueba de servicios, evaluación de cambios y gestión del conocimiento, que busca hacer disponible el conocimiento que se va adquiriendo para que esté disponible en todas las etapas del ciclo de vida, entre otros (Best Management Practice, 2011).

Operación del servicio

Esta fase describe las mejores prácticas para la gestión de servicios en ambientes de producción. Incluye guías para alcanzar la efectividad y eficacia en la entrega y soporte de servicios que aseguren brindar valor a los clientes, usuarios y proveedor del servicio. Entre los temas tratados en esta fase están la gestión de incidentes, gestión de problemas, gestión de eventos, resolución de solicitudes y procesos de gestión de accesos (Best Management Practice, 2011).

Mejora continua del servicio

Guía para la creación y mantenimiento de valor para los clientes a través del mejoramiento de la estrategia, el diseño, la transición y la operación del servicio. Entre los temas tratados están las métricas del servicio, la demostración del valor a través de métricas y el desarrollo de evaluaciones de línea base y madurez (Best Management Practice, 2011).

2.2.1. Origen del marco de referencia

ITIL fue desarrollado a inicios de la década de los 80 por la Central Communications and Telecommunications Agency (CCTA) o Agencia Central de Comunicaciones y Telecomunicaciones, una oficina del gobierno británico (Cartlidge & Lillycrop, 2012).

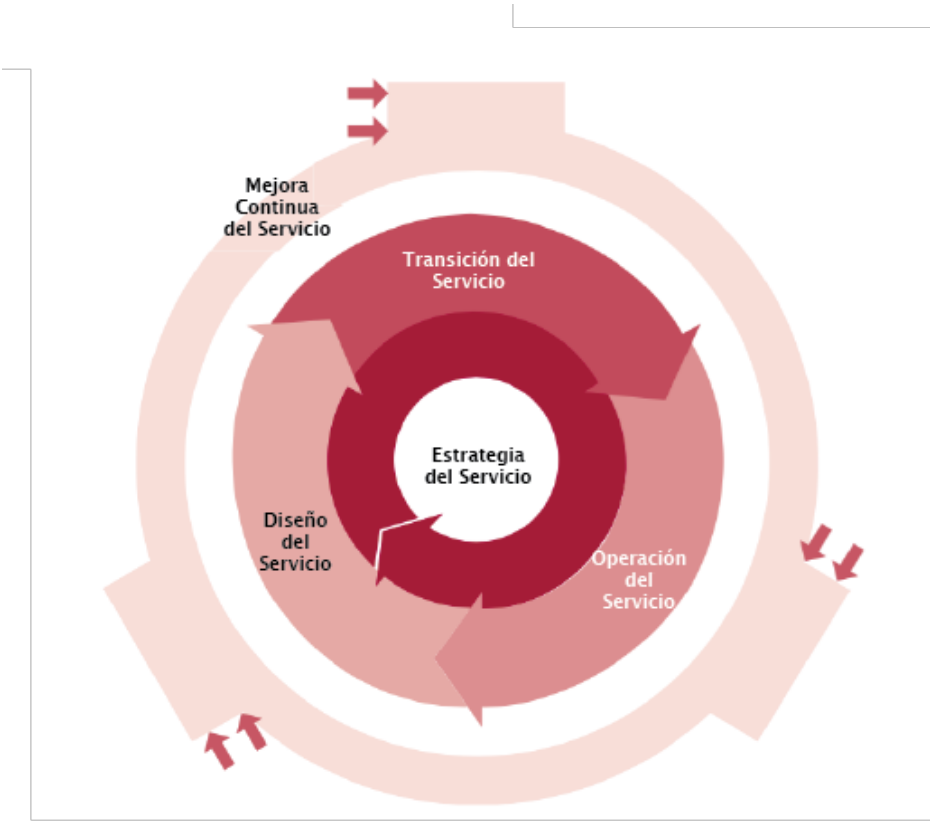


Figura 2.3 Ciclo de vida de los servicios ITIL. Fuente: ITIL

En 2011, se publicaron las ediciones ITIL 2011, que es la versión más reciente y que consiste en una nueva revisión para mejorar la claridad y la consistencia a través de los cinco libros del marco de referencia y para introducir pequeñas adiciones que le permitan mantenerse actualizado y acorde con las últimas demandas de la industria.

2.3. Operación del servicio

Como ya se mencionó, los servicios son un medio para generar valor a los clientes al producir los resultados que ellos desean, sin que deban asumir los costos y riesgos específicos asociados. Los servicios facilitan los resultados mejorando el desempeño de las tareas asociadas y reduciendo el efecto de las restricciones, las cuales pueden incluir regulaciones legales, falta de presupuesto o capacidad, o bien limitaciones tecnológicas.

De acuerdo con lo Best Management Practice (2011) “específicamente un servicio de TI es aquel que brinda un proveedor de servicios de TI, que puede ser el departamento de TI mismo, o bien una organización subordinada a ésta. Un servicio de TI es una combinación de tecnologías de información, personas y procesos” (p. 13).
En la fase de operación del servicio es donde la estrategia de servicio, el diseño de servicio y la transición del servicio se ven reflejados para entregar el valor al cliente, es aquí donde se hacen visibles para el cliente los resultados que espera (Best Management Practice, 2011).

En el contexto de TI la gestión de servicios (ITSM o IT Service Management) se refiere a la implementación y gestión de servicios de TI de calidad que satisfagan las necesidades y requerimientos del negocio. La gestión de los servicios de TI está a cargo de los proveedores de servicios de TI a través de una combinación de personas, procesos y recursos de tecnologías de información. Un proveedor de servicios de TI puede ser cualquiera organización dentro del departamento de TI de una empresa y puede ofrecer servicios a clientes internos o externos (Best Management Practice, 2011).

Recordemos que el valor de un servicio se considera como el nivel con que este llena las expectativas del cliente. Los servicios no tienen un valor intrínseco, sino que el valor proviene de lo que el servicio le permite alcanzar a quien lo consume. Desde la perspectiva del cliente, el valor consiste en alcanzar los objetivos del negocio. El valor de un servicio de crea a través de la combinación de dos elementos primarios que son la utilidad (aptitud para el propósito) y garantía (aptitud para el uso) (Best Management Practice, 2011).

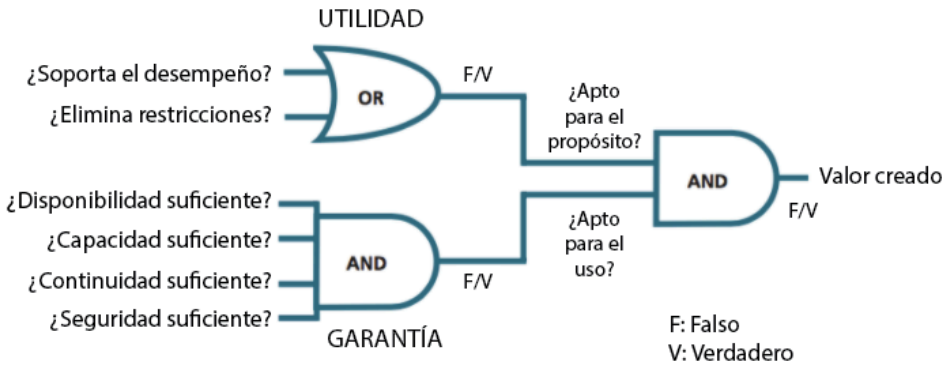


Figura 2.4 Lógica de creación de valor a través de un servicio. Fuente: ITIL 2011 Service Operation

La figura 2.4 ilustra la forma en que un servicio presenta ambas características: utilidad y garantía. En términos generales la utilidad se refiere a lo que el servicio hace y sirve para determinar si el servicio provee los resultados requeridos. Por su parte la garantía se refiere a la forma en que el servicio es entregado y sirve para determinar si este se adecua a los requerimientos de uso del negocio, por ejemplo, si es lo suficientemente seguro, si está disponible cuando se necesita y si cuenta con la capacidad suficiente para satisfacer la demanda.

2.3.1. Procesos

En esta sección se describirán los procesos y actividades de la operación del servicio. Los procesos son: gestión de eventos, gestión de incidentes, resolución de solicitudes, gestión de problemas y gestión de acceso.

2.3.1.1. Gestión de eventos

La definición de evento que da Best Management Practice (2011) dice que:

> Un evento se puede definir como cualquier cambio de estado significativo desde la perspectiva de la gestión de un elemento de configuración (CI, del inglés configuration item) o de un servicio de TI. Ejemplos típicos de eventos son las notificaciones creadas por los servicios de TI, los elementos de configuración o CIs, o bien, las herramientas de monitoreo. (pp. 58)

Una efectiva operación del servicio depende de la capacidad de reconocer cualquier cambio de estado en la infraestructura. Esto se consigue gracias a los sistemas de monitoreo y control que tienen como base dos tipos de herramientas, a saber: las de monitoreo activo y las de monitoreo pasivo. Las primeras son aquellas que permiten conocer el estado y disponibilidad de los CIs, mientras que las segundas detectan y correlacionan alertas operacionales y comunicaciones generadas por CIs.

1. Propósito

Conducir los eventos a través de su ciclo de vida que consiste básicamente en la detección y clasificación del evento, así como en la determinación de las acciones de control necesarias.

2. Objetivos

- Detectar todos los cambios de estado que sean significativos para la gestión de un CI o un servicio de TI.
- Determinar la medida de control adecuada para el evento y comunicarla según corresponda.
- Proveer los disparadores o puntos de inicio de los procesos y actividades de gestión dentro de la operación del servicio.
- Proveer los medios para comparar el desempeño actual contra el esperado de acuerdo con estándares o SLAs.
- Proveer las bases para el aseguramiento, reporte y mejora del servicio.

3. Valor para la empresa

Usualmente se da de forma indirecta. Por ejemplo, cuando gracias a la detección temprana de incidentes se pueden tomar las acciones de remediación antes de que se dé un impacto negativo en los servicios de TI. Cuando, también, a través de tareas automatizadas se pueden liberar recursos humanos costosos que pueden ser empleados en actividades de mayor valor agregado, que tengan que ver con innovación, búsqueda de nuevas formas de aprovechar los recursos tecnológicos disponibles, entre otros.

4. Tipos de eventos

Existen múltiples tipos de eventos, como por ejemplo:

- Informativos: cuando notifican de la ocurrencia de un evento que no implica un incidente potencial.
- De advertencia: cuando se presenta una situación que podría implicar un incidente potencial.
- De excepción o error: cuando se presenta una situación fuera de lo normal o condición aceptable.

5. Filtrado de eventos

Es importante identificar los eventos que tienen significado relevante para el negocio en operación para enfocar el monitoreo y actividades relacionadas solamente en ellos y descartar los que únicamente aportarían ruido a las tareas de soporte de operaciones.

6. Consideraciones de diseño en la gestión de eventos

Algunas consideraciones claves a tener en cuenta durante la gestión de eventos son las siguientes:

- ¿Qué se debe monitorear?
- ¿Qué tipo de monitoreo se requiere? Por ejemplo: activo, pasivo; de desempeño o de resultados.
- ¿Cuándo es necesario generar el evento?
- ¿Qué tipo de información se debe comunicar durante el evento?
- ¿A quién va dirigida la información del evento?
- ¿Quién es el responsable de clasificar el evento, enviar las notificaciones, escalar el evento según corresponda, ejecutar las acciones apropiadas y otros?

7. Actividades

La Figura 2.5 ilustra el proceso de gestión de eventos. Es una representación genérica de alto nivel que sirve como referencia, pero que no pretende ser una descripción absoluta y completa del proceso. En ella se pueden ver las actividades y decisiones que se deben tomar en el proceso de gestión de un evento.

En términos generales la gestión de eventos ocurre de manera tal que primero se presenta el evento, se notifica la ocurrencia del evento, se registra el evento en algún sistema de gestión, se clasifica el evento y por último se ejecutan las acciones que se haya determinado que corresponden de acuerdo con el tipo de evento ocurrido.

8. Riesgos y retos

Se pueden enfrentar una serie de retos, como por ejemplo obtener los recursos necesarios para adquirir las herramientas y para hacerlas funcionar de la forma adecuada. También, desplegar las herramientas de monitoreo de la infraestructura de TI puede ser una actividad que consuma gran cantidad de recursos y tome mucho tiempo en completarse.

Por otra parte, encontrar el balance adecuado entre la frecuencia de envío de información y la prontitud en que un evento puede ser detectado para no saturar el tráfico de red es otro reto que se puede enfrentar.

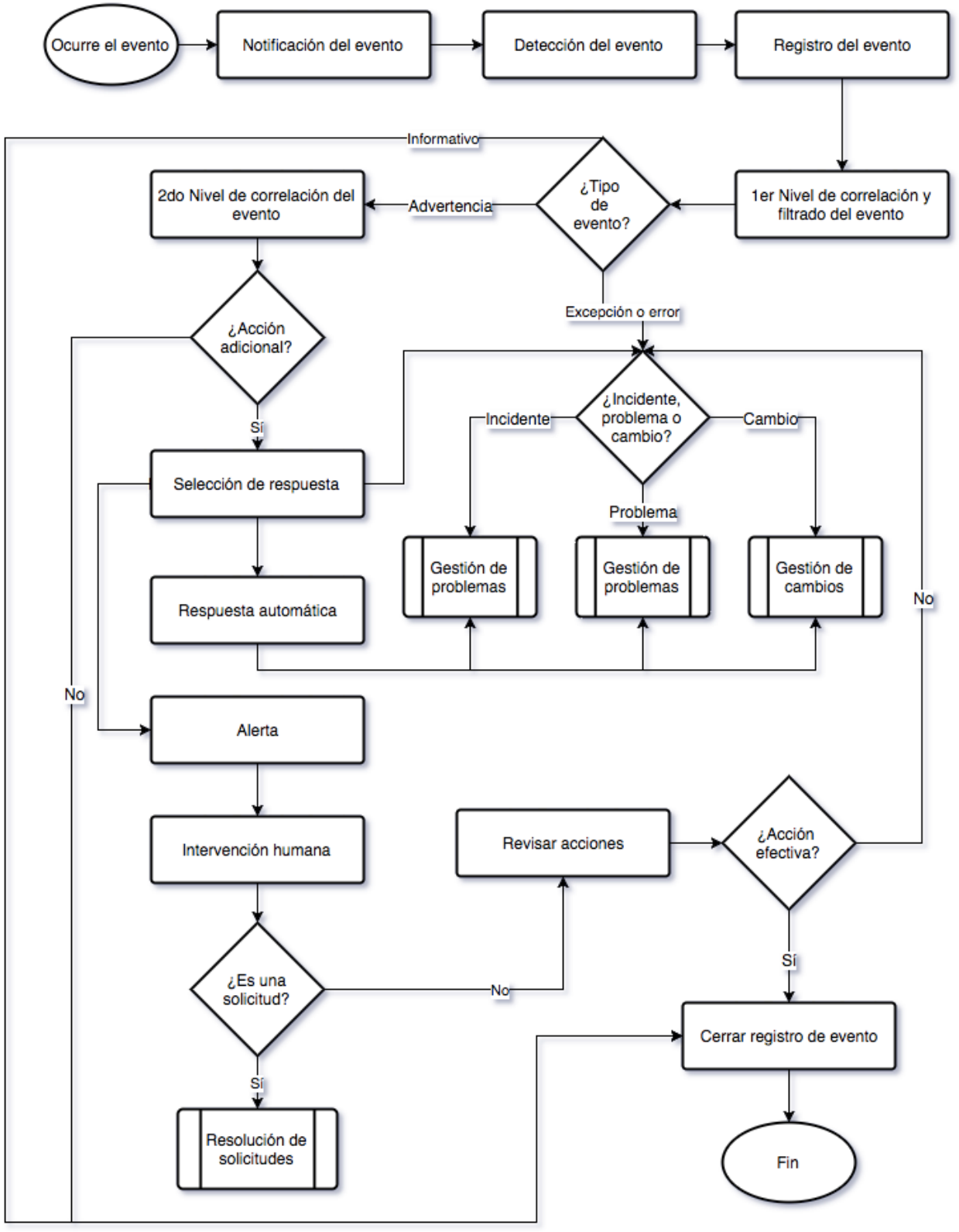


Figura 2.5 Proceso de gestión de eventos. Fuente: ITIL 2011 Service Operation

2.3.1.2. Gestión de incidentes

Según Best Management Practice (2011) un incidente se define como:

> Una interrupción no planeada de un servicio de TI, una disminución en la calidad de un servicio de TI o bien una falla en un CI que todavía no ha impactado un servicio de TI (por ejemplo, cuando falla uno de los discos de un arreglo en espejo). (p. 72).

De acuerdo con lo anterior, la gestión de incidentes es el proceso responsable del ciclo de vida de los incidentes, los cuales pueden ser identificados por personal técnico, detectados por herramientas de monitoreo, reportados en comunicados de los usuarios, o bien reportados por proveedores o socios comerciales (Best Management Practice, 2011).

1. Propósito

Reestablecer los servicios interrumpidos en el menor tiempo posible y minimizar el impacto negativo que se haya podido provocar a la calidad del servicio afectado.

2. Objetivos

- Asegurar que los métodos y procedimientos estandarizados se utilizan para producir respuestas, análisis, documentación, seguimiento y reportes eficientes de los incidentes.
- Aumentar la visibilidad de los incidentes y sus comunicados para el personal administrativo y soporte de TI.
- Mejorar la percepción hacia el departamento de TI a través de un enfoque profesional en la expedita resolución de incidentes.
- Alinear las actividades y prioridades de la gestión de incidentes con los de la empresa.
- Mantener el nivel de satisfacción de los usuarios con respecto al nivel de calidad de los servicios de TI.

3. Valor para la empresa

Reducir el trabajo no planeado y costos producto de incidentes. Detectar y reducir los incidentes rápidamente para que los servicios estén disponibles por más tiempo, para alinear las actividades de TI con las prioridades de la empresa, de tal manera que los recursos se asignen dinámicamente donde son requeridos.

También, para incorporar mejoras a los servicios gracias al conocimiento que se adquiere sobre los incidentes y las formas de evitarlos y para que el centro de servicios pueda identificar necesidades de capacitación o mejora de los servicios, ya sea desde la perspectiva de la empresa o del departamento de TI.

4. Modelos de incidentes

Sirven para definir las acciones a ejecutar, las herramientas a utilizar y los tiempos límite a dedicar para las actividades de resolución, los responsables, procedimientos de escalación y más, de tal manera que cuando se presente un incidente con ciertas características, se conozca de antemano qué hacer.

Existen incidentes que por su grado de impacto en los procesos de negocio tienen una gran urgencia en ser resueltos, se les conoce como incidentes graves (MI o major incident en inglés). En estos casos la necesidad de reestablecer los servicios afectados implica que los tiempos para realizar las actividades de resolución del incidente son más cortos y se requiere de equipos de trabajo que se mantengan enfocados en buscar las soluciones (Best Management Practice, 2011).

5. Actividades

La Figura 2.6 ilustra el proceso de gestión de incidentes. Al igual que en el caso de gestión de eventos, esta no es la única forma en que se pueden gestionar los incidentes, pero sirve de referencia para que la empresa pueda definir su propio proceso.

Cada incidente debe ser registrado para darle seguimiento hasta su resolución. Seguidamente se debe asignar una categoría, es decir, se debe clasificar. También, se le asigna una prioridad sobre la base de dos criterios, a saber: urgencia e impacto. El primero se refiere a la prontitud en que debe ser resuelto y el segundo se relaciona con la cantidad de sistemas y usuarios que han sido afectados.

Posteriormente, se realizan las actividades de resolución que incluyen investigaciones, diagnósticos, involucramiento expertos y niveles de soporte (escalaciones), así como la coordinación de las actividades para implementar la solución encontrada. Finalmente se hace las pruebas de éxito de la solución y se al cierre documental del incidente (Best Management Practice, 2011).

6. Riesgos y retos

Se da el reto de contar con la capacidad de detectar incidentes lo más cerca de su origen como sea posible, mediante configuración adecuada de herramientas, capacitación a los usuarios y el uso de grupos especializados en el centro de servicios, además se debe convencer al personal técnico y usuarios de la importancia de registrar todos los incidentes y documentarlos detalladamente.

Por otra parte, entre los riesgos podemos mencionar que podría darse saturación del servicio de soporte debido a falta de personal o falta de capacitación ante un eventual incremento de los incidentes. También, podría faltar información oportuna, debido a la carencia de fuentes adecuadas.

2.3.1.3. Resolución de solicitudes

De acuerdo con Best Management Practice (2011) una solicitud se puede describe de la siguiente forma:

El término “solicitud de servicio” es una descripción general para una gran variedad de peticiones que hacen los usuarios al departamento de TI y sus dependencias. Por lo general tienen que ver con cambios pequeños, de costo y riesgos bajos, como por ejemplo: un cambio de contraseña, la instalación de software, reubicar equipo de cómputo, entre otros. También, pueden ser simples peticiones de información. (pp. 86)

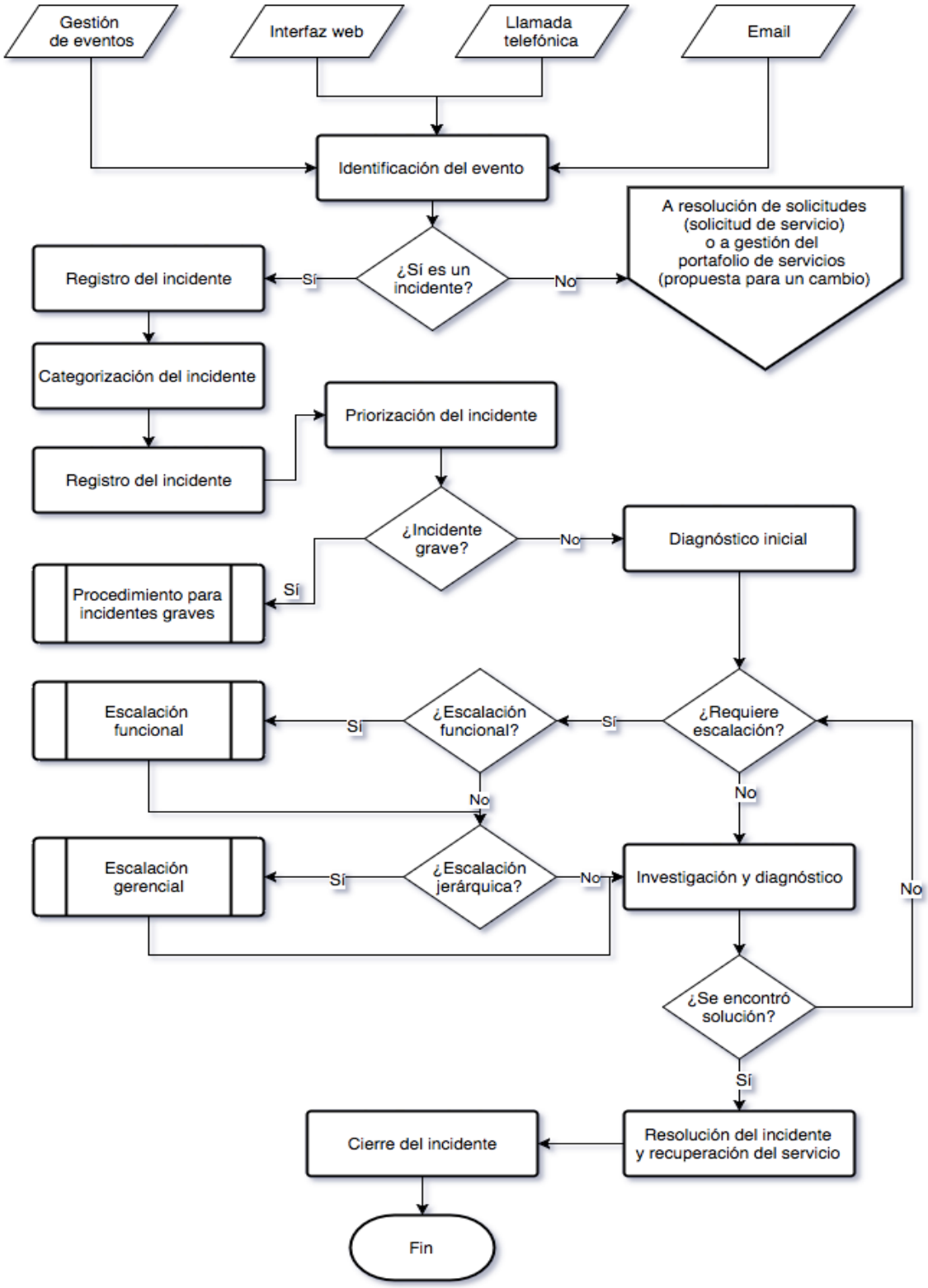


Figura 2.6 Proceso de gestión de incidentes. Fuente: ITIL 2011 Service Operation

1. Propósito

El propósito del proceso de resolución de solicitudes es asumir la responsabilidad de gestionar el ciclo de vida de las solicitudes de usuarios de los servicios de TI.

2. Objetivos

- Mantener una alta satisfacción de parte de los clientes y usuarios de los servicios de TI a través de una gestión eficiente y profesional de sus solicitudes de servicio.
- Proveer un canal para que los usuarios puedan solicitar servicios estándar, para los cuales existe una autorización y un proceso definido previamente.
- Proveer a los usuarios la información necesaria sobre los servicios disponibles para que puedan solicitarlos.
- Obtener y entregar los componentes de los servicios estándar, como por ejemplo licencias de software.
- Brindar asistencia con quejas, comentarios o solicitudes de información general.

3. Valor para la empresa

Capacidad de proveer un acceso rápido y eficiente a los servicios estándar de TI, reducir la burocracia en la solicitud de servicios y la resolución de peticiones reduciendo el costo, mediante la centralización y estandarización del proceso.

4. Modelos de resolución de solicitudes

Algunas de las solicitudes pueden recibirse con una alta frecuencia, por lo que resulta conveniente definir modelos que permitan gestionar estas peticiones de forma consistente y eficiente. Se les conoce como solicitudes estándar y el procedimiento para completarlas es bien conocido y ha sido depurado por el departamento de TI (Best Management Practice, 2011).

5. Actividades

Una descripción general del proceso de resolución de solicitudes se presenta en la Figura 2.7, la cual ilustra una de las formas de ejecutar el proceso, sin que necesariamente sea la única. Cada organización deberá definir su propio proceso sobre la base de las recomendaciones que plantea este marco de referencia.

Una vez recibida la solicitud se procede con el debido registro, se valida para asegurarse de no estar ante un incidente o una solicitud de cambio.

Las solicitudes deben, también, categorizarse y asignársele una prioridad tomando en cuenta criterios de urgencia e impacto, así como ser autorizadas y asignadas a la persona o equipo de personas adecuadas para que trabajen en su resolución. Por último, se procede con el cierre documental de la solicitud (Best Management Practice, 2011).

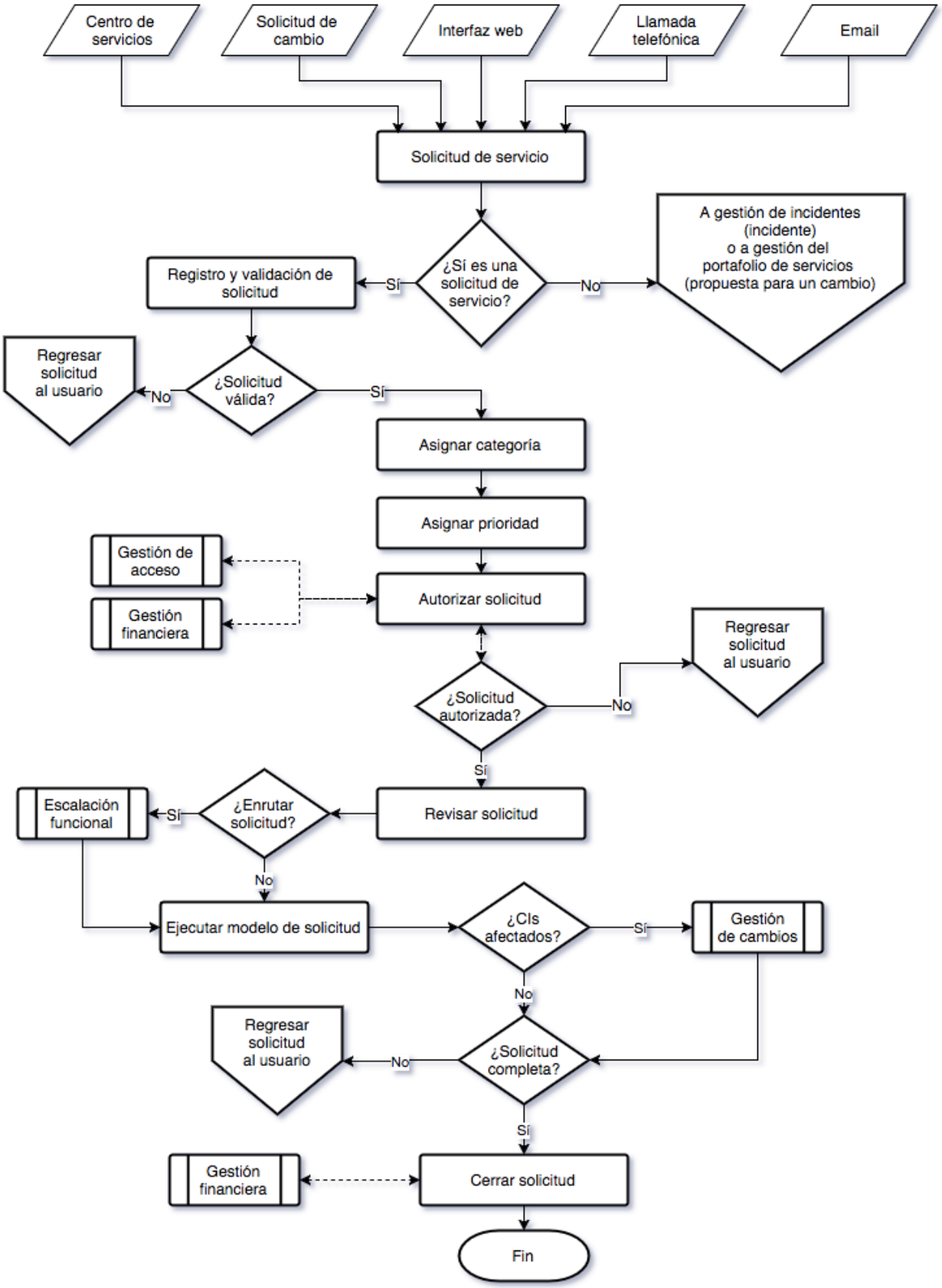


Figura 2.7 Proceso de resolución de solicitudes. Fuente: ITIL 2011 Service Operation

6. Riesgos y retos

Entre los retos está definir con claridad y documentar detalladamente los tipos de solicitudes para que se pueda tener una clara distinción entre una solicitud estándar un una solicitud de cambio. Establecer mecanismos de autoservicio para los usuarios, así como acordar cuáles servicios serán considerados estándar y quién estará autorizado a solicitarlos.

Por el lado de los riesgos puede ocurrir que el alcance del proceso no esté definido con claridad, por lo que el personal no va a estar seguro de hasta dónde llegan sus responsabilidades dentro del proceso. También, es posible que las herramientas con que se cuentan para que los usuarios hagan sus solicitudes no sean las mejores y con esto se dificulte la comunicación con ellos y por ende baje el nivel de satisfacción, entre otros.

2.3.1.4. Gestión de problemas

Best Management Practice (2011) define la gestión de problemas como “el proceso responsable del manejo del ciclo de vida de los problemas, donde un problema, según ITIL, se define como el punto de origen de uno o más incidentes” (p. 97).

1. Propósito

Resolver o eliminar fallas subyacentes en la infraestructura de TI a través de la investigación y documentación de incidentes, de tal manera que estos no se vuelvan a presentar. Esto se logra mediante la búsqueda e identificación de la causa raíz u origen de los incidentes (Best Management Practice, 2011).

2. Objetivos

- Prevenir la ocurrencia de incidentes producto de problemas en la infraestructura de TI.
- Eliminar los incidentes recurrentes.
- Minimizar el impacto de los incidentes que no se pueden prevenir.

3. Valor para la empresa

Aumentar la disponibilidad de los servicios de TI mediante la reducción de la frecuencia en que ocurren los incidentes y el tiempo que estos requieren en ser resueltos. También, en reducir los costos de la utilización de recursos en resolver los mismos incidentes en repetidas ocasiones.

4. Actividades

La figura 2.8 ilustra el proceso de gestión de problemas y al igual que en los procesos descritos anteriormente, este no es la única forma de implementar el proceso, pero es una buena referencia.

La detección del problema es el punto de partida y puede surgir del registro de múltiples incidentes por parte del centro de servicios que considera que tienen un origen común, o del análisis de incidentes que realiza un grupo de soporte, o bien a través de herramientas de detección de fallas en la infraestructura, entre otros escenarios.

De forma similar como ocurre con los incidentes, los problemas se clasifican en categorías, se les asigna una prioridad de acuerdo con su nivel de urgencia, impacto y severidad. Una vez hecho esto se realiza una investigación para encontrar la causa raíz del problema y con ello

encontrar una solución definitiva. Sin embargo, mientras esto ocurre es posible implementar una solución temporal para mitigar el impacto del incidente.

Finalmente, con la solución definitiva implementada se procede con el cierre documental del problema y todos los incidentes asociados (Best Management Practice, 2011).

5. Riesgos y retos

Uno de los retos es la dependencia de una efectiva y eficiente gestión de incidentes y las herramientas utilizadas para ello. Otro reto es contar con personal capacitado para resolver problemas; así como procurar una buena relación y comunicación entre el personal de distintos niveles de soporte.

Entre los riesgos están que el proceso podría verse saturado de problemas que no se pueden atender debido a la falta de personal capacitado, o falta de herramientas adecuadas para realizar las investigaciones, o porque los objetivos no están alineados con los de la empresa.

2.3.1.5. Gestión de acceso

De acuerdo con Best Management Practice (2011) el proceso de gestión de acceso se define como:

> Proceso mediante el cual se les permite a los usuarios debidamente autorizados el uso de un servicio, al mismo tiempo que se impide que usuarios no autorizados lo utilicen. En algunas empresas también se conoce a este proceso como administración de derechos o administración de la identidad. (p. 110).

1. Propósito

Proveer a los usuarios el derecho de utilizar un servicio o un grupo de servicios. Por tanto, se refiere a la ejecución de las políticas y acciones definidas por la gestión de la seguridad de la información.

2. Objetivos

- Gestionar el acceso a los servicios sobre la base de las políticas y acciones definidas en el proceso de gestión de la seguridad de la información.
- Responder oportuna y eficientemente ante solicitudes de acceso a servicios, cambios en los permisos de acceso o eliminación de permisos de acceso a servicios.
- Asegurar que no se dé un uso incorrecto o abusivo de los permisos de acceso.

3. Valor para la empresa

Asegurar la protección de la confidencialidad de la información, mediante el control del acceso a los servicios de TI. Mitigar la introducción de datos erróneos en los sistemas de información por parte de usuarios inexpertos, entre otros (Best Management Practice, 2011).

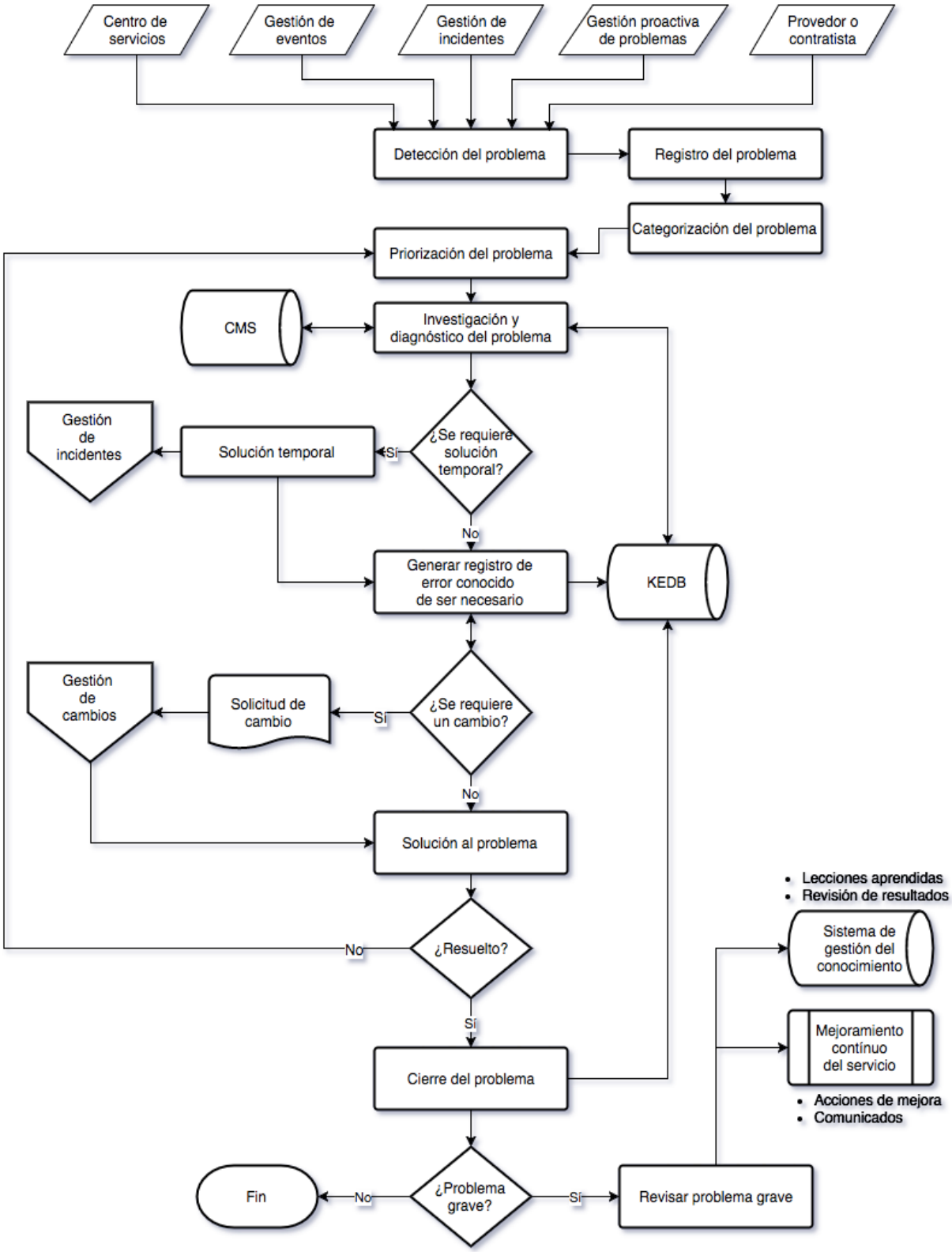


Figura 2.8 Proceso de gestión de problemas. Fuente: ITIL 2011 Service Operation

4. Actividades

En la figura 2.9 se muestra una representación del proceso de gestión de acceso, que si bien es cierto no es la única forma en que se puede gestionar el acceso a los servicios de TI, es una buena referencia que las organizaciones pueden utilizar para definir su propio proceso.

El proceso inicia con la solicitud que se recibe, la cual se valida desde dos perspectivas: que el usuario que solicita el acceso es quien dice ser y que realmente necesita utilizar el servicio solicitado. Si la solicitud es válida se aplican las políticas definidas por gestión de la seguridad de la información y se traslada la solicitud a la persona o equipo de personas competentes para procesarla (Best Management Practice, 2011).

5. Riesgos y retos

Uno de los retos es monitorear y reportar la actividad de acceso a servicios de TI, así como los incidentes relacionados con este campo. También, verificar la identidad de los usuarios y la validez del requerimiento de acceso, vincular múltiples permisos de acceso a usuarios individuales, determinar el estado actual de un usuario, restringir el acceso a usuarios no autorizados, entre otros.

Quizás el principal riesgo sea no poder realizar eficientemente las tareas de gestión de acceso, debido a la carencia de herramientas tecnológicas que apoyen las actividades complejas como controlar el acceso a través de puertas traseras en interfaces entre aplicaciones, cambios en las reglas definidas en los firewalls para satisfacer necesidades especiales, controlar el acceso a servicios por parte de terceros, entre otros (Best Management Practice, 2011).

2.3.2. Organización de la operación del servicio

A continuación se describen los conceptos generales de cómo se organiza la administración de los servicios de TI en relación con la operación del servicio. No existe una forma única de organización y le corresponde al departamento de TI de cada empresa definir con claridad los roles y responsabilidades para ejecutar los procesos y actividades descritas anteriormente (Best Management Practice, 2011).

2.3.2.1. Funciones

Además de los procesos descritos antes, el marco de referencia plantea cuatro funciones importantes en la operación del servicio, a saber: centro de servicios, administración técnica, operaciones de TI y administración de aplicaciones.

Centro de servicios

El centro de servicios es el punto de contacto para que los usuarios puedan acceder a los servicios de soporte en caso de una interrupción de un servicio, de necesitar pedir un servicio o, incluso, para algunos casos de solicitudes de cambios. Provee un punto de contacto comunicación para los usuarios y un punto de coordinación para los grupos de soporte de TI y para que funcione de manera efectiva es usual que se separa de las otras funciones de la operación del servicio (Best Management Practice, 2011).

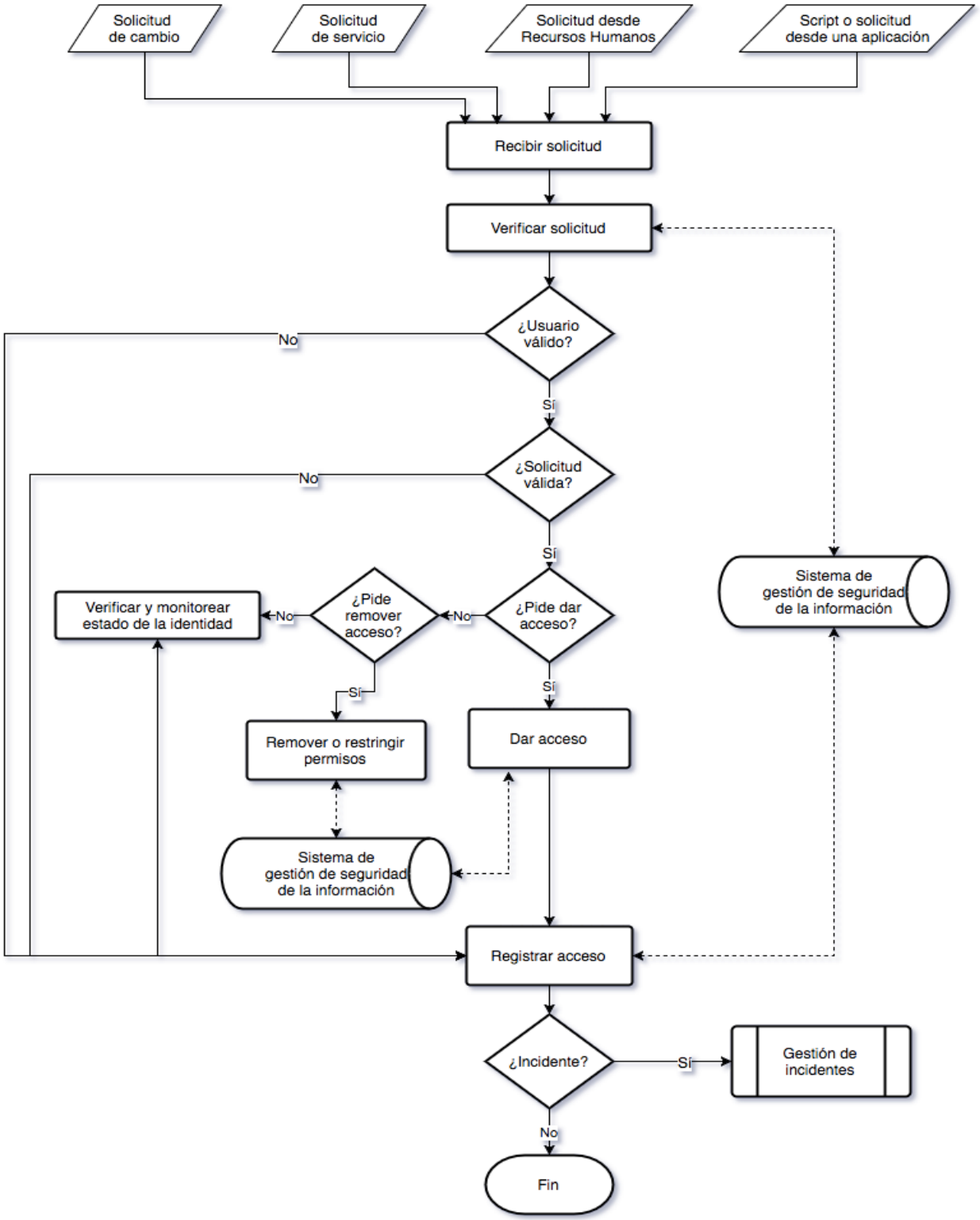


Figura 2.9 Proceso de gestión de acceso. Fuente: ITIL 2011 Service Operation

Administración técnica

Esta función provee las destrezas técnicas y los recursos específicos para brindar soporte a la operación de los servicios de TI y a la administración de la infraestructura. También, juega un papel importante en el diseño, las pruebas, la implementación de nuevos servicios, así como de la mejora de los existentes.

En empresas pequeñas es posible que esta función esté asignada a un único departamento, sin embargo en empresas de gran tamaño lo usual es que la función esté distribuida en múltiples departamentos técnicos especializados (Best Management Practice, 2011).

Administración de las operaciones de TI

Esta función se encarga de las actividades operacionales diarias que se requieren para gestionar los servicios de TI y el soporte de la infraestructura de TI. En algunas empresas esta función la desempeña un único departamento, pero en otras las actividades y el personal está distribuido en departamentos distintos y especializados (Best Management Practice, 2011).

Administración de aplicaciones

La responsabilidad de esta función es gestionar las aplicaciones a través de su ciclo de vida. También juega un papel importante en el diseño, las pruebas y el mejoramiento de las aplicaciones que forman parte de los servicios de TI. Usualmente se distribuye en distintos departamentos de acuerdo con el portafolio de aplicaciones, de tal manera que haya grupos especializados para atender las necesidades particulares de las aplicaciones (Best Management Practice, 2011).

2.3.2.2. Roles

En esta sección se mencionan algunos de los roles que propone el marco de referencia para la operación del servicio y que sirven como ejemplo, sin embargo cada empresa deberá definir los que más se ajustan a sus requerimientos y objetivos estratégicos. En el Anexo I se incluyen las responsabilidades asociadas a cada rol.

2.3.3. Consideraciones tecnológicas

En el soporte de la operación del servicio existen requerimientos tecnológicos generales y también particulares a cada uno de los procesos y funciones. Entre los requerimientos más comunes está contar con una herramienta de flujo de trabajo que permita gestionar el ciclo de vida de incidentes, problemas, solicitudes, eventos y acceso. También, disponer de un sistema integrado de gestión de servicios de TI, una base de datos de errores conocidos y tecnologías de servicios de directorio (Best Management Practice, 2011). (Daine, 2016).

Proceso/Función	Nombre del rol
Generales	Dueño del servicio
	Dueño del proceso
	Gerente de proceso
	Ejecutor de proceso
Gestión de incidentes	Dueño del proceso
	Gerente del proceso
	Analista de primer nivel
	Analista de segundo nivel
	Analista de tercer nivel
Gestión de problemas	Dueño del proceso
	Gerente del proceso
	Analista de problemas
Resolución de solicitudes	Dueño del proceso
	Gerente del proceso
	Analista
Gestión de eventos	Dueño del proceso
	Gerente del proceso
	Otros roles
Gestión de acceso	Dueño del proceso
	Gerente del proceso
	Otros roles
Centro de servicios	Gerente del proceso
	Supervisor
	Analista
	Súper usuario
Administración técnica	Gerente técnico/líder de equipo
	Analista técnico/arquitecto
	Operador técnico
Administración de operaciones de TI	Gerente de operaciones
	Jefe de turno
	Analista
	Operador
Administración de aplicaciones	Gerente de aplicaciones/líder de equipo
	Analista de aplicaciones /arquitecto

Tabla 2.2 Roles y responsabilidades en la operación del servicio. Fuente: ITIL 2011 Service Operation

2.4. DevOps

Cada vez es más evidente en las empresas la necesidad de desarrollar soluciones de software más rápido, integrando múltiples tecnologías y con la participación de personal con las más variadas capacidades. Todo esto no resulta sencillo de lograr.

El esquema tradicional de desarrollo de software implicaba la existencia de dos grandes áreas de trabajo. Por un lado, el equipo de desarrollo a cargo de la creación del software y por el otro el equipo que debía integrar y hacer funcionar ese software en la infraestructura de la empresa.

Este esquema dio resultado en su momento, pero ahora las empresas requieren no solo que las nuevas soluciones de software se integren rápidamente en los ambientes de producción, sino que sus funcionalidades se adapten mucho más rápido a lo que los clientes necesitan, que el software sea de mejor calidad y a un menor costo. Para esto se requiere algo más que dos equipos trabajando por separado.

DevOps viene a proponer un nuevo enfoque de cómo integrar el desarrollo de software con las operaciones de TI. Tradicionalmente, equipos de trabajo aislados interactúan a través de un complejo sistema de tiquetes y procedimientos de solicitudes llenos de rituales que pueden requerir la intervención de un director. Un equipo que aplique un enfoque DevOps habla del producto a través de su ciclo de vida, discute requerimientos, funcionalidades, calendarios, recursos y todo lo demás que pueda ser relevante. La atención se centra en el producto, no construyendo feudos y amasando poder político (Walls, 2013).

DevOps también se relaciona con un movimiento cultural porque quienes desarrollan software y quienes ejecutan las actividades en operaciones de TI son personas y es necesario que comprendan la importancia de trabajar en conjunto con la mirada puesta siempre en buscar formas de aportar valor al negocio.

Con DevOps el departamento de operaciones de TI no desaparece, sino que se convierte en una parte del área de desarrollo y en vez de visualizar a un súper desarrollador que comprenda *big data*, optimización de sitios web, aplicaciones de componentes de capa media y tolerancia a fallas en ambientes altamente distribuidos, lo que se requieren son especialistas en operaciones dentro de los equipos de desarrollo (Loukides, 2012).

Existen varios enfoques en que DevOps puede implementarse en las empresas. A continuación, se presentarán dos propuestas de implementación de DevOps. La primera de ellas es la que plantea UpGuard que es una empresa de consultoría en el ámbito de la Administración de la Configuración y que consta de cinco pasos, los cuales se describen seguidamente.

Paso 1: Obtener apoyo de la alta gerencia. Buscar apoyo de los principales líderes en la empresa, promover la colaboración de los mandos medios con el fin de obtener un compromiso de parte de la organización para la implementación de DevOps.

Paso 2: Aplicar un pensamiento sistemático. Extender el uso de Agile más allá del desarrollo de software (generación de código) y buscar que los sistemas complejos se puedan partir en componentes más simples.

Paso 3: Identificar ineficiencias en el sistema. Identificar los puntos de falla en los sistemas y donde estos se vuelven ineficientes para automatizar los componentes individuales adecuadamente.

Paso 4: Invertir en el recurso humano. Tanto los desarrolladores como los especialistas en operaciones deben desarrollar nuevas habilidades.

Paso 5: Medir el éxito de DevOps. Medir aspectos como: frecuencia de implementación de nuevas versiones, tasa de fallas causadas por cambios, tiempo medio en restaurar los servicios (MTTR), tiempo requerido para aplicar un cambio, entre otros.

Una segunda propuesta de implementación de DevOps es la que plantea New Relic en su publicación *Kickstarting DevOps* (New Relic, 2017). Consta de cuatro pasos que se describen a continuación.

Paso 1: Alinearse con las metas del negocio. Conocer cuáles son los objetivos estratégicos de la empresa.

Paso 2: Caracterizar el ambiente actual. Identificar el estado actual del entorno para que se pueda medir el progreso.

Paso 3: Obtener el apoyo de las partes interesadas. Involucrar a las personas con influencia y poder para obtener el apoyo necesario durante la implementación.

Paso 4: Establecer y dar seguimiento a indicadores de desempeño. Medir el éxito de DevOps en aspectos como: frecuencia de implementación de nuevas versiones, tasa de fallas causadas por cambios, tiempo medio en restaurar los servicios (MTTR), tiempo requerido para aplicar un cambio, entre otros.

2.5. Agile

Tradicionalmente los productos de software se han desarrollado utilizando la metodología de cascada, la cual consiste básicamente ejecutar una serie de pasos uno tras otro hasta finalizar con el producto esperado.

Todo empieza con la fase de planeación en la que el equipo de trabajo escribe en conjunto los requerimientos que deberá satisfacer el producto de software. Luego el equipo documenta todos los pasos a seguir y estima el tiempo que les tomará tener el software listo. Posteriormente, todas las partes interesadas revisan el plan de trabajo. Una vez que el plan ha sido aprobado, los

desarrolladores comienzan a escribir el código. Cuando tienen el producto terminado, se prueba exhaustivamente y, por último, se entrega al cliente (Dimes, 2015).

Sin embargo, esta metodología de trabajo tienes varios problemas, siendo el principal su rigidez. Todo debe estar por escrito antes de empezar a escribir la primera línea de código, asume que los requerimientos identificados al inicio son los único y que no cambian durante el ciclo de vida del desarrollo del producto, las estimaciones casi nunca coinciden con el tiempo efectivo empleado para crear el producto, entre otros inconvenientes que terminan provocando el fracaso de muchos proyectos.

Agile es un marco de referencia que propone un enfoque distinto en el desarrollo de software y que básicamente plantea que los productos de software deben crearse a través de múltiples iteraciones de corta duración, en donde cada una de ellas genere un producto terminado que se pueda mostrar al cliente y demás partes interesadas. Cada una de esas iteraciones incluye la planeación, el diseño, la codificación, las pruebas, y otros (Dimes, 2015).

Agile también establece que en el desarrollo de software deben considerarse otros factores además del tecnológico como lo son el entorno organizacional y el humano. El tecnológico se refiere los aspectos técnicos y prácticos, al cómo hacer las cosas y las situaciones que se presentan al escribir código. El organizacional se relaciona con aspectos administrativos y culturales, al entorno de trabajo y otras situaciones que trascienden el equipo. Por último, el humano incluye los aspectos cognitivo y social, el aprendizaje y las relaciones interpersonales entre compañeros, jefes y clientes (Hazzan & Dubinsky, 2009).

El Manifiesto Agile resume el enfoque de este marco de referencia en los resultados, por encima las estructuras rígidas y medios para producir software. La figura 2.10 ilustra este manifiesto.

En cuanto a las metodologías Agile, una de las que más aceptación ha tenido es Scrum que Schwaber y Sutherland (2016) definen como “un marco de referencia en el que las personas pueden abordar problemas complejos y adaptativos, a la vez que de forma productiva y creativa entregan productos del más alto valor posible” (p. 3).

Scrum consiste en equipos multidisciplinarios Scrum y sus roles, eventos, artefactos y reglas asociadas que ejecutan el trabajo de forma cíclica. Cada uno de estos componentes sirven a un propósito específico. Scrum se basa en la teoría de control de procesos por empirismo, el cual asegura que el conocimiento procede de la experiencia y de tomar decisiones basándose en lo que se conoce. Tiene tres pilares en los que se fundamenta: transparencia, inspección y adaptación. La figura 2.11 ilustra el flujo de trabajo y los ciclos de Scrum (Schwaber & Sutherland, 2016).

Transparencia: Todos en el equipo Scrum usan el mismo lenguaje y tienen la misma visibilidad de lo que se está haciendo.

Inspección: El trabajo del equipo Scrum se inspecciona con regularidad para detectar y corregir desviaciones indeseadas.

Adaptación: Si la inspección detecta una desviación fuera de los límites aceptables, el trabajo se adapta para evitar desviaciones mayores y mantener el enfoque en lo que es realmente necesario.

Figura 2.10 Manifiesto Agile. Fuente: Agile Software Engineering

Scrum prescribe cuatro eventos formales o reuniones, contenidos dentro del Sprint, para la inspección y adaptación:

Planificación del Sprint (Sprint Planning): El equipo Scrum decide y acuerda cuánto trabajo podrá realizarse en el sprint.

Scrum Diario (Daily Scrum): El equipo Scrum revisa brevemente el estado actual del trabajo y si existen impedimentos para que el trabajo se pueda realizar.

Revisión del Sprint (Sprint Review): El equipo Scrum hace una inspección del trabajo realizado en función del trabajo por hace para identificar formas de optimizar el valor del trabajo que el equipo puede hacer en los siguientes sprints.

Retrospectiva del Sprint (Sprint Retrospective): El equipo Scrum hace una revisión del trabajo hecho durante el sprint. Se acostumbra basar la revisión en las preguntas: ¿Qué se hizo bien?, ¿Qué se hizo mal? y ¿Qué se puede hace para mejorar el desempeño del equipo en próximos sprints?

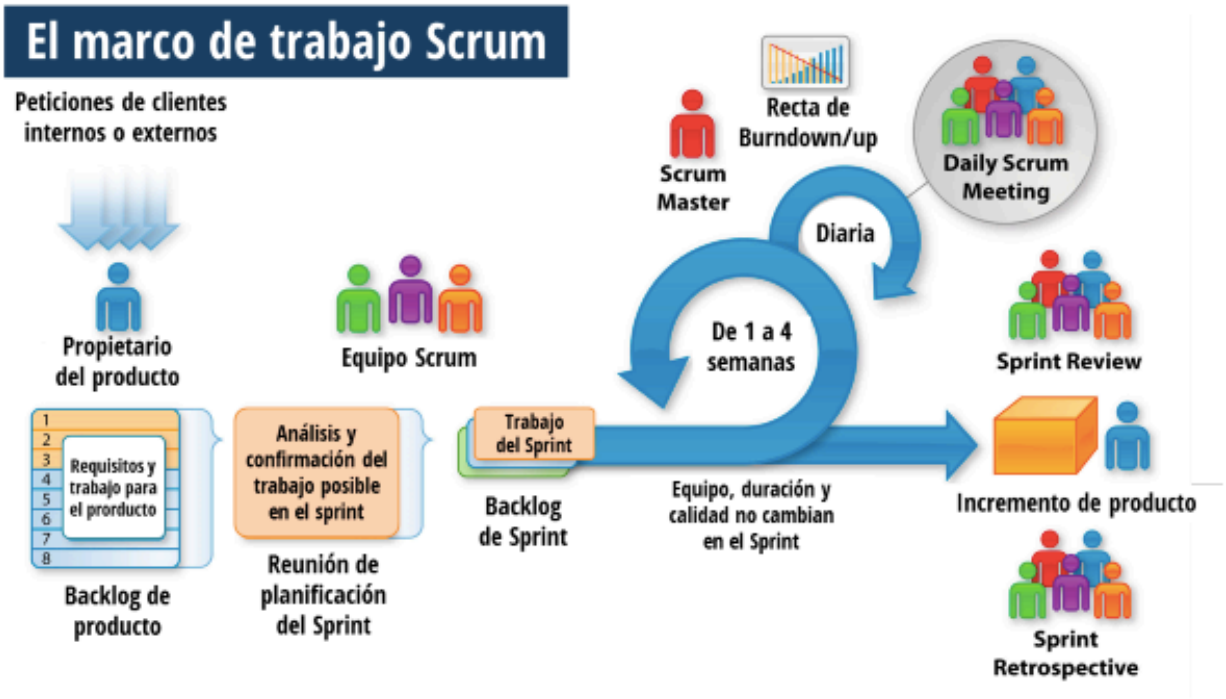


Figura 2.11 Metodología Scrum. Fuente: www.itnove.com

El equipo Scrum consiste en un Dueño de Producto (Product Owner), el Equipo de Desarrollo (Development Team) y un Scrum Master. Los equipos Scrum son autoorganizados y multifuncionales. Tienen todas las competencias necesarias para llevar a cabo el trabajo sin depender de personas que no son parte del equipo. El modelo de equipo en Scrum está diseñado para optimizar la flexibilidad, la creatividad y la productividad (Schwaber & Sutherland, 2016).

Dueño del Producto: es el responsable de maximizar el valor del producto y el trabajo del Equipo de Desarrollo.

Equipo de Desarrollo: consiste en los profesionales que realizan el trabajo para poder entregar un incremento de producto terminado que potencialmente se pueda poner en producción al final de cada Sprint.

Scrum Master: es el responsable de asegurar que Scrum se entienda y se adopte. Guía al equipo en la aplicación correcta de Scrum y procura eliminar los obstáculos que puedan impedir que el equipo haga su trabajo. (Schwaber & Sutherland, 2016)

2.6. Relación entre ITIL, DevOps y Agile

Para algunas personas ITIL no es compatible con DevOps porque el primero tiene un enfoque basado en procesos del tipo cascada, donde existen fases o etapas de un ciclo de vida que se van ejecutando de manera secuencial. Mientras que DevOps se basa en un enfoque más dinámico, más ágil y menos estructurado que tiene como objetivo primordial la entrega de resultados en el menor tiempo posible y con la menor cantidad de fallas (Daine, 2016).

En contraposición con lo anterior, varios expertos en el campo de soporte de operaciones sostienen que DevOps puede ser un complemento ideal para ITIL en las empresas. Esta es la posición de Gene Kim, quien es un investigador experimentado en soporte de TI, así como de autor de varios libros entre los que están *The Phoenix Project* y *The DevOps Handbook*. En relación con la compatibilidad entre ITIL y DevOps Gene (2016) dice que:

> ITIL es muy consistente en sus planteamientos y entre ellos está la gestión de entregas de nuevas versiones de software y DevOps viene a facilitar la automatización de ese proceso. Se ha malinterpretado la idea de que el personal DevOps odia los procesos, cuando en realidad lo que no le agrada son las aprobaciones del proceso de gestión de cambios porque es gente a quien le gusta la automatización y ejecución rápida de las tareas.

Sobre la misma línea de pensamiento, Kaimar Karu, Director de Estrategia de Producto y Desarrollo en Axelos, indica en Daine (2016) lo siguiente:

> El truco para sacar el mayor provecho de ITIL es asegurar la adopción de la mentalidad de gestión de servicios y la adopción de la guía de buenas prácticas de acuerdo con las necesidades específicas de la organización. DevOps ayuda a que esto ocurra proveyendo soporte adicional al “cómo” en relación con los conceptos fundamentales de la gestión de servicios, creando valor a través de la colaboración y manteniendo el enfoque en el cliente.

La compatibilidad entre ITIL y DevOps va más allá y tambien se relaciona con la incorporación de metodologías ágiles que faciliten y permitan el desarrollo rápido de procesos automatizados en el soporte y creación de servicios de TI. Esto es lo que piensa Jayne Groll quien es presidenta de la ITSM Academy y miembro de la Junta Directiva del DevOps Institute (DOI) en Diane (2016):

> DevOps no disminuye el valor de ITIL, lo valida y lo hace más maduro. De manera más importante, DevOps finalmente establece las conexiones entre ITIL, Agile y otros métodos y marcos de referencia en la automatización del ámbito de IT.

3. Capítulo III: Marco metodológico

A continuación se describe la metodología que se usará en el desarrollo del presente proyecto, la cual está organizada en fases que serán descritas en detalle más adelante. Posteriormente se hablará sobre las técnicas a emplear para la recopilación de los datos que permitirán conocer a fondo el proceso actual de soporte, los recursos con que se cuenta, el contexto organizacional en que se desarrolla el proceso, el conocimiento que existe en la empresa sobre ITIL, DevOps y Agile; para más adelante poder diseñar y proponer los procesos que sugiere ITIL para una adecuada ejecución de la operación del servicio, apoyados en el enfoque DevOps y los principios Agile.

Se empleará el enfoque cualitativo en el desarrollo del proyecto, el cual Hernández et al. (2010) describen de la siguiente forma:

> Los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, primero, para descubrir cuáles son las preguntas de investigación más importantes, y después, para rellenarlas y responderlas. La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien “circular” y no siempre la secuencia es la misma, varía de acuerdo con cada estudio en particular. (p. 7)

Se mencionan y describen, también, las herramientas que permitirán recopilar y procesar estos datos con el objetivo de producir los resultados que se esperan de acuerdo con los objetivos planteados en este proyecto.

3.1. Descripción de la metodología

En el desarrollo del presente proyecto se empleará el método deductivo que Bernal (2010) define como:

> El método de razonamiento que consiste en tomar conclusiones generales para obtener explicaciones particulares. El método se inicia con el análisis de los postulados, teoremas, leyes, principios, etcétera, de aplicación universal y de comprobada validez, para aplicarlos a soluciones o hechos particulares. (pp. 59)

Se partirá del análisis de ITIL® 2011, específicamente en la fase operación de servicio, como marco de referencia de buenas prácticas para la gestión de los servicios de tecnologías de información, DevOps como enfoque de integración y colaboración entre desarrollo y operaciones y los principios Agile como marco de referencia para la optimización de los procesos. Se buscará aplicarlo en el diseño del proceso de soporte de aplicaciones de seguridad de información por parte del equipo de trabajo InfoSec Costa Rica.

La metodología consiste de cinco fases, a saber: análisis de la situación actual, conocimiento del marco de referencia organizacional para la operación del servicio en Intel, lista de verificación de elementos de ITIL, DevOps y Agile, diseño de procesos y hoja de ruta de implementación y, por último, evaluación y mejoras. La figura 12 ilustra las fases de esta metodología.

3.2. Fases de la metodología

A continuación, se describe cada una de las fases de la metodología utilizada en el desarrollo del presente proyecto. La figura 3.1 muestra las distintas fases y la forma en que éstas se relacionan entre sí.

3.2.1. Fase 1: Análisis de la situación actual

En esta primera fase el objetivo es conocer la situación actual del proceso de soporte de aplicaciones de seguridad de información que ejecuta el grupo InfoSec de Intel Costa Rica, con el fin de determinar las condiciones en que se presta el servicio, conocer el origen de la demanda del servicio, los recursos disponibles, el nivel de conocimiento del personal, entre otros.

La información se obtendrá usando como guía la metodología propuesta por Dumas et al. (2013) que se describió en el marco teórico. Específicamente para este proyecto se aplicarán los siguientes pasos:

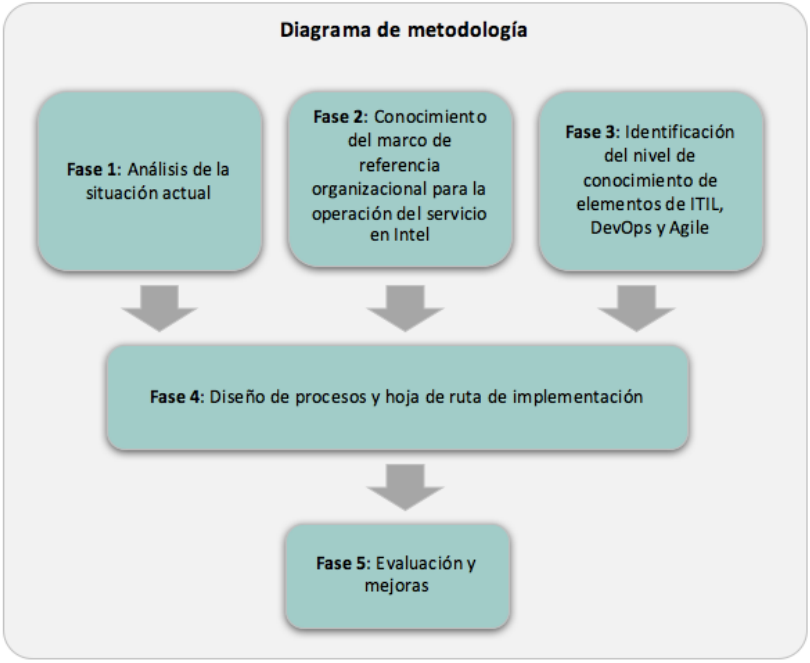


Figura 3.1 Diagrama de metodología. Fuente: Elaboración propia

3.2.1.1. Identificar roles

En este paso se van a identificar las personas a quienes se les considera los expertos en el actual proceso de soporte, desde el punto de vista de conocimiento del negocio, conocimiento técnico sobre las aplicaciones, las herramientas y tecnologías utilizadas.

3.2.1.2. Recopilar la información.

La información del proceso se pretende recopilar mediante lectura de documentos técnicos sobre las aplicaciones, el proceso, documentos sobre políticas de seguridad, entre otros. Asimismo, se pretende observar el proceso en ejecución y tomar nota sobre la forma en que se ejecuta y la participación de los expertos.

También, una vez identificados los expertos se realizarán entrevistas abiertas donde se les pedirá que brinden información acerca del proceso, de la forma en que ellos realizan sus actividades, de la relación que pueda existir entre su rol y los objetivos del departamento o la empresa, entre otros.

3.2.1.3. Modelar el proceso

Con la información obtenida en los pasos anteriores se creará un modelo del proceso utilizando BPMN (Business Process Model and Notation) que es una notación estándar para modelar procesos.

En el modelo se pretenden identificar los límites del proceso, las actividades y eventos esenciales, los recursos y las transiciones entre ellos, el flujo de control y cualquier otro elemento adicional que se llegue a considerar relevante para comprender con claridad el proceso.

3.2.1.4. Asegurar la calidad del modelo

Por último, se hará una revisión del modelo creado con el propósito de asegurar que se respeta el uso de BPMN, que las características del proceso representado reflejan el proceso actual que ejecuta InfoSec de Intel Costa Rica y que el modelo es fácilmente interpretado y comprendido por miembros del equipo de trabajo y de otras partes interesadas.

3.2.2. Fase 2: Conocimiento del marco de referencia organizacional para la operación del servicio en Intel

En esta fase se pretende conocer si existen políticas o directrices establecidas a lo interno de la empresa, la unidad de negocio, el departamento o el grupo de trabajo acerca del uso de metodologías, marcos de referencia, guías de buenas prácticas, entre otros, para el soporte de aplicaciones o desarrollo de la operación del servicio en términos generales.

3.2.3. Fase 3: Lista de verificación de elementos de ITIL, DevOps y Agile

Será importante identificar el nivel de conocimiento que existe en la empresa sobre ITIL, DevOps y Agile, por tanto, se utilizarán listas de verificación que permitirán conocer cuáles elementos de estos marcos de referencia están siendo utilizados en la organización.

3.2.4. Fase 4: Diseño de procesos y hoja de ruta de implementación

Siguiendo las recomendaciones de ITIL, DevOps y Agile y tomando en consideración los datos obtenidos en las fases previas, se propondrá un diseño de los procesos sugeridos en esta fase, así como una hoja de implementación que pueda servir de guía ante una eventual decisión de implementar los procesos por parte de la empresa.

3.2.5. Fase 5: Evaluación y mejoras

Ni las empresas ni los procesos son estáticos, sino que evolucionan con el tiempo, por lo que se propondrán acciones para evaluar la forma en que se estén ejecutando los procesos propuestos en la fase anterior, de tal manera que se puedan identificar oportunidades de mejoras.

3.3. Participantes

Los miembros de la organización elegidos para brindar toda la información relacionada con la empresa, el proceso actual y más corresponden a dos líderes técnicos, el primero de ellos es líder técnico del equipo de soporte de aplicaciones de seguridad de información y el segundo es el líder técnico del equipo de operaciones.

3.4. Técnicas

Entre las técnicas a utilizar en el desarrollo del proyecto están las mencionadas por Bernal (2010):

- **Entrevistas**: consiste en recoger información mediante un proceso directo de comunicación entre entrevistador(es) y entrevistado(s).
- **Observación**: proceso riguroso que permite conocer, de forma directa, el objeto de estudio para luego describir y analizar situaciones sobre la realidad estudiada. (p. 57)

Asimismo, se recolectarán datos mediante documentos, registros, materiales y artefactos como listas de verificación para evaluar el uso de ITIL, DevOps y Agile que, de acuerdo con Hernández et al. (2010) “sirven al investigador para conocer los antecedentes de un ambiente, las experiencias, vivencias o situaciones y su funcionamiento cotidian (p. 433)”.

3.5. Herramientas

Seguidamente se describirán las herramientas o instrumentos utilizados en la recolección de datos y análisis de resultados de acuerdo con las distintas fases de la metodología empleada.

3.5.1. Análisis de la situación actual

Modelos BPMN

Para la elaboración de modelos de procesos se utilizará la versión 3.1 de Bizagi Modeler que es un producto de software para la creación de modelos de procesos usando BPMN.

Tabla con información sobre roles y responsabilidades a ser identificados en el proceso de soporte de aplicaciones de seguridad de la información.

Nombre del rol	Descripción y responsabilidades
Rol 1	• Descripción • Responsabilidad • Responsabilidad
Rol 2	• Descripción • Responsabilidad • Responsabilidad

Tabla 3.1 Roles identificados en el actual proceso de soporte. Fuente: Elaboración propia

En la recopilación de datos se hará entrevistas con los participantes y se utilizará la siguiente guía.

Guía de entrevista
Preguntas a los expertos - ¿Cuáles son los procesos o actividades de soporte que se ejecutan en la organización? Describa los procesos de soporte. - Comente las interacciones que existen con otras organizaciones o equipos de trabajo. - ¿Cuáles son los roles que existen en esos procesos? Comente los roles y las interacciones entre ellos, tanto dentro de la organización de soporte como con otras organizaciones participantes. - ¿Cada rol está asignado a una persona distinta o puede haber múltiples roles desempeñados por una misma persona? a. Mencione ejemplos. b. ¿Qué pasa cuando se dan cambios en el personal? Contrataciones, despidos, renuncias, ascensos, reubicaciones, etc.

Tabla 3.2 Guía de entrevista para identificar los roles en los procesos de soporte. Fuente: Elaboración propia

3.5.2. Conocimiento del marco de referencia organizacional para la operación del servicio en Intel

Dentro de las empresas es posible que existan directrices que establecen lineamientos sobre marcos de referencia, metodologías, guías de buenas prácticas y otros, que las organizaciones deben acatar.

Con el fin de determinar si existen este tipo de lineamientos en Intel, ya sea a nivel corporativo o a nivel de Intel Costa Rica, se realizarán entrevistas a los expertos utilizando la siguiente guía.

Guía de entrevista
Preguntas a los expertos **1.** ¿Cuáles marcos de referencia o metodologías relacionados con servicios de TI se utilizan en Intel o Intel Costa Rica? **2.** ¿Se utilizan por decisión propia de cada organización o por mandato del departamento de TI? **3.** ¿Cuentan con alguna herramienta tecnológica para apoyar el uso del marco de referencia o metodología? **4.** ¿Cada organización tiene libertad de elegir usar o no el marco de referencia o metodología? ¿Pueden usar alguno otro que consideren más apropiado?

Tabla 3.3 Guía de entrevista para conocer el marco de referencia organizacional. Fuente: Elaboración propia

La información recopilada en esta fase se resumirá en la tabla descrita a continuación.

Marco de referencia, metodología, guía de buenas prácticas	Directriz	Herramienta tecnológica
Marco 1	Descripción	Herramienta
Guía	Descripción	Herramienta

Tabla 3.4 Marcos de referencia, metodologías y guías de buenas prácticas en Intel. Fuente: Elaboración propia

3.5.3. Listas de verificación de elementos de ITIL, DevOps y Agile

Para identificar el nivel de conocimiento y uso que existe en la empresa sobre las prácticas recomendadas por ITIL se utilizarán listas de verificación. Las respuestas de los participantes serán analizadas para determinar qué tanto se conoce y usan las prácticas recomendadas por este marco de referencia para la gestión de los servicios de TI.

ITIL

Para evaluar el conocimiento y grado de utilización de ITIL, específicamente la fase operación de servicio que es a la que se hace referencia en este documento, se usará el cuestionario "Service Operation Readiness Assessment" que está disponible en el sitio web de UCISA que es la Asociación de Sistemas de Información de las Universidades (Universities and Colleges Information Systems Association) del Reino Unido.

Este es un extracto del documento que por su extensión se incluirá como un anexo (Anexo II) al final del documento. Todo el contenido de la lista de verificación está en idioma inglés y no se hizo la traducción al español porque los participantes y todo el personal en Intel dominan ese idioma, de tal manera que no representa una limitante en la recopilación de datos.

A continuación, se muestran el encabezado del formulario y tres preguntas de cada sección del cuestionario, las dos primeras y la última.

	Data entry	
	Below are the only valid entries for the assessment	
	Each person must use the drop-down box and select an 2answer for each question for each process area.	
1	Initial - processes and activities are adhoc or chaotic or undefined	
2	Repeatable - basic processes and activities are established and there is a level of discipline and adherence	
3	Defined - All processes and activities are defined, documented, standardised and integrated together	
4	Managed - Processes are measured by collecting detailed data on the processes and their quality and appropriately improved	
5	Optimising - Continuous process improvement is adopted. Process and activities are mature	
	Step 1 - Enter the names of the participants here:	
	Participant 1	
	Participant 2	
	Step 2 - Now have each participant answer each question for each Service Operation area, under their name.	
1	**Service Management as a Practice**	Participant 1
1	Service Management is clearly defined	Not applicable
2	We know what our services are	Not applicable
19	Interfaces to other Service Lifecycle stages are clearly defined	Not applicable
	SCORE	0
2	**Service Operation Principles**	Participant 1
1	Distinctive functions, groups, teams, departments and divisions are defined	Not applicable
2	We have a balance between an internal IT view and external business view	Not applicable
29	We participate in the definition and maintenance of Service Management Tool work instructions	Not applicable
	SCORE	0
3	**Service Operation Processes**	Participant 1
1	We have defined Event Management's Purpose, Goal and Objective	Not applicable
2	We have defined Event Management's Scope	Not applicable
87	We have defined Access Management's Challenges, Critical Success Factors and Risks	Not applicable
	SCORE	0
4	**Common Service Operation Activities**	Participant 1
1	We know where we are on the technology centric Vs business centric scale	Not applicable
2	Monitoring and control is a continual cycle	Not applicable
42	Mainframe management is a mature practice	Not applicable
	SCORE	0
5	**Organising Service Operation**	Participant 1
1	The Service Desk function is defined	Not applicable
2	We have Justification for and the Role of the Service Desk defined	Not applicable
42	We have Hybrid Organisation Structures of the above	Not applicable
	SCORE	0

6	**Service Operation Technology Considerations**	Participant 1
1	We have Integrated IT Service Management Technology	Not applicable
2	We offer Self Help	Not applicable
25	We have IT Service Continuity Planning for ITSM Support Tools	Not applicable
	SCORE	0
7	**Implementing Service Operation**	Participant 1
1	We actively Manage Change in Service Operation	Not applicable
2	We monitor and manage Change Triggers	Not applicable
10	With Planning & Implementing Service Management Technologies we manage the timing of technology deployment	Not applicable
	SCORE	0

Tabla 3.5 Muestra del cuestionario ITIL. Fuente UCISA

Los resultados se resumirán en un gráfico de radar como el que se muestra a continuación en la figura 3.2.

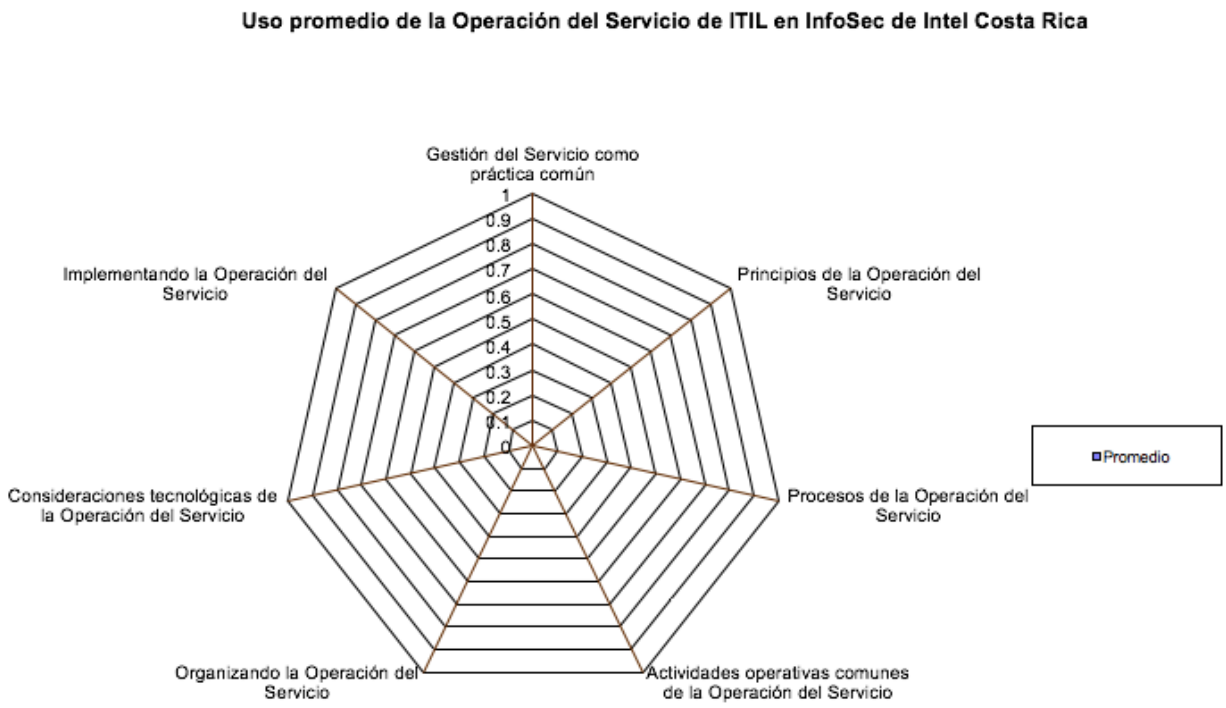


Figura 3.2 Gráfico radar con resumen de resultados de la lista de verificación ITIL. Fuente UCISA

DevOps

Para evaluar el grado de conocimiento y aplicación del enfoque DevOps se utilizará la lista de verificación propuesta por Steve Pereira y disponible en http://devopschecklist.com. Esta lista consta de 48 preguntas agrupadas en las siguientes categorías: alineamiento, contexto, capacitación, ciclo de vida, organización y proceso.

Esta lista de verificación también está en inglés y al igual que con la anterior no se tradujo al español puesto que no se consideró necesario debido a la razón antes expuesta.

THE DEVOPS CHECKLIST	
Alignment	
☐	We prioritize according to business objectives.
☐	We volunteer for tasks rather than having them assigned.
☐	Our team has clear objectives that correspond with our company vision.
☐	Our product team is focused on sustainable velocity rather than current speed.
☐	We focus on time to repair rather than time between issues.
☐	DevOps is not isolated to a specific role in our organization.
☐	DevOps is not isolated to a specific team in our organization.
☐	Our operational functions are seen as a source of competitive advantage.
Context	
☐	Representation from our operations team is involved in development sprint planning.
☐	We make potential changes visible to all members of our product team.
☐	We have an automated system for running tasks and receiving notifications with our team chat.
☐	We consult with auditors and regulators regularly and seek guidance when designing systems.
☐	Our team is encouraged to question tasks and priorities.
☐	We have a centralized instant message system including all members of our product team.
☐	All members of our product team have access to environment status, metrics and history.
☐	All members of our product team have access to code status, metrics and history.
Learning	
☐	We cultivate an environment of continuous learning.
☐	We regularly celebrate our product team's learnings and success internally.
☐	We regularly share our product team's learnings and success with the rest of our organization.
☐	We openly discuss failures in order to share learning.
☐	We identify skills needed to improve or address future objectives.
☐	We strive to examine how we complete our work, and how effectively we complete it.
☐	We estimate based on measurement and past experience.
Lifecycle	
☐	Our software development cycle is 2 weeks or less.
☐	Our software development cycle is defined by releasing a working change into production.
☐	We stop development upon discovering a defect and prioritize its repair.
☐	Developers or product owners are able to deploy our product to production.
☐	We have automated testing prior to automated production deployment.
☐	Our configuration of systems is automated.
☐	Our deployed system configuration is immutable.
☐	Our release and deployment automation is environment agnostic.

Organization	
☐	Our subject matter expertise is not isolated to individuals.
☐	We enable peer and cross-functional review for changes.
☐	Our organization is configured around cross-functional teams.
☐	Our teams are customer and product oriented.
☐	We review priorities on a regular basis.
☐	Our developers have access to production-like systems to work and test on.
☐	Our developers have access to production-like data to work and test against.
☐	Our developers have access to dependencies required to build and test software.
Process	
☐	Our organization follows agile development practices.
☐	We practice blameless postmortems.
☐	We regularly examine constraints in our delivery process.
☐	Our system configuration is committed into version control.
☐	Our documentation is version controlled and shared.
☐	We maintain a backlog of tasks, visible to all team members and available for comment.
☐	We practice test or behavior driven development.
☐	We test our changes against a merge with our mainline code.
☐	We test our changes against production-equivalent load and use patterns.

Tabla 3.6 Cuestionario DevOps. Fuente http://devopschecklist.com/

El resultado de la lista de verificación se resumirá en la siguiente tabla que califica con un porcentaje el grado de presencia de cada categoría en la organización.

DevOps	%	Elementos presentes en la organización
Alineamiento		Se unifican la dirección grupal e individual y las metas en torno a la visión de la empresa.
Contexto		La información relevante y de contacto está disponible para quien la necesite en el momento en que la necesita.
Capacitación		Se promueve el crecimiento personal y se fomenta el entendimiento a través de la mejora continua.
Ciclo de vida		Se mantiene un enfoque en el software como un producto que merece atención, cuidad y reflexión dentro de un ecosistema que cambia constantemente.
Organización		Se provee una estructura para la interacción y cohesión que apoya la colaboración y productividad.
Proceso		Se crean rituales para fomentar la consistencia y confianza propiciando un marco de referencia para la mejora continua.
Total		

Tabla 3.7 Resumen de resultados de la lista de verificación DevOps. Fuente: http://devopschecklist.com/

Agile

Para evaluar el grado de conocimiento y aplicación de los principios Agile, así como de una metodología correspondiente, en este caso Scrum, se utilizará la lista propuesta por Henrik Kniberg, específicamente la versión 2.2 y que está disponible en http://www.crisp.se/scrum/checklist. Esta lista de verificación también está en inglés y tampoco se tradujo por la misma razón mencionada en el caso de ITIL. La figura 3.3 muestra el formulario con las preguntas propuestas.

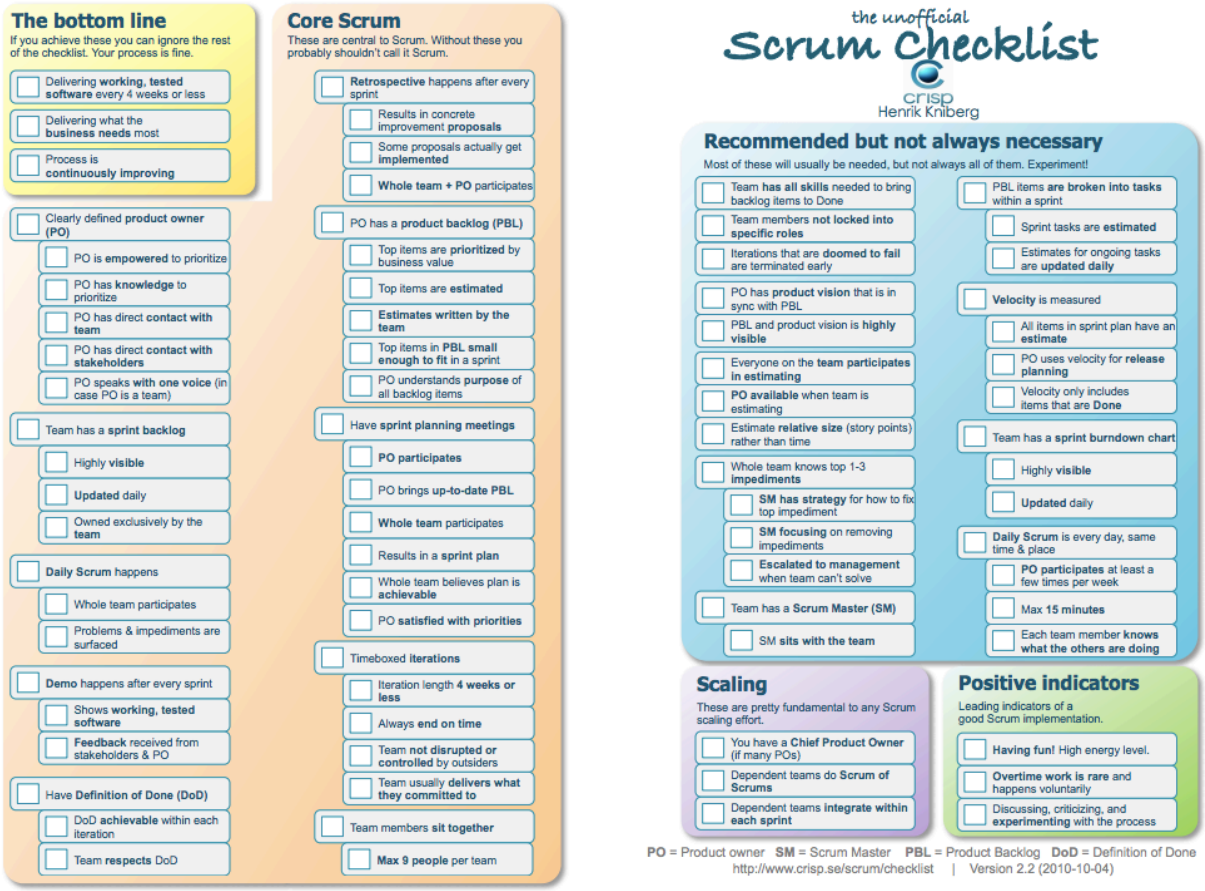


Figura 3.3 Lista de verificación Agile (Scrum). Fuente: Henrik Kniberg

Los resultados de esta lista de verificación se resumirán en una tabla con el siguiente formato.

Scrum	Elementos presentes en la organización
Elementos esenciales de Scrum	• Elemento 1 • Elemento 2
Elementos recomendados de Scrum	• Elemento 1 • Elemento 2
Escalamiento de Scrum	• Elemento 1 • Elemento 2
Indicadores positivos	• Elemento 1 • Elemento 2

Tabla 3.8 Elementos de Scrum como metodología Agile utilizados en InfoSec de Intel Costa Rica. Fuente: Elaboración propia.

3.5.4. Diseño de procesos y hoja de ruta de implementación

Diagramas

Los procesos propuestos serán representados con diagramas BPMN y habrá uno para cada proceso que propone ITIL en la operación del servicio.

3.5.5. Evaluación y mejoras

Las encuestas representan un recurso valioso para la captura de información que servirá posteriormente para evaluar y mejorar los procesos aquí propuestos. La siguiente tabla muestra el formato en que se presentarán algunas preguntas que pueden ser incluidas en encuestas.

Pregunta	Tipo de Respuesta
Pregunta 1	Descripción de la escala para la respuesta.
Pregunta 2	Descripción de la escala para la respuesta.
Pregunta n	Descripción de la escala para la respuesta.

Tabla 3.9 Ejemplos de preguntas para encuesta de evaluación de calidad de servicios. Fuente: Elaboración propia.

Además de las encuestas, los indicadores de desempeño son herramientas de gran utilidad en los procesos de mejora continua. Ejemplos de indicadores se presentarán en una tabla con el siguiente formato.

Proceso	Indicador	Unidad de Medida	Frecuencia	Observaciones
Gestión de Eventos	• Indicador 1 … • Indicador n			
Gestión de Incidentes	• Indicador 1 … • Indicador n			
Resolución de Solicitudes	• Indicador 1 … • Indicador 2			
Gestión de Problemas	• Indicador 1 … • Indicador 2			
Gestión de Acceso	• Indicador 1 … • Indicador 2			

Tabla 3.10 Indicadores iniciales recomendados para evaluar y mejorar los procesos propuestos para la operación del servicio. Fuente: Elaboración propia.

4. Capítulo IV: Análisis de resultados

En este capítulo se presentará un análisis de los datos recopilados en la empresa, el cual permitirá, en primera instancia, describir el proceso de soporte de aplicaciones de seguridad de la información tal y como se realiza actualmente y, luego, se hará una propuesta de cómo debería ser el mismo proceso de acuerdo con el planteamiento de buenas prácticas que hace ITIL y considerando, también, los principios de Agile y el enfoque DevOps.

4.1. Análisis de la situación actual

En este apartado se documenta la información que se obtuvo durante el análisis del estado actual del proceso de soporte de aplicaciones de seguridad de la información.

4.1.1. Identificar roles

Mediante entrevistas con los participantes, se identificaron cuatro roles en el proceso de soporte que se describen a continuación en la tabla 4.1.

Nombre del rol	Descripción y responsabilidades
Agente de soporte	• Es la persona encargada de brindar soporte a las aplicaciones de seguridad de información. • Implementa los cambios en la infraestructura de aplicaciones en coordinación con el equipo de desarrollo. • Coordina el consumo de servicios con otros departamentos de TI de los cuales depende el funcionamiento de las aplicaciones, tales como hosting, redes, almancenamiento, entre otros. • Recibe las notificaciones de incidentes y los lleva al equipo scrum.
Scrum de desarrollo	• Es la persona en cargada de implementar nuevas funcionalidades y cambios en las aplicaciones. • Colabora con los agentes de soporte en la solución de incidentes.
Dueño de servicio	• Es el representante de la aplicación soportada o el servicio dentro del portafolio que reune a ciertas aplicaciones soportadas. • Presenta las solicitudes de cambio ante el equipo scrum. • Valida los cambios implementados en las aplicaciones. • Valida las soluciones a los incidentes de las aplicaciones.
Servicio de dependencia	• Son los servicios que se requieren para el buen funcionamiento de las aplicaciones y que son brindados por otras organizaciones dentro del departamento de TI (hosting, redes, centros de datos y otros).

Tabla 4.1 Roles identificados en el actual proceso de soporte. Fuente: Elaboración propia.

4.1.2. Recopilar información del proceso actual

La información se recopiló mediante entrevistas a miembros del equipo de soporte de aplicaciones de seguridad de la información, lectura de documentación técnica de las aplicaciones soportadas (cabe aclarar que esta documentación no pudo ser incluida en el presente documento debido a restricciones de propiedad intelectual de la empresa) y observación del proceso actual de soporte.

Las entrevistas se realizaron al líder técnico del proceso actual de soporte, así como al líder técnico del equipo de soporte de operaciones que existe dentro del equipo de soporte de aplicaciones. En el Anexo III se pueden ver las minutas de las entrevistas.

En el proceso actual de soporte de aplicaciones de seguridad de información se atienden los incidentes y las solicitudes de cambios. A estas últimas se les presta mucha atención principalmente porque de acuerdo con los entrevistados, se descubrió que la falta de una adecuada gestión de cambios es la principal causa de los incidentes que se atienden.

No existe un proceso actual de gestión de problemas claramente definido dentro del equipo de soporte de aplicaciones. Sin embargo, el equipo de soporte de operaciones colabora con el proceso de gestión de problemas que existe en el departamento de Seguridad de la Información, que es la organización padre a la que pertenece InfoSec de Intel Costa Rica. Los procesos de gestión de eventos y gestión de acceso no se llevan a cabo.

La gestión de los incidentes inicia con el recibimiento de una notificación proveniente de los dueños de los servicios (aplicaciones) soportados por parte del equipo de soporte de operaciones. Una vez recibida la notificación se toma nota del incidente y se lleva a la reunión diaria del Scrum de desarrollo donde se le asigna una prioridad y se determina quién será responsable de resolverlo. Esta persona responsable no necesariamente es quien hará todas las actividades necesarias para resolverlo; de ser requerido, debe coordinar y solicitar ayuda, tanto de otros miembros del equipo de soporte como de otras organizaciones y departamentos.

Una vez que el incidente se ha resuelto, el equipo de soporte de operaciones notifica al usuario que reportó el incidente para que proceda a validar la solución implementada. La figura 4.1 muestra una representación del proceso actual de gestión de incidentes en notación BPMN.

En cuanto a las solicitudes de cambios, el proceso actual inicia cuando un dueño de servicio pide un cambio. Estas solicitudes las recibe el equipo de soporte y se llevan a la reunión diaria del Scrum de desarrollo donde se le asigna una prioridad, se convierte en historias de usuario y se asignan responsables, que son principalmente los desarrolladores.

Cuando los desarrolladores han terminado su trabajo, se prueba el cambio para asegurar el correcto funcionamiento de la funcionalidad implementada o de la exactitud de los datos corregidos. Si todo está bien, el equipo de soporte de operaciones procede a implementar el cambio en producción coordinando, de ser necesario, la colaboración de otros equipos u

organizaciones que brindan servicios de hosting, redes, Directorio Activo (Active Directory), y otros.

Una vez que se ha completado la implementación del cambio, el equipo de soporte de operaciones notifica al dueño de la aplicación para que procedan a validarlo. La figura 4.2 muestra una representación de los procesos actuales de gestión de cambios y resolución de solicitudes en notación BPMN.

Los procesos de gestión de eventos y gestión de acceso no se realizan de manera formal. Tampoco la gestión de problemas se lleva a cabo de manera formal, pero el equipo de soporte de operaciones participa/colabora con en el proceso de gestión de problemas que realiza la organización padre a la que pertenece InfoSec de Intel Costa Rica.

4.1.3. Modelar el proceso

En esta sección se incluyen diagramas BPMN que muestran la forma en que el proceso actual de soporte de aplicaciones gestiona los incidentes (figura 4.1) y las solicitudes de cambios (figura 4.2). Los demás procesos que se incluyen en la operación de servicio de ITIL no se representan porque no se llevan a cabo de manera formal en la organización.

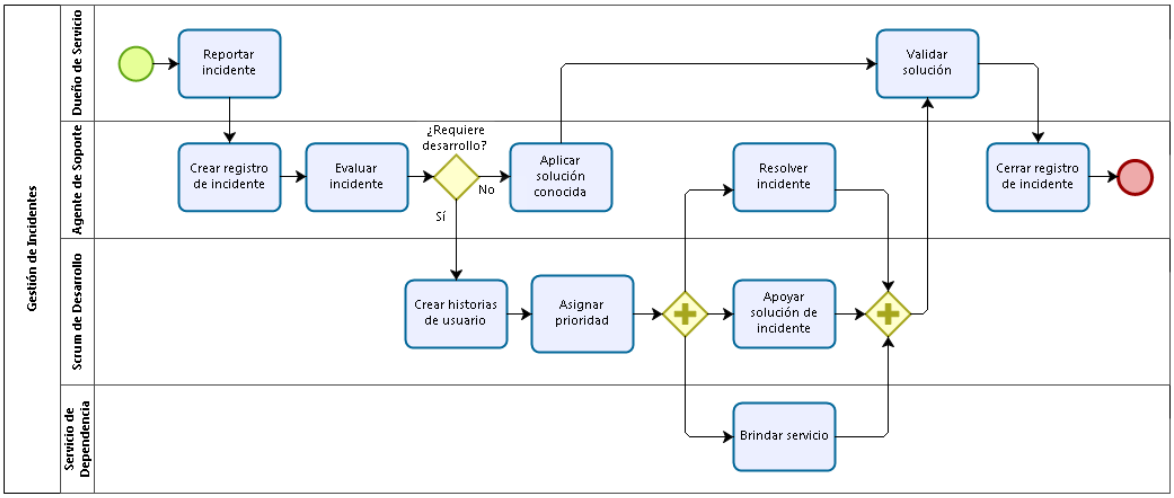


Figura 4.1 Proceso actual de gestión de incidentes. Fuente: Entrevista a experto

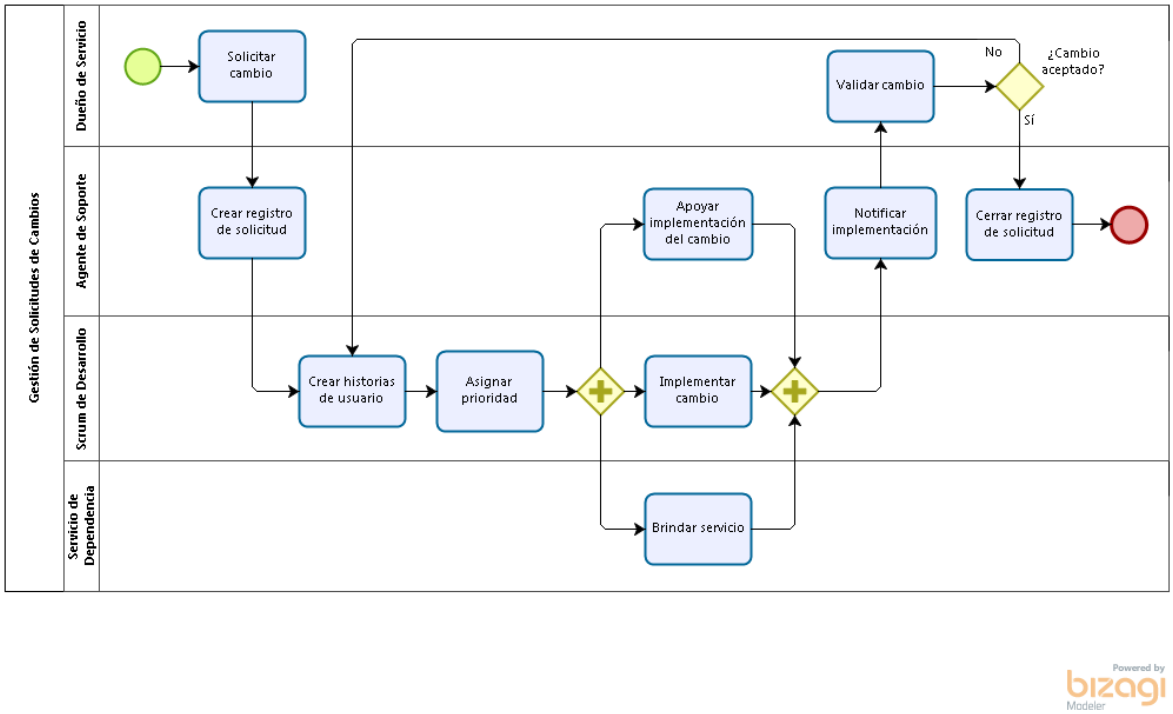


Figura 4.2 Proceso actual de resolución de solicitudes de cambios. Fuente: entrevista a experto

4.1.4. Asegurar la calidad del modelo

La descripción correcta de los procesos mediante los modelos BPMN fue confirmada por los participantes por medio de un correo electrónico que se incluye en la figura 4.3.

4.2. Marco de referencia institucional

En entrevistas con los participantes se obtuvo la información referente a los lineamientos emitidos en torno al uso de marcos de referencia y metodologías relacionados con la prestación y soporte de servicios de TI tanto a nivel corporativo, como en el contexto del departamento de TI e Intel Costa Rica.

Asimismo, el autor de este documento tuvo la oportunidad de estar presente en algunas de las sesiones informativas que desarrolló la gerencia de TI mientras era empleado de Intel, lo que le permitió confirmar la información suministrada por los participantes. Esta posibilidad del autor de aportar al proyecto como un participante más está respaldada por Hernández Sampieri, Fernández Collado, & Baptista Lucio (2010) que mencionan que:

> En la indagación cualitativa, los instrumentos no son estandarizados, en ella se trabaja con múltiples fuentes de datos, que pueden ser entrevistas, observaciones directas, documentos, material audiovisual, etc. (p. 409)

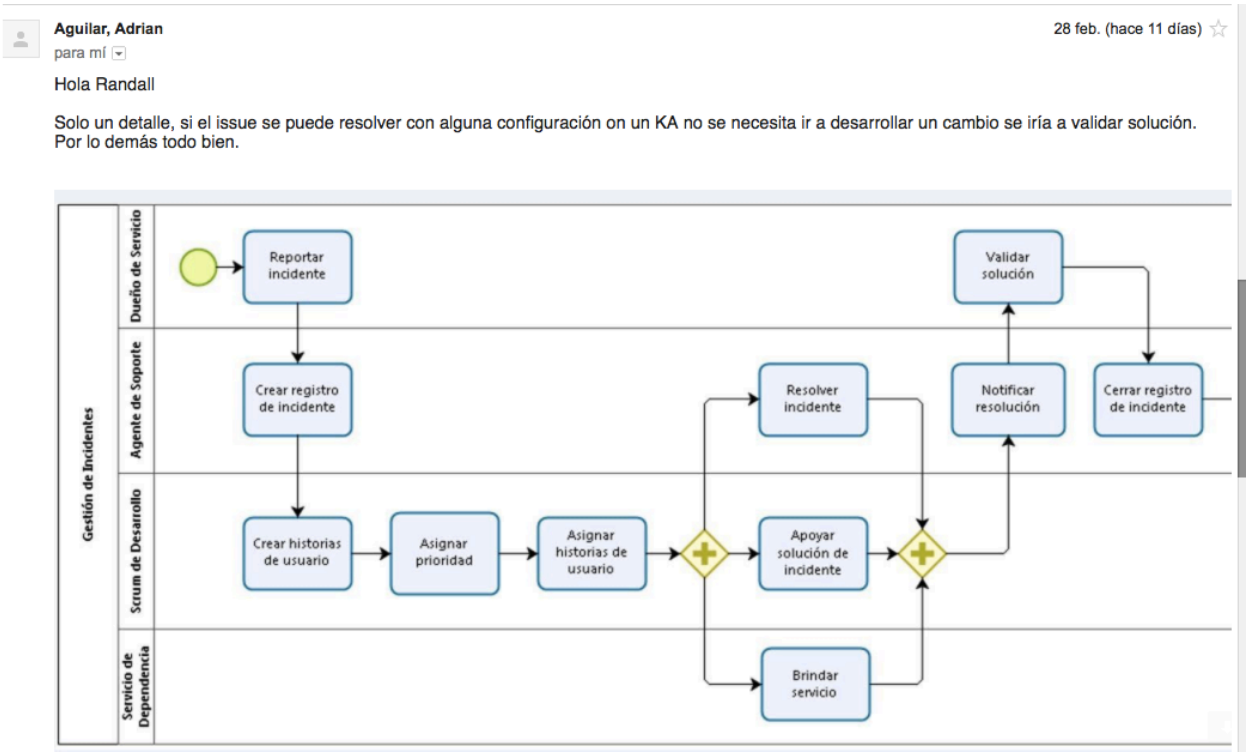


Figura 4.3 Validación de los modelos por parte de los participantes. Fuente: Correo electrónico

A nivel del departamento de TI existen directrices que procuran la estandarización y el uso de buenas prácticas en los procesos que se ejecutan en las distintas organizaciones del departamento. Por lo general están relacionadas con marcos de referencia de buenas prácticas, sin embargo, también pueden hacer referencia a herramientas o tecnologías específicas.

En el caso de la gestión de servicios de TI en Intel, se debe utilizar ITIL. Actualmente la versión oficialmente utilizada es la del 2007, conocida como ITIL v3. Sin embargo, las distintas organizaciones dentro del departamento de TI cuentan con la potestad de actualizar sus procesos a ITIL si consideran que la actualización les traerá beneficios y les ayudará a aportar valor a la empresa.

Para apoyar la implementación de ITIL la empresa cuenta con infraestructura de TI que está a disposición de todos los departamentos, así como un producto de software de nombre ServiceNow (ServiceNow, 2016) que facilita la creación de registros para cada uno de los procesos definidos por el marco de referencia, así como el seguimiento que cada rol le da a esos registros conforme se avanza en los procesos. Además, existe un Centro de Servicios que apoya las implementaciones de ITIL en las distintas organizaciones del departamento de TI.

A inicios del 2016 se emitió una nueva directriz en la que se solicita que todas las organizaciones deben utilizar metodologías Agile en sus procesos y combinarlas con el enfoque DevOps con el

fin de hacer los procesos más eficientes y aportar más valor a los negocios de la empresa a través de una adaptación más rápida a las exigencias del mercado en que opera Intel.

En el Departamento de TI se encentran disponibles una serie de herramientas que permiten la automatización de actividades como el monitoreo de sistemas a través de System Center Operations Manager (SCOM) de Microsoft o la administración de la configuración a través de Puppet, que es utilizado en otras organizaciones dentro del departamento.

En el Anexo VII puede encontrarse más información sobre las herramientas aquí mencionadas, en caso de que el lector desee conocer un poco más acerca de éstas. Cabe mencionar que el autor formó parte de Intel durante diez años, tiempo en el cual tuvo la oportunidad de tener conocimiento sobre el uso exitoso de algunas de estas herramientas en otras organizaciones pertenecientes al Departamento de TI.

La metodología Agile más ampliamente utilizada en la empresa es Scrum y la herramienta que emplean para apoyar el uso de esta metodología es JIRA (Atlassian, 2016), además de la reciente incorporación de CA Agile Central, anteriormente conocida como Rally (Computer Associates, 2016). Sin embargo, la directriz no establece cuáles herramientas deben ser utilizadas, por lo que cada organización cuenta con la libertad para elegir aquellas que consideran más adecuadas y que mejor se ajustan a sus características operativas y de conformación de recursos.

La tabla 4.2 resume las directrices emitidas por el departamento de TI en temas relacionados con el presente proyecto.

Marco de referencia, metodología, guía de buenas prácticas	Directriz	Herramienta tecnológica
ITIL	Se promueve el uso de ITIL v3 en todas las organizaciones que ofrecen servicios de TI.	ServiceNow
DevOps	El departamento de TI solicita a todas sus organizaciones que empleen el enfoque DevOps en sus procesos.	Puppet, Jenkins, Docker, Git, Team City, SCOM.
Agile	El departamento de TI solicita a todas sus organizaciones que utilicen metodologías ágiles en sus procesos. Aunque este tipo de metodologías se aplican principalmente al desarrollo de software, se busca que otros procesos puedan beneficiarse de sus bondades.	JIRA, CA Agile Central (antes llamado Rally)

Tabla 4.2 Marcos de referencia, metodologías y guías de buenas prácticas en Intel.

4.3. Listas de verificación

Con el objetivo de evaluar el grado de conocimiento y utilización ITIL, DevOps y metodologías ágiles se procedió a entregar cuestionarios que los participantes respondieron. Los resultados de estas evaluaciones se presentan a continuación.

4.3.1. ITIL 2011

El cuestionario aplicado evaluó qué tanto se aplican los principios de la operación del servicio de ITIL, sus procesos, las actividades operativas comunes, qué tan organizado está el proceso actual en función de la operación del servicio, la consideración de las tecnologías, cuán implementada está la operación del servicio de ITIL, así como una consideración general de la gestión del servicio en la organización.

Los cuestionarios completos con sus respetivas respuestas se pueden encontrar en el Anexo IV. Seguidamente se presenta en la figura 4.4 el resumen de los resultados obtenidos con las respuestas de los participantes.

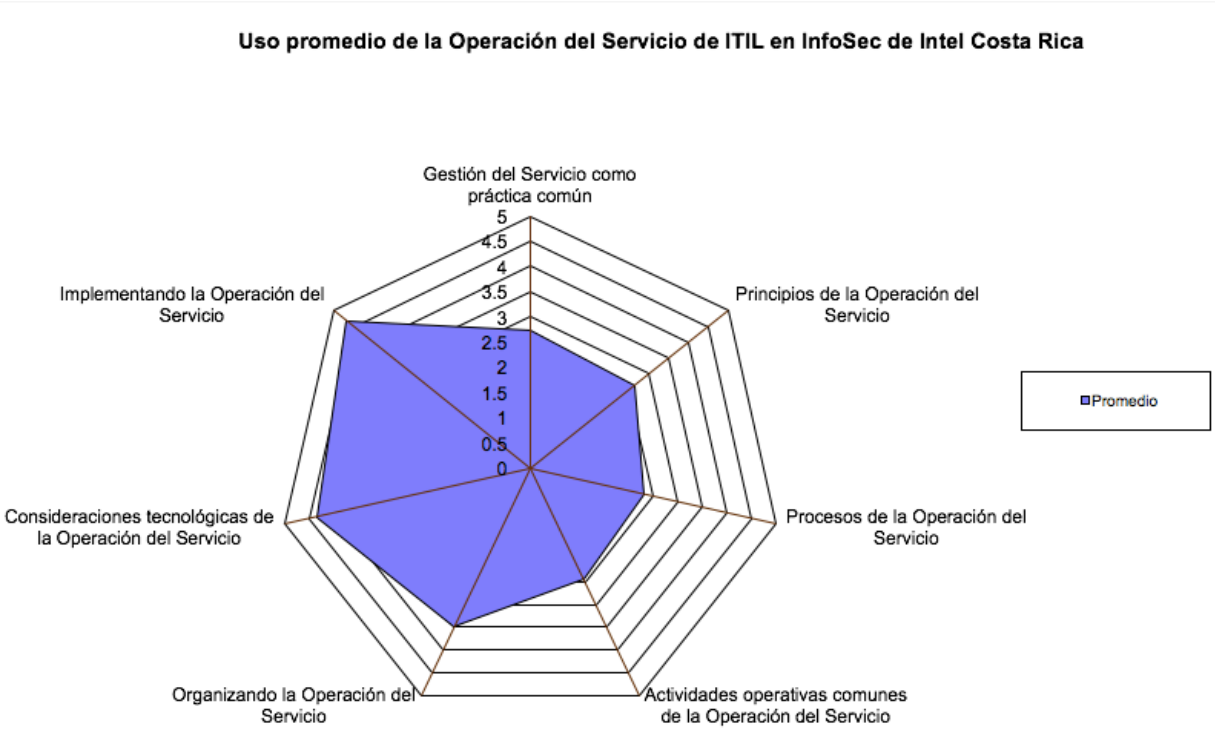


Figura 4.4 Resultados de lista de verificación ITIL. Fuente: UCISA

Se puede ver cómo, a pesar de que algunos elementos de ITIL están presentes en el proceso actual de soporte, en la actualidad los mayores esfuerzos se centran en la organización e

implementación del proceso de soporte en torno a este marco de referencia. Esto coincide con lo observado en la evaluación del estado actual del proceso de soporte donde solamente se realiza la gestión de incidentes y gestión de solicitudes de cambios. Los demás procesos de la operación del servicio no están presentes de manera formal.

4.3.2. DevOps

Se pidió a los participantes miembros de la organización que respondieran a las preguntas del cuestionario de la tabla 3.6 y los resultados se resumen a continuación en la tabla 4.3. Los resultados individuales de cada participante se pueden ver en el Anexo V.

DevOps	%	Elementos presentes en la organización
Alineamiento	94	Unificar la dirección y los objetivos individuales y colectivos alrededor de la visión estratégica de la empresa.
Contexto	69	Hacer que la información y los contactos relevantes estén disponibles para quien los necesite, cuando los necesite.
Aprendizaje	71	Apoyar el crecimiento personal y fomentar la comprensión del negocio a través de la mejora continua.
Ciclo de vida	26	Enfocarse en el software como un producto que merece cuidado, atención y reflexión dentro de un ecosistema que cambia constantemente.
Organización	63	Proveer una estructura que fomente la interacción y la cohesión para apoyar la colaboración y productividad.
Proceso	84	Crear rituales para fomentar la consistencia y confianza, creando un marco de referencia para la mejora continua.
Total	**68**	

Tabla 4.3 Resultados de la lista de verificación DevOps en InfoSec de Intel Costa Rica. Fuente: Cuestionario aplicado

Considerando estos resultados se puede ver cómo el alineamiento obtuvo un 94% lo que quiere decir que la organización tiene una clara visión de los objetivos de la empresa y mantiene los suyos propios alineados a ellos. Por su parte, el aprendizaje obtuvo un 71%, es decir, se busca promover el entrenamiento de los miembros del equipo, así como la estimulación de un entorno de confianza que sirva de plataforma para la mejora continua del desempeño y resultados del equipo de trabajo.

Por otra parte, de los resultados se desprende que hay un aspecto que podría considerarse negativo y es que el enfoque sobre los productos que soportan y que corresponde al ciclo de vida de las aplicaciones de seguridad de información obtuvo solamente un 26%, es decir,

requiere una mejora entorno a la importancia y trascendencia que tiene este tipo de productos en entornos rápidamente cambiantes como es el mercado de tecnologías en que se desempeña la empresa.

4.3.3. Agile

Una vez aplicada la lista de verificación descrita en la figura 3.3 se obtuvieron los resultados que se presentan a continuación en la tabla 4.4. En la columna correspondiente a las respuestas de los participantes, un "punto" significa que el elemento está presente. Como se puede ver en la matriz anterior, los elementos esenciales de Scrum están presentes en la organización, así como otros elementos recomendados que permiten comprobar una buena comprensión de la metodología.

Scrum	Elementos presentes en la organización	Participante 1	Participante 2
Elementos escenciales de Scrum	El dueño del producto (PO) está definido claramente	•	
	Se tiene un backlog del sprint	•	•
	Se hace una reunión scrum diaria	•	•
	Se recibe retroalimentación de interesados y PO	•	•
	Se tiene una definición de "terminado"	•	•
	Se tiene la reunión de retrospectiva al final de cada sprint	•	•
	El equipo respeta la definición de "terminado"	•	
	El PO tiene un backlog de producto (PBL)	•	•
	Se tienen reuniones de planeación del sprint	•	•
	Las iteraciones son de duración fija	•	•
	Los miembros del equipo están ubicados físicamente juntos en la oficina	•	
Elementos recomendados de Scrum	El equipo cuenta con las habilidades necesarias para llevar todos los elementos del backlog al estado "terminado".	•	•
	Miembros del equipo no encasillados en roles específicos		•
	Iteraciones condenadas al fracaso se terminan temprano		
	El PO tiene la visión del producto que está sincronizada con el PBL	•	•
	PBL y la visión del producto son altamente visibles		•
	Todos en el equipo participan en el cálculo de estimaciones	•	•
	El PO está disponible cuando el equipo está estimando	•	•
	Se estima un tamaño relativo (puntos de historia) en vez de tiempo	•	•
	Todo el equipo conoce los impedimentos principales	•	•
	El equipo tiene un Scrum Master (SM)	•	•
	Los elementos del PBL se dividen en tareas dentro de un sprint	•	•

	Todos los elementos en el plan del sprint tienen un estimado	•	•
	El PO usa la velocidad para planeación de versiones		•
	La velocidad del equipo solo incluye ementos que están terminados	•	•
	El equipo tiene un gráfico de trabajo pendiente del sprint	•	•
	La reunión scrum diaria es cada día, a la misma hora y en el mismo lugar	•	•
Escalamiento de Scrum	Hay un Dueño de Producto en Jefe (si hay muchos PO)	•	•
	Equipos dependientes hacen scrum de scrums	•	•
	Equipos dependientes se integran en cada sprint		•
Indicadores positivos	El equipo se diverte, hay un alto nivel de energía	•	•
	El sobretrabajo es raro y ocurre voluntariamente	•	•
	Se discute, se critica y se experimenta con el proceso	•	•

Tabla 4.4 Elementos de Scrum como metodología Agile utilizados en InfoSec de Intel Costa Rica. Fuente: Entrevistas con participantes.

Como se puede ver en la matriz anterior, los elementos esenciales de Scrum están presentes en la organización, así como otros elementos recomendados que permiten comprobar que existe una buena comprensión de la metodología en la organización.

Las respuestas completas de los participantes pueden verse en el Anexo VI.

4.4. Diseño de procesos y hoja de ruta de implementación

En esta sección se plantea una posible implementación para los procesos que propone ITIL en la fase de operación del servicio, en los que también se incorporan elementos de DevOps y Agile.

El enfoque utilizado para combinar los elementos de los distintos marcos de referencia se aplica en todos los procesos de la misma forma, por ese motivo se describe en este punto y no dentro de la descripción particular de cada proceso.

Los procesos que se proponen toman en cuenta diversos factores, entre los que se puede mencionar el conocimiento existente en la empresa de los marcos de referencia como ITIL, DevOps y Agile, la infraestructura de TI disponible, el marco de referencia organizacional representado en políticas y directrices y otros.

Como se pudo ver en la sección 4.3.1, al aplicar la lista de verificación de ITIL operación de servicio, se constató que el personal de InfoSec de Intel Costa Rica tiene un buen nivel de conocimiento del marco de referencia y que hay esfuerzos por implementarlo en la organización,

por lo que en los procesos propuestos se busca aprovechar ese conocimiento. Asimismo, se pretende utilizar el Centro de Servicios que está implementado y disponible dentro del departamento de TI, como se pudo comprobar en la sección 4.2, para que funcione como primer nivel de servicio. De la misma forma, se busca aprovechar las herramientas disponibles, así como el conocimiento que el personal tiene de éstas, con el fin de llevar los costos de implementación de los procesos propuestos casi a cero y mitigar el riesgo de rechazo por parte de quienes están familiarizados con su uso.

En cuanto a DevOps, de acuerdo con lo que se pudo observar en la sección 4.3.2, se pretende aprovechar el alto grado de alineamiento que existe entre los objetivos de la organización y del departamento de TI, el interés en hacer que la información necesaria para los procesos de la organización esté disponible y la necesidad de mejorar el enfoque que existe en el software como un producto que merece atención y cuidado en un entorno de cambios constantes.

Para ello, se busca incorporar en los procesos propuestos un mayor grado de automatización en los procesos de soporte, mediante la implementación de mecanismos para el monitoreo automático de aplicaciones, la generación y envío automáticos de notificaciones a partir de eventos, la recuperación automática de servicios apoyada en la gestión automática de la configuración, entre otros.

En el ámbito de DevOps se promueve el trabajo coordinado entre los desarrolladores y el personal de soporte de operaciones a través de la atención de incidentes y solicitudes en los que se requiera implementar un cambio en alguna aplicación, o bien, que implique el desarrollo de alguna solución automatizada, como, por ejemplo, un elemento de gestión de configuración.

En lo que respecta a Agile, se propone el uso de Scrum para gestionar y coordinar los trabajos de desarrollo y soporte en los que se requiera la participación de recursos pertenecientes a ambos grupos y que son necesarios para, por ejemplo, implementar un cambio en alguna aplicación. Lo anterior se basa en el hecho de que, de acuerdo con lo observado en la sección 4.3.3, en la organización existe un muy buen conocimiento de la metodología, lo que facilitará su implementación.

Si bien es cierto, la principal referencia de los procesos aquí propuestos es ITIL, también se incorporaron elementos de Agile y DevOps, como vimos anteriormente, para obtener procesos que puedan satisfacer las actuales demandas de flexibilidad, agilidad, rapidez, adaptabilidad, eficiencia y eficacia en la obtención de resultados y creación de valor en la empresa.

4.4.1. Diseño de procesos

Seguidamente se describen los procesos que se proponen para el soporte de aplicaciones de seguridad de la información dentro de InfoSec de Intel Costa Rica. Antes, se mencionan y describen los roles que forman parte de dichos procesos, ya que son comunes en la mayoría de ellos.

Rol 1: Usuario

Se refiere a los usuarios de las aplicaciones de seguridad de la información a las que se brinda el servicio de soporte.

Rol 2: Primer Nivel de Soporte
Corresponde al servicio que presta el Centro de Servicios y que se utilizaría como punto de contacto y primer nivel de soporte ante solicitudes de servicio y reporte de incidentes.

Rol 3: Segundo Nivel de Soporte
Se refiere al equipo de soporte de operaciones dentro de InfoSec de Intel Costa Rica.

Rol 4: Scrum de Desarrollo
Corresponde al equipo de desarrollo dentro de InfoSec de Intel Costa Rica.

4.4.1.1. Gestión de eventos

El proceso que se propone para la gestión de eventos se basa fundamentalmente en las recomendaciones de ITIL, pero además incorpora elementos de DevOps para la ejecución proactiva de acciones a través de la implementación de monitoreo de eventos y reactiva mediante la administración automatizada de la configuración, que permitan prevenir incidentes y, con ello, mitigar el impacto negativo que estos puedan tener sobre los servicios soportados.

Asimismo, procura aprovechar la implementación de Scrum existente en la organización para agilizar la realización y seguimiento de tareas relacionadas con el monitoreo y control de eventos, así como cualquiera otra actividad vinculada con la gestión de eventos, de tal manera que se garantice su realización de acuerdo con criterios objetivos de prioridad e importancia para la empresa.

Monitoreo y control

Los sistemas de monitoreo y control representan el corazón de la gestión de eventos porque permiten conocer el estado actual y los cambios de estado del total de los elementos de configuración (CI) que están bajo la responsabilidad de la organización. Asimismo, se pueden utilizar para ejecutar acciones correctivas sobre los CIs monitoreados, de acuerdo con los criterios de funcionamiento, configuración y disponibilidad que se hayan definido.

En vista de que la organización es responsable del soporte de aplicaciones, el monitoreo estará centrado en los componentes de las aplicaciones, que pueden ser servicios web, bases de datos, sitios web hospedados en servidores internos, entre otros. El monitoreo de componentes de infraestructura como servidores y elementos de red también deben ser tomados en cuenta si no están siendo cubiertos por otras organizaciones dedicadas a ello dentro de la empresa y cuyos servicios sean utilizados por InfoSec de Intel Costa Rica.

Se recomienda utilizar alguna herramienta para la administración automatizada de la configuración, que puede ser Puppet y así aprovechar que está disponible en Intel y que ha sido utilizada con éxito en otras organizaciones dentro de la empresa, de tal manera que no solamente se pueda saber si el estado de un CI cambió, sino también ejecutar alguna acción correctiva si

fuera necesario. Es importante destacar que utilizar un enfoque de administración automática de la configuración permite además mantener las aplicaciones en un estado consistente en cada uno de los ambientes que existan, ya sea desarrollo, pruebas o producción, por ejemplo.

El departamento de IT en Intel cuenta con herramientas de monitoreo que pueden ser utilizadas por parte de InfoSec de Intel Costa Rica, como, por ejemplo, SCOM (System Center Operations Manager de Microsoft), ya sea de forma complementaria o bien para conocer el estado actual de los CIs y con base en ello definir alguna acción a realizar o simplemente registrarlo para obtener métricas de desempeño o disponibilidad que puedan ser utilizadas por otros procesos.

Notificaciones

En primer lugar, deben definirse los destinos de las notificaciones de manera tal que cuando se detecte un evento se tenga claro a quién debe dirigirse la notificación, ya sea por medio de la herramienta de administración de la configuración o de la herramienta de monitoreo.

Las herramientas de administración de la configuración permiten el envío de notificaciones a quienes corresponda, tanto acerca del cambio de estado que se detectó, como de la acción realizada para evitar la generación de un incidente o bien mitigar el impacto negativo en la aplicación soportada.

Esto último es un beneficio adicional de utilizar este tipo de herramientas porque no solamente se sabrá que se presentó un cambio en el estado de un CI, sino que también se podrá saber si la acción correctiva resultó exitosa o se requiere de una acción adicional por parte del personal de soporte, en cuyo caso se agregará a la lista de tareas por hacer y que será dispuesta a través del equipo Scrum.

Diagrama

El proceso propuesto se ilustra en el diagrama BPMN de la figura 4.5

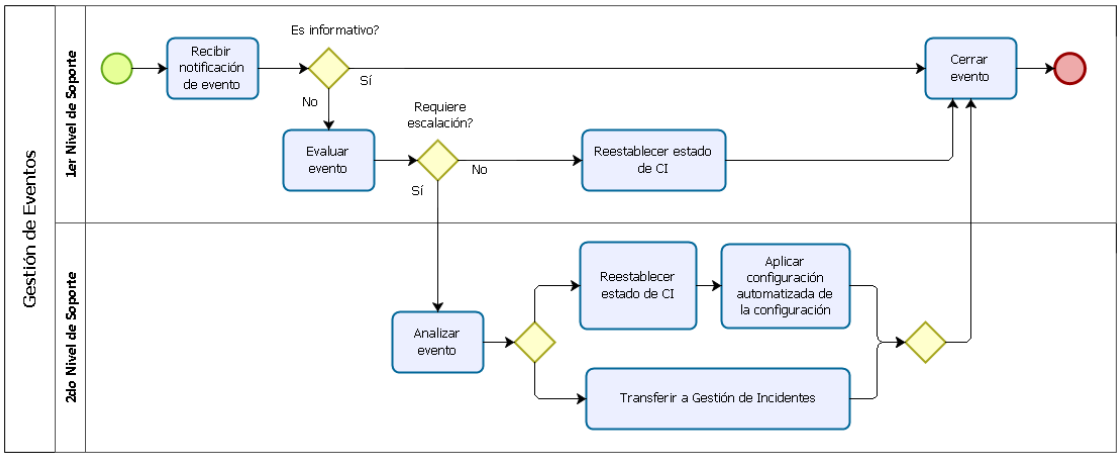


Figura 4.5 Proceso de gestión de eventos. Fuente: Elaboración propia

Como se puede ver en el diagrama, si el evento requiere de la intervención del segundo nivel, se puede incorporar la administración automatizada de la configuración para gestionar de forma automática el cambio de estado del CI implicado, de tal manera que, cuando se dispare el evento en el futuro, el estado pueda ser reestablecido automáticamente, con lo que se puede prevenir la generación de un incidente que impactaría alguna de las aplicaciones soportadas.

La automatización de la administración de la configuración puede llevarse a cabo mediante el uso de herramientas como Puppet que, como hemos visto, está disponible en Intel y se ha utilizado en otros procesos de soporte. De esta manera, se fomenta el enfoque el uso de elementos DevOps dentro del proceso de soporte de aplicaciones.

4.4.1.2. Gestión de incidentes

Al igual que en el caso de la gestión de eventos, el proceso propuesto para la gestión de incidentes tiene como base las recomendaciones hechas por ITIL, junto con algunos elementos de DevOps y Scrum con el fin de que el proceso sea ágil y cuente con la flexibilidad suficiente para soportar los cambios que demanda el mercado en que se desempeña la empresa.

Niveles de soporte

En el proceso propuesto hay tres niveles de soporte, donde los incidentes pasarán de un nivel a otro según el grado de complejidad de su solución. Los niveles se describen a continuación.

El primer nivel de soporte estaría en el Centro de Servicios, con el fin de recibir los reportes de incidentes, ya sea por parte de los usuarios de las aplicaciones soportadas, o bien a través de alertas emitidas por las herramientas de la gestión de eventos. Asimismo, haría un primer diagnóstico para determinar si el incidente es conocido y existe una solución ya documentada.

También, serviría de punto de contacto con los usuarios para mantenerlos informados del estado actual del incidente.

El segundo nivel de soporte lo brindaría el equipo de soporte de operaciones, que haría un diagnóstico avanzado con el fin de determinar si el incidente puede ser resuelto por ellos únicamente o requieren de la participación de los desarrolladores para implementar un cambio en la aplicación o de otros departamentos o equipos de soporte. Adicionalmente, este nivel se encargaría de llevar el incidente al equipo de Scrum a través del cual se asignaría una prioridad al incidente, se crearían las historias de usuario correspondientes y se asignarían éstas a quienes serían los responsables de encontrar la solución e implementarla.

Habría un tercer nivel de soporte que corresponde a los desarrolladores, quienes ante un incidente complejo intervendrían para buscar y, posteriormente, implementar una solución a través de un cambio en la aplicación afectada, trabajando en coordinación con el equipo de soporte de operaciones.

Integración de la gestión de cambios

A diferencia de ITIL, la gestión de cambios no sería un proceso distinto e independiente, sino que los cambios se administrarían durante la gestión de incidentes si la falla que provoca el incidente tiene como origen, por ejemplo, un defecto en la aplicación que requiere la intervención de los desarrolladores para corregirlo, o bien, implica un cambio en la configuración de la aplicación.

El objetivo que se persigue es que la solución al incidente pueda encontrarse e implementarse en el menor tiempo posible gracias a la agilidad que ofrece Scrum, de tal manera que, aunque el cambio deba ser aprobado por quien corresponda, las partes interesadas estarían participando o tendrían representación en el equipo Scrum, por lo que se agilizaría la gestión del cambio al obtener respuestas en plazos más cortos. El responsable de gestionar el cambio sería el 2do nivel de soporte.

Herramientas de apoyo

Como se ha mencionado antes, la herramienta más utilizada para gestionar los incidentes en Intel es ServiceNow. El proceso que aquí se propone no especifica una herramienta a utilizar, sin embargo, no descarta el uso de ServiceNow en vista de que es la herramienta para la gestión de los servicios de TI que el departamento de TI sugiere usar.

Ahora bien, como el proceso incorpora el uso de Scrum se recomienda el uso de una herramienta que soporte este tipo de metodología, de manera tal que se pueda dar seguimiento, no solamente a las historias de usuario, sino al incidente mismo. En este caso, se recomienda el uso de JIRA, ya que esta herramienta se utiliza en Intel y está disponible para que las organizaciones la utilicen en sus procesos.

Diagrama

El proceso propuesto para la gestión de incidentes se muestra en el diagrama PBMN de la figura 4.6

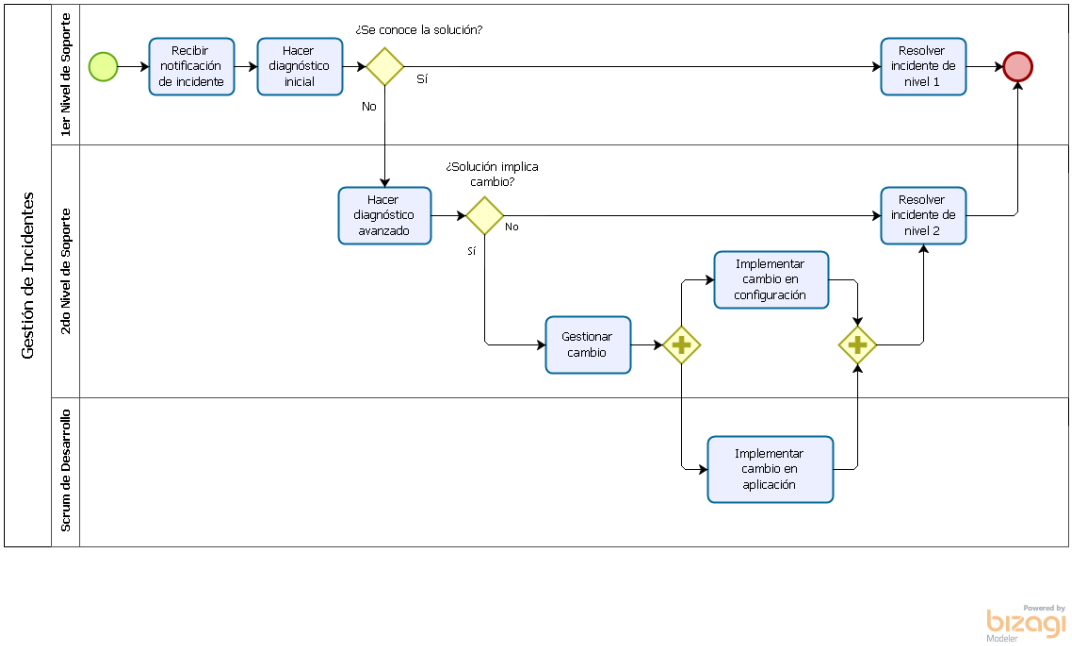


Figura 4.6 Proceso propuesto para gestión de incidentes. Fuente: elaboración propia

Podemos ver en el diagrama cómo se incorpora al proceso de gestión de incidentes la gestión de cambios, donde el segundo nivel es el responsable de gestionar el cambio, es decir, de asegurar el cumplimiento de los procedimientos implicados en el procesamiento de un cambio, como lo es la obtención de las aprobaciones correspondientes.

El cambio requerido puede estar relacionado con el código de la aplicación o con uno o más elementos de la configuración de ésta, como, por ejemplo, archivos de configuración, archivos y servicios de dependencias, entre otros. Si se da el primer escenario, la implementación del cambio estaría a cargo de los desarrolladores, mientras que, si se da el segundo, será una tarea para el equipo de soporte, que corresponde al segundo nivel de soporte.

De esta manera, se busca darle mayor agilidad a la implementación de cambios que tienen relación con incidentes y, a la vez, se está promoviendo el uso del enfoque DevOps al procurar el trabajo coordinado entre el segundo nivel de soporte que corresponde el equipo de soporte de aplicaciones y al equipo de desarrolladores.

4.4.1.3. Resolución de solicitudes

El proceso propuesto para la resolución de solicitudes, al igual que los anteriores, procura la incorporación de elementos de ITIL, DevOps y Agile con el objetivo de contar con un proceso altamente flexible y ágil que permita atender las solicitudes de servicio en el menor tiempo posible, al disponer de los recursos necesarios para satisfacer los requerimientos de cada solicitud y en un contexto de participación multidisciplinaria coordinada a través del equipo Scrum.

Niveles de soporte

Se proponen tres niveles de soporte para la resolución de solicitudes, donde la participación de cada nivel estará determinada por el grado de complejidad del requerimiento.

El primer nivel es quien recibe la solicitud y determina si la solicitud está dentro de la lista de solicitudes estándar, en cuyo caso procede a procesarla. Si no es una solicitud estándar, entonces, la escala al segundo nivel quien se encargará de llevarla al equipo Scrum para que se le asigne una prioridad, se creen las historias de usuario y se asignen responsables de realizarlas.

Las historias de usuario pueden tener como responsables a miembros del segundo nivel, o bien del equipo de desarrollo, quienes trabajarán en conjunto para resolver la solicitud. Una vez hecho esto, el primer nivel se encargará de cerrar el registro de la solicitud.

Integración de la gestión de cambios

En caso de que una solicitud implique un cambio, el mismo proceso de resolución de solicitudes se encargará de coordinar el cambio a través del equipo Scrum, con lo que se aprovechará la participación coordinada entre los roles de desarrollo y soporte de operaciones.

Diagrama

El diagrama BPMN de la figura 4.7 ilustra el proceso de resolución de solicitudes propuesto.

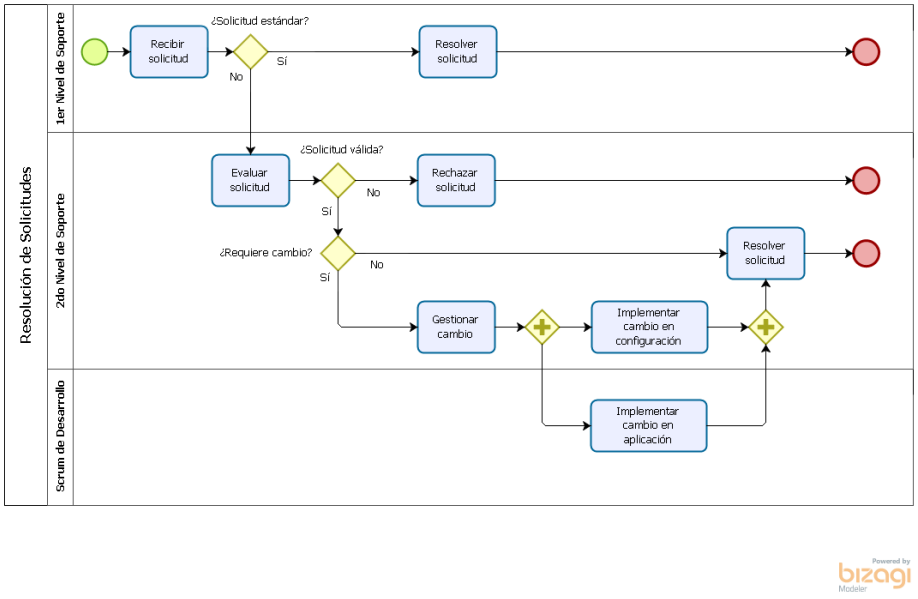


Figura 4.7 Proceso propuesto para resolución de solicitudes. Fuente: elaboración propia

Se puede observar en el diagrama cómo las solicitudes estándar son procesadas por el primer nivel de soporte, mientras que las solicitudes especiales son procesadas por el segundo nivel, quienes se encargan de validar que la solicitud cumpla con los requerimientos correspondientes y, de no ser así, será rechazada.

En este proceso, al igual que en la gestión de incidentes, se incorpora la gestión de cambios para aportar mayor agilidad al proceso, de tal manera que las solicitudes de los clientes puedan ser satisfechas en el menor tiempo posible. Aquí también el segundo nivel es el responsable de gestionar el cambio y este puede estar relacionado con una modificación en el código de la aplicación o en algún elemento de su configuración.

Si el cambio se relaciona con el código de la aplicación, se implementará a través de Scrum, con lo cual se aporta agilidad y rapidez a la implementación. Asimismo, si el cambio está relacionado con la configuración de la aplicación, este se puede implementar a través de la administración automatizada de la configuración, que puede realizarse mediante el uso de Puppet, como ya se ha mencionado antes.

4.4.1.4. Gestión de problemas

La propuesta para el proceso de gestión de problemas se basa en el trabajo coordinado entre el equipo de soporte (2do nivel) y el equipo de desarrollo, esto a través de la metodología Scrum. De esta forma tanto la investigación para encontrar el origen de los incidentes, como el diseño de una solución permanente y su correspondiente implementación se realizarán en conjunto entre soporte y desarrollo.

Este enfoque busca aprovechar las fortalezas de cada perfil de trabajadores, tanto de los miembros del equipo de soporte de operaciones, como de los desarrolladores y no realizar esfuerzos independientes que tienden a producir resultados menos satisfactorios, porque cada grupo se enfoca en el problema desde su punto de vista.

Integración de la gestión de cambios

Al igual que en la gestión de incidentes, la gestión de cambios no sería un proceso distinto e independiente, sino que los cambios se administrarían dentro del mismo proceso de gestión de problemas si el origen de los incidentes se relaciona con, por ejemplo, un defecto en la aplicación que requiere la intervención de los desarrolladores para corregirlo, o bien, implica un cambio en la configuración de la aplicación.

De nuevo, el objetivo que se persigue es que la solución al problema pueda encontrarse e implementarse en el menor tiempo posible gracias a la agilidad que ofrece Scrum. El responsable de gestionar el cambio sería el 2do nivel de soporte.

Herramientas de apoyo

Al igual que en la gestión de incidentes, la herramienta más utilizada para este fin en Intel es ServiceNow, por tanto, se recomienda aprovechar el conocimiento y familiaridad que existe con.

Si la resolución del problema requiere de la implementación de un cambio en la aplicación o en la configuración de ésta, del mismo modo que se sugiere hacer en los procesos anteriores, el

uso de JIRA puede ser de gran utilidad para apoyar la gestión del cambio y darles seguimiento a las historias de usuario en la metodología Scrum.

Diagrama

El proceso propuesto para la gestión de problemas se representa en el diagrama BPMN de la figura 4.8

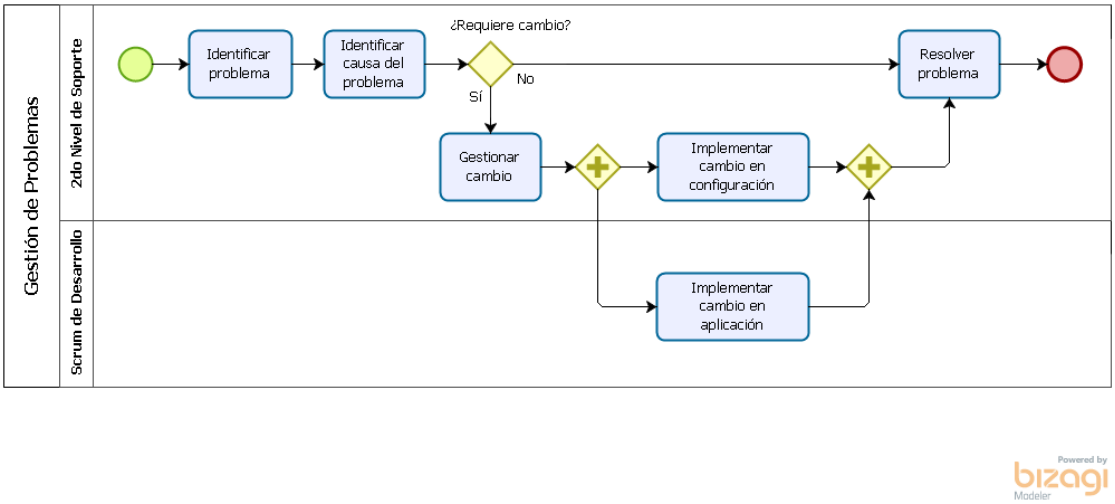


Figura 4.8 Proceso propuesto para gestión de problemas. Fuente: elaboración propia

La incorporación de la gestión de cambios en los procesos de la operación del servicio es un factor común en los procesos propuestos en el presente documento. En la gestión de problemas no es diferente.

Podemos ver en el diagrama cómo el segundo nivel es el responsable de gestionar el problema, así como de implementar el cambio si este está relacionado con algún elemento de la configuración de la aplicación, que podría estar gestionada automáticamente a través de Puppet que, como ya se ha mencionado antes, está disponible en Intel y ha sido utilizado en otros procesos de soporte.

Si el cambio se relaciona con el código de la aplicación, entonces, serán los desarrolladores quienes lo implementen mediante su propio Scrum de desarrollo, con lo cual se aporta agilidad y rapidez a la implementación del cambio.

4.4.1.5. Gestión de acceso

En el proceso de gestión de acceso interviene fundamentalmente el equipo de soporte (2do nivel), quien será el responsable de brindar, actualizar o eliminar el acceso solicitado cuando se trate de una solicitud estándar, es decir, ya se conoce el procedimiento para resolver la solicitud.

Sin embargo, cuando el acceso solicitado no es conocido previamente, se recurre al Scrum de desarrollo para definir, priorizar y coordinar las tareas a ejecutar para resolver la solicitud, de este modo se tendrá un criterio objetivo para decidir el lugar que tendrá la solicitud dentro de la lista de tareas por hacer en el equipo de soporte.

Administración de la configuración

El acceso otorgado o removido debe actualizarse en el proceso de administración de la configuración para que sea persistente dentro del esquema de automatización de configuraciones establecido para prevenir incidentes.

Diagrama

La propuesta para el proceso de gestión de acceso se ilustra con el diagrama BPMN de la figura 4.9

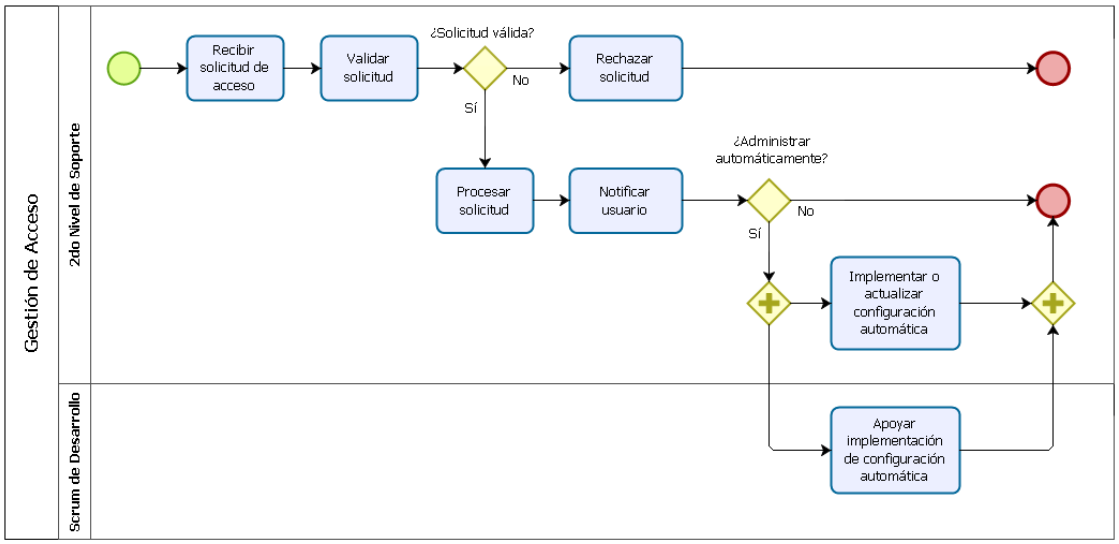


Figura 4.9 Proceso propuesto para gestión de acceso. Fuente: elaboración propia

En la gestión de acceso participan el segundo nivel y el equipo de desarrolladores. Los primeros se encargan de validar la solicitud, así como de procesarla si determinan que es válida. También, se propone administrar la configuración de forma automática, apoyando el proceso con el uso de herramientas como Puppet, de tal manera que el acceso a los servicios y recursos pueda otorgarse o denegarse de manera ágil.

Esto pone de manifiesto las propuestas del enfoque DevOps, donde la automatización y el trabajo coordinado entre el equipo de soporte y los desarrolladores aporte más valor a la empresa, lo cual se puede ver en el diagrama cuando el Scrum de desarrollo brinda su colaboración para implementar elementos de configuración automatizada que requieren de la generación de código para el manejo de recursos de la aplicación como, por ejemplo, archivos de configuración, o bien,

de servicios de dependencia como bases de datos o elementos de red, por mencionar un par de ejemplos.

4.4.2. Hoja de ruta de implementación

En esta sección se plantea una propuesta de hoja de ruta para la implementación de los procesos para poner en marcha el servicio de soporte de aplicaciones de seguridad de la información. La figura 4.10 muestra la hoja de ruta propuesta. En el caso de una implementación esta hoja de ruta puede ser utilizada como base para elaborar un plan más detallado.

Figura 4.10 Hoja de ruta de implementación de procesos propuestos. Fuente: elaboración propia

El orden de implementación de los procesos propuestos en esta hoja de ruta se debe a que la gestión de incidentes y resolución de solicitudes requieren atención inmediata por parte del equipo de soporte de aplicaciones. Los demás procesos, aunque no menos importantes, se podrán ir implementando posteriormente a un ritmo acelerado gracias al conocimiento y familiaridad que tiene el personal con operación de servicio de ITIL, Agile y DevOps, tal y como

se pudo ver en los resultados de las listas de verificación de los marcos de referencia antes mencionados.

Una vez implementados la gestión de incidentes y la resolución de solicitudes, se sugiere implementar la gestión de eventos para identificar aquellos que podrían generar un incidente y atenderlos de manera proactiva, de tal manera que se puedan reducir el número de incidentes que se presenten y deban ser procesados y resueltos.

Posteriormente, se recomienda implementar la gestión de problemas para atacar los incidentes recurrentes y encontrarles una solución definitiva, con lo que se esperaría que el número de incidentes que deben ser procesados en la gestión de incidentes disminuya.

Seguidamente, se propone implementar la gestión de acceso para contar con soluciones estándar para el otorgamiento o remoción de accesos en las distintas aplicaciones a las que se les brinda soporte, de tal forma que todas las solicitudes de acceso no tengan que se procedas manualmente.

Por último, se implementaría el proceso de evaluación y mejoras para buscar oportunidades de hacer que el servicio de soporte de aplicaciones sea cada vez más satisfactorio para los clientes de la organización.

Aprobaciones organizacionales

El proceso de soporte propuesto en este proyecto estaría funcionando en el contexto del equipo de trabajo InfoSec de Intel Costa Rica y brindaría el servicio de soporte al Departamento de Seguridad de la Información, dentro de Tecnologías de la Información. Esto lo que significa es que la aprobación para que el proceso pueda ser implementado deberá provenir principalmente del gerente de InfoSec de Intel Costa Rica y en segunda instancia del gerente de la organización directamente superior a esta.

Herramientas

En principio, no se requieren de nuevas herramientas para implementar el proceso aquí propuesto, ya que se estarían utilizando las ya existentes, tanto para la gestión de los tiquetes como para el desarrollo de la metodología Scrum, a saber: ServiceNow y JIRA respectivamente. Además, Intel cuenta con más herramientas para el apoyo de otros procesos y actividades como SCOM para el monitoreo de sistemas y Puppet para la administración de la configuración, entre otras. Debido a esta razón, este aspecto no se representa en la hoja de ruta.

Entrenamiento

Se propone brindar dos tipos de entrenamientos. El primero se relaciona con los marcos de referencia sobre los cuales se basan los procesos aquí propuestos. Si bien es cierto, el personal del equipo de trabajo de InfoSec de Intel Costa Rica tiene algún grado de conocimiento sobre ITIL, Agile (Scrum) y DevOps, es importante asegurarse de que todos los miembros del equipo

estén familiarizados con estos conjuntos de buenas prácticas, por lo que podría ser necesario que reciban entrenamiento en este campo.

El segundo tipo de entrenamiento se relaciona con los procesos mismos. Es importante que todos los miembros del equipo comprendan con claridad cómo funcionan los procesos aquí propuestos, de tal manera que la calidad del servicio de soporte brindado no se vea afectada, principalmente durante la etapa de implementación.

Riesgos

El principal riesgo que existe al implementar el proceso de soporte propuesto aquí es que el tiempo requerido por parte del personal en adaptarse a un esquema de trabajo en el que se presenta una combinación de elementos de varios marcos de referencia, sea mayor al esperado, debido principalmente a que el personal de Intel está acostumbrado a gestionar los servicios de TI basado principalmente en un solo marco de referencia que es ITIL.

Este riesgo puede ser mitigado mediante el apoyo en la experiencia del personal de la organización que cuenta con conocimiento de los marcos de referencia, aunque no los haya utilizado de manera combinada.

Un segundo riesgo que se presenta se relaciona con la posibilidad de que la gerencia de Seguridad de la Información, que es la organización a la que pertenece InfoSec de Intel Costa Rica, dentro del Departamento de TI, no brinde las aprobaciones correspondientes para que los procesos sean implementados.

En caso de no contar con las aprobaciones para el establecimiento de todos los procesos aquí propuestos, se recomienda buscar las aprobaciones que permitan implementar los primeros procesos propuestos, a saber, gestión de incidentes y resolución de solicitudes, ya que, como se pudo ver en el análisis de la situación actual, estos procesos están parcialmente implementados, por lo que se requeriría implementar menos cambios en el proceso y la organización.

Costos asociados

Como se pudo ver en la evaluación del marco de referencia organizacional, Intel cuenta con herramientas tecnológicas para la gestión de incidentes, eventos, problemas y más, para el apoyo de Scrum, para el monitoreo de sistemas, para la automatización de la administración de la configuración, entre otras, que pueden ser utilizadas en la implementación del proceso aquí propuesto, así como en el funcionamiento normal del proceso, por lo que, en primera instancia, no sería necesaria la adquisición de herramientas.

Lo que se podría considerar como un gasto relacionado con la implementación del proceso propuesto es el tiempo que el personal dedicaría a recibir el entrenamiento asociado a los marcos de referencia empleados, como lo son ITIL, Agile (Scrum) y DevOps, ya que sí es importante que todos comprendan y estén familiarizados con los conceptos más importantes que estos conjuntos de buenas prácticas promueven.

4.5. Evaluación y mejoras

Con el fin de evaluar los procesos propuestos en el presente proyecto e identificar oportunidades de mejora se sugiere realizar las siguientes actividades de forma cíclica con una frecuencia que deberá ser definida oportunamente por InfoSec de Intel Costa Rica.

La evaluación y mejora de los procesos se basa en ejecutar una serie de siete pasos, propuestos por ITIL, que describen cómo medir la calidad y rendimiento de los procesos propuestos para generar información que le permita a la organización crear un plan de mejora del servicio.

- Paso 1: Identificar qué se debe medir.
- Paso 2: Identificar qué se puede medir.
- Paso 3: Recopilar los datos necesarios.
- Paso 4: Procesar los datos recopilados.
- Paso 5: Analizar los datos obtenidos.
- Paso 6: Proponer mejoras a los procesos.
- Paso 7: Implementar las medidas propuestas.

En la recolección de los datos se puede realizar una encuesta que, entre otras preguntas, podría incluir las que se muestran en la tabla 4.5 para identificar el grado de percepción de calidad que tiene el usuario con respecto a los servicios brindados a través de los procesos propuestos.

Además de las encuestas, se recomienda definir indicadores que permitan evaluar el desempeño de cada uno de los procesos. En el Anexo I se pueden ver indicadores de desempeño de los procesos que ITIL propone para la operación de servicio. En la tabla 4.6 se muestran algunos indicadores que se recomienda utilizar.

Pregunta	Tipo de Respuesta
¿Cuál es su nivel de satisfacción con respecto a la solución propuesta?	Escala de 1 a 10 donde 1 es “Insatisfecho” y 10 es “Completamente satisfecho”.
¿Cuál es su nivel de satisfacción con respecto al soporte recibido?	Escala de 1 a 10 donde 1 es “Insatisfecho” y 10 es “Completamente satisfecho”.
¿Cuál es su nivel de satisfacción con respecto al servicio de TI recibido?	Escala de 1 a 10 donde 1 es “Insatisfecho” y 10 es “Completamente satisfecho”.
¿Cómo considera el trato recibido por parte del agente del Centro de Servicios?	Escala de 1 a 10 donde 1 es “Grosero” y 10 es “Extraordinario”.
¿Cómo considera la capacidad técnica del personal de soporte?	Escala de 1 a 10 donde 1 es “Deficiente” y 10 es “Excelente”.
¿Está satisfecho con el tiempo de resolución del incidente/solicitud?	Escala de 1 a 10 donde 1 es “Insatisfecho” y 10 es “Completamente satisfecho”.

¿Cuán anuente estaría a recomendar a otros el servicio?	Escala de 1 a 10 donde 1 es “Renuente” y 10 es “Muy anuente”.

Tabla 4.5 Ejemplos de preguntas para encuesta de evaluación de calidad de servicios. Fuente: Elaboración propia.

Como se pudo ver en la sección 4.2, en Intel la implementación de ITIL se apoya en el uso de la herramienta ServiceNow, que permite el manejo de los datos que se generan en los distintos procesos de soporte en relación con incidentes, problemas, solicitudes y más. Esto quiere decir que los datos que se requieren para generar los indicadores aquí propuestos se pueden obtener de ServiceNow, lo que facilita la generación de los indicadores, puesto que no será necesario gestionar el acceso a los datos en distintas fuentes.

Proceso	Indicador	Unidad de Medida	Frecuencia
Gestión de Eventos	• Eventos/alertas generadas sin que se haya presentado una degradación de servicios (falsos positivos).	Valor absoluto	Mensual Trimestral
	• Notificaciones de eventos.	Valor absoluto	Mensual Semanal Trimestral
	• Eventos por CI.	Valor absoluto	Mensual
	• Porcentaje de eventos que resultaron en incidentes.	Porcentaje	Semanal Mensual Trimestral
Gestión de Incidentes	• Número y porcentaje de incidentes asignados incorrectamente.	Valor absoluto Porcentaje	Semanal Mensual Trimestral
	• Número y porcentaje de incidentes procesados por agente del centro de servicios.	Valor absoluto Porcentaje	Mensual Trimestral
	• Número de escalaciones producto de incidentes no resueltos dentro del tiempo acordado para su resolución.	Valor absoluto	Semanal Mensual Trimestral
	• Tiempo de resolución de incidentes.	Minutos	Mensual Trimestral
	• Incidentes originados por la implementación de un cambio.	Valor absoluto	Mensual Trimestral

Resolución de Solicitudes	• Tiempo promedio transcurrido en el manejo de la solicitud. • Porcentaje de solicitudes no resueltas a tiempo. • Tamaño de la lista de solicitudes pendientes. • Número de incidentes relacionados con amenazas de seguridad originados en actividades de resolución de solicitudes.	Minutos Porcentaje Valor absoluto Valor absoluto	Mensual Trimestral Semanal Mensual Trimestral Mensual Trimestral Mensual Trimestral
Gestión de Problemas	• Tamaño de la cola de problemas pendientes en cada servicio. • Porcentaje de problemas asignados incorrectamente. • Cantidad de incidentes asociados con un problema. • Tiempo promedio en resolver un problema.	Valor absoluto Porcentaje Valor absoluto Días	Mensual Trimestral Mensual Trimestral Mensual Trimestral Mensual Trimestral
Gestión de Acceso	• Tiempo de resolución promedio de incidentes relacionados con accesos indebidos. • Incidentes provocados por configuraciones incorrectas de permisos. • Porcentaje de solicitudes de acceso que no fueron procesadas dentro de los plazos establecidos en los acuerdos de nivel de servicio.	Minutos Valor absoluto Porcentaje	Mensual Trimestral Semanal Mensual Trimestral Semanal Mensual Trimestral

Tabla 4.6 Indicadores iniciales recomendados para evaluar y mejorar los procesos propuestos para la operación del servicio. Fuente: Elaboración propia.

Con los datos obtenidos se identificarán las oportunidades para mejorar los procesos y se gestionarán los cambios que permitirán implementar dichas mejoras. Este proceso debe ser repetido indefinidamente, con el fin de mantener los procesos siempre actualizados con respecto a las necesidades del negocio, de tal manera que aporten el más alto valor posible a la empresa.

5. Capítulo V: Conclusiones

A continuación, se presentan las conclusiones del proyecto, así como las limitaciones identificadas y los trabajos que han de desarrollarse posteriormente.

5.1. Conclusiones generales

En el capítulo I del presente documento se plantearon cuatro objetivos específicos que se lograron alcanzar a lo largo del desarrollo del proyecto. Seguidamente, se ofrece una recapitulación de cada uno de ellos, así como las conclusiones correspondientes en cada caso.

El primero objetivo trató acerca del análisis del estado actual del servicio de soporte de aplicaciones de seguridad de la información brindado por InfoSec de Intel Costa Rica. En este caso, se logró analizar su estado actual y se identificaron los roles presentes en el proceso, que sirvieron como base para la propuesta de los procesos de la operación del servicio que se presentó posteriormente.

El segundo objetivo consistió en la evaluación de las características de implementación de la fase de operación del servicio de ITIL en los procesos de soporte de aplicaciones en Intel. Aquí se logró evaluar las características presentes en la implementación de la operación de servicio de ITIL, se pudo identificar recursos como herramientas tecnológicas como ServiceNow, JIRA y los servicios de computación en la nube, así como el conocimiento del personal sobre ITIL, Agile y DevOps, que sirven de apoyo a la implementación de los procesos de la operación de servicio. Algunos de estos recursos fueron tomados en cuenta en los procesos propuestos.

El tercer objetivo consistió en la formulación de una propuesta de implementación de los procesos de la fase de operación de servicio de ITIL, tomando en consideración conceptos DevOps y Agile. En este caso, se consiguió presentar una propuesta para cada uno de los procesos de la operación de servicio de ITIL, en los cuales se logró incorporar elementos de Agile como el uso de Scrum para gestionar las solicitudes de servicios, los cambios en las aplicaciones, la implementación de soluciones a incidentes complejos, entre otros. Asimismo, se incorporaron elementos de DevOps como la automatización de la administración de la configuración y de los procesos de puesta en operación de los cambios en las aplicaciones.

Por último, el cuarto objetivo trató de plantear acciones de evaluación y mejora continua para el proceso de soporte. Aquí, se propusieron acciones para evaluar el desempeño de los procesos, mediante indicadores de desempeño como la cantidad de eventos por cada CI, el tiempo de resolución de los incidentes, o bien, la cantidad de incidentes provocados por configuraciones incorrectas relacionadas con permisos, que permitan identificar deficiencias para que sean corregidas. También, se propusieron mecanismos de evaluación de los procesos como encuestas, para medir el grado de satisfacción de los usuarios del servicio de soporte.

Adicionalmente, el desarrollo del presente proyecto permitió comprobar que es posible la combinación de ITIL, Agile (Scrum) y DevOps para diseñar un proceso para el soporte de aplicaciones, que permita obtener beneficios de cada uno de los marcos de referencia antes

mencionados como, por ejemplo, la posibilidad de incorporar la gestión de cambios dentro de la gestión de incidentes y problemas, la incorporación de procesos automáticos para la administración de la configuración, el trabajo en conjunto entre el equipo de soporte y los desarrolladores, entre otros, sin que necesariamente haya conflictos en cuanto a la forma en que se deban aplicar las buenas prácticas recomendadas.

El personal de Intel cuenta con conocimiento en ITIL®, Agile, específicamente en la metodología Scrum y DevOps, por lo que las necesidades de entrenamiento no son tan grandes y esto favorece una futura implementación de los procesos, ya que su comprensión se espera que sea más sencilla y en un menor plazo. Asimismo, el personal también está familiarizado con las herramientas que se utilizarían para apoyar los procesos de soporte como lo son ServiceNow y JIRA. Lo anterior se determinó en el análisis de la situación actual y en el marco de referencia organizacional.

Los costos asociados a la implementación de los procesos serían bajos porque Intel cuenta con recursos para la gestión de servicios de TI, como lo son ServiceNow para apoyar la implementación de ITIL, JIRA para apoyar la implementación de Scrum y, en el área de DevOps, se cuentan con herramientas para apoyar la automatización de múltiples tareas, tales como servicios de infraestructura de servidores, almacenamiento, monitoreo, servicios en la nube y muchos otros.

Por último, pero no por eso menos importante, cabe destacar el beneficio de utilizar listas de verificación para conocer el grado de conocimiento que existe en una organización con respecto a los marcos de referencia como ITIL, Agile y DevOps. Sin embargo, se recomienda simplificar el formulario usado para evaluar el nivel de conocimiento de ITIL, ya que el aquí utilizado tienen un gran número de preguntas que pueden requerir mucho tiempo por parte de las personas entrevistadas para responderlas.

5.2. Limitaciones del proyecto

El proyecto no profundiza en la implementación de las funciones que propone ITIL dentro de la operación de servicio, ya que esas funciones han sido implementadas en Intel, que están al servicio de las distintas organizaciones dentro del Departamento de TI y que el equipo InfoSec de Intel Costa Rica puede hacer uso de ellas.

5.3. Trabajos pendientes

El plan de implementación de los procesos aquí propuestos deberá ser desarrollado posteriormente. En el presente documento solo se presenta una hoja de ruta que permite la visualización de las etapas que deberán ser consideradas en la definición del plan antes mencionado.

6. Capítulo VI: Apéndices y anexos

6.1. Anexo I - Operación del servicio de ITIL 2011

ITIL 2011

ITIL es un conjunto de buenas prácticas y métodos para la gestión de los servicios de TI. Su nombre proviene del inglés Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologías de Información (ClydeBank Technology, 2015).

ITIL es un marco de referencia público para la gobernanza de los servicios de TI. Se centra en la continua medición y mejora de la calidad con que se proveen los servicios de TI, desde el punto de vista del negocio y del cliente. Este enfoque es uno de los principales factores por los que ITIL ha tenido gran aceptación y éxito a nivel mundial y ha contribuido a que las empresas que lo han implementado obtengan beneficios como:

- Aumento de la satisfacción del cliente con respecto a los servicios de TI.
- Aumento de la disponibilidad de los servicios lo que ha impactado positivamente la rentabilidad del negocio.
- Ahorro financiero a partir de la eliminación de duplicidad de tareas y mejor manejo de los recursos.
- Disminución del tiempo que tardan los nuevos productos y servicios en llegar al mercado.
- Mejora de los procesos de toma de decisiones y reducción de los factores de riesgo.

(Cartlidge & Lillycrop, 2012)

ITIL propone que los servicios presentan un ciclo de vida organizado en las fases que podemos apreciar en la Figura 4 y que se listan a continuación:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

Estrategia del servicio

En el centro del ciclo de vida está la fase de Estrategia del Servicio que es donde comienza la creación de valor a través de la comprensión de los objetivos estratégicos de la organización, en la cual cada activo incluyendo personas, procesos y productos debe brindar soporte a la estrategia.

Entre los temas tratados en esta fase del ciclo de vida están el desarrollo de mercados, características de tipos de proveedores internos y externos, activos de servicios, portafolio de servicios, gestión de las relaciones de negocios, gestión de demanda, gestión financiera, desarrollo organizacional, estrategia de riesgos, entre otros.

Diseño del servicio

Para que los servicios generen verdadero valor al negocio deben ser diseñados teniendo en mente los objetivos estratégicos de la empresa. También, en el diseño de servicios se considera a todo el Departamento de TI como una sola entidad que brinda y da soporte a los servicios de TI. En esta fase es donde la estrategia definida en la fase previa se convierte en un plan para alcanzar los objetivos estratégicos del negocio.

El diseño no comprende solamente servicios nuevos, sino que también contempla aquellos existentes que deben ser ajustados para incrementar o mantener su nivel de valor entregado a los clientes. Contempla también la continuidad de los servicios, el logro de niveles de servicio, conformidad con estándares y regulaciones, coordinación de diseños, gestión del catálogo de servicios, gestión de los niveles de servicio, gestión de la disponibilidad, capacidad y continuidad de los servicios, gestión de la seguridad de la información, gestión de los proveedores, entre otros.

Transición del servicio

La transición del servicio ofrece una guía para el desarrollo y mejoramiento de las capacidades para incorporar nuevos y renovados servicios en el ambiente de producción, es decir, donde ya existen otros servicios que están siendo consumidos por los clientes y a los que ya se les brinda soporte.

Aquí se describe cómo en una organización se da la transición de un estado a otro mientras se mantiene control del riesgo y se brinda soporte a la gestión del conocimiento necesario para la toma de decisiones. En términos generales garantiza que el valor identificado en la fase de estrategia del servicio y codificado en la fase de diseño del servicio atraviese una transición efectiva para que pueda ser llevado a la realidad en la fase de operación del servicio.

Los temas tratados son la planificación de la transición y soporte, gestión de cambios, gestión de activos y configuración, gestión de versiones y despliegues, validación y prueba de servicios, evaluación de cambios y gestión del conocimiento, que busca hacer disponible el conocimiento que se va adquiriendo para que esté disponible en todas las etapas del ciclo de vida, entre otros.

Operación del servicio

La fase de operación de servicio describe las mejores prácticas para la gestión de servicios en ambientes de producción, es decir, donde ya son consumidos por los clientes. Incluye guías para alcanzar la efectividad y eficacia en la entrega y soporte de servicios que aseguren brindar valor a los clientes, usuarios y proveedor del servicio.

Entre los temas tratados en esta fase están la gestión de incidentes, gestión de problemas, gestión de eventos, resolución de solicitudes y procesos de gestión de accesos.

Mejora continua del servicio

La mejora continua del servicio ofrece una guía para la creación y mantenimiento de valor para los clientes a través del mejoramiento de la estrategia, el diseño, la transición y la operación del

servicio. Combina principios, prácticas y métodos de gestión de calidad, gestión de cambios y mejoramiento de las capacidades.

Obtiene retroalimentación desde todas las fases del ciclo de vida y lo utiliza para identificar oportunidades de mejora en todas ellas. Entre los temas tratados están las métricas del servicio, la demostración del valor a través de métricas y el desarrollo de evaluaciones de línea base y madurez.

Origen del marco de referencia

ITIL fue desarrollado a inicios de la década de los 80 por la Central Communications and Telecommunications Agency (CCTA) o Agencia Central de Comunicaciones y Telecomunicaciones, una oficina del gobierno británico (Cartlidge & Lillycrop, 2012).

La primera versión de ITIL consistía de 31 libros que abarcaban todos los aspectos de la prestación de servicios de TI. Entre el 2000 y el 2004 esta versión inicial fue revisada y reemplazada por la versión ITIL v2 que consistía de siete libros mejor conectados entre sí que consolidaban el marco de referencia de forma consistente. Posteriormente en 2007 se publicó una nueva revisión que llamaron ITIL v3 y que estaba constituida por cinco libros principales que abarcaban el ciclo de vida de los servicios de TI.

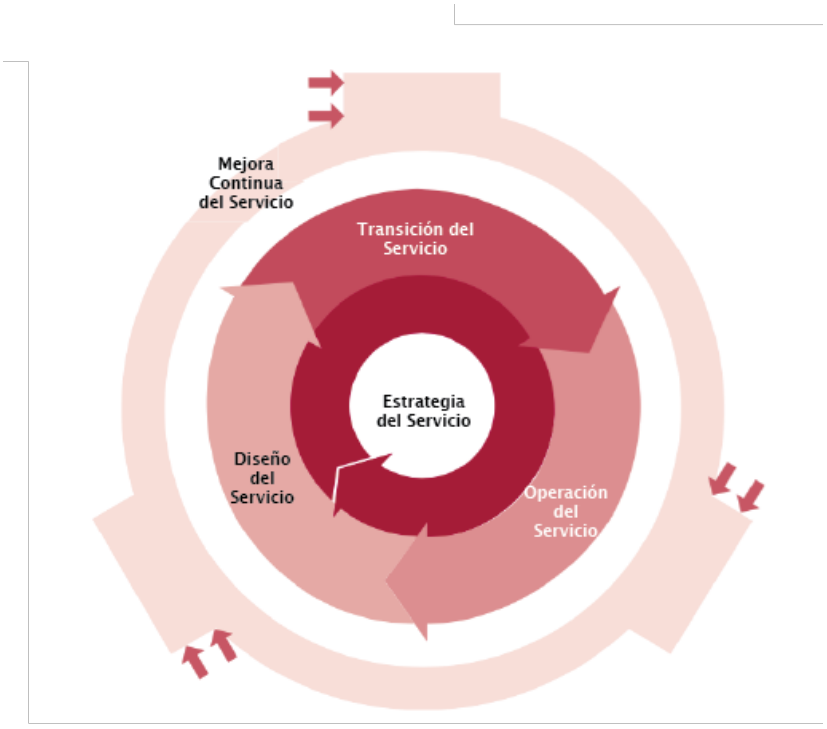


Figura 1. Ciclo de vida de los servicios ITIL. Fuente: ITIL

En 2011 se publicaron las ediciones ITIL 2011, que es la versión más reciente y que consiste en una nueva revisión para mejorar la claridad y la consistencia a través de los cinco libros del marco

de referencia y para introducir pequeñas adiciones que le permitan mantenerse actualizado y acorde con las últimas demandas de la industria.

Operación del servicio

Como ya se mencionó, los servicios son un medio para generar valor a los clientes al producir los resultados que ellos desean, sin que deban asumir los costos y riesgos específicos asociados. Los servicios facilitan los resultados mejorando el desempeño de las tareas asociadas y reduciendo el efecto de las restricciones, las cuales pueden incluir regulaciones legales, falta de presupuesto o capacidad, o bien limitaciones tecnológicas.

Específicamente un servicio de TI es aquel que brinda un proveedor de servicios de TI, que puede ser el Departamento de TI mismo, o bien una organización subordinada a ésta. Un servicio de TI es una combinación de tecnologías de información, personas y procesos (Best Management Practice, 2011).

Las necesidades y resultados deseados por los clientes tienden a variar en el tiempo, por lo que los proveedores de servicios de TI necesitan asegurarse de que los servicios que ofrecen continúan satisfaciendo a los clientes y para ello es importante tener presente la forma en que los servicios se pueden clasificar. La siguiente tabla muestra la clasificación de los servicios.

Servicios Centrales	Son aquellos servicios que entregan los resultados básicos que uno o más clientes desean. Representan el valor que el cliente desea y por el cual está dispuesto a pagar. Forman parte esencial de la propuesta de valor ofrecida al cliente y proveen las bases para que estos se mantengan consumiendo dichos servicios y estén satisfechos.
Servicios Habilitadora	Son aquellos servicios que hacen posible la entrega de los servicios centrales. Estos servicios podrían o no ser visibles a los clientes, sin embargo, ellos no los perciben como tales. Son factores que permiten que el cliente pueda consumir el servicio “real” (servicio central).
Servicios de Mejora	Son aquellos servicios que se agregan a los servicios centrales para hacerlos más atractivos y con ellos lograr que los clientes los consuman con mayor frecuencia, o bien que elijan por encima del que ofrece otro proveedor.

Clasificación de los servicios. Fuente: ITIL 2011 Service Operation

En la fase de operación del servicio es donde la estrategia de servicio, el diseño de servicio y la transición del servicio se ven reflejados para entregar el valor al cliente, es aquí donde se hacen visibles para el cliente los resultados que espera.

Para los negocios, el uso de servicios de TI se ha convertido en una utilidad y quieren que estén disponibles de la misma forma en que ocurre con el suministro de agua potable, la electricidad o

el teléfono. Pero no es suficiente con incorporar lo último de la tecnología para los servicios de TI sean confiables y de alta calidad, también se necesita de una gestión profesional, que responda a las necesidades del cliente y que se enfoque en generar valor al negocio.

La gestión de servicios es un conjunto de capacidades organizaciones especializadas en entregar valor a los clientes a través de la prestación de servicios. Mientras más maduras estén estas capacidades, más probabilidades habrá de producir servicios de alta calidad que satisfagan las necesidades de los clientes de manera constante y consistente, con un enfoque de bajo costo y siendo entregados de manera oportuna. La acción de transformar capacidades y recursos en servicios de valor es el eje principal de la gestión de servicios (Best Management Practice, 2011).

A diferencia de la gestión de otros sectores como manufactura, minería o agricultura, la gestión de servicios se enfrenta a los siguientes retos que la distinguen:

- La naturaleza intangible de los resultados y productos intermedios de los procesos de un servicio, lo que los hace difíciles de medir, controlar y validar.
- La demanda está estrechamente relacionada con actividades y elementos propios de los clientes tales como procesos, aplicaciones, documentos y transacciones que estimulan la producción del servicio consumido.
- El alto nivel de contacto entre productores y consumidores de servicios. No se pueden almacenar los resultados de un servicio como sí ocurre con los inventarios de productos.
- La naturaleza perecedera de la capacidad y los resultados de un servicio. Habrá valor para el cliente en un servicio en tanto el suministro de este sea constante y su calidad sea consistente.

En el contexto de TI la gestión de servicios (ITSM o IT Service Management) se refiere a la implementación y gestión de servicios de TI de calidad que satisfagan las necesidades y requerimientos del negocio. La gestión de los servicios de TI está a cargo de los proveedores de servicios de TI a través de una combinación de personas, procesos y recursos de tecnologías de información. Un proveedor de servicios de TI puede ser cualquiera organización dentro del Departamento de TI de una empresa y puede ofrecer servicios a clientes internos o externos.

El proveedor de servicios de TI debe trabajar en la forma de mantener un balance entre ofrecer un servicio que satisfaga las necesidades del cliente, su expectativa de desempeño y su capacidad de pago del costo. También, debe mantener la comunicación con el cliente para informarle de cualquier situación que impida que el servicio sea entregado conforme el acuerdo de servicio al que llegaron.

Para definir los acuerdos se utiliza un Acuerdo de Nivel de Servicio o SLA (Service Level Agreement) entre el proveedor del servicio de TI y el cliente. Este documento describe el servicio de TI, los objetivos de nivel del servicio y especifica las responsabilidades tanto del proveedor como del cliente. Un mismo SLA puede abarcar múltiples servicios o clientes.

Otro de los elementos a considerar en la gestión de los servicios de TI corresponde a las partes interesadas o stakeholders en inglés, término a utilizar de aquí en adelante. Los stakeholders tienen algún interés en una organización, un proyecto, un servicio, entre otros. y pueden interesarse por las actividades, objetivos,recursos o entregables de la gestión de servicios. Ejemplos de stakeholders son las organizaciones, los proveedores de servicio, los clientes, los usuarios, los socios, los empleados, los accionistas, los dueños y los proveedores.

Recordemos que el valor de un servicio se considera como el nivel con que este llena las expectativas del cliente. Los servicios no tienen un valor intrínseco, sino que el valor proviene de lo que el servicio le permite alcanzar a quien lo consume. Desde la perspectiva del cliente, el valor consiste en alcanzar los objetivos del negocio. El valor de un servicio de crea a través de la combinación de dos elementos primarios que son la utilidad (aptitud para el propósito) y garantía (aptitud para el uso).

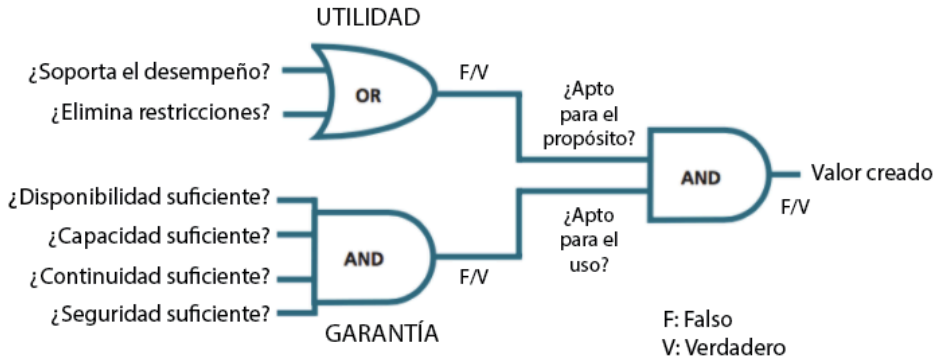


Figura 2. Lógica de creación de valor a través de un servicio. Fuente: ITIL 2011 Service Operation

La figura 5 ilustra la forma en que un servicio presenta ambas características: utilidad y garantía. En términos generales la utilidad se refiere a lo que el servicio hace y sirve para determinar si el servicio provee los resultados requeridos. Por su parte la garantía se refiere a la forma en que el servicio es entregado y sirve para determinar si este se adecua a los requerimientos de uso del negocio, por ejemplo, si es lo suficientemente seguro, si está disponible cuando se necesita y si cuenta con la capacidad suficiente para satisfacer la demanda.

Procesos

En esta sección se describirán los procesos y actividades de los cuales se depende para que la operación del servicio se pueda realizar de forma efectiva. Los procesos definidos por ITIL en esta fase del ciclo de vida de los servicios de TI son: gestión de eventos, gestión de incidentes, resolución de solicitudes, gestión de problemas y gestión de acceso. A pesar de que algunos de estos procesos se utilizan a través de todo el ciclo de vida, se ubican en esta fase porque son escenciales para que la operación del servicio sea efectiva.

Esta es una breve descripción de cada uno de los procesos, que más adelante se describirán en detalle.

La gestión de eventos es el proceso que monitorea todos los eventos que ocurren en la infraestructura de TI para comprobar que opera normalmente y para detectar condiciones excepcionales que deben ser atendidas adecuada y oportunamente.

La gestión de incidentes se centra en reestablecer un servicio que haya sufrido una degradación de su nivel o se haya interrumpido, con el fin de minimizar el impacto negativo en el negocio.

La gestión de problemas se encarga de realizar análisis de causa raíz para resolver los eventos e incidentes desde su orígen y evitar que ocurran. Es importante resaltar que existe una distinción entre incidentes y problemas con el fin de evitar el riesgo de que:

- Las actividades de resolución de incidentes se extiendan mientras se busca el origen del problema, en vez de reestablecer el servicio afectado.
- Los registros de los incidentes se cerrarían muy pronto sin que se tomaran acciones para evitar que se presenten de nuevo.
- Los registros de incidentes se mantendrían abiertos por más tiempos mientras mientras se concretan los análisis de causa raíz, lo que impediría que se cuente con indicadores precisos sobre el momento en que un servicio fue reestablecido.

La resolución de solicitudes es el proceso que se encarga de gestionar las solicitudes de los clientes o usuarios desde que son planteadas hasta que se han completado. Se mantiene un registro de las solicitudes para darle seguimiento a su estado. Una solicitud puede ser, por ejemplo, requerir asistencia con la adquisición de un servicio, con la forma de consumir un servicio, con el cambio de una contraseña, para agregar un usuario, entre otros escenarios.

La gestión de acceso se refiere al proceso de permitirle a usuarios autorizados el uso de un servicio y asegurar que los usuarios no autorizados no lo pueden consumir. Se basa en la capacidad de identificar con precisión a los usuarios debidamente autorizados y gestionar su acceso a los servicios de acuerdo al rol y a la organización al que pertenecen.

Gestión de eventos

Un evento se puede definir como cualquier cambio de estado significativo desde la perspectiva de la gestión de un elemento de configuración (CI, del inglés configuration item) o de un servicio de TI. Ejemplos típicos de eventos son las notificaciones creadas por los servicios de TI, los elementos de configuración o CIs, o bien, las herramientas de monitoreo.

Una efectiva operación del servicio depende de la capacidad de reconocer cualquier cambio de estado en la infraestructura. Esto se consigue gracias a los sistemas de monitoreo y control, que tienen como base dos tipos de herramientas, a saber: las de monitoreo activo y las de monitoreo pasivo. Las primeras son aquellas que permiten conocer el estado y disponibilidad de los CIs, mientras que las segundas detectan y correlacionan alertas operacionales y comunicaciones generadas por CIs.

1. Propósito

El propósito de la gestión de eventos es conducir a estos a través de su ciclo de vida que consiste básicamente en la detección del evento, clasificacción del evento y determinación de las acciones de control necesarias, lo que la convierte en la base del monitoreo y control de operaciones. Y si con los eventos se pueden programar acciones de notificación del tipo informativo, de advertencia o de excepciones, se cuenta con las bases para automatizar muchas de las rutinas de gestion de operaciones, por ejemplo, ejecutar secuencias de comandos en dispositivos remotos, iniciar la ejecución de tareas programas, o bien, labores más complejas como el balanceo de carga en múltiples equipos.

2. Objetivos

Por otra parte, la gestión de eventos cuenta con los siguientes objetivos:

- Detectar todos los cambios de estado que sean significativos para la gestión de un CI o un servicio de TI.
- Determinar la medida de control adecuada para el evento y comunicarla según corresponda.
- Proveer los disparadores o puntos de inicio de los procesos y actividades de gestión dentro de la operación del servicio.
- Proveer los medios para comparar el desempeño actual contra el esperado de acuerdo con estándares o SLAs.
- Proveer las bases para el aseguramiento y reporte de servicio, así como para el mejoramiento de este. Este objetivo se describe en detalle en el mejoramiento continuo del servicio, que es otra fase del ciclo de vida de los servicios de TI.

3. Valor para la empresa

En lo que respecta al valor que la gestión de eventos aporta al negocio, usualmente se da de forma indirecta, por ejemplo cuando gracias a la detección temprana de incidentes se pueden tomar las acciones de remediación antes de que se de un impacto negativo en los servicios de TI. Cuando, también, a través de tareas automatizadas se puede liberar recursos humanos costosos que pueden ser empleados en actividades de mayor valor agregado, que tengan que ver con innovación, búsqueda de nuevas formas de aprovechar los recursos tecnológicos disponibles, entre otras actividades.

4. Políticas

La gestión de eventos se apoya en políticas que guían las labores que se deben realizar. Estas políticas buscan estandarizar el trabajo a realizarse y la forma en que debe hacerse. Los siguientes son ejemplos de estas políticas:

- Las notificaciones de los eventos deben ser dirigidas a quienes les corresponde realizar las acciones y tomar las decisiones competentes. Esto evita que lleguen quienes no están relacionados con el evento reciban notificaciones que no portan ningún valor a su trabajo. Esta política implica que deben identificarse los departamentos, equipos de trabajo o individuos que deben responder ante un evento dado.

- La gestión de eventos y su correspondiente soporte deberían estar centralizados en la medida de lo posible, con el fin de evitar conflictos en el manejo de los eventos. Así, cuando se recibe una notificación de un evento, el personal sabrá qué hacer y se evita que no se tenga conocimiento de cómo reaccionar ante un evento desconocido porque no le corresponde.
- Todos los eventos deben utilizar un protocolo estandar de mensajería y bitácoras para que se facilite la interpretación y lectura, ya sea por personas o sistemas automáticos.
- Las acciones de manejo de eventos deben ser automatizadas hasta donde sea posible para reducir el riesgo de incidentes provocados por errores humanos.
- Debe existir un esquema de clasificación estándar que establezca un manejo y un proceso de escalación comunes para los eventos basado en su clasificación. Esto implica que existe de antemano un conjunto de acciones a ejecutar de acuerdo con el tipo de evento que se presenta.
- Todos los eventos conocidos deben ser capturados y registrados en una bitácora, con el fin de apoyar los procesos de análisis de causa raíz que buscan resolver problemas complejos. Deben existir mecanismos adecuados para el registro y almacenamiento de los eventos, para asegurar su conservación por el tiempo que sea necesario, para manipular los datos, para filtrar la información y otras acciones.

5. Tipos de eventos

Existen múltiples tipos de eventos, como por ejemplo:

- Informativos: cuando notifican de la ocurrencia de un evento que no implica un incidente potencial. Usualmente no requiere de ninguna acción de respuesta. Por ejemplo, cuando un usuario ha iniciado sesión.
- De advertencia: cuando se presenta una situación que podría implicar un incidente potencial. Es posible que se dé una acción de respuesta. Por ejemplo, cuando el nivel de memoria utilizada en un servidor alcanza un 90% de su nivel máximo.
- De excepción o error: cuando se presenta una situación fuera de lo normal o condición aceptable. Es posible que se haya generado un incidente a partir de este tipo de eventos, Generalmente se da una acción de respuesta. Por ejemplo, cuando el nivel de utilización del CPU de un servidor rebasa el nivel aceptable.

6. Filtrado de eventos

Es importante identificar los eventos que tienen significado relevante para el negocio en operación, porque un mismo evento puede indicar algo distinto dependiendo del contexto en que se dé o del momento en que ocurra. Por ejemplo, cuando un usuario debidamente autorizado ingresa a una aplicación, nada fuera de lo normal ocurre. Sin embargo, si ese mismo usuario tuvo un cambio de rol y ahora trabaja en otro departamento, es posible que ya tenga acceso a la aplicación, por tanto, si intenta ingresar de nuevo al sistema, los mecanismo de monitoreo y control deberían notificar de lo sucedido, ya que podría estarse dando un intento de accerder a la aplicación de manera fraudulenta.

Los eventos y los tipos de eventos que son relevantes no son estáticos y pueden evolucionar junto con el negocio mismo, por tanto, es necesario mantener un enfoque de evaluación y mejora

continua en la gestión de eventos para asegurar que todos los eventos monitoreados se mantienen relevantes y descartar aquellos que han perdido vigencia, así como incorporar los otros que aporten valor al aseguramiento de una operación del servicio eficaz y eficiente.

7. Consideraciones de diseño en la gestión de eventos

Algunas consideraciones claves a tener en cuenta durante la gestión de eventos son las siguientes:

- ¿Qué se debe monitorear?
- ¿Qué tipo de monitoreo se requiere? Por ejemplo: activo, pasivo; de desempeño o de resultados.
- ¿Cuándo es necesario generar el evento?
- ¿Qué tipo de información se debe comunicar durante el evento?
- ¿A quién va dirigida la información del evento?
- ¿Quién es el responsable de clasificar el evento, enviar las notificaciones, escalar el evento según corresponda, ejecutar las acciones apropiadas, etc.?
- ¿Cómo se van a generar los eventos?
- ¿Cómo se van a clasificar los eventos?
- ¿Cómo se van a enviar las notificaciones y cómo se harán las escalaciones?
- ¿Qué datos se incluirán en el registro del evento?
- ¿Dónde se almacenará la información del evento?

8. Actividades, métodos y técnicas

La Figura 6 ilustra el proceso de gestión de eventos. Es una representación genérica de alto nivel que sirve como referencia, pero que no pretende ser una descripción absoluta y completa del proceso. En ella se pueden ver las actividades y decisiones que se deben tomar en el proceso de gestión de un evento.

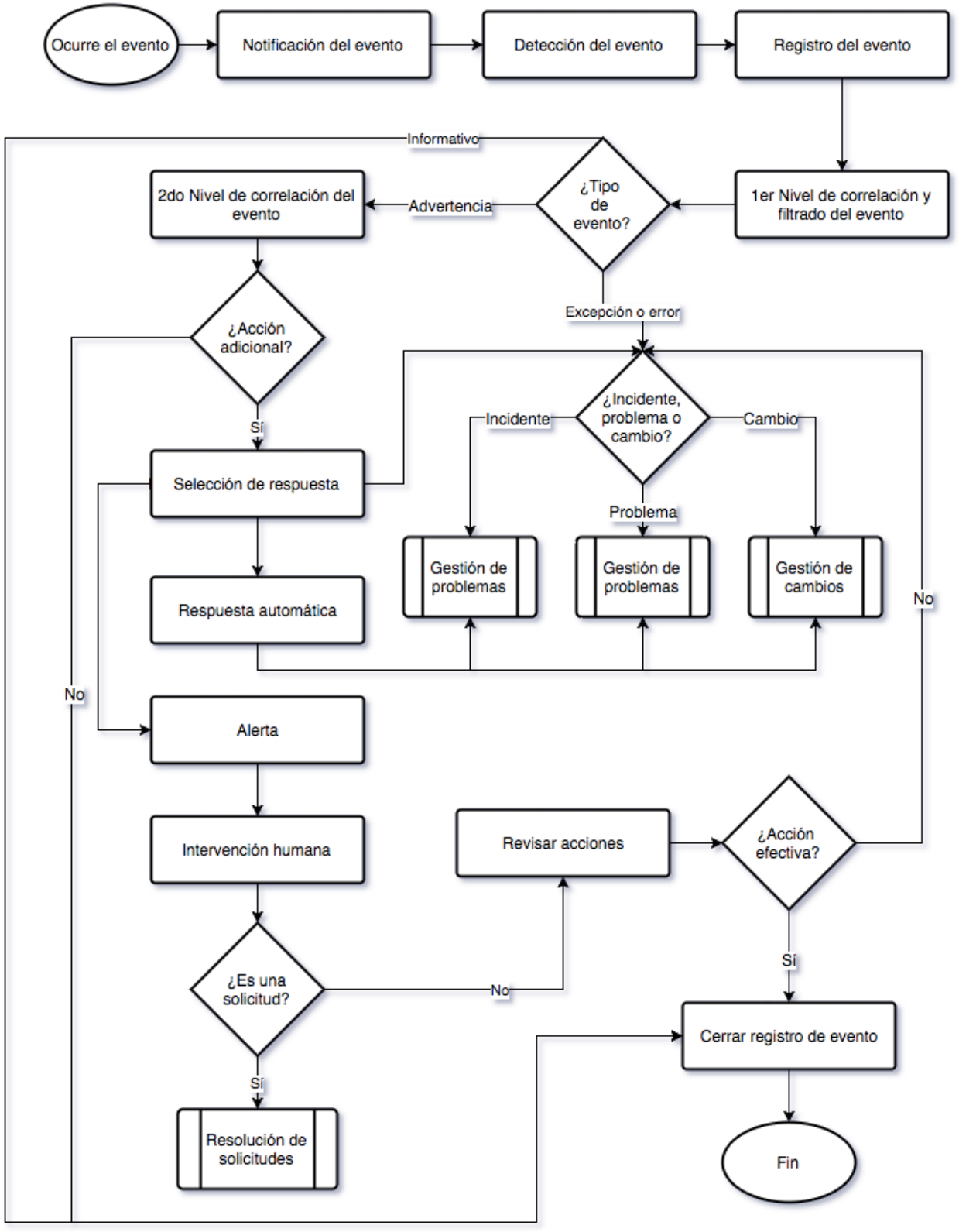


Figura 3. Proceso de gestión de eventos. Fuente: ITIL 2011 Service Operation

Lo primero que sucede es que el evento se presenta y esto se da de manera constante, pero no todos los eventos se detectan ni se registran. Por eso es importante identificar y definir cuáles eventos tienen un significado valioso para la operación del servicio.

Posteriormente se da la notificación del evento, en la cual se debe incluir información que ayude a la toma de decisiones. Incluir solamente códigos de error no es una buena práctica, ya que a pesar de que puede tener la intención de apegarse a un estándar de mensajes, puede hacer difícil decidir qué hacer con el evento, cómo reaccionar ante él.

Una vez que la notificación se ha generado, será detectado por un agente corriendo en el mismo sistema, o bien, será transmitida a una herramienta de gestión específicamente diseñada para leerla e interpretarla apropiadamente.

Tanto el evento como las acciones posteriores deben ser registrados. Esto debería hacerse a través de un sistema de gestión de eventos. Sin embargo, de no contar con uno de estos, el evento se puede registrar en la bitácora de la aplicación, pero deben existir mecanismos que permitan asegurar que los datos ahí almacenados estarán disponibles durante las investigaciones que puedan surgir a partir de la existencia de un registro de incidente o de un problema.

El propósito del primer nivel de filtrado y correlación es determinar la relevancia del evento. Es necesario determinar si el evento requiere que se le preste atención y se ejecuten las acciones del caso, o bien si debe ignorarse. Una vez que se ha determinado que el evento es relevante, se debe clasificar para saber qué significado tiene, si es meramente informativo, es una advertencia o bien indica que se ha presentado un error o un caso exepcional.

El segundo nivel de correlación permite determinar los pasos a seguir en caso de que el evento sea de un tipo tal que requiera atención. Asimismo, será necesario decidir si se requiere de acciones adicionales, tales como:

- Generar un registro de incidente,
- Generar una soliciitud de cambio,
- Ejecutar scripts que realicen actividades específicas, como por ejemplo reiniciar un dispositivo,
- Notificar a sistemas o personas acerca de la ocurrencia del evento, etc.

Una vez llegado a este punto será necesario elegir el tipo de respuesta ante el evento, que puede ser automática si se ha definido previamente, pero también puede ser que se requiera la intervención de una persona. Puede que sea necesario seguir la ruta de escalación si el evento lo amerita, por ejemplo.

Las acciones de revisión se refieren a que es importante asegurase de que, de acuerdo con las acciones que se llevaron a cabo, el proceso se desarrolló correctamente. Por ejemplo, si una de las acciones ejecutadas fue reiniciar un dispositivo, es importante verificar que dicho dispositivo esté funcionando adecuadamente después de haber sido reiniciado.

Por último, a pesar de que la mayoría de eventos no se “cierran” ni se “abren”, puede darse que un evento asociado a un incidente permanezca abierto en tanto el incidente no se haya resuelto.

9. Disparadores, entradas, salidas

El proceso de gestión de eventos puede ser iniciado por cualquir cambio de estado, pero la clave estará en definir con claridad cuáles de esos cambios de estados son los que ameritan que se les preste atención y que se reaccione ante ellos. Ejemplos de disparadores del proceso pueden ser:

- Cuando se dan excepciones al nivel de desempeño de un CI, previamente definido en las espepcificaciones de diseño.
- Cuando se presenta un error en un proceso de negocio que está siendo monitoreado.
- Cuando se completa la ejecución de una tarea programada.
- Cuando un usuario o un proceso automatizado accede a una aplicación o una base de datos.

Por lo general las entradas al proceso de gestión de eventos provienen del diseño de servicio o de la transición del servicio. Por ejemplo:

- Requerimientos de nivel de servicio o nivel operacional asociados a eventos y sus acciones correspondientes.
- Alarmas, alertas y umbrales para eventos específicos.
- Tablas de correlación de eventos, reglas, códigos de eventos, etc.
- Roles y responsabilidades para la clasificación de eventos y realizar las comunicaciones correspondientes.
- Procedimientos operativos para clasificar, registrar, escalar y comunicar eventos.

Entre las salidas del proceso de gestión de eventos tenemos las siguientes:

- Eventos que han sido comunicados, escalados y procesados según las acciones correspondientes.
- Registros de los eventos, las acciones realizadas, las comunicaciones emitidas, etc.
- Eventos que indican que ha ocurrido un incidente.

10. Gestión de la información

Información clave que se maneja en la gestión de eventos incluye lo siguiente:

- Mensajes, como los del tipo SNMP (Simple Network Management Protocol o Protocolo Simple de Administración de Red) que es una forma estandarizada de transmitir información técnica acerca del estado de componentes de la infraestructura de TI.
- Bases de datos como las utilizadas para gestionar la información de dispositivos.
- Agentes de software de herramientas de monitoreo.

Aunque no hay existe un registro estandar para almacenar los datos de los eventos, ya que el contenido exacto va a depender de la herramienta utilizada en la gestión de eventos, los siguientes datos se consideran como los más importantes:

- Dispositivo
- Componente
- Tipo de falla
- Fecha y hora
- Parámetros de la falla o error
- Identificador único del evento para poder darle seguimiento
- Valor

11. Factores críticos de éxito (Critical Success Factors, CSF) e indicadores clave de desempeño (Key Performance Indicators, KPI)

Cada organización debería definir sus propios factores críticos de éxito de acuerdo con los objetivos que tenga definidos para el proceso en particular. Cada uno de esos factores de éxito tiene asociada una serie de indicadores de desempeño, que serán utilizados para determinar el grado de madurez y las oportunidades de mejora en el proceso.

Los siguientes son ejemplos de CSFs y KPIs.

CSF	KPI
Detectar todos los cambios de estado que sean relevantes en la gestión de CIs y servicios de TI	• Número y proporción de eventos en comparación con el número de incidentes. • Número y porcentaje de cada tipo de evento según plataforma o aplicación en relación con la cantidad total de plataformas y aplicaciones que ofrezcan servicios de TI.
Asegurar que todos los eventos son comunicados a quien corresponda para que se ejecuten las acciones que procedan	• Número y porcentaje de eventos que requirieron o tuvieron de intervención humana. • Número de incidentes que ocurrieron y porcentaje de estos que se dispararon sin un evento asociado.
Proveer las bases para el aseguramiento del servicio, los reportes y la mejora del servicio	• Número y porcentaje de eventos duplicados. Este dato será útil para afinar los mecanismos de generación de eventos y reducir los datos innecesarios. • Número de eventos/alertas generadas sin que se haya presentado una degradación de servicios (falsos positivos).

Ejemplos de factores críticos de éxito y sus correspondientes indicadores clave de desempeño.
Fuente: ITIL 2011 Service Operation

12. Riesgos y retos

Se pueden enfrentar una serie de retos, como por ejemplo obtener los recursos necesarios para adquirir las herramientas y para hacerlas funcionar de la forma adecuada, de tal manera que provean los beneficios esperados. Otro reto es poder configurar las herramientas de tal manera que puedan filtrar los datos relevantes y no aporten información de relleno que podría dificultar la adecuada interpretación de lo realmente importante.

Desplegar las herramientas de monitoreo de la infraestructura de TI puede ser una actividad que consuma gran cantidad de recursos y tome mucho tiempo en completarse. También, estas herramientas de monitoreo podrían producir un alto tráfico de red que puede llegar a impactar negativamente otros sistemas, obligando a reducir la frecuencia de envío de información, aunque esto aumente el tiempo en que un evento puede ser descubierto.

Aunque se requiera tiempo para adquirir las destrezas necesarias para el correcto aprovechamiento de las herramientas de monitoreo, es importante establecer procedimientos para configurar el monitoreo de nuevos CIs, de tal manera que se mantenga la cobertura de monitoreo y no se ponga en riesgo la inversión hecha en estas herramientas.

Gestión de incidentes

En el contexto de ITIL, un incidente se define como una interrupción no planeada de un servicio de TI, una disminución en la calidad de un servicio de TI o bien una falla en un CI que todavía no ha impactado un servicio de TI (por ejemplo, cuando falla uno de los discos de un arreglo en espejo).

De acuerdo con lo anterior, la gestión de incidentes es el proceso responsable del ciclo de vida de los incidentes, los cuales pueden ser identificados por personal técnico, detectados por herramientas de monitoreo, reportados en comunicados de los usuarios, o bien reportados por proveedores o socios comerciales.

1. Propósito

El propósito de la gestión de incidentes es reestablecer los servicios interrumpidos en el menor tiempo posible y minimizar el impacto negativo que se haya podido provocar a la calidad del servicio afectado. Donde los parámetros de calidad están previamente definidos en el acuerdo de servicio.

2. Objetivos

Los objetivos de la gestión de servicio son:

- Asegurar que los métodos y procedimientos estandarizados se utilizan para producir respuestas, análisis, documentación, seguimiento y reportes eficientes de los incidentes.
- Aumentar la visibilidad de los incidentes y sus comunicados para el personal administrativo y soporte de TI.
- Mejorar la percepción hacia el Departamento de TI a través de un enfoque profesional en la expedita resolución de incidentes.
- Alinear las actividades y prioridades de la gestión de incidentes con los de la empresa.
- Mantener el nivel de satisfacción de los usuarios con respecto al nivel de calidad de los servicios de TI.

3. Valor para la empresa

Gracias a la gestión de incidentes la empresa se beneficia de varias formas, pero principalmente de contar con capacidades para reducir el trabajo no planeado y costos producto de incidentes, para detectar y reducir los incidentes rápidamente para que los servicios estén disponibles por

más tiempo, para alinear las actividades de TI con las prioridades de la empresa, de tal manera que los recursos se asignen dinámicamente donde son requeridos.

También, para incorporar mejoras a los servicios gracias al conocimiento que se adquiere sobre los incidentes y las formas de evitarlos y para que el centro de servicios pueda identificar necesidades de capacitación o mejora de los servicios, ya sea desde la perspectiva de la empresa o del Departamento de TI.

4. Políticas

Las políticas que guían la gestión de incidentes consideran lo siguiente:

- Los incidentes y su estado deben ser comunicados de manera oportuna y efectiva, de tal manera que los procesos de negocio que puedan verse afectados estén al tanto del impacto que puedan sufrir.
- Los incidentes deben ser resueltos dentro de los plazos establecidos por los acuerdos de servicio existentes en la empresa. Debe haber acceso a los recursos, tanto humanos como tecnológicos que permitan una pronta resolución.
- Se debe procurar mantener el nivel de satisfacción al cliente en todo momento y para ello debe contarse con personal calificado para este fin.
- Los incidentes y toda la información relativa a ellos deben registrarse y mantenerse en un sistema adecuado que facilite la comunicación del estado de los incidentes a las partes interesadas en darle seguimiento.
- Todos los registros de los incidentes deben guardar información común, de tal modo que se facilite la comunicación entre las áreas de soporte y que puedan realizarse las labores de gestión de incidentes sin contratiempos debido a interpretaciones incorrectas de los datos o a la falta de ellos.
- Los criterios para clasificar, priorizar y escalar los incidentes deben estar claramente definidos y nunca depender del criterio particular del personal de soporte.

5. Modelos de incidentes

Debido a que muchos de los incidentes que se presentan no son nuevos, sino que ya han ocurrido antes y posiblemente sigan ocurriendo, es recomendable definir modelos de incidentes, de tal manera que se conozca de antemano qué hacer cuando se presenten, cuáles herramientas utilizar y cuáles son los tiempos que deberían tenerse en cuenta para completar las actividades relacionadas con su resolución.

Los modelos de incidentes deben incluir los siguientes elementos:

- Los pasos a seguir en el manejo del incidente y el orden cronológico en que deben seguirse.
- Responsabilidades, es decir, quién debe hacer cada cosa.
- Precauciones que deben tomarse antes de trabajar en la resolución del incidente, como por ejemplo respaldar la información, los archivos de configuración, entre otros.
- Tiempos para completar las actividades.
- Procedimientos de escalación, es decir, a quién debe contactarse y en qué momento.
- Preservar evidencias que pueden ser útiles en caso de incidentes relacionados con seguridad, por ejemplo.

Existen incidentes que por su grado de impacto en los procesos de negocio tienen una gran urgencia en ser resueltos, se les conoce como incidentes graves (MI o major incident en inglés). En estos casos la necesidad de reestablecer los servicios afectados implica que los tiempos para realizar las actividades de resolución del incidente son más cortos y se requiere de equipos de trabajo que se mantengan enfocados en buscar las soluciones.

El seguimiento que se le da a los incidentes se hace mediante el monitoreo del estado, el cual puede tener uno de los siguientes valores:

- Abierto: cuando un incidente se ha identificado, pero no se asignó todavía a ningún grupo de soporte.
- En progreso: cuando el incidente ha sido asignado a un grupo de soporte y se encuentra en proceso de investigación.
- Resuelto: se implementó una solución al incidente, pero no se ha confirmado aún el restablecimiento del servicio por parte del cliente o usuario final.
- Cerrado: cuando el cliente o usuario final ha confirmado que el servicio se reestableció y las operaciones volvieron a su estado normal.

6. Actividades, métodos y técnicas

La Figura 7 ilustra el proceso de gestión de incidentes. Al igual que en el caso de gestión de eventos, esta no es la única forma en que se pueden gestionar los incidentes, pero sirve de referencia para que la empresa pueda definir su propio proceso.

A pesar de que no se puede trabajar en resolver un incidente que no se sabe que existe, es inaceptable desde el punto de vista de la empresa que el personal de soporte de TI espere a que el cliente o usuario final se vea afectado por una falla en un servicio y haga el respectivo reporte del incidente. Deben utilizarse todos los recursos disponibles para anticipar cualquier impacto negativo en los servicios de TI.

Cada incidente debe ser registrado con su respectiva fecha y hora, sin importar el medio por el cual fue notificado. Esto permite que cada incidente se trabaje y se le pueda dar seguimiento de forma individual y que se pueda reconocer el trabajo que se haya realizado en su resolución. También, para contar con indicadores que ayuden a medir, controlar y mejorar los procesos.

Entre los datos que cada registro de incidente debe incluir están: identificador único, categoría, nivel de urgencia, nivel de impacto, prioridad, fecha y hora, identificación de la persona o grupo que registró el incidente, información del cliente/usuario, descripción de los síntomas, estado, actividades realizadas para resolver el incidente y cuándo ocurrieron, fecha y hora en que fue resuelto, fecha y hora en que fue cerrado, entre otros datos.

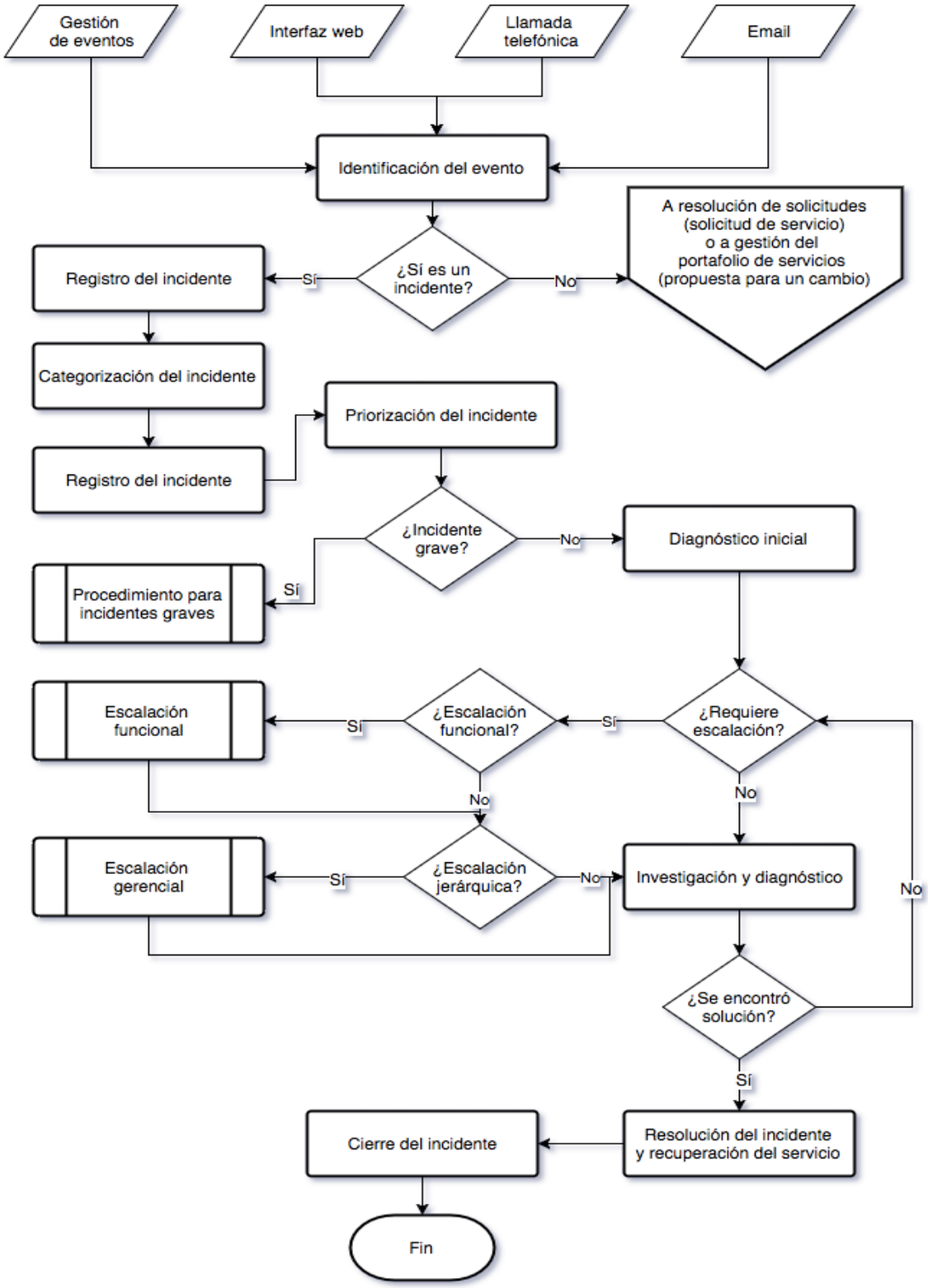


Figura 4. Proceso de gestión de incidentes. Fuente: ITIL 2011 Service Operation

Como parte del registro del incidente debe indicarse una categoría, que puede estar definida en varios niveles y que podría cambiar conforme avanzan la investigación y las actividades de

resolución, por eso es importante revisar la categoría más adelante y no necesariamente dejar el valor ingresado inicialmente.

También es necesario indicar la prioridad, para lo cual generalmente se consideran dos factores, a saber: urgencia e impacto. La urgencia se refiere a qué tan pronto es que el negocio requiere que se resuelva el incidente, mientras que el impacto se refiere más bien a cuántos sistemas o usuarios se ven afectados, o también al impacto financiero que puede tener el incidente (pérdida de dinero por falla en sistema de producción de bienes, por ejemplo).

Una vez que se inician las actividades de resolución del incidente, debe estar muy claro que si se requiere de más conocimiento técnico para encontrar una solución, o bien ya ha transcurrido el tiempo permitido para el actual nivel de soporte trabaje el incidente, este debe ser transferido al siguiente grupo de soporte en la jerarquía de escalación.

Las actividades de resolución del incidente implican que se deben realizar investigaciones y diagnósticos para dar con las causas del problema y cada una de las actividades debe quedar registrada como parte de la documentación del incidente. Asimismo, cuando participan en conjunto distintos grupos de soporte es importante coordinar las acciones a realizar con el fin de evitar conflictos que puedan dar al trate con la solución.

Una vez definida una solución deben coordinarse las acciones para implementarla, así como las pruebas necesarias para garantizar el buen funcionamiento del servicio de TI afectado. Como ya se ha mencionado antes, todas estas acciones deben ser documentadas en detalle en el registro del incidente.

Finalmente, se debe dar el cierre del incidente una vez que se haya verificado que el cliente o usuario final está satisfecho con la solución implementada. Como parte de las actividades de cierre se debe validar que la categoría indicada es la correcta, se solicita retroalimentación al cliente o suario final, se completa la documentación y se define si se requieren acciones adicionales en caso de que el incidente se haya resuelto sin haber identificado la causa raíz, en cuyo caso el incidente sería utilizado en el proceso de gestión de problemas que será descrito más adelante.

7. Disparadores, entradas, salidas

Los incidentes pueden ser iniciados de muchas formas. Quizás la más común es cuando un usuario reporta una falla a través del centro de servicios o mediante un sistema de reporte de incidentes. Sin embargo, cada vez es más frecuente que sean las herramientas utilizadas en la gestión de eventos sean las que hagan los reportes de los incidentes.

En cuanto a las entradas del proceso de gestión de incidentes, algunos ejemplos pueden ser:

- Información acerca de los elementos de configuración y su estado.
- Informacióon acerca de errores conocidos y su solución.
- Comunicados acerca de los incidentes y sus síntomas.

- Comunicados acerca de solicitudes de cambios y nuevas versiones que han sido implementados recientemente o está planeada su implementación.
- Comunicados de eventos que fueron iniciados por el proceso de gestión de eventos.
- Objetivos operativos y de nivel de servicio.
- Retroalimentación por parte del cliente sobre el nivel general de satisfacción sobre la calidad de la gestión de incidentes.
- Criterios acordados para priorizar y escalar incidentes.

Entre las salidas del proceso de gestión de incidentes, tenemos estos ejemplos:

- Incidentes resueltos y las acciones que permitieron alcanzar la solución.
- Registro del incidente actualizado con información detallada.
- Clasificación del incidente actualizada para que pueda ser utilizada posteriormente en el proceso de gestión de problemas.
- Registro de problema para aquellos incidentes donde no se identificó una causa raíz.
- Validación de que los incidentes ocurridos no se presentaron debido a problemas resueltos anteriormente.
- Retroalimentación sobre incidentes relacionados con cambios y nuevas versiones.
- Identificación de CIs afectados por incidentes.

8. Gestión de la información

La mayor parte de la información que se utiliza en la gestión de incidentes proviene de lals herramientas utilizadas en el proceso y de las que se obtienen datos como: el historial del incidente o del problema, las categorías, scripts de diagnóstico que ayudan en los diagnósticos iniciales.

También se obtienen datos directamente del registro del incidente, tales como: el identificador, la casificación, la fecha y hora de registro y actividades realizadas, la identificación de las personas que actualizan los datos del registro, la información de contacto de las organizaciones o usuarios afectados, categoría, impacto, urgencia y prioridad, entre otros.

9. Factores críticos de éxito (Critical Success Factors, CSF) e indicadores clave de desempeño (Key Performance Indicators, KPI)

Al igual que ocurre en la gestión de eventos, se presentan a continuación ejemplos de factores críticos de éxito e indicadores clave de desempeño, sin embargo cada organización debe definir los propios de acuerdo con su nivel de madurez.

CSF	KPI
Resolver incidentes lo más rápido posible para minimizar el impacto a la empresa	• Tiempo en resolver el incidente, desglosado por código de impacto • Desglose de incidentes según etapa (registro, en progreso, cerrado, etc.) • Porcentaje de incidentes cerrados por el centro de servicios sin haber sido escalados • Número de incidentes resueltos sin que haya habido afectación de servicios

Mantener la calidad de los servicios de TI	• Total de incidentes (como medida de control) • Tamaño de la cola de incidentes para cada servicio de TI • Número y porcentaje de incidentes graves para cada servicio de TI
Asegurar que los métodos y procedimientos estandarizados se usen eficientemente para responder, analizar, documentar y dar seguimiento a los incidentes con el fin de mantener la confianza en IT	• Número y porcentaje de incidentes asignados incorrectamente • Número y porcentaje de incidentes categorizados incorrectamente • Número y porcentaje de incidentes procesados por agente del centro de servicios • Número y porcentaje de incidentes relacionados con cambios y nuevas versiones
Ejemplos de CSFs y sus correspondientes KIPs. Fuente: ITIL 2011 Service Operation	

10. Riesgos y retos

En la gestión de incidentes se pueden presentar retos que dificulten el éxito del procesoL tales como contar con la capacidad de detectar incidentes lo más cerca de su origen como sea posible. Esto va a requerir el uso y configuración adecuada de herramientas de gestión de eventos, capacitación a los usuarios que reportan incidentes y el uso de grupos especializados en el centro de servicios.

Asimismo, será muy conveniente convencer al personal, tanto técnico como a los usuarios, de la importancia de registrar todos los incidentes y documentarlos detalladamente, ya que toda la información que se incluya, tanto de síntomas, diagnóstico e investigaciones, como de las actividades realizadas para resolver la falla, serán muy valiosas para crear conocimiento que ayudará a reducir el número de incidentes a futuro, así como a resolver rápidamente aquellos que se sigan presentando.

Por otra parte, entre los riesgos podemos mencionar que podría darse el escenario en que un gran número de incidentes saturen el servicio de soporte debido a falta de personal o falta de capacitación de dicho personal. También, podría faltar información oportuna debido a la carencia de fuentes adecuadas.

Resolución de solicitudes

El término “solicitud de servicio” es una descripción general para una gran variedad de peticiones que hacen los usuarios al Departamento de TI y sus dependencias. Por lo general tienen que ver con cambios pequeños, de costo y riesgo bajos, como por ejemplo: un cambio de contraseña, la instalación de software o reubicar equipo de cómputo. También, pueden ser simples peticiones de información.

Debido a su naturaleza de bajo costo y la alta frecuencia con que se reciben, este tipo de solicitudes se gestionan en un proceso independiente de la gestión de incidentes y de cambios.

El éxito en la resolución de este tipo de solicitudes contribuye significativamente a mantener la satisfacción del cliente y una buena percepción por parte de la dirección de la empresa hacia los servicios de TI.

1. Propósito

El propósito del proceso de resolución de solicitudes es asumir la responsabilidad de gestionar el ciclo de vida de las solicitudes de usuarios de los servicios de TI.

2. Objetivos

Como objetivos de la resolución de solicitudes podemos citar los siguientes:

- Mantener una alta satisfacción de parte de los clientes y usuarios de los servicios de TI a través de una gestión eficiente y profesional de sus solicitudes de servicio.
- Proveer un canal para que los usuarios puedan solicitar servicios estándar, para los cuales existe una autorización y un proceso definido previamente.
- Proveer a los usuarios la información necesaria sobre los servicios disponibles para que puedan solicitarlos.
- Obtener y entregar los componentes de los servicios estándar, como por ejemplo licencias de software.
- Brindar asistencia con quejas, comentarios o solicitudes de información general.

3. Valor para la empresa

El valor que aporta este proceso a la empresa radica en la capacidad de proveer un acceso rápido y eficiente a los servicios estándar de TI que el negocio requiere y puede utilizar para mejorar la productividad y la calidad de sus productos y servicios. Asimismo, en la capacidad de reducir la burocracia en la solicitud de servicios y la resolución de dichas peticiones, reduciendo a su vez el costo mediante la centralización y estandarización del proceso.

4. Políticas

Las políticas del proceso de resolución de solicitudes pueden incluir los siguientes aspectos:

- Las actividades realizadas para completar una solicitud deben seguir un flujo de proceso previamente definido (un modelo). De este modo se puede lograr que esta labor se haga de manera eficiente y consistente.
- El responsable de la solicitud recibida debe ser una función centralizada, como el caso del centro de servicios, para que exista un único punto de contacto entre el solicitante y el proveedor del servicio.
- Cuando una solicitud implica un impacto en un CI debe ser transferida al proceso de gestión de cambios, de ese modo este proceso podrá mantener el control de las variaciones que pueda sufrir al CI.
- Todas las solicitudes deben ser registradas, controladas, coordinadas y gestionadas a través de un sistema único que permita manejar su ciclo de vida.
- Todas las solicitudes deben ser aprobadas antes de realizar cualquier trabajo para completarlas. Esto garantiza que no se desperdicien recursos y que se apliquen los controles de seguridad establecidos.
- Deben existir criterios acordados para establecer la prioridad de las solicitudes, de tal manera que éstas se atiendan en conformidad con las prioridades y objetivos de la empresa.

- Las informaciones acerca del estado de las solicitudes deben ser claras y gestionadas por el único punto de contacto entre el usuario y el proveedor del servicio. Usualmente es el centro de servicios.

5. Modelos de resolución de solicitudes

Algunas de las solicitudes pueden recibirse con una alta frecuencia, por lo que resulta conveniente definir modelos que permitan gestionar estas peticiones de forma consistente y eficiente. Se les conoce como solicitudes estándar y el procedimiento para completarlas es bien conocido y ha sido depurado por el Departamento de TI.

6. Actividades, métodos y técnicas

Una descripción general del proceso de resolución de solicitudes se presenta en la Figura 8, la cual ilustra una de las formas de ejecutar el proceso, sin que necesariamente sea la única. Cada organización deberá definir su propio proceso sobre la base de las recomendaciones que plantea este marco de referencia.

Antes de que se haya recibido una solicitud formal de un servicio no debe empezarse a trabajar en ella. Por lo general estas solicitudes llegarán a través del centro de servicios, pero también pueden darse a través del proceso de gestión de cambios o un sistema automático de recepción de solicitudes y se creará un registro con toda la información que se pueda capturar para que no sea necesario (en la medida de lo posible) ir de nuevo hasta el usuario.

Uno de los pasos más importantes es determinar lo efectivamente se está ante una solicitud de un servicio, un incidente o una solicitud de un cambio, en cuyo caso sería transferida a los procesos de gestión de incidentes o gestión de cambios respectivamente. Si se determinó que sí es una solicitud, entonces debe crearse un registro en el sistema correspondiente.

Al igual que sucede en los procesos de gestión descritos anteriormente, el registro de solicitud debe contener toda la información relevante al pedido para que exista un historial que facilite el trabajo propio de la solicitud y otras labores de soporte que puedan ser requeridas a futuro.

Entre los datos a registrar están: un identificador único, la categoría, el nivel de urgencia, el impacto, la prioridad, la fecha y hora del registro, datos del solicitante, descripción de la solicitud, estado, entre otros. Apoyado en esta información se debe validar la solicitud para asegurar que no está fuera del alcance del servicio, ya que algún usuario podría solicitar una nueva funcionalidad, lo cual haría que el pedido no fuera una solicitud estándar, sino una solicitud de un cambio.

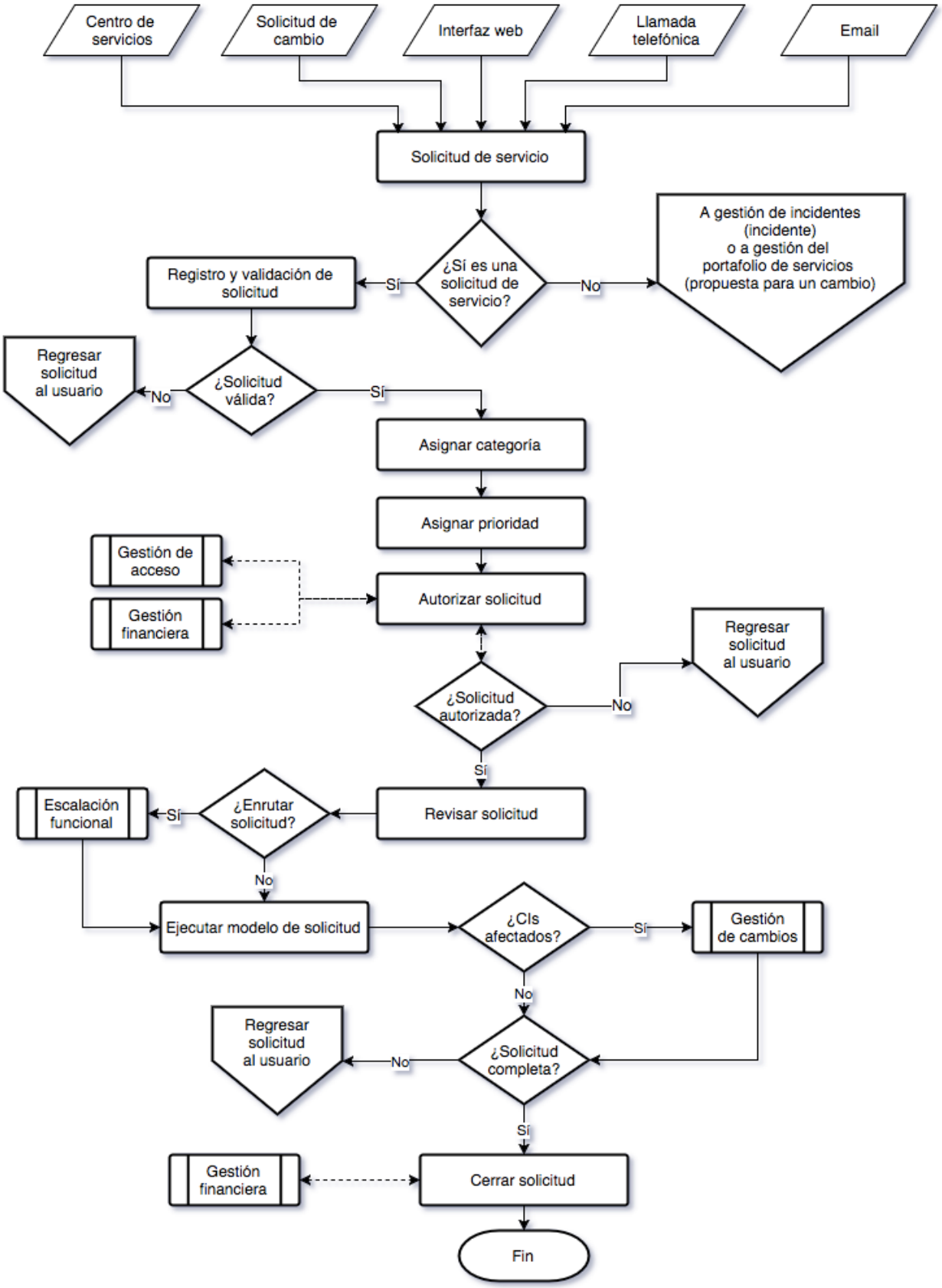

Centro de servicios
Solicitud de cambio
Interfaz web
Llamada telefónica
Email
Solicitud de servicio
¿Sí es una solicitud de servicio?
Sí
No
A gestión de incidentes (incidente) o a gestión del portafolio de servicios (propuesta para un cambio)
Registro y validación de solicitud
¿Solicitud válida?
No
Sí
Regresar solicitud al usuario
Asignar categoría
Asignar prioridad
Gestión de acceso
Gestión financiera
Autorizar solicitud
¿Solicitud autorizada?
No
Regresar solicitud al usuario
Sí
Revisar solicitud
¿Enrutar solicitud?
Sí
Escalación funcional
No
Ejecutar modelo de solicitud
¿CIs afectados?
Sí
Gestión de cambios
No
¿Solicitud completa?
No
Regresar solicitud al usuario
Sí
Gestión financiera
Cerrar solicitud
Fin

Figura 5. Proceso de resolución de solicitudes. Fuente: ITIL 2011 Service Operation

Las solicitudes deben categorizarse, de esa manera se podrá saber qué tipo de petición se recibe y también brinda la posibilidad de contar con información estadística que ayuda a identificar, por ejemplo, cuáles servicios son los más solicitados. Estos son algunos ejemplos de categorías:

- Por servicio
- Por actividad
- Por tipo
- Por función
- Por tipo de CI

También es importante priorizar las solicitudes y al igual que ocurre con los incidentes, los principales criterios para definir la prioridad se basan en la urgencia y el impacto, que tienen el mismo significado que en el proceso de gestión de incidentes y que consideran los mismos factores como, por ejemplo, la cantidad de usuarios afectados o la cantidad de pérdidas que genera para la empresa.

Otra de las condiciones que debe cumplirse para empezar el trabajo de una solicitud es que ésta debe estar debidamente autorizada, ya sea una autorización sencilla como en el caso de las solicitudes estándar, o bien una autorización más rigurosa cuando, por ejemplo, haya costos adicionales asociados.

Una vez confirmada la autorización, se procede a asignar la solicitud a la función que le corresponda completarla. Usualmente aquellas solicitudes donde solamente se pide información las atiende y resuelve el centro de servicios, pero si se requiere algo más complejo, entonces la solicitud se escala y asigna a la función competente.

Por último, se procede al cierre de la solicitud una vez que se hayan completado todas las actividades implicadas y que se haya confirmado que el usuario está satisfecho con la labor realizada.

7. Disparadores, entradas y salidas

Las solicitudes de servicios usualmente inician con una llamada al centro de servicios por parte del usuario. Aunque también se pueden crear mediante aplicaciones web o aplicaciones para dispositivos móviles que hayan sido implementadas para facilitar la tarea a los usuarios.

Como entradas al proceso de resolución de solicitudes podemos tener:

- Solicitudes de trabajo
- Formularios de autorización
- Solicitudes de servicios
- Solicitudes de cambios
- Pedidos a través de llamadas telefónicas, chats, email, etc.
- Solicitudes de información

En cuanto a las salidas del proceso tenemos los siguientes ejemplos:

- Solicitud de servicio rechazada
- Reportes de estado de las solicitudes
- Solicitudes satisfechas
- Incidentes (en caso de la solicitud realmente haya sido un incidente)
- Solicitud de cambio estándar
- Actualización de datos de un CI
- Solicitudes cerradas o canceladas

8. Gestión de la información

La resolución de solicitudes depende de la información del pedido formal de un servicio, la cual puede incluir lo siguiente:

- ¿Cuál servicio está siendo solicitado?
- ¿Quién solicitó y autorizó el servicio?
- ¿A quién se asignó la solicitud y qué acciones ha realizado?
- Fecha y hora de cuando se registró la solicitud en el sistema
- Detalles del cierre cuando se completa la solicitud.

9. Factores críticos de éxito (Critical Success Factors, CSF) e indicadores clave de desempeño (Key Performance Indicators, KPI)

De la misma forma en que ocurre en los dos procesos descritos anteriormente, cada organización tiene que definir sus propios CSFs y KPIs de acuerdo con su nivel de madurez. Sin embargo, en la siguiente tabla se muestran algunos que pueden servir de ejemplo o punto de partida.

CSF	KPI
Las solicitudes deben ser resueltas de manera eficiente y a tiempo en concordancia con los acuerdos de nivel de servicio	• El tiempo transcurrido en el manejo de la solicitud • El número y porcentaje de solicitudes resueltas dentro de los tiempos límite acordados • El desglose de las solicitudes según el estado (registro, en progreso, cerrada, etc.) • Número total de solicitudes
Solamente las solicitudes autorizadas deben ser resueltas	• Porcentaje de solicitudes debidamente autorizadas que se resolvieron • Número de incidentes relacionados con amenazas de seguridad originados en actividades de resolución de solicitudes
Mantener el nivel de satisfacción de los usuarios	• Nivel de satisfacción del usuario con el manejo de las solicitudes (medido mediante algún tipo de encuesta) • Número de incidentes relacionados con actividades de resolución de solicitudes • Tamaño de la lista de solicitudes pendientes

Ejemplos de CSFs y sus correspondientes KIPs. Fuente: ITIL 2011 Service Operation

10. Riesgos y retos

Los siguientes son retos que se pueden presentar al tener un proceso exitoso de resolución de solicitudes. Uno de ellos es definir con claridad y documentar detalladamente los tipos de solicitudes para que se pueda tener una clara distinción entre una solicitud estándar un una solicitud de cambio. También, establecer mecanismo de autoservicio para que los usuarios puedan interactuar de forma directa con el proceso de resolución de solicitudes, sin necesidad de recurrir al centro de servicios.

Asimismo, acordar cuáles servicios serán considerados estándar y quién estará autorizado a solicitarlos. Mantener el nivel de satisfacción de los usuarios con respecto a la resolución de solicitudes, lo que ayudará a generar una percepción positiva de los servicios de TI.

Por el lado de los riesgos puede ocurrir que el alcance del proceso no esté definido con claridad, por lo que el personal no va a estar seguro de hasta dónde llegan sus responsabilidades dentro del proceso. También, es posible que las herramientas con que se cuentan para que los usuarios hagan sus solicitudes no sean las mejores y con esto se dificulte la comunicación con ellos y por ende baje el nivel de satisfacción, entre otros.

Gestión de problemas

Gestión de problemas es el proceso responsable del manejo del ciclo de vida de los problemas, donde un problema, según ITIL, se define como el punto de origen de uno o más incidentes.

1. Propósito

La gestión de problemas busca resolver o eliminar fallas subyacentes en la infraestructura de TI a través de la investigación y documentación de incidentes, de tal manera que estos no se vuelvan a presentar. Esto se logra mediante la búsqueda e identificación de la causa raíz de los incidentes.

2. Objetivos

Los objetivos de la gestión de problemas son los siguientes:

- Prevenir la ocurrencia de incidentes producto de problemas en la infraestrutura de TI.
- Eliminar los incidentes recurrentes.
- Minimizar el impacto de los incidentes que no se pueden prevenir.

3. Valor para la empresa

El valor aportado a la empresa por parte de este proceso radica en aumentar la disponibilidad de los servicios de TI mediante la reducción de la frecuencia en que ocurren los incidentes y el tiempo que estos requieren en ser resueltos. También, en reducir los costos de la utilización de recursos en resolver los mismos incidentes en repetidas ocasiones, así como evitar el uso de soluciones temporales que no tienen el efecto esperado.

4. Políticas

Esta es una lista de ejemplos de políticas que pueden ser aplicadas en la gestión de problemas:

- A los problemas se les debe dar seguimiento de forma separada de los incidentes. Básicamente porque los primeros implican actividades proactivas, mientras que los estos últimos demandan acciones reactivas.

- Los problemas deben registrarse y manejarse en un único sistema de información para centralizar la documentación, facilitar las investigaciones y poder compartir la información de manera ágil.
- Todos los problemas deben apegarse a un esquema de clasificación estandar que sea consistente en toda la empresa. Esto permite un acceso más eficiente a la información durante las investigaciones y ayuda en el soporte de los procesos de diagnóstico.

5. Modelos de problemas

Aunque lo usual es que cada problema sea único, varios problemas podrían tener una base común en el desarrollo de las investigaciones, lo que propiciaría la creación de modelos. Sin embargo, al igual que en los procesos anteriormente descritos, queda a criterio de cada organización si define estos modelos.

Es de utilidad tener guías que permitan definir rápidamente si uno o más incidentes requieren de la creación de un registro de problema. Los siguientes criterios pueden ayudar a definir esas guías:

- Cuando el proceso de gestión de incidentes no puede asociar un incidente a un problema previamente creado o a un error conocido.
- Análisis de tendencias de incidentes revela que podría existir un problema.
- Cuando se presenta un incidente grave y es necesario encontrar la causa raíz.
- Otras funciones del Departamento de TI determinan que existe un problema que debe ser resuelto.
- Cuando el centro de servicios ha resuelto un incidente, pero no ha identificado la causa definitiva y sospecha que el incidente puede seguir presentándose.
- Análisis de un incidente por parte de un equipo de soporte revela que puede existir un problema subyacente.
- Cuando se recibe la notificación de parte de un proveedor de servicios indicando que existe un problema que debe ser resuelto.

6. Actividades, métodos y técnicas

La figura 9 ilustra el proceso de gestión de problemas y al igual que en los procesos descritos anteriormente, este no es la única forma de implementar el proceso, pero es una buena referencia.

La detección del problema es el punto de partida y puede surgir del registro de múltiples incidentes por parte del centro de servicios que considera que tienen un origen común, o del análisis de incidentes que realiza un grupo de soporte, o bien a través de herramientas de detección de fallas en la infraestructura, entre otros escenarios.

Independientement del método de detección del problema, este debe registrarse junto con toda la información que se pueda recopilar de los incidentes que lo originaron. Aunque no es exahustiva, la siguiente es una lista de los datos típicos que se registran en cada problema:

- Detalles del usuario
- Detalles del servicio
- Detalles del equipo

- Fecha y hora del registro del problema
- Información de prioridad y categoría
- Descipción del incidente
- Identificadores de los incidentes
- Detalles de todos los diagnósticos o acciones de recuperación realizadas

La categorización de los problemas debería realizarse bajo los mismos parámetros que se utilizan para categorizar incidentes, de manera tal que sea más sencillo establecer una relación entre ellos.

En lo que respecta a la priorización, ésta debería realizarse de forma similar a como ocurre con los incidentes, donde el impacto y la urgencia se utilizan para darle un valor a la prioridad. Del mismo modo debe considerarse también la severidad del problema que en este contexto se refiere a qué tan serio es el problema tanto desde la perspectiva del cliente como de infraestructura. Por ejemplo:

- ¿Se puede reparar el sistema o necesita ser reemplazado?
- ¿Cuánto va a costar la solución del problema?
- ¿Cuántas personas con las destrezas adecuadas se van a necesitar para resolver el problema?
- ¿Cuánto tiempo va a tomar resolver el problema?
- ¿Cuál es la extensión del problema (en términos de CIs afectados)?

En este punto es necesario realizar una investigación que produzca un diagnóstico que lleve a dar con el origen del problema. Para ello deben destinarse todos los recursos necesarios y acordes con el nivel de urgencia, severidad e impacto del problema.

En ocasiones es posible utilizar soluciones temporales a los incidentes con el objetivo de reestablecer el servicio afectado, mientras las investigaciones continuan hasta encontrar una solución definitiva al problema. Todas estas soluciones temporales que puedan surgir deben ser documentadas en detalle en el registro del problema.

Cuando se ha encontrado la causa raíz de un problema y también una solución temporal y ambos están debidamente documentados, se conoce como un error conocido, cuyo fin es facilitar la identificación de incidentes y acortar el tiempo requerido para resolverlos; mientras las investigaciones continuan para encontrar una solución definitiva al problema.

Una vez que se haya encontrado una solución definitiva y se conozcan los detalles de cómo implementarla, incluyendo las posibles solicitudes de cambios que deberán pasar por el proceso de gestión de cambios. Todo esto debe hacerse para garantizar que la solución propuesta no tendrá ningún impacto negativo en el servicio que se pretende reparar. Si al problema aun no se le encuentra una solución definitiva o bien la solución tiene un costo muy alto en comparación con el beneficio, el registro puede permanecer abierto, con su respectiva solución temporal para mitigar el impacto de los incidentes.

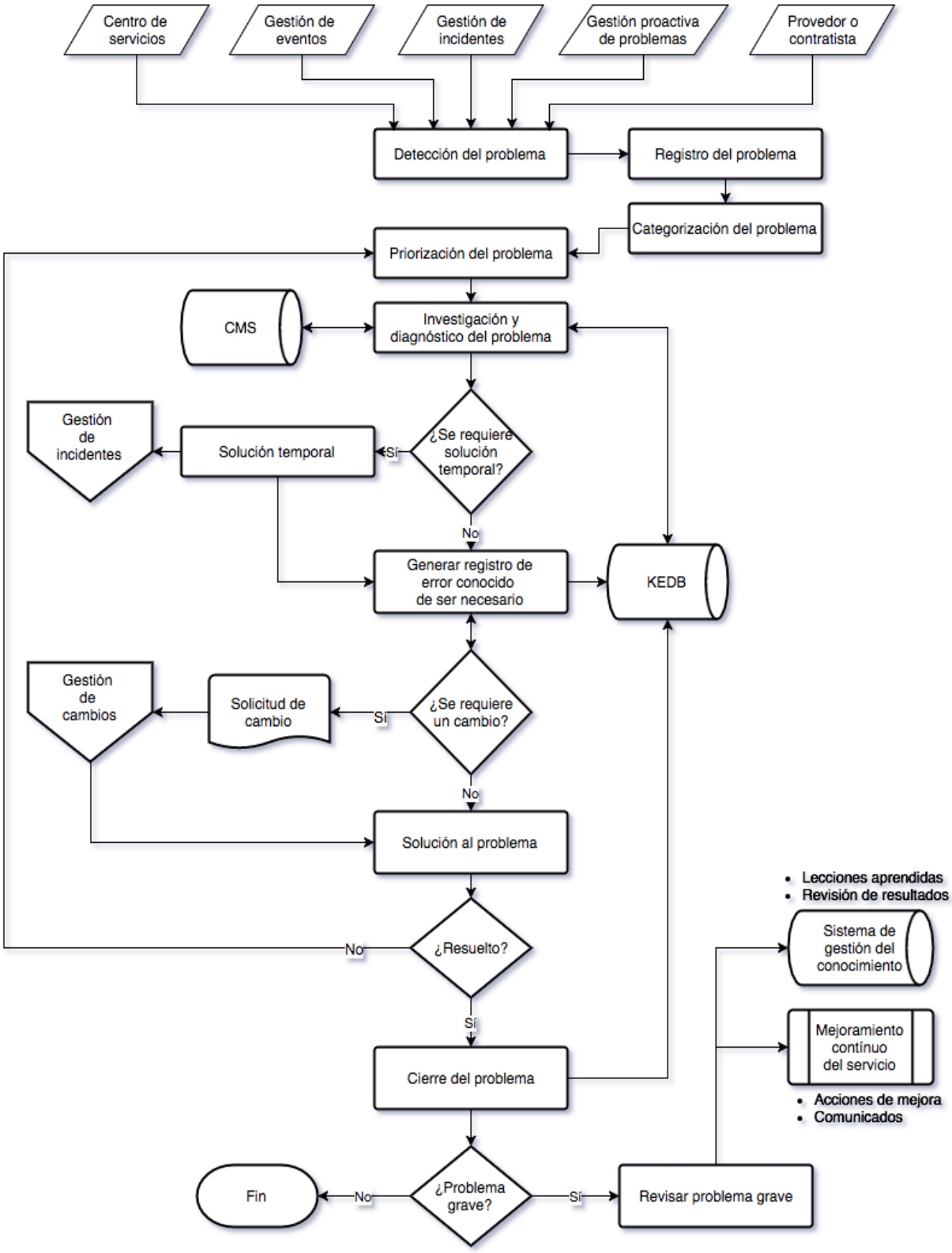


Figura 6. Proceso de gestión de problemas. Fuente: ITIL 2011 Service Operation

Una vez que la solución definitiva se haya implementado, el registro del problema se puede cerrar, al igual que todos aquellos incidentes asociados a éste. Es necesario verificar que el registro contiene toda la documentación del caso (historial de investigaciones, acciones correctivas, entre otros datos).

Por último, si se tuvo que lidiar con un problema grave es necesario hacer una revisión cuando todo lo que se hizo para resolver el problema aun esté fresco en la memoria, a modo de documentar las lecciones aprendidas. Esta revisión debe enfocarse en los siguientes aspectos:

- Las cosas que se hicieron bien
- Las cosas que no se hicieron bien
- Qué se puede hacer mejor en el futuro
- Cómo evitar que ocurra nuevamente
- Determinar si existe responsabilidad de terceras partes y se hay acciones de seguimiento que se requieren ejecutar

7. Disparadores, entradas y salidas

El proceso de gestión de incidentes suele ser iniciado por actividades reactivas producto de incidentes y por lo general por parte del centro de servicios. Puede iniciarse, también, a partir de las etapas de pruebas de productos o servicios, específicamente en la etapa de aceptación del cliente o usuario, o bien cuando se realizan actividades proactivas como análisis de tendencias o patrones en incidentes, o bitácoras de sistemas, entre otras.

Las entradas que puede tener este proceso pueden ser como las siguientes:

- Registros de incidentes que han generado la creación de un problema.
- Información acerca de CIs y su estado.
- Comunicados sobre incidentes y sus síntomas.
- Comunicados sobre solicitudes de cambios y nuevas versiones que se han implementado o están por ser implementadas.
- Objetivos de nivel operativo o de servicio.
- Criterios acordados para priprizar y escalar problemas.
- Resultados de las actividades de análisis de riesgo.

En cuanto a las salidas del proceso podemos encontrar las siguientes:

- Problemas resueltos y las actividades realizadas para implementar dicha solución.
- Los registros del problema debidamente actualizados con toda la información histórica de lo que se hizo.
- Registros de solicitudes de cambio para corregir las fallas en la infraestructura.
- Soluciones temporales a los incidentes.
- Registros de errores conocidos.
- Reportes de la gestión de problemas.
- Resultados de la revisión de problemas graves.

8. Gestión de la información

La mayor parte de la información utilizada en la gestión de problemas proviene de fuentes como: sistemas de gestión de la configuración y de las bases de datos de errores conocidos.

9. Factores críticos de éxito (Critical Success Factors, CSF) e indicadores clave de desempeño (Key Performance Indicators, KPI)

Cada organización se basará ensu nivel de madurez para definir los CSFs y KPIs que considere adecuados de acuerdo con los objetivos de la empresa. A continuación se muestran algunos ejemplos de CSFs y KPIs del proceso de gestión de problemas.

CSF	KPI
Minimizar el impacto en el negocio de incidentes que no se pueden prevenir	• Número de errores conocidos agregados a la KEDB • El porcentaje de exactitud de la KEDB (obtenido a través de auditorías) • Porcentaje de incidentes cerrados por el centro de servicios sin referencias a otros niveles de soporte • Promedio del tiempo requerido para resolver los incidentes asociados al problema
Mantener el nivel de calidad de los servicios de TI mediante la disminución de incidentes recurrentes	• Número total de problemas (medida de control) • Tamaño de la cola de problemas pendientes en cada servicio • Número de problemas repetidos en cada servicio
Realizar las actividades de gestión de problemas con calidad y profesionalismo para mantener la confianza del negocio en las capacidades de TI	• Número de problemas graves (abiertos, cerrados y pendientes) • Porcentaje de revisiones de problemas graves realizadas con éxito • Número y porcentaje de problemas asignados incorrectamente • Número de problemas que excedieron su plazo para ser resueltos • Costo promedio por problema

Ejemplos de CSFs y sus correspondientes KIPs. Fuente: ITIL 2011 Service Operation

10. Riesgos y retos

La gestión de problemas presenta retos tales como una importante dependencia de una efectiva gestión de incidentes y las herramientas utilizadas para ellos, de manera que los problemas se puedan identificar rápidamente y se pueda realizar una muy buena clasificación. Otro reto es contar con personal capacitado para resolver problemas, ya que usualmente el personal de soporte describe el origen de los poblemas tomando en cuenta solamente los síntomas o las acciones realizadas para resolverlos.

Relacionar los problemas con los incidentes puede ser difícil si no se utiliza el mismo sistema de información para darles seguimiento. Asegurar que el personal de soporte cuenta con el conocimiento técnico para hacer su trabajo y con el conocimiento del negocio que le permita

comprender la importancia de los servicios que soporta. Procurar una buena relación entre el personal de distintos niveles de soporte, para que la comunicación entre ellos sea eficaz mientras trabajan en conjunto para resolver problemas.

En lo que respecta a los riesgos, el proceso podría verse saturado de problemas que no se pueden atender debido a la falta de personal capacitado, o porque no se cuenta con las herramientas adecuadas para realizar las investigaciones, o bien porque los objetivos no están alineados con los de la empresa.

Gestión de acceso

La gestión de acceso se refiere al proceso mediante el cual se le permite a los usuarios debidamente autorizados el uso de un servicio, al mismo tiempo que se impide que usuarios no autorizados lo utilicen. En algunas empresas también se conoce a este proceso como administración de derechos o administración de la identidad.

1. Propósito

El propósito de la gestión de acceso consiste en proveer a los usuarios el derecho de utilizar un servicio o un grupo de servicios. Por tanto, se refiere a la ejecución de las políticas y acciones definidas por la gestión de la seguridad de la información.

2. Objetivos

Estos son los objetivos de la gestión de acceso:

- Gestionar el acceso a los servicios sobre la base de las políticas y acciones definidas en el proceso de gestión de la seguridad de la información.
- Responder oportuna y eficientemente ante solicitudes de acceso a servicios, cambios en los permisos de acceso o eliminación de permisos de acceso a servicios.
- Asegurar que no se dé un uso incorrecto o abusivo de los permisos de acceso.

3. Valor para la empresa

El valor que la gestión de acceso tiene para la empresa es que asegura la protección de la confidencialidad de la información mediante el control del acceso a los servicios de TI, asegura que el personal cuenta con los permisos adecuados para ejecutar sus funciones de manera efectiva, mitigar la introducción de datos erróneos en los sistemas de información por parte de usuarios inexpertos, ofrecer la capacidad de revocar un permiso de manera oportuna en caso de ser necesario por razones de seguridad, por ejemplo.

4. Políticas

Entre las políticas que cada organización define de acuerdo con sus objetivos de control de acceso a los servicios que soporta están los siguientes ejemplos:

- La administración de los accesos y las actividades relacionadas deben fundamentarse en las políticas y controles definidos en en proceso de gestión de la seguridad de la información.
- Se deben registrar y almacenar todas las acciones de acceso a los servicios de tal modo que se puedan realizar labores de análisis con el fin de determinar si se da un uso inapropiado o abusivo de los servicios.
- Los permisos de acceso a los servicios deben estar alineados con los cambios más recientes de roles o funciones del personal para evitar accesos indebidos a los servicios.

- Se debe mantener un historial de todos los accesos a los servicios, incluyendo quién accedió o intentó acceder y cuándo lo hizo. Esto con el fin de proveer información a los procesos de auditoría.
- Los procesos de manejo, escalaciones y comunicaciones de eventos relacionados con seguridad de la información deben estar claramente definidos y alineados con lo que establecen las políticas definidas por el proceso de gestión de la seguridad de la información.
- Debido a que lo usual es que los usuarios utilicen varios servicios similares o relacionados entre sí, es más eficiente definir grupos de servicios y aplicar los controles sobre estos en vez de hacerlo de manera individual sobre cada uno de los servicios.

5. Actividades, métodos y técnicas

En la figura 10 se muestra una representación del proceso de gestión de acceso, que si bien es cierto no es la única forma en que se puede gestionar el acceso a los servicios de TI, es una buena referencia que las organizaciones pueden utilizar para definir su propio proceso.

El acceso o restricción de acceso a un servicio puede solicitarse por medio de varios mecanismos entre los que están:

- Una solicitud generada por los sistemas de recursos humanos. Este escenario usualmente se da por contratación, ascenso o reubicación de personal.
- Una solicitud de cambio del proceso de gestión de cambios.
- Una solicitud enviada a través del servicio de resolución de solicitudes.
- La ejecución de una rutina automatizada que cuenta con autorización previa.

Una vez que se ha recibido la solicitud se verifica su validez, lo cual se hace desde dos perspectivas:

- Que el usuario que solicita el acceso es quien dice ser. Esto usualmente se logra mediante la validación de un nombre de usuario y una contraseña, aunque dependiendo del servicio al que se pretende acceder se pueden utilizar mecanismos adicionales como biometría, dispositivos de encripción, llaves electrónicas de acceso, entre otros.
- Que el usuario realmente necesita utilizar el servicio solicitado. En este caso la validación puede requerir fuentes adicionales como por ejemplo un comunicado de Recursos Humanos en el caso de empleado nuevo, una notificación de un gerente autorizando el acceso, por citar algunos ejemplos.

Cuando llega el momento de proveer el acceso lo que el proceso hace es aplicar las políticas definidas por gestión de la seguridad de la información, como ya se ha mencionado antes y no tomar decisiones en torno a si el usuario debe tener acceso al servicio o no. Por lo general una vez que se ha confirmado la validez de la solicitud se procede a trasladar la orden de otorgar el permiso al grupo de soporte encargado del servicio en cuestión.

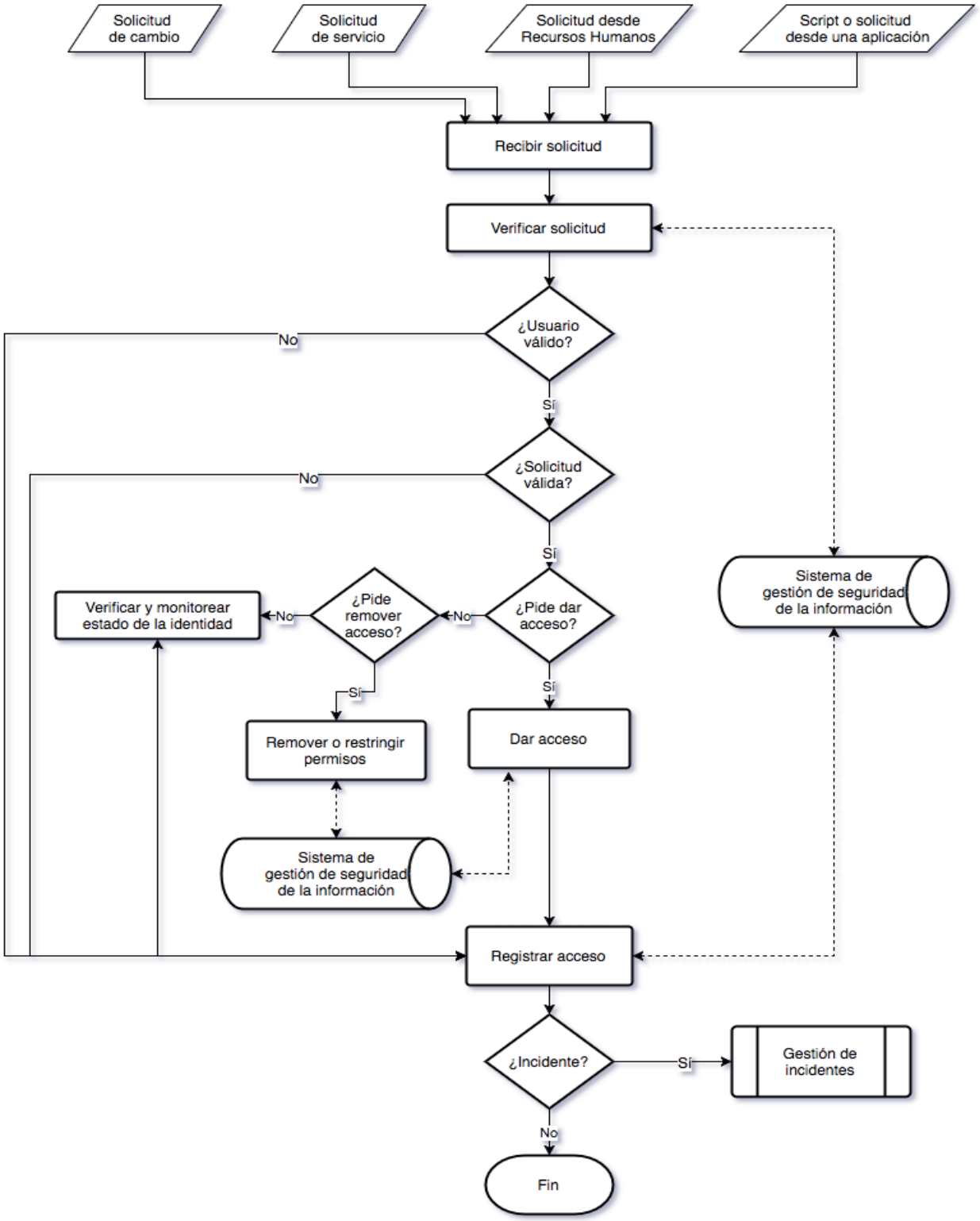


Figura 7. Proceso de gestión de acceso. Fuente: ITIL 2011 Service Operation

Es muy usual que los usuarios tengan cambios de roles dentro de las organizaciones y por ende cambien sus necesidades de acceso a servicios de TI. Ejemplos de esos cambios pueden ser múltiples, pero entre los más frecuentes están: cambio de funciones, ascensos, transferencias entre departamentos, renuncia o fallecimiento, retiro, sanción disciplinaria y despidos.

Los permisos de acceso se deben registrar y monitorear para garantizar que no se utilicen inapropiadamente. Esta información debe estar disponible en caso de que se presente la necesidad de realizar investigaciones por accesos indebidos o auditorías.

La gestión de acceso no solamente se encarga de otorgar permisos para acceder a los servicios, sino también de remover esos permisos cuando sea necesario. Al igual que ocurre cuando se debe brindar un acceso, la decisión no la toma este proceso sino que se basa y aplica las políticas que define el proceso de gestión de seguridad de la información y, del mismo modo, se usan criterios similares para determinar en qué momento debe hacerse (despido, traslado, fallecimiento, retiro).

6. Disparadores, entradas y salidas

El proceso de gestión de acceso se puede iniciar a partir de una solicitud para que un usuario o grupo de usuarios accedan a uno o más servicios. Esa petición puede venir de una solicitud de cambio, una solicitud de un servicio, una solicitud de Recursos Humanos, una solicitud de un gerente, entre otras.

Las entradas que puede tener este proceso dentro de la operación del servicio están:

- Políticas de seguridad de la información.
- Requerimientos operacionales o de nivel de servicio para otorgar acceso a servicios, para realizar actividades relacionadas con la gestión del acceso o para responder ante eventos de la gestión de acceso.
- Solicitudes de cambio autorizadas para realizar modificaciones a los permisos.
- Otras solicitudes autorizadas para dar o remover permisos.

Como salidas del proceso de gestión de acceso tenemos los siguientes ejemplos:

- El otorgamiento de los permisos solicitados en conformidad con las políticas de seguridad de la información correspondientes.
- Registros de permisos otorgados e historial completo.
- Registro de permisos y el historial de estos se han negado y los motivos por los cuales se negaron.
- Notificaciones oportunas de uso abusivo o inapropiado de permisos.

7. Gestión de la información

La identidad de los usuarios es un elemento fundamental en la gestión de acceso a servicios de TI. Por tanto es importante identificar de forma única a cada individuo, para lo cual se recurre al uso de múltiples piezas de información para generar la identidad, tales como el nombre, la

dirección, el departamento donde trabaja, características biométricas, fecha de vencimiento del contrato de servicios, entre otros.

Es usual que se definan perfiles de usuarios y grupos de servicios que se asocian para facilitar la gestión del acceso, de modo tal que los permisos no se otorgan a individuos y servicios directamente, sino que se hace a través de perfiles de usuario y grupos de servicios. Esta es una buena práctica que se recomienda a las organizaciones poner en práctica.

8. Factores críticos de éxito (Critical Success Factors, CSF) e indicadores clave de desempeño (Key Performance Indicators, KPI)

Al igual que en los procesos descritos anteriormente, cada organización deberá definir sus propios CSFs y KPIs tomando en cuenta su nivel de madurez en la gestión del acceso a los servicios de TI. Sin embargo, a continuación se mencionan varios ejemplos que pueden servir de guía.

CSF	KPI
Asegurar que la confidencialidad, integridad y disponibilidad de los servicios se protege en concordancia con las políticas de seguridad	• Porcentaje de incidentes relacionados con accesos indebidos o intentos de acceso • Número de descubrimientos hechos por auditorías de configuraciones incorrectas de permisos debido a cambios de rol o término de relación laboral • Número de incidentes que requieren un restablecimiento de los permisos de acceso • Número de incidentes provocados por configuraciones incorrectas de permisos
Proveer acceso a servicios de manera oportuna y según las necesidades de la empresa	• Porcentaje de solicitudes de acceso que fueron procesadas dentro de los plazos establecidos en los acuerdos de nivel de servicio
Comunicar oportunamente cualquier uso abusivo o inapropiado de un servicio	• Duración promedio de incidentes relacionados con accesos indebidos a servicios

Ejemplos de CSFs y sus correspondientes KIPs. Fuente: ITIL 2011 Service Operation

9. Riesgos y retos

Entre los retos que la gestión de acceso puede enfrentar están: monitorear y reportar la actividad de acceso a servicios de TI, así como los incidentes relacionados con este campo. Verificar la identidad de los usuarios. También, verificar la validez del requerimiento de acceso a un servicio por parte de un usuario o grupo de usuarios, vincular múltiples permisos de acceso a usuarios individuales, determinar el estado actual de un usuario (activo, miembro de un departamento, ascendido, entre otros), restringir el acceso a usuarios no autorizados, crear y mantener una base de datos con todos los usuarios y los permisos de cada uno de ellos.

Por su parte los riesgos que se pueden presentar tienen que ver con la carencia de herramientas tecnológicas que apoyen las actividades de gestión de permisos, controlar el acceso a través de

puertas traseras como interfaces entre aplicaciones y cambios en las reglas definidas en los cortafuegos (firewalls) para satisfacer necesidades especiales, controlar el acceso a servicios por parte de terceros como un proveedor, asegurar que existen los niveles de acceso necesarios para permitir que todos los usuarios puedan hacer uso de los servicios según sus requerimientos, entre otros.

Actividades comunes en la operación del servicio

En la operación del servicio se realizan una serie de actividades que tienden a ser comunes en todos los departamentos de TI en las empresas y que están muy vinculadas con el uso y gestión de herramientas tecnológicas y cuyo empleo debe estar alineado con los objetivos estratégicos del negocio. Sin embargo, el grado de madurez que tienen las empresas no siempre les permite enfocar el uso de tecnologías en el mejoramiento de los servicios, en muchos casos cuando la empresa está en los primeros niveles de madurez el enfoque se mantiene en los beneficios que la tecnología por sí sola pueda aportar.

La figura 11 muestra una visión general de la relación entre el nivel de madurez de las empresas y el enfoque existente en ellas sobre el uso de las tecnologías. En ella se puede ver que, conforme se avanza en la escala de nivel de madurez, más alineado está el uso de las tecnologías con los objetivos de la empresa y el mejoramiento de los servicios que soportan esos objetivos.

Aunque en ocasiones se quiera separar la gestión de los servicios de la gestión de la tecnología resulta imposible porque no se puede conseguir proveer servicios de alta calidad si no se mantienen alineados todos los niveles de tecnología con los servicios mismos. La gestión de servicios involucra a personas, procesos y tecnología.

A continuación se describen brevemente las actividades que con mayor frecuencia se observan en la operación del servicio. Una descripción más amplia de cada una de ellas se puede encontrar en el libro “ITIL 2011 Service Operation” de Best Management Practice, incluido en las referencias bibliográficas de este documento.

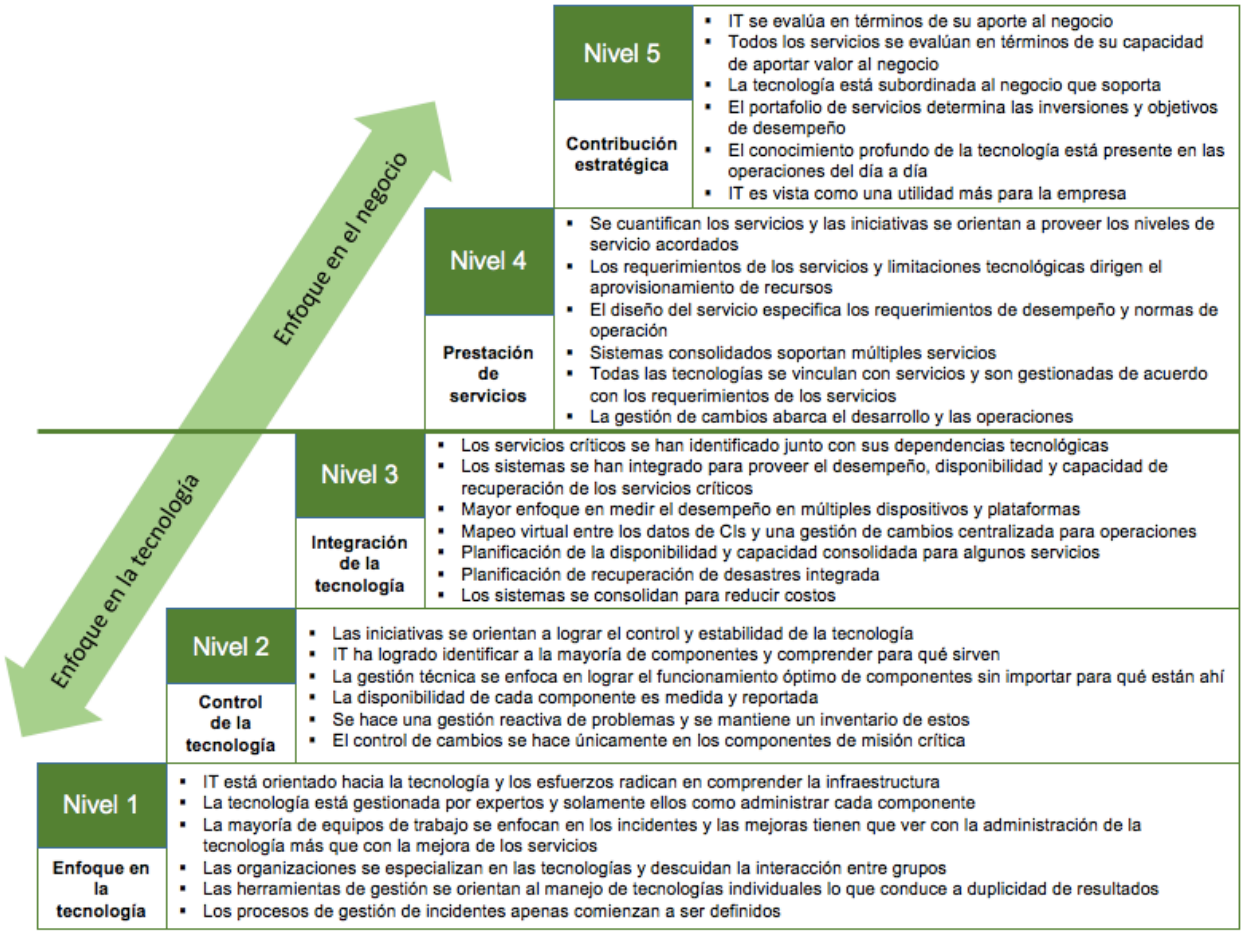


Figura 8. Evolución del nivel de madurez en la gestión de la tecnología. Fuente: ITIL 2011 Service Operation

Monitoreo y control

La medición y el control de los servicios se basa en el monitoreo, los reportes y las acciones subsecuentes. En este ciclo es fundamental para la prestación, soporte y mejoramiento de los servicios de TI.

El monitoreo se refiere a la actividad de observar una situación para detectar cambios que se dan en el tiempo. En el contexto de la operación del servicio esto implica el uso de herramientas para monitorear el estado de los distintos elementos de tecnología utilizados para la prestación de los servicios, garantizar que aprovechamiento de las recursos de acuerdo con los niveles acordados, detectar situaciones fuera de lo normal en la infraestructura o cambios no autorizados, por ejemplo.

Los reportes se refieren a la capacidad de analizar, producir y distribuir los resultados de las actividades de monitoreo para que la persona o grupo responsable pueda tomar las decisiones y ejecutar las acciones que les competen.

El control se refiere al proceso de administrar la utilización o comportamiento de un dispositivo, un sistema o un servicio. En el contexto de la operación del servicio implica que se usen herramientas para definir las condiciones que se consideren como operaciones normales y cuáles no, así como regular el desempeño de dispositivos, sistemas y servicios.

Operaciones de IT

Como parte de la operación del servicio hay actividades que resultan necesarias para soportar el buen funcionamiento de los servicios prestados, actividades tales como el uso de tareas programadas que se encargan de ejecutar labores de mantenimiento de dispositivos, procesamiento de datos, auditorías, análisis proactivos de detección de incidentes o amenazas de seguridad, entre otras.

Otra de las actividades de gran importancia es el respaldo y recuperación de datos, las cuales deben realizarse siguiendo una estrategia, no solamente para el respaldo sino también para la recuperación de los datos. Es indispensable considerar factores como ubicación física de las fuentes de datos, de los dispositivos, de los usuarios de los sistemas que consumen los datos, la legislación del lugar donde se realiza el respaldo o la restauración, entre muchos otros.

Otra actividad de gran importancia es la administración de impresiones y resultados. Aunque en la actualidad la mayoría de los resultados producto del procesamiento de datos se transmite y utiliza en medios digitales, es frecuente la necesidad de ofrecer servicios de impresión física de resultados. Para ello deben tomarse en cuenta factores como ubicación de los centros de impresión, autorizaciones, deshecho de material impreso, entre otros.

Administración de servidores

En prácticamente todas las empresas el uso de servidores, ya sean físicos o virtuales es amplio y muy frecuente, por lo que resulta necesario contar con procedimientos y procesos para realizar una adecuada gestión de este recurso en aspectos como el mantenimiento del sistema operativo, componentes físicos, ubicación física en la empresa, acceso físico y remoto, entre otros.

En la actualidad es muy frecuente el consumo de servicios de infraestructura como un servicio o IaaS (Infrastructure as a Service), por lo tanto, es también importante contar con procesos y procedimientos para la administración de este tipo de tecnología, ya que no siempre se va a tener que administrar el servidor como tradicionalmente se conoce, sino solamente un servicio o la configuración de este, a través de un proveedor.

Administración de red

Debido a que la gran mayoría de servicios de TI dependen de la capacidad de estar conectados, ya sea a otros servicios o a dispositivos, resulta esencial contar con una buena gestión de red que servirá no solamente para consumir a los servicios, sino para que el personal de soporte de operaciones pueda acceder y administrar los distintos componentes de los servicios.

Las responsabilidades que implica la administración de red tienen que ver con todo aquello necesario para garantizar el adecuado funcionamiento de las redes locales, metropolitanas y de área ancha con que cuente la empresa. Esto quiere decir que, entre otras cosas, deberá

encargarse de diseñar las redes, administrar los componentes físicos y virtuales de las redes, coordinar los servicios de soporte de proveedores, monitorear el tráfico de red, administrar los mecanismos de seguridad como cortafuegos, por ejemplo.

Almacenamiento de información

Es posible que se requiera de un grupo dedicado de manera exclusiva a la administración del almacenamiento de datos que estaría a cargo de los componentes de hardware utilizados, las políticas y procedimientos para el almacenamiento de datos, que deberán apegarse a la legislación del lugar donde opere la empresa, definir el tipo de infraestructura de almacenamiento a utilizar, logística para almacenar los datos, entre otros.

Administración de bases de datos

La administración es otra de las actividades que podría requerir de la creación de un grupo dedicado. Sin embargo, va a depender de los requerimientos propios del negocio si se implementa de esta manera, o se establecer procedimientos de administración de bases de datos en cada uno de los equipos que administran y soportan las aplicaciones.

Entre las responsabilidades de esta actividad están la creación y mantenimiento de bases de datos, gestión de la disponibilidad y desempeño de las bases de datos, administración de todos los componentes de las bases de datos, monitoreo de la utilización, entre otros.

Administración de los servicios de directorio

Un servicio de directorio es un software especializado que administra la información acerca de los recursos disponibles en la red y quiénes tienen acceso a ellos. Algunas de las actividades que se realizan son las que tienen que ver con la ubicación de los recursos en la red, gestionar los permisos de los usuarios o grupos de usuarios sobre los recursos en la red, definir convenciones de nombres para los recursos, asegurar la consistencia de los nombres y el acceso de los recursos en las distintas redes de la empresa, vincular los recursos con organizaciones dentro de la empresa para facilitar el control del acceso a los recursos, entre otros.

Soporte de equipo móvil y de escritorio

En vista de que actualmente se utilizan múltiples dispositivos para acceder a los servicios de TI tales como computadoras de escritorio y portátiles, teléfonos celulares, tabletas, dispositivos de IoT (Internet of Things o Internet de las Cosas), es de suma importancia brindar soporte a todos esos dispositivos para garantizarle a los usuarios que siempre podrán acceder a los servicios de TI que se brindan.

Administración de los componentes de capa media

Los componentes de capa media son componentes de software que permiten la integración de sistemas o aplicaciones distribuidas, permite la transferencia eficiente de datos entre esas aplicaciones y sistemas, que a su vez son elementos fundamentales sobre los cuales dependen muchos de los servicios de TI que se ofrecen. Estos componentes se vuelven cada vez más importantes dentro de las empresas en la medida que aumenta el uso de arquitecturas de aplicaciones basadas en servicios.

Administración de los servicios de internet/web

Muchas empresas conducen sus negocios a través de internet por lo que son altamente dependientes de la disponibilidad y desempeño de sus sitios web. En esos casos es recomendable que exista un grupo dedicado exclusivamente al soporte de esos componentes de infraestructura y que se encargaría entre otras actividades de administrar cortafuegos y otros mecanismos de seguridad, definir la arquitectura para servicios basados en la web, manejo de incidentes relacionados con los sitios web, gestionar el soporte brindado por proveedores, monitorear el desempeño de los sitios web, entre otros.

Administración de centros de datos

Esta actividad se refiere a la administración de los edificios donde operan los centros de datos y centros de cómputo. Implica entre muchas otras cosas velar por el mantenimiento del estado físico de los centros de datos, gestionar el acceso de personas y equipo, monitorear y administrar el consumo de energía, administrar las condiciones de temperatura, ventilación, capacidad, por ejemplo.

Mejoramiento de las actividades operacionales

Todo personal de operaciones debe estar constantemente buscando nuevas formas de mejorar los procesos para aumentar la calidad de los servicios de TI, a la vez que se reducen los costos de operación. Entre las actividades que ofrecen oportunidades de mejora están la automatización de tareas manuales, la revisión de procedimientos improvisados que inicialmente se introdujeron para resolver situaciones en el corto plazo, pero que presentan el riesgo potencial de convertirse en la norma, auditorías operacionales, la comunicación clara entre grupos de soporte, capacitación del personal, por ejemplo.

Organización de la operación del servicio

A continuación se describen los conceptos generales de cómo se organiza la administración de los servicios de TI en relación con la operación del servicio. No existe una forma única de organización y le corresponde al Departamento de TI de cada empresa definir la forma en que organiza la operación del servicio siguiendo las recomendaciones del marco de referencia y considerando aspectos como el tamaño y requerimientos de la empresa, así como las limitaciones de recursos.

Para que la operación del servicio sea exitosa, se tendrán que definir con claridad los roles y responsabilidades para ejecutar los procesos y actividades descritas anteriormente. Estos roles deben ser asignados a individuos y a una apropiada estructura organizacional de equipos, grupos o funciones.

Funciones

A continuación se describen brevemente las cuatro funciones más importantes, a saber: centro de servicios, administración técnica, operaciones de TI y administración de aplicaciones.

Centro de servicios

El centro de servicios es el punto de contacto para que los usuarios puedan acceder a los servicios de soporte en caso de una interrupción de un servicio, de necesitar pedir un servicio o, incluso, para algunos casos de solicitudes de cambios. Provee un punto de contacto comunicación para los usuarios y un punto de coordinación para los grupos de soporte de TI y

para que funcione de manera efectiva es usual que se separa de las otras funciones de la operación del servicio.

Administración técnica

Esta función provee las destrezas técnicas y los recursos específicos para brindar soporte a la operación de los servicios de TI y a la administración de la infraestructura. También, juega un papel importante en el diseño, las pruebas, la implementación de nuevos servicios, así como de la mejora de los existentes.

En empresas pequeñas es posible que esta función esté asignada a un único departamento, sin embargo en empresas de gran tamaño lo usual es que la función esté distribuida en múltiples departamentos técnicos especializados.

Administración de las operaciones de TI

Esta función se encarga de las actividades operacionales diarias que se requieren para gestionar los servicios de TI y el soporte de la infraestructura de TI. En algunas empresas esta función la desempeña un único departamento, pero en otras las actividades y el personal está distribuido en departamentos distintos y especializados.

Administración de aplicaciones

La responsabilidad de esta función es gestionar las aplicaciones a través de su ciclo de vida. También juega un papel importante en el diseño, las pruebas y el mejoramiento de las aplicaciones que forman parte de los servicios de TI. Usualmente se distribuye en distintos departamentos de acuerdo con el portafolio de aplicaciones, de tal manera que haya grupos especializados para atender las necesidades particulares de las aplicaciones.

Roles

Una serie de roles deben ser ejecutados para soportar la operación del servicio. En esta sección se mencionan algunos que sirven como ejemplo, sin embargo cada empresa deberá definir los que más se ajustan a sus requerimientos y objetivos estratégicos.

Distribución de roles	Nombre del rol	Responsabilidades
Generales	Dueño del servicio	• Asegurar que la prestación y soporte del servicio satisfaga los requerimientos acordados • Comprender las necesidades del negocio y traducirlas servicios que las satisfagan • Asegurar una comunicación clara con el cliente sobre inquietudes e inconvenientes que se den • Identificar junto con el cliente oportunidades de mejorar los servicios • Representar el servicio en toda la empresa • Participar en la definición de los acuerdos de nivel y operación del servicio
	Dueño del proceso	• Apoyar, diseñar y gestionar los cambios del proceso y sus métricas • Definir la estrategia del proceso

		• Asegurar que la documentación del proceso esté correcta y actualizada • Definir políticas y estándares para el proceso • Proveer los recursos que el proceso requiere para ejecutar sus actividades • Asegurar que el personal técnico cuenta con el conocimiento técnico y del negocio requerido • Revisar oportunidades de mejorar la productividad y eficiencia del proceso
	Gerente de proceso	• Trabajar con el dueño del proceso en la planeación y coordinación de las actividades • Asegurar que las actividades se ejecutan según lo esperado a través del ciclo de vida del servicio • Asignar el personal en los roles apropiados • Administrar los recursos del proceso • Monitorear el desempeño del proceso • Identificar oportunidades de mejora
	Ejecutor de proceso	• Ejecutar una o más actividades del proceso • Comprender cómo su rol contribuye a generar valor para el negocio a través del servicio que soporta • Trabajar en equipo con gerentes, compañeros, usuarios y clientes • Asegurar que las entradas, salidas e interfaces de sus actividades son correctas • Crear y actualizar registro de la ejecución de actividades
Gestión de incidentes	Dueño del proceso	• Mismas responsabilidades del dueño del servicio, pero para la gestión de incidentes • Diseñar modelos y flujos de trabajo • Trabajar en equipo con los otros dueños de proceso bajo un enfoque integrado en la gestión de servicios de TI
	Gerente del proceso	• Mismas responsabilidades del gerente de proceso, pero para la gestión de incidentes • Planear y gestionar el soporte de las herramientas y procesos • Coordinar la interacción con otros procesos de la gestión de servicios de TI • Procurar la eficiencia y efectividad del proceso • Generar información para la toma de decisiones • Monitorear la efectividad del proceso • Desarrollar y mantener los sistemas utilizados • Gestionar los incidentes graves • Identificar oportunidades de mejora
	Analista de primer nivel	• Registrar incidentes • Dirigir incidentes a los grupos de soporte apropiados cuando sea necesario • Colaborar en la priorización, clasificación y análisis iniciar de incidentes • Supervisar, monitorear e informar sobre el estado de incidentes

		• Monitorear el estado y avance de la resolución de incidentes • Mantener al usuario y centro de servicios informados sobre el estado del incidente
	Analista de segundo nivel	• Similares a las del analista de primer nivel, pero con un poco más de conocimiento técnico • Enfocarse más en el análisis del incidente y menos en la atención de usuarios
	Analista de tercer nivel	• Grupos de soporte especializados en: redes, servicios de voz, servidores, estaciones de trabajo, aplicaciones, bases de datos, mantenimiento de hardware, etc.
Gestión de problemas	Dueño del proceso	• Mismas responsabilidades del dueño de proceso de gestión de incidentes, pero para la gestión de problemas
	Gerente del proceso	• Mismas responsabilidades del gerente de proceso, pero para la gestión de problemas • Planear y gestionar el soporte de las herramientas y procesos • Coordinar la interacción con otros procesos de la gestión de servicios de TI • Servir de enlace entre los grupos de soporte para resolver los problemas según los acuerdos de nivel de servicio • Mantenimiento de la base de datos de errores conocidos (KEDB) • Cierre formal de los problemas • Servir de enlace con terceras partes • Coordinar, ejecutar y documentar las actividades de seguimiento a problemas graves
	Analista de problemas	• Revisar los datos de análisis de incidentes • Priorizar y clasificar correctamente los problemas • Investigar los problemas asignados hasta encontrar su causa raíz • Trabajar en equipo • Generar solicitudes de cambios que resuelven problemas • Monitorear el progreso de soluciones a errores conocidos • Actualizar la KEDB • Colaborar en el manejo de errores graves para encontrar su causa raíz
Resolución de solicitudes	Dueño del proceso	• Mismas responsabilidades del gerente de proceso, pero para la resolución de solicitudes • Diseñar modelos y flujos de trabajo • Trabajar en equipo con los otros dueños de proceso bajo un efoque integrado en la gestión de servicios de TI
	Gerente del proceso	• Mismas responsabilidades del gerente de proceso, pero para la resolución de solicitudes

		• Planear y gestionar el soporte de las herramientas y procesos • Coordinar la interacción con otros procesos de la gestión de servicios de TI • Manejar el personal, inquietudes, solicitudes y preocupaciones o problemas de usuarios y la administración de la empresa • Asegurar que las actividades del proceso se ejecuten en concordancia con los objetivos del nivel de servicio • Obtener retroalimentación de usuarios sobre calidad del servicio • Detectar necesidades de recursos para satisfacer la demanda del servicio • Revisar la asignación de prioridades y autorización de solicitudes para asegurar que sean correctas
	Analista	• Ser punto de contacto y garante de que las solicitudes se procesan • Hacer análisis inicial de las solicitudes para identificar recursos requeridos para procesarla • Establecer la comunicación con otros recursos de TI que se van a involucrar • Realizar las escalaciones requeridas • Asegurar que las solicitudes se registran apropiadamente
Gestión de eventos	Dueño del proceso	• Mismas responsabilidades del dueño de proceso, pero para la gestión de eventos • Diseñar modelos y flujos de trabajo • Trabajar en equipo con los otros dueños de proceso bajo un enfoque integrado en la gestión de servicios de TI
	Gerente del proceso	• Mismas responsabilidades del gerente de proceso, pero para la gestión de eventos • Planear y gestionar el soporte de las herramientas y procesos • Coordinar la interacción con otros procesos de la gestión de servicios de TI
	Otros roles	• El personal del centro de servicios puede tener alguna participación cuando se requiere comunicación con el usuario • El personal técnico de administración de aplicaciones generalmente realiza la gestión de eventos en la operación del servicio. También participa en el manejo de incidentes y problemas relacionados con eventos
Gestión de acceso	Dueño del proceso	• Mismas responsabilidades del gerente de proceso, pero para la gestión de acceso • Diseñar modelos y flujos de trabajo • Trabajar en equipo con los otros dueños de proceso bajo un enfoque integrado en la gestión de servicios de TI
	Gerente del proceso	• Mismas responsabilidades del gerente de proceso, pero para la gestión de acceso

		• Planear y gestionar el soporte de las herramientas y procesos • Coordinar la interacción con otros procesos de la gestión de servicios de TI
	Otros roles	• El centro de servicios puede servir como medio para ingresar solicitudes de acceso. También para manejar la comunicación con los usuarios • El personal técnico de administración de aplicaciones generalmente se encarga de la gestión de acceso en la operación del servicio de los sistemas bajo su control. • Colaboran con el manejo de incidentes y problemas.
Centro de servicios	Gerente del proceso	• Designar personal para cada rol • Manejar el personal • Gestionar las actividades • Ser un punto de escalación para el supervisor del centro de servicios • Servicio al cliente en un sentido amplio • Informar a los altos mandos sobre incidentes o problemas que pueden impactar negativamente el negocio • Monitorear el desempeño del centro de servicios • Identificar oportunidades de mejora
	Supervisor	• Asegurar que exista personal calificado en todo momento, para lo cual puede distribuirlo en turnos • Colaborar en la gestión del recurso humano si se requiere • Ser un punto de escalación si se presentan situaciones difíciles con los usuarios • Representar al centro de servicios en reuniones • Coordinar la capacitación del personal • Servir de enlace con la alta administración de la empresa • Servir de enlace con la gestión de cambios • Colaborar con los analistas cuando hay sobrecarga de trabajo
	Analista	• Brindar primer nivel de soporte, atender a los usuarios de los servicios, manejar los incidentes o solicitudes a través del sistema de gestión de servicios de TI
	Súper usuario	• Facilitar la comunicación entre IT y el resto de la empresa a nivel operativo • Reforzar el enfoque del usuario sobre los niveles de servicio acordados • Brindar capacitación • Brindar apoyo en manejo de incidentes menores o solicitudes sencillas • Escalar incidentes y solicitudes de usuario si no las pueden resolver directamente • Asistir al centro de servicios en general
Administración técnica	Gerente técnico/líder de equipo	• Asumir labores de liderazgo, toma de decisiones y control para el departamento • Aportar conocimiento técnico y liderazgo en las áreas en que se trabaja el departamento

		• Asegurar que en el equipo mantiene el nivel de conocimiento y experiencia requeridos • Informar a la alta gerencia sobre cualquier problema técnico relevante a su departamento • Manejar al personal del departamento
	Analista técnico/arquitecto	• Trabajar con usuarios y demás partes interesadas en la determinación de sus necesidades • Determinar los requerimientos de sistemas que se pueden satisfacer de acuerdo con las limitaciones financieras y tecnológicas • Definir y mantener el conocimiento sobre la integración de los sistemas y sus dependencias • Realizar análisis de costo-beneficio para determinar los medios más adecuados para satisfacer los requerimientos establecidos • Desarrollar modelos operacionales que aseguren un buen desempeño y uso óptimo de recursos • Asegurar una adecuada configuración de la tecnología de acuerdo con la arquitectura de la empresa, las herramientas y habilidades del personal disponibles • Asegurar un desempeño consistente y confiable de la infraestructura para prestar servicios que aporten valor al negocio
	Operador técnico	• Mismas responsabilidades del operador en la administración de operaciones de TI
Administración de operaciones de TI	Gerente de operaciones	• Asumir labores de liderazgo, toma de decisiones y control para el departamento • Informar a la alta gerencia sobre cualquier problema técnico relevante a su departamento • Manejar al personal del departamento
	Jefe de turno	• Asumir labores de liderazgo, toma de decisiones y control durante su turno • Asegurar que actividades operacionales se realicen satisfactoriamente de acuerdo con las políticas y procedimientos de la empresa • Servir de enlace con otros jefes de turno para garantizar que se dé continuidad al trabajo al pasar de un turno a otro • Manejar a los analistas de su turno • Velar por la salud y seguridad del personal en su turno
	Analista	• Personal técnico de operaciones experimentado que determina las maneras más eficientes de ejecutar las actividades de operaciones
	Operador	• Ejecutar las actividades del día a día: hacer respaldos de información, monitoreo del estado de los sistemas, administrar dispositivos de impresión, mantenimiento de bases de datos y servidores, instalación de equipos, etc.

Administración de aplicaciones	Gerente de aplicaciones/líder de equipo	• Asumir labores de liderazgo, toma de decisiones y control durante su turno • Aportar conocimiento técnico y liderazgo en las áreas en que se trabaja el departamento • Mantener comunicación con usuarios y clientes acerca del desempeño de las aplicaciones y requerimientos del negocio • Asegurar que en el equipo mantiene el nivel de conocimiento y experiencia requeridos • Informar a la alta gerencia sobre cualquier problema técnico relevante a su departamento • Manejar al personal del departamento
	Analista de aplicaciones /arquitecto	• Trabajar con usuarios y demás partes interesadas en la determinación de sus necesidades • Determinar los requerimientos de sistemas que se pueden satisfacer de acuerdo con las limitaciones financieras y tecnológicas • Realizar análisis de costo-beneficio para determinar los medios más adecuados para satisfacer los requerimientos establecidos • Desarrollar modelos operacionales que aseguren un buen desempeño y uso óptimo de recursos • Velar por que las aplicaciones se diseñen para ser administradas de acuerdo con la arquitectura, herramientas y destrezas disponibles en la empresa

Roles y responsabilidades en la operación del servicio. Fuente: ITIL 2011 Service Operation

Consideraciones tecnológicas

En el soporte de la operación del servicio existen requerimientos tecnológicos generales y en particulares a cada uno de los procesos y funciones. Entre los requerimientos generales se pueden mencionar los siguientes:

- Opciones de autoayuda para que los usuarios puedan satisfacer algunas de sus necesidades de soporte y plantear solicitudes de servicios.
- Herramienta de flujo de trabajo que permita gestionar el ciclo de vida de incidentes, problemas, solicitudes, eventos, etc.
- Un sistema integrado para la administración de la configuración.
- Tecnología de descubrimiento de componentes conectados a la red, de distribución automática de software y control de licencias.
- Herramientas para control remoto de dispositivos tales como computadoras de usuarios y servidores.
- Utilidades de diagnóstico de incidentes.
- Herramientas para generar reportes que apoyen los procesos de análisis y diagnóstico de incidentes, problemas, etc.
- Cuadro de mando integral que facilite la visibilidad de los niveles de desempeño y disponibilidad de los servicios.
- Herramientas de integración con el negocio.

- Tecnologías de software como un servicio o SaaS (Software as a Service).

En la gestión de incidentes se requieren tecnologías y herramientas como las siguientes:

- Un sistema integrado de gestión de servicios de TI.
- Herramientas de control del flujo de trabajo y escalación automática.

En el proceso de resolución de solicitudes:

- Un sistema integrado de gestión de servicios de TI.

En la gestión de problemas herramientas de este tipo serán de gran utilidad:

- Un sistema integrado de gestión de servicios de TI.
- Integración con el proceso de gestión de cambios.
- Sistema integrado para la administración de la configuración.
- Una base de datos de errores conocidos.

En la gestión de acceso:

- Herramientas para la gestión de recursos humanos.
- Tecnologías de servicios de directorio.
- Capacidades para la gestión del acceso en aplicaciones, sistemas operativos, componentes de capa media, etc.
- Sistemas para la gestión de cambios.

En el centro de servicios:

- Herramientas de telefonía
- Herramientas de soporte
    - Base de datos de errores conocidos
    - Rutinas automatizadas de diagnóstico
    - Interfaz web de autoayuda para el usuario
    - Control remoto de dispositivos
- Plan de continuidad de servicios para las herramientas de soporte de la gestión de servicios de TI.

Retos, riesgos y factores críticos de éxito

Existen una serie de retos en la operación del servicio que deben ser enfrentados y manejados apropiadamente. Entre esos retos se pueden mencionar los siguientes:

- Falta de unión y coordinación entre el personal de desarrollo y el de operaciones.
- Encontrar justificación para las necesidades de inversión y gasto.
- Mantener al mismo tiempo el enfoque en el soporte de todos los servicios prestados.
- Gestionar las múltiples formas de medir los diferentes datos relevantes de cada uno de los tipos de componentes que soportan los servicios.
- El manejo de equipos de trabajo virtuales.

Por otra parte, también hay factores críticos de éxito que son de gran importancia y que deben lograse para poder alcanzar una operación del servicio que tenga los resultados que la empresa necesita.

- Apoyo de la alta gerencia
- Apoyo de las unidades de negocio
- Líderes comprometidos con el éxito del proceso que sirvan de modelo para que los demás miembros de la organización los sigan.
- Contar con la cantidad de recurso humano suficiente y con las capacidades necesarias.
- Capacitación en la gestión de servicios de TI.
- Contar con las herramientas adecuadas para la gestión de servicios de TI.
- Validez de los mecanismos y procesos de pruebas que aseguren la incorporación de nuevos servicios que funcionen correctamente.
- Contar con las métricas adecuadas y las capacidades de consulta y despliegue de información que faciliten la supervisión y el monitoreo de la calidad de los servicios prestados.

Por último, tenemos los riesgos que se pueden presentar.

- Interrupción de un servicio crítico, lo que implica un fuerte impacto negativo en la empresa.
- Recursos financieros insuficientes.
- Pérdida de personal clave en el soporte de servicios.
- Resistencia al cambio por parte del personal.
- Falta de apoyo por parte de la alta gerencia.
- Diseño defectuoso de un servicio.
- Diferencias en la percepción de calidad de servicio por parte de los clientes o usuarios.

6.2. Anexo II – Lista de verificación para la operación del servicio de ITIL 2011

	Data entry	
	Below are the only valid entries for the assessment	
	Each person must use the drop-down box and select an answer for each question for each process area.	
1	Initial - processes and activities are adhoc or chaotic or undefined	
2	Repeatable - basic processes and activities are established and there is a level of discipline and adherence	
3	Defined - All processes and activities are defined, documented, standardised and integrated together	
4	Managed - Processes are measured by collecting detailed data on the processes and their quality and appropriately improved	
5	Optimising - Continuous process improvement is adopted. Process and activities are mature	
	Step 1 - Enter the names of the participants here:	
	Participant 1	
	Participant 2	
	Participant 3	
	Participant 4	
	Participant 5	
	Participant 6	
	Participant 7	
	Participant 8	
	Participant 9	
	Participant 10	
	Step 2 - Now have each participant answer each question for each Service Operation area, under their name.	
1	**Service Management as a Practice**	Participant 1
1	Service Management is clearly defined	Not applicable
2	We know what our services are	Not applicable
3	We have clearly defined functions and processes across the lifecycle	Not applicable
4	We are able to measure the processes in a relevant matter	Not applicable
5	The reason a process exists is to deliver a specific result	Not applicable
6	Every process delivers its primary result to a customer or stakeholder	Not applicable
7	The goals of Service Operation are defined	Not applicable
8	The objectives of Service Operation are defined	Not applicable
9	The purpose of Service Operation is Defined	Not applicable
10	The Scope of Service Operation is defined	Not applicable
11	The Event Management process is defined	Not applicable
12	The Incident and Problem Management process is defined	Not applicable
13	The Request fulfilment process is defined	Not applicable
14	The Access Management process is defined	Not applicable
15	The Service Desk function is defined	Not applicable
16	The Technical Management function is defined	Not applicable
17	The IT operations Management function is defined	Not applicable
18	The Application Management function is defined	Not applicable

19	Interfaces to other Service Lifecycle stages are clearly defined	Not applicable
	SCORE	0
2	**Service Operation Principles**	Participant 1
1	Distinctive functions, groups, teams, departments and divisions are defined	Not applicable
2	We have a balance between an internal IT view and external business view	Not applicable
3	We balance stability interests versus responsiveness to changes	Not applicable
4	We balance quality of service versus cost of service	Not applicable
5	We balance reactiveness versus proactiveness	Not applicable
6	All Service operation staff is fully aware that they are providing a service to the business	Not applicable
7	We have a clear definition of It service objectives and performance criteria	Not applicable
8	We have linkage of IT Service specifications to the performance of the IT infrastructure	Not applicable
9	We have a definition of operational performance requirements	Not applicable
10	We have a mapping of services and technology	Not applicable
11	We have the ability to model the effect of changes in technology and changes to business requirements	Not applicable
12	We have appropriate cost models to evaluate ROI and cost reduction strategies	Not applicable
13	Operational health is monitored with a set of Vital signs	Not applicable
14	We have routine Operational communication and templates (where appropriate)	Not applicable
15	We have formalised communication between IT Shifts/Departments	Not applicable
16	We have formalised performance reporting	Not applicable
17	We have formalised communication in projects	Not applicable
18	We have formalised communication related to exceptions	Not applicable
19	We have formalised communication related to emergencies	Not applicable
20	We have training on new or customised processes and service designs	Not applicable
21	We have communication of strategy and design to our service operation teams formalised	Not applicable
22	The means of communication (email, sms etc) are defined	Not applicable
23	We have a structured, regular Operations Meeting	Not applicable
24	We have structured, regular Department, Group and Team Meetings	Not applicable
25	We have structured, regular Customer Meetings	Not applicable
26	We participate in the definition and maintenance of process manuals for all processes we are involved in	Not applicable
27	We establish our own technical procedures manuals	Not applicable
28	We participate in the creation and maintenance of planning documents	Not applicable
29	We participate in the definition and maintenance of Service Management Tool work instructions	Not applicable
	SCORE	0
3	**Service Operation Processes**	Participant 1
1	We have defined Event Management's Purpose, Goal and Objective	Not applicable
2	We have defined Event Management's Scope	Not applicable
3	We have defined Event Management's Value to the business	Not applicable
4	We have defined Event Management's Policies, Principles and basic concepts	Not applicable
5	The "Event Occurs" process activity is specified	Not applicable
6	The "Event Notification" process activity is specified	Not applicable
7	The "Event Detection" process activity is specified	Not applicable
8	The "Event Filtering" process activity is specified	Not applicable
9	The "Significance of Events Categorisation" process activity is specified	Not applicable
10	The "Event Correlation" process activity is specified	Not applicable
11	The "Trigger" process activity is specified	Not applicable
12	The "Response Selection" process activity is specified	Not applicable
13	The "Review Actions" process activity is specified	Not applicable
14	The "Close Actions" process activity is specified	Not applicable

15	We have defined Event Management's Triggers, Imputs, Outputs and interfaces	Not applicable
16	We have defined Event Management's KPIs and metrics	Not applicable
17	We have defined Event Management's Information Management reporting	Not applicable
18	We have defined Event Management's Challenges, Critical Success Factors and Risks	Not applicable
19	We have defined Incident Management's Purpose, Goal and Objective	Not applicable
20	We have defined Incident Management's Scope	Not applicable
21	We have defined Incident Management's Value to the business	Not applicable
22	We have defined Incident Management's Policies, Principles and basic concepts	Not applicable
23	Timescales are agreed for all incident handling stages	Not applicable
24	Incident Models are defined	Not applicable
25	Major Incidents are defined	Not applicable
26	The "Incident Identification" process activity is specified	Not applicable
27	The "Incident logging" process activity is specified	Not applicable
28	The "Incident categorisation" process activity is specified	Not applicable
29	The "Incident Prioritisation" process activity is specified	Not applicable
30	The "Initial Diagnosis" process activity is specified	Not applicable
31	The "Incident Escalation" process activity is specified	Not applicable
32	The "Incident Identification" process activity is specified	Not applicable
33	The "Investigation and Diagnosis" process activity is specified	Not applicable
34	The "Resolution and recovery" process activity is specified	Not applicable
35	The "Incident Closure" process activity is specified	Not applicable
36	We have defined Incident Management's Triggers, Imputs, Outputs and interfaces	Not applicable
37	We have defined Incident Management's KPIs and metrics	Not applicable
38	We have defined Incident Management's Information Management reporting	Not applicable
39	We have defined Incident Management's Challenges, Critical Success Factors and Risks	Not applicable
40	We have defined Request Fulfilment's Purpose, Goal and Objective	Not applicable
41	We have defined Request Fulfilment's Scope	Not applicable
42	We have defined Request Fulfilment's Value to the business	Not applicable
43	We have defined Request Fulfilment's Policies, Principles and basic concepts	Not applicable
44	The "Menu Selection" activity is specified	Not applicable
45	The "Financial approval" activity is specified	Not applicable
46	The "Other approval" activity is specified	Not applicable
47	The "Fulfilment" activity is specified	Not applicable
48	The "Closure" activity is specified	Not applicable
49	We have defined Request Fulfilment's Triggers, Imputs, Outputs and interfaces	Not applicable
50	We have defined Request Fulfilment's KPIs and metrics	Not applicable
51	We have defined Request Fulfilment's Information Management reporting	Not applicable
52	We have defined Request Fulfilment's Challenges, Critical Success Factors and Risks	Not applicable
53	We have defined Problem Management's Purpose, Goal and Objective	Not applicable
54	We have defined Problem Management's Scope	Not applicable
55	We have defined Problem Management's Value to the business	Not applicable
56	We have defined Problem Management's Policies, Principles and basic concepts	Not applicable
57	The "Problem Detection" process activity is specified	Not applicable
58	The "Problem Logging" process activity is specified	Not applicable
59	The "Problem Categorisation" process activity is specified	Not applicable
60	The "Problem Prioritisation" process activity is specified	Not applicable
61	The "Problem Investigation and Diagnosis" process activity is specified	Not applicable
62	The "Workarounds" process activity is specified	Not applicable
63	The "Raising a known error record" process activity is specified	Not applicable

64	The "Problem Resolution" process activity is specified	Not applicable
65	The "Problem Closure" process activity is specified	Not applicable
66	The "Major Problem Review" process activity is specified	Not applicable
67	The "Errors detected in the development environment" process activity is specified	Not applicable
68	We have defined Problem Management's Triggers, Imputs, Outputs and interfaces	Not applicable
69	The CMS acts as a valuable source for Problem Management	Not applicable
70	We have a Known Error Database to allow quicker diagnosis and resolution	Not applicable
71	We have defined Problem Management's KPIs and metrics	Not applicable
72	We have defined Problem Management's Information Management reporting	Not applicable
73	We have defined Problem Management's Challenges, Critical Success Factors and Risks	Not applicable
74	We have defined Access Management's Purpose, Goal and Objective	Not applicable
75	We have defined Access Management's Scope	Not applicable
76	We have defined Access Management's Value to the business	Not applicable
77	We have defined Access Management's Policies, Principles and basic concepts	Not applicable
78	The "Requesting Access" process activity is specified	Not applicable
79	The "Verification" process activity is specified	Not applicable
80	The "Providing Rights" process activity is specified	Not applicable
81	The "Monitoring Identity Status" process activity is specified	Not applicable
82	The "Logging and Tracking Access" process activity is specified	Not applicable
83	The "Removing or restricting rights" process activity is specified	Not applicable
84	We have defined Access Management's Triggers, Imputs, Outputs and interfaces	Not applicable
85	We have defined Access Management's KPIs and metrics	Not applicable
86	We have defined Access Management's Information Management reporting	Not applicable
87	We have defined Access Management's Challenges, Critical Success Factors and Risks	Not applicable
	SCORE	0
4	**Common Service Operation Activities**	Participant 1
1	We know where we are on the technology centric Vs business centric scale	Not applicable
2	Monitoring and control is a continual cycle	Not applicable
3	We use tools to monitor the status of key CIs and key operational activities	Not applicable
4	We ensure that specified conditions are met (or not met), and if not to raise an alert to the appropriate group (e.g. the availability of key network devices)	Not applicable
5	We ensure that the performance or utilisation of a component or system is within a specified range (e.g. disk space or memory utilization)	Not applicable
6	We detect abnormal types or levels of activity in the infrastructure (e.g. potential security threats)	Not applicable
7	We detect unauthorised changes (e.g. introduction of software)	Not applicable
8	We ensure compliance with the organisation's policies (e.g. inappropriate use of email)	Not applicable
9	We track outputs to the business and ensure that they meet quality and performance requirements	Not applicable
10	We track any information that is used to measure Key Performance Indicators	Not applicable
11	We use tools to collate the output of monitoring into information that can be disseminated to various groups, functions or processes	Not applicable
12	We interpret the meaning of that information	Not applicable
13	We determining where that information would best be used	Not applicable
14	We ensure that decision makers have access to the information that will enable them to make decisions	Not applicable
15	We route the reported information to the appropriate person, group or tool	Not applicable
16	We use tools to define what conditions represent normal operations or abnormal operations	Not applicable
17	We regulate performance of devices, systems or services	Not applicable
18	We Measure availability from an IT and Organisation perspective	Not applicable

19	We Initiate corrective action, which could be automated (e.g. reboot a device remotely or run a script), or manual (e.g. notify operations staff of the status)	Not applicable
20	We manage the monitor control loop	Not applicable
21	We have defined what needs to be monitored	Not applicable
22	We have internal and external monitoring and control	Not applicable
23	We manage different types of monitoring	Not applicable
24	We monitor in test environments	Not applicable
25	We manage reporting and action upon monitoring	Not applicable
26	We perform service operation audits	Not applicable
27	In IT operations we have a defined Console Management/Operations Bridge	Not applicable
28	In IT operations we have a defined job scheduling role	Not applicable
29	In IT operations we have a defined back-Up and Restore role	Not applicable
30	In IT operations we have a defined Print and Output Role	Not applicable
31	Mainframe management is a mature practice	Not applicable
32	Server Management and support is a mature practice	Not applicable
33	Network management is a mature practice	Not applicable
34	Storage and archive is a mature practice	Not applicable
35	Database Administration is a mature practice	Not applicable
36	Directory Services Management is a mature practice	Not applicable
37	Desktop Support is a mature practice	Not applicable
38	Middleware management is a mature practice	Not applicable
39	Internet/Web Management/Mainframe Management is a mature practice	Not applicable
40	Facilities and Data Centre Management is a mature practice	Not applicable
41	Information Security Management within Service Operation is a mature practice	Not applicable
42	Mainframe management is a mature practice	Not applicable
	SCORE	0
5	**Organising Service Operation**	Participant 1
1	The Service Desk function is defined	Not applicable
2	We have Justification for and the Role of the Service Desk defined	Not applicable
3	We have Service Desk Objectives	Not applicable
4	We have a clear Service Desk Organisational Structure	Not applicable
5	Service Desk Staffing is managed	Not applicable
6	We have Service Desk Metrics	Not applicable
7	We investigate(d) Outsourcing the Service Desk	Not applicable
8	The Technical Management Role is defined	Not applicable
9	We have clear Technical Management Objectives	Not applicable
10	We have defined Generic Technical Management Activities	Not applicable
11	We have a clear Technical Management Organisation	Not applicable
12	We have Technical Design and Technical Maintenance and Support	Not applicable
13	We have Technical Management Metrics	Not applicable
14	We have Technical Management Documentation	Not applicable
15	The IT Operations Management role is defined	Not applicable
16	IT Operations Management Objectives are defined	Not applicable
17	We have a IT Operations Management Organisation	Not applicable
18	We have IT Operations Management Metrics	Not applicable
19	We have IT Operations Management Documentation	Not applicable
20	The Application Management Role is defined	Not applicable
21	We have Application Management Objectives	Not applicable
22	We have Application Management Principles	Not applicable
23	The Application Management Lifecycle is defined	Not applicable
24	We have deined Application Management Generic Activities	Not applicable
25	We have a clear Application Management Organisation	Not applicable

26	We have defined Application Management Roles and Responsibilities	Not applicable
27	We have Application Management Metrics	Not applicable
28	We have Application Management Documentation	Not applicable
29	We have clear Service Desk Roles	Not applicable
30	We have Technical Management Roles	Not applicable
31	We have IT Operations Management Roles	Not applicable
32	We have Applications Management Roles	Not applicable
33	We have Event Management Roles	Not applicable
34	We have Incident Management Roles	Not applicable
35	We have Request Fulfilment Roles	Not applicable
36	We have Problem Management Roles	Not applicable
37	We have Access Management Roles defined	Not applicable
38	We are organised by Technical Specialisation	Not applicable
39	We are organised by Activity	Not applicable
40	We are organised to Manage Processes	Not applicable
41	IT Operations are organised by Geography	Not applicable
42	We have Hybrid Organisation Structures of the above	Not applicable
	SCORE	0
6	**Service Operation Technology Considerations**	Participant 1
1	We have Integrated IT Service Management Technology	Not applicable
2	We offer Self Help	Not applicable
3	We have a Workflow or Process Engine	Not applicable
4	We have an Integrated CMS	Not applicable
5	We have Discovery/Deployment /Licensing Technology	Not applicable
6	We have Remote Control	Not applicable
7	We have Diagnostic Utilities	Not applicable
8	We have Reporting facilities	Not applicable
9	We have Dashboards	Not applicable
10	We have Integration with Business Service Management	Not applicable
11	We have Event Management technology	Not applicable
12	We have Incident Management technology	Not applicable
13	We have Integrated ITSM technology	Not applicable
14	We have Workflow and Automated Escalation	Not applicable
15	We have Request Fulfilment applications	Not applicable
16	We have Problem Management applications	Not applicable
17	We have Integrated Service Management Technology	Not applicable
18	We have Change Management applications	Not applicable
19	We have an Integrated CMS	Not applicable
20	We have a Known Error Database	Not applicable
21	We have Access Management applications	Not applicable
22	We have a Service Desk tool	Not applicable
23	We have Service desk specific Telephony infrastructure	Not applicable
24	The Service desk has access to Support Tools	Not applicable
25	We have IT Service Continuity Planning for ITSM Support Tools	Not applicable
	SCORE	0
7	**Implementing Service Operation**	Participant 1
1	We actively Manage Change in Service Operation	Not applicable
2	We monitor and manage Change Triggers	Not applicable
3	We manage Change Assessment	Not applicable
4	We have Measurement of Successful Change defined	Not applicable
5	We Assess and Manage Risks in Service Operation	Not applicable

6	Operational Staff is involved in Service Design and Transition	Not applicable
7	With Planning & Implementing Service Management Technologies we check Licenses	Not applicable
8	With Planning & Implementing Service Management Technologies we check deployment	Not applicable
9	With Planning & Implementing Service Management Technologies we do capacity checks	Not applicable
10	With Planning & Implementing Service Management Technologies we manage the timing of technology deployment	Not applicable
	SCORE	0

6.3. Anexo III – Minutas de reuniones con participantes y correos con información sobre la empresa

1:1 Con Adrián InfoSec

Monday, August 1, 2016 5:06 PM

Asistentes: Adrián, Randall

Notas:

- Todos los procesos se están orientando a DevOps a través de Agile
- Change Management se está implementando a través de Agile, con Scrum meetings
  - Springs de 2, 3 semanas dependiendo de la aplicación o servicio
  - Releases semanales
  - Herramienta utilizada es Jira, pero se piensa incorporar Rally
- Principales servicios o grupos de aplicaciones en las que se trabajan actualmente: IDAM, Controls & Compliance
- Enfoque en Change Management (CM) e Incident Management (IM). Pero principalmente CM porque se descubrió que la principal causa de incidentes se debía a cambios mal manejados.
- El departamento de TI emitió una directriz en la que se indica que:
  - Deben aplicarse metodologías ágiles en todos los procesos
    - Desarrollo de software
    - Soporte de operaciones
    - Se utiliza Scrum
    - CA Agile Central (Rally)
      - http://www.ca.com/us/products/ca-agile-central.html
  - Debe aplicarse un enfoque DevOps de tal manera que los equipos de ingeniería y soporte de operaciones trabajen en conjunto para lograr los objetivos del departamento y por tanto de la empresa.
    - El equipo de soporte de operaciones está integrado al equipo de desarrollo de software que utiliza Scrum para gestionar el trabajo.
- El marco de referencia ITIL v3 es el que se utiliza para la gestión de los servicios de TI.
- La gestión de los servicios de TI se apoya en el uso de ServiceNow como herramienta tecnológica.

1:1 Con Adrián InfoSec

Wednesday, October 19, 2016 10:30 AM

Asistentes: Adrián, Randall

Agenda:

- Identificar los roles que participan en el proceso de soporte de aplicaciones, incluyendo otros equipos u organizaciones.

Notas:

- Gestión de Cambios "oficial" en la organización
  - Requester (dueño de aplicación)
  - Implementer
    - Soporte de operaciones (Ops)
  - Tester
    - Miembros del equipo de desarrollo validan el cambio luego de su implementación
  - Builder
    - Es un desarrollador que asegura que el paquete desarrollado está en producción

- Gestión de Cambios actual
  - Requester (dueño de la aplicación)
  - Scrum para dar seguimiento al desarrollo que requiere el cambio
  - Ops apoya la implementación del cambio
  - Si hubiera dependencia de servicios para implementar el cambio Ops coordina el trabajo de esas dependencias (Hosting de servidores, almacenamiento, redes)
  - Ops realiza las tareas requeridas para obtener la aprobación del cambio a nivel del portafolio de aplicaciones.

- Gestión de Incidentes
  - A través de un registro Major Incident (MI)
  - Ops realiza las tareas asociadas
  - Scrum para dar seguimiento a las tareas asociadas

6.4. Anexo IV – Respuestas de los participantes a lista de verificación ITIL

	Data entry			
	Below are the only valid entries for the assessment			
	Each person must use the drop-down box and select an answer for each question for each process area.			
1	Initial - processes and activities are adhoc or chaotic or undefined			
2	Repeatable - basic processes and activities are established and there is a level of discipline and adherence			
3	Defined - All processes and activities are defined, documented, standardised and integrated together			
4	Managed - Processes are measured by collecting detailed data on the processes and their quality and appropriately improved			
5	Optimising - Continuous process improvement is adopted. Process and activities are mature			
	Step 1 - Enter the names of the participants here:			
	Vargas Martinez, Guillermo			
	Aguilar, Adrian			
	Step 2 - Now have each participant answer each question for each Service Operation area, under their name.			
1	**Service Management as a Practice**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	Service Management is clearly defined	2	5	7
2	We know what our services are	2	5	7
3	We have clearly defined functions and processes across the lifecycle	1	3	4
4	We are able to measure the processes in a relevant matter	1	3	4
5	The reason a process exists is to deliver a specific result	3	5	8
6	Every process delivers its primary result to a customer or stakeholder	1	3	4
7	The goals of Service Operation are defined	1	4	5
8	The objectives of Service Operation are defined	1	5	6
9	The purpose of Service Operation is Defined	2	5	7
10	The Scope of Service Operation is defined	1	4	5
11	The Event Management process is defined	1	2	3
12	The Incident and Problem Management process is defined	2	4	6
13	The Request fulfilment process is defined	2	3	5
14	The Access Management process is defined	1	5	6
15	The Service Desk function is defined	Not applicable	2	2
16	The Technical Management function is defined	Not applicable	3	3
17	The IT operations Management function is defined	Not applicable	3	3
18	The Application Management function is defined	Not applicable	2	2
19	Interfaces to other Service Lifecycle stages are clearly defined	Not applicable	2	2
	SCORE	20	51	71

2	**Service Operation Principles**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	Distinctive functions, groups, teams, departments and divisions are defined	1	4	5
2	We have a balance between an internal IT view and external business view	Not applicable	4	4
3	We balance stability interests versus responsiveness to changes	Not applicable	3	3
4	We balance quality of service versus cost of service	Not applicable	3	3
5	We balance reactiveness versus proactiveness	Not applicable	3	3
6	All Service operation staff is fully aware that they are providing a service to the business	3	2	5
7	We have a clear definition of It service objectives and performance criteria	2	5	7
8	We have linkage of IT Service specifications to the performance of the IT infrastructure	Not applicable	3	3
9	We have a definition of operational performance requirements	Not applicable	4	4
10	We have a mapping of services and technology	1	5	6
11	We have the ability to model the effect of changes in technology and changes to business requirements	Not applicable	3	3
12	We have appropriate cost models to evaluate ROI and cost reduction strategies	Not applicable	2	2
13	Operational health is monitored with a set of Vital signs	2	2	4
14	We have routine Operational communication and templates (where appropriate)	1	2	3
15	We have formalised communication between IT Shifts/Departments	1	3	4
16	We have formalised performance reporting	1	3	4
17	We have formalised communication in projects	1	3	4
18	We have formalised communication related to exceptions	Not applicable	3	3
19	We have formalised communication related to emergencies	1	1	2
20	We have training on new or customised processes and service designs	1	3	4
21	We have communication of strategy and design to our service operation teams formalized	1	3	4
22	The means of communication (email, sms etc) are defined	1	4	5
23	We have a structured, regular Operations Meeting	2	5	7
24	We have structured, regular Department, Group and Team Meetings	2	5	7
25	We have structured, regular Customer Meetings	Not applicable	5	5
26	We participate in the definition and maintenance of process manuals for all processes we are involved in	Not applicable	1	1
27	We establish our own technical procedures manuals	Not applicable	1	1
28	We participate in the creation and maintenance of planning documents	Not applicable	5	5
29	We participate in the definition and maintenance of Service Management Tool work instructions	Not applicable	5	5
	SCORE	21	95	116

3	**Service Operation Processes**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	We have defined **Event Management**'s Purpose, Goal and Objective	Not applicable	1	1
2	We have defined Event Management's Scope	Not applicable	1	1

3	We have defined Event Management's Value to the business	Not applicable	1	1
4	We have defined Event Management's Policies, Principles and basic concepts	Not applicable	1	1
5	The "Event Occurs" process activity is specified	Not applicable	3	3
6	The "Event Notification" process activity is specified	Not applicable	3	3
7	The "Event Detection" process activity is specified	Not applicable	3	3
8	The "Event Filtering" process activity is specified	Not applicable	3	3
9	The "Significance of Events Categorisation" process activity is specified	Not applicable	2	2
10	The "Event Correlation" process activity is specified	Not applicable	2	2
11	The "Trigger" process activity is specified	Not applicable	4	4
12	The "Response Selection" process activity is specified	Not applicable	2	2
13	The "Review Actions" process activity is specified	Not applicable	2	2
14	The "Close Actions" process activity is specified	Not applicable	2	2
15	We have defined Event Management's Triggers, Imputs, Outputs and interfaces	Not applicable	1	1
16	We have defined Event Management's KPIs and metrics	1	1	2
17	We have defined Event Management's Information Management reporting	Not applicable	1	1
18	We have defined Event Management's Challenges, Critical Success Factors and Risks	Not applicable	1	1
19	We have defined **Incident Management**'s Purpose, Goal and Objective	2	4	6
20	We have defined Incident Management's Scope	2	4	6
21	We have defined Incident Management's Value to the business	2	4	6
22	We have defined Incident Management's Policies, Principles and basic concepts	2	4	6
23	Timescales are agreed for all incident handling stages	Not applicable	3	3
24	Incident Models are defined	Not applicable	3	3
25	Major Incidents are defined	Not applicable	5	5
26	The "Incident Identification" process activity is specified	Not applicable	5	5
27	The "Incident logging" process activity is specified	Not applicable	5	5
28	The "Incident categorisation" process activity is specified	1	5	6
29	The "Incident Prioritisation" process activity is specified	1	3	4
30	The "Initial Diagnosis" process activity is specified	1	5	6
31	The "Incident Escalation" process activity is specified	1	2	3
32	The "Incident Identification" process activity is specified	1	3	4
33	The "Investigation and Diagnosis" process activity is specified	1	4	5
34	The "Resolution and recovery" process activity is specified	1	4	5
35	The "Incident Closure" process activity is specified	1	4	5
36	We have defined Incident Management's Triggers, Imputs, Outputs and interfaces	1	3	4
37	We have defined Incident Management's KPIs and metrics	1	1	2
38	We have defined Incident Management's Information Management reporting	1	1	2
39	We have defined Incident Management's Challenges, Critical Success Factors and Risks	Not applicable	1	1
40	We have defined **Request Fulfilment**'s Purpose, Goal and Objective	2	2	
41	We have defined Request Fulfilment's Scope	2	2	4

42	We have defined Request Fulfilment's Value to the business	2	2	4
43	We have defined Request Fulfilment's Policies, Principles and basic concepts	2	2	4
44	The "Menu Selection" activity is specified	Not applicable	2	2
45	The "Financial approval" activity is specified	Not applicable	2	2
46	The "Other approval" activity is specified	Not applicable	2	2
47	The "Fulfilment" activity is specified	1	2	3
48	The "Closure" activity is specified	Not applicable	2	2
49	We have defined Request Fulfilment's Triggers, Imputs, Outputs and interfaces	Not applicable	2	2
50	We have defined Request Fulfilment's KPIs and metrics	1	2	3
51	We have defined Request Fulfilment's Information Management reporting	1	2	3
52	We have defined Request Fulfilment's Challenges, Critical Success Factors and Risks	Not applicable	2	2
53	We have defined Problem Management's Purpose, Goal and Objective	Not applicable	3	3
54	We have defined Problem Management's Scope	Not applicable	3	3
55	We have defined Problem Management's Value to the business	Not applicable	2	2
56	We have defined Problem Management's Policies, Principles and basic concepts	Not applicable	3	3
57	The "Problem Detection" process activity is specified	Not applicable	2	2
58	The "Problem Logging" process activity is specified	Not applicable	2	2
59	The "Problem Categorisation" process activity is specified	Not applicable	2	2
60	The "Problem Prioritisation" process activity is specified	Not applicable	2	2
61	The "Problem Investigation and Diagnosis" process activity is specified	Not applicable	3	3
62	The "Workarounds" process activity is specified	Not applicable	3	3
63	The "Raising a known error record" process activity is specified	Not applicable	2	2
64	The "Problem Resolution" process activity is specified	Not applicable	2	2
65	The "Problem Closure" process activity is specified	Not applicable	1	1
66	The "Major Problem Review" process activity is specified	Not applicable	2	2
67	The "Errors detected in the development environment" process activity is specified	Not applicable	1	1
68	We have defined Problem Management's Triggers, Imputs, Outputs and interfaces	Not applicable	1	1
69	The CMS acts as a valuable source for Problem Management	Not applicable	2	2
70	We have a Known Error Database to allow quicker diagnosis and resolution	Not applicable	3	3
71	We have defined Problem Management's KPIs and metrics	Not applicable	2	2
72	We have defined Problem Management's Information Management reporting	Not applicable	0	0
73	We have defined Problem Management's Challenges, Critical Success Factors and Risks	Not applicable	0	0
74	We have defined **Access Management**'s Purpose, Goal and Objective	Not applicable	4	4
75	We have defined Access Management's Scope	Not applicable	3	3
76	We have defined Access Management's Value to the business	Not applicable	3	3
77	We have defined Access Management's Policies, Principles and basic concepts	Not applicable	3	3
78	The "Requesting Access" process activity is specified	Not applicable	4	4

79	The "Verification" process activity is specified	Not applicable	3	3
80	The "Providing Rights" process activity is specified	Not applicable	5	5
81	The "Monitoring Identity Status" process activity is specified	Not applicable	5	5
82	The "Logging and Tracking Access" process activity is specified	Not applicable	1	1
83	The "Removing or restricting rights" process activity is specified	Not applicable	2	2
84	We have defined Access Management's Triggers, Imputs, Outputs and interfaces	Not applicable	3	3
85	We have defined Access Management's KPIs and metrics	Not applicable	1	1
86	We have defined Access Management's Information Management reporting	Not applicable	1	1
87	We have defined Access Management's Challenges, Critical Success Factors and Risks	Not applicable	1	1
	SCORE	31	213	244
4	**Common Service Operation Activities**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	We know where we are on the technology centric Vs business centric scale	Not applicable	3	3
2	Monitoring and control is a continual cycle	1	3	4
3	We use tools to monitor the status of key CIs and key operational activities	1	1	2
4	We ensure that specified conditions are met (or not met), and if not to raise an alert to the appropriate group (e.g. the availability of key network devices)	1	3	4
5	We ensure that the performance or utilisation of a component or system is within a specified range (e.g. disk space or memory utilization)	Not applicable	2	2
6	We detect abnormal types or levels of activity in the infrastructure (e.g. potential security threats)	1	2	3
7	We detect unauthorised changes (e.g. introduction of software)	2	2	4
8	We ensure compliance with the organisation's policies (e.g. inappropriate use of email)	Not applicable	5	5
9	We track outputs to the business and ensure that they meet quality and performance requirements	3	2	5
10	We track any information that is used to measure Key Performance Indicators	2	2	4
11	We use tools to collate the output of monitoring into information that can be disseminated to various groups, functions or processes	3	2	5
12	We interpret the meaning of that information	3	2	5
13	We determining where that information would best be used	2	4	6
14	We ensure that decision makers have access to the information that will enable them to make decisions	1	5	6
15	We route the reported information to the appropriate person, group or tool	1	4	5
16	We use tools to define what conditions represent normal operations or abnormal operations	Not applicable	2	2
17	We regulate performance of devices, systems or services	1	1	2
18	We Measure availability from an IT and Organisation perspective	3	1	4
19	We Initiate corrective action, which could be automated (e.g. reboot a device remotely or run a script), or manual (e.g. notify operations staff of the status)	1	2	3
20	We manage the monitor control loop	1	1	2
21	We have defined what needs to be monitored	Not applicable	4	4

22	We have internal and external monitoring and control	Not applicable	2	2
23	We manage different types of monitoring	1	4	5
24	We monitor in test environments	1	0	1
25	We manage reporting and action upon monitoring	Not applicable	2	2
26	We perform service operation audits	3	3	6
27	In IT operations we have a defined Console Management/Operations Bridge	Not applicable	0	0
28	In IT operations we have a defined job scheduling role	Not applicable	0	0
29	In IT operations we have a defined back-Up and Restore role	Not applicable	0	0
30	In IT operations we have a defined Print and Output Role	Not applicable	0	0
31	Mainframe management is a mature practice	Not applicable	2	2
32	Server Management and support is a mature practice	3	2	5
33	Network management is a mature practice	3	5	8
34	Storage and archive is a mature practice	Not applicable	4	4
35	Database Administration is a mature practice	3	1	4
36	Directory Services Management is a mature practice	3	5	8
37	Desktop Support is a mature practice	Not applicable	2	2
38	Middleware management is a mature practice	Not applicable	0	0
39	Internet/Web Management/Mainframe Management is a mature practice	Not applicable	0	0
40	Facilities and Data Centre Management is a mature practice	Not applicable	5	5
41	Information Security Management within Service Operation is a mature practice	Not applicable	5	5
42	Mainframe management is a mature practice	Not applicable	0	0
	SCORE	44	95	139
5	**Organising Service Operation**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	The Service Desk function is defined	3	2	5
2	We have Justification for and the Role of the Service Desk defined	3	2	5
3	We have Service Desk Objectives	3	2	5
4	We have a clear Service Desk Organisational Structure	3	2	5
5	Service Desk Staffing is managed	3	2	5
6	We have Service Desk Metrics	3	2	5
7	We investigate(d) Outsourcing the Service Desk	Not applicable	0	0
8	The Technical Management Role is defined	Not applicable	5	5
9	We have clear Technical Management Objectives	Not applicable	3	3
10	We have defined Generic Technical Management Activities	Not applicable	5	5
11	We have a clear Technical Management Organisation	Not applicable	5	5
12	We have Technical Design and Technical Maintenance and Support	Not applicable	3	3
13	We have Technical Management Metrics	Not applicable	0	0
14	We have Technical Management Documentation	Not applicable	2	2
15	The IT Operations Management role is defined	2	5	7
16	IT Operations Management Objectives are defined	2	5	7
17	We have a IT Operations Management Organisation	2	5	7
18	We have IT Operations Management Metrics	2	4	6
19	We have IT Operations Management Documentation	Not applicable	4	4
20	The Application Management Role is defined	Not applicable	4	4

21	We have Application Management Objectives	Not applicable	4	4
22	We have Application Management Principles	Not applicable	2	2
23	The Application Management Lifecycle is defined	Not applicable	2	2
24	We have deined Application Management Generic Activities	Not applicable	2	2
25	We have a clear Application Management Organisation	Not applicable	3	3
26	We have defined Application Management Roles and Responsibilities	Not applicable	3	3
27	We have Application Management Metrics	Not applicable	3	3
28	We have Application Management Documentation	Not applicable	3	3
29	We have clear Service Desk Roles	Not applicable	5	5
30	We have Technical Management Roles	Not applicable	4	4
31	We have IT Operations Management Roles	Not applicable	5	5
32	We have Applications Management Roles	Not applicable	5	5
33	We have Event Management Roles	Not applicable	0	0
34	We have Incident Management Roles	Not applicable	5	5
35	We have Request Fulfilment Roles	Not applicable	5	5
36	We have Problem Management Roles	Not applicable	5	5
37	We have Access Management Roles defined	Not applicable	5	5
38	We are organised by Technical Specialisation	Not applicable	4	4
39	We are organised by Activity	Not applicable	3	3
40	We are organised to Manage Processes	Not applicable	5	5
41	IT Operations are organised by Geography	Not applicable	5	5
42	We have Hybrid Organisation Structures of the above	Not applicable	5	5
	SCORE	26	145	171
6	**Service Operation Technology Considerations**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	We have Integrated IT Service Management Technology	Not applicable	5	5
2	We offer Self Help	2	5	7
3	We have a Workflow or Process Engine	1	5	6
4	We have an Integrated CMS	1	5	6
5	We have Discovery/Deployment /Licensing Technology	Not applicable	3	3
6	We have Remote Control	Not applicable	5	5
7	We have Diagnostic Utilities	Not applicable	5	5
8	We have Reporting facilities	Not applicable	0	0
9	We have Dashboards	2	5	7
10	We have Integration with Business Service Management	Not applicable	5	5
11	We have Event Management technology	Not applicable	5	5
12	We have Incident Management technology	Not applicable	5	5
13	We have Integrated ITSM technology	Not applicable	5	5
14	We have Workflow and Automated Escalation	Not applicable	5	5
15	We have Request Fulfilment applications	Not applicable	5	5
16	We have Problem Management applications	Not applicable	5	5
17	We have Integrated Service Management Technology	Not applicable	5	5
18	We have Change Management applications	Not applicable	5	5
19	We have an Integrated CMS	Not applicable	3	3
20	We have a Known Error Database	Not applicable	5	5
21	We have Access Management applications	Not applicable	5	5

22	We have a Service Desk tool	Not applicable	5	5
23	We have Service desk specific Telephony infrastructure	Not applicable	5	5
24	The Service desk has access to Support Tools	Not applicable	5	5
25	We have IT Service Continuity Planning for ITSM Support Tools	Not applicable	5	5
	SCORE	6	116	122
7	**Implementing Service Operation**	**Vargas Martinez, Guillermo**	**Aguilar, Adrian**	**Total**
1	We actively Manage Change in Service Operation	Not applicable	5	5
2	We monitor and manage Change Triggers	Not applicable	5	5
3	We manage Change Assessment	Not applicable	5	5
4	We have Measurement of Successful Change defined	Not applicable	5	5
5	We Assess and Manage Risks in Service Operation	Not applicable	5	5
6	Operational Staff is involved in Service Design and Transition	Not applicable	5	5
7	With Planning & Implementing Service Management Technologies we check Licenses	Not applicable	5	5
8	With Planning & Implementing Service Management Technologies we check deployment	Not applicable	5	5
9	With Planning & Implementing Service Management Technologies we do capacity checks	Not applicable	5	5
10	With Planning & Implementing Service Management Technologies we manage the timing of technology deployment	Not applicable	2	2
	SCORE	0	47	47

6.5. Anexo V – Respuestas de los participantes a la lista de verificación de DevOps

Detalle de los resultados del cuestionario aplicado al participante 1.

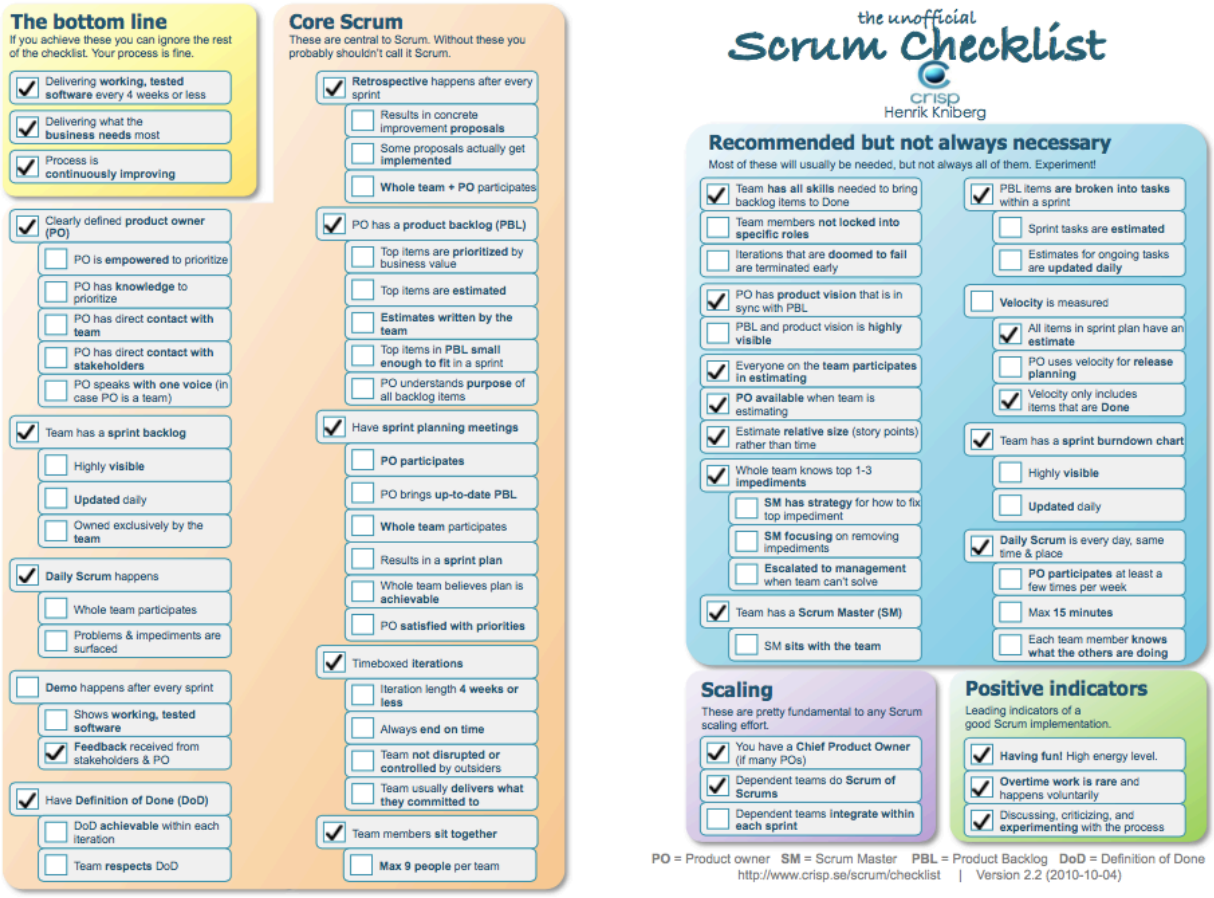
DevOps	%	Elementos presentes en la organización
Alineamiento	100	Unificar la dirección y los objetivos individuales y colectivos alrededor de la visión estratégica de la empresa.
Contexto	50	Hacer que la información y los contactos relevantes estén disponibles para quien los necesite, cuando los necesite.
Aprendizaje	71	Apoyar el crecimiento personal y fomentar la comprensión del negocio a través de la mejora continua.
Ciclo de vida	38	Enfocarse en el software como un producto que merece cuidado, atención y reflexión dentro de un ecosistema que cambia constantemente.
Organización	88	Proveer una estructura que fomente la interacción y la cohesión para apoyar la colaboración y productividad.
Proceso	89	Crear rituales para fomentar la consistencia y confianza, creando un marco de referencia para la mejora continua.
Total	**73**	

Detalle de los resultados del cuestionario aplicado al participante 2.

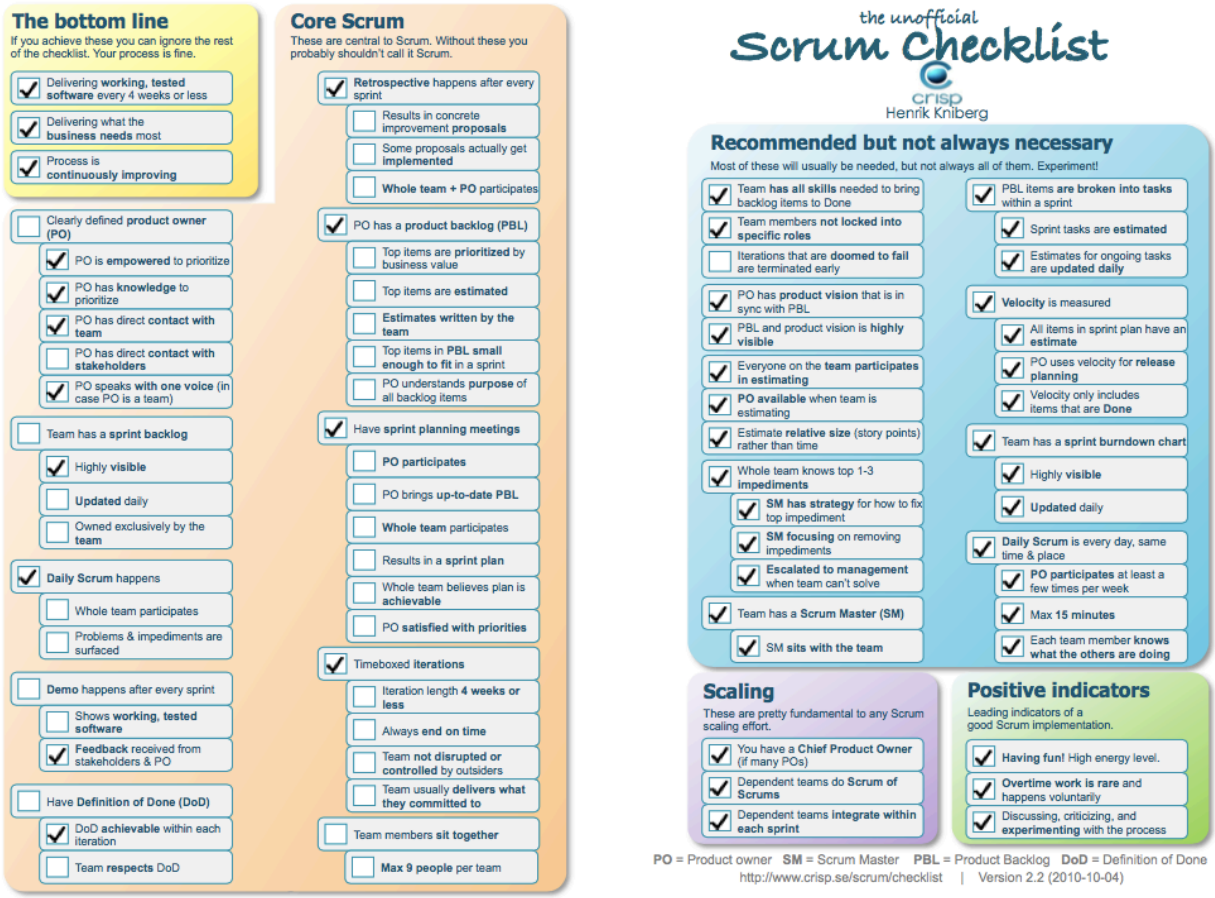
DevOps	%	Elementos presentes en la organización
Alineamiento	88	Unificar la dirección y los objetivos individuales y colectivos alrededor de la visión estratégica de la empresa.
Contexto	88	Hacer que la información y los contactos relevantes estén disponibles para quien los necesite, cuando los necesite.
Aprendizaje	71	Apoyar el crecimiento personal y fomentar la comprensión del negocio a través de la mejora continua.
Ciclo de vida	13	Enfocarse en el software como un producto que merece cuidado, atención y reflexión dentro de un ecosistema que cambia constantemente.
Organización	38	Proveer una estructura que fomente la interacción y la cohesión para apoyar la colaboración y productividad.
Proceso	78	Crear rituales para fomentar la consistencia y confianza, creando un marco de referencia para la mejora continua.
Total	**63**	

6.6. Anexo VI – Respuestas de los participantes a la lista de verificación de Scrum

Respuestas completas la lista de verificación aplicada al participante 1.



Respuestas completas la lista de verificación aplicada al participante 2.



The bottom line

If you achieve these you can ignore the rest of the checklist. Your process is fine.

- [x] Delivering **working, tested software** every 4 weeks or less
- [x] Delivering what the **business needs** most
- [x] Process is **continuously improving**

Core Scrum

These are central to Scrum. Without these you probably shouldn't call it Scrum.

- [ ] Clearly defined **product owner (PO)**
  - [x] PO is **empowered** to prioritize
  - [x] PO has **knowledge** to prioritize
  - [x] PO has direct **contact with team**
  - [ ] PO has direct **contact with stakeholders**
  - [x] PO speaks **with one voice** (in case PO is a team)
- [ ] Team has a **sprint backlog**
  - [x] Highly **visible**
  - [ ] **Updated** daily
  - [ ] Owned exclusively by the **team**
- [x] **Daily Scrum** happens
  - [ ] Whole team participates
  - [ ] Problems & impediments are surfaced
- [ ] **Demo** happens after every sprint
  - [ ] Shows **working, tested software**
  - [x] **Feedback** received from stakeholders & PO
- [ ] Have **Definition of Done (DoD)**
  - [x] DoD **achievable** within each iteration
  - [ ] Team **respects** DoD
- [x] **Retrospective** happens after every sprint
  - [ ] Results in concrete improvement **proposals**
  - [ ] Some proposals actually get **implemented**
  - [ ] **Whole team + PO** participates
- [x] PO has a **product backlog (PBL)**
  - [ ] Top items are **prioritized** by business value
  - [ ] Top items are **estimated**
  - [ ] **Estimates written by the team**
  - [ ] Top items in **PBL small enough to fit** in a sprint
  - [ ] PO understands **purpose** of all backlog items
- [x] Have **sprint planning meetings**
  - [ ] **PO participates**
  - [ ] PO brings **up-to-date PBL**
  - [ ] **Whole team** participates
  - [ ] Results in a **sprint plan**
  - [ ] Whole team believes plan is **achievable**
  - [ ] PO **satisfied with priorities**
- [x] Timeboxed **iterations**
  - [ ] Iteration length **4 weeks or less**
  - [ ] Always **end on time**
  - [ ] Team **not disrupted or controlled** by outsiders
  - [ ] Team usually **delivers what they committed to**
- [ ] Team members **sit together**
  - [ ] **Max 9 people** per team

the unofficial **Scrum Checklist**

crisp

Henrik Kniberg

Recommended but not always necessary

Most of these will usually be needed, but not always all of them. Experiment!

- [x] Team **has all skills** needed to bring backlog items to Done
- [x] Team members **not locked into specific roles**
- [ ] Iterations that are **doomed to fail** are terminated early
- [x] PO has **product vision** that is in sync with PBL
- [x] PBL and product vision is **highly visible**
- [x] Everyone on the **team participates in estimating**
- [x] **PO available** when team is estimating
- [x] Estimate **relative size** (story points) rather than time
- [x] Whole team knows top 1-3 **impediments**
  - [x] **SM has strategy** for how to fix top impediment
  - [x] **SM focusing** on removing impediments
  - [x] **Escalated to management** when team can't solve
- [x] Team has a **Scrum Master (SM)**
  - [x] SM **sits with the team**
- [x] PBL items **are broken into tasks** within a sprint
  - [x] Sprint tasks are **estimated**
  - [x] Estimates for ongoing tasks are **updated daily**
- [x] **Velocity** is measured
  - [x] All items in sprint plan have an **estimate**
  - [x] PO uses velocity for **release planning**
  - [x] Velocity only includes items that are **Done**
- [x] Team has a **sprint burndown chart**
  - [x] Highly **visible**
  - [x] **Updated** daily
- [x] **Daily Scrum** is every day, same time & place
  - [x] **PO participates** at least a few times per week
  - [x] Max **15 minutes**
  - [x] Each team member **knows what the others are doing**

Scaling

These are pretty fundamental to any Scrum scaling effort.

- [x] You have a **Chief Product Owner** (if many POs)
- [x] Dependent teams do **Scrum of Scrums**
- [x] Dependent teams **integrate within each sprint**

Positive indicators

Leading indicators of a good Scrum implementation.

- [x] **Having fun!** High energy level.
- [x] **Overtime work is rare** and happens voluntarily
- [x] Discussing, criticizing, and **experimenting** with the process

PO = Product owner **SM** = Scrum Master **PBL** = Product Backlog **DoD** = Definition of Done

http://www.crisp.se/scrum/checklist | Version 2.2 (2010-10-04)

6.7. Anexo VII – Herramientas tecnológicas para el apoyo de la gestión de servicios en el Departamento de TI de Intel.

ServiceNow
ServiceNow es un producto para automatizar las operaciones de Tecnología de Información de las empresas a través de un conjunto de aplicaciones que automatizan los flujos de trabajo y proporcionan la integración entre los procesos de negocio relacionados. Es un producto de paga.

JIRA
JIRA es una aplicación basada en web para el seguimiento de errores, de incidentes, de solicitudes de servicio y para la gestión operativa de proyectos. Permite crear historias de usuario y distribuir tareas entre los miembros el equipo de trabajo, entre muchas otras funcionalidades. Es un producto de paga.

Puppet
Puppet es una herramienta tecnológica que permite conocer en detalle la infraestructura de TI conformada por los componentes físicos en centros de datos, entornos virtualizados, servicios de infraestructura en la nube o en contenedores. Puppet mantiene la configuración en un estado determinado de forma automática, asegurando la consistencia e integridad de los sistemas, mientras permite aplicar los cambios de manera ágil conforme evoluciona la empresa. Es un producto que existe en su versión de código abierto y versión de paga.

System Center Operations Manager (SCOM)
SCOM permite supervisar infraestructuras de manera flexible y eficiente, contribuye a garantizar la regularidad del rendimiento y la disponibilidad de aplicaciones críticas, además de permitir la supervisión completa de nubes y centros de datos públicos y privados. Es un producto de paga.

Jenkins
Jenkins es una herramienta de código abierto que, mediante un gran número de complementos, permite la automatización de la puesta en operación del código de cualquier tipo de software a través de procesos de integración continua y entrega continua.

Docker
Docker es una plataforma de software que le permite crear, probar e implementar aplicaciones rápidamente. Docker empaqueta software en unidades estandarizadas llamadas contenedores que incluyen todo lo necesario para que el software se ejecute, incluidas bibliotecas, herramientas de sistema, código y tiempo de ejecución. Es un producto de código abierto.

Git

Git es un sistema distribuido de control de código fuente o SCM (en inglés Source Code Management). Permite el control de versiones y el trabajo simultáneo de los equipos de trabajo sobre un mismo repositorio o conjunto de archivos que contienen el código fuente. Es un producto de código abierto.

TeamCity

TeamCity es una herramienta que permite la implementación de procesos de integración continua de forma automática. Es un producto de paga.

CA Agile Central

CA Agilice Central es una plataforma empresarial diseñada para apoyar la implementación de desarrollo de software mediante prácticas ágiles de forma escalable. Es un producto de paga.

7. Capítulo VII: Bibliografía

Atlassian. (2016). *La herramienta de desarrollo de software líder de los equipos ágiles*. Obtenido de https://es.atlassian.com/software/jira?_mid=5af657d8be8528ba700948433f060358&aceid=&adposition=1t1&adgroup=20440470982&campaign=325695382&creative=81925779382&device=c&keyword=jira&matchtype=p&network=g&placement=&gclid=CjwKEAjwnebABRCjpvr13dHL8DsSJABB-ILJmFJPF8crZDD0Y86Slk2OwQpz6bCefYbRnYX_45lTzBoC2Y3w_wcB

Axelos. (2015). *ITIL®*. Obtenido de https://www.axelos.com/best-practice-solutions/itil

Axelos. (2016a). *ITIL®*. Obtenido de https://www.axelos.com/best-practice-solutions/itil

Axelos. (2016b). *The Key Benefits of ITIL*. Obtenido de https://www.axelos.com/Corporate/media/Files/Key%20Benefits/ITIL_Value_Proposition.pdf

BPM-Offensive Berliner. (27 de 10 de 2015). *BPMNPoster*. Recuperado de http://www.bpmb.de/index.php/BPMNPoster

Bernal, C. A. (2010). *Metodología de la Investigación*. Bogotá: Pearson.

Best Management Practice. (2011). *ITIL® Service Operation*. Londres: TSO (The Stationery Office).

Cartlidge, A., & Lillycrop, M. (Eds.). (2012). *An Introductory Overview of ITIL® 2011.* Londres: TSO (The Stationery Of ce). Recuperado de https://www.tsoshop.co.uk/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

ClydeBank Technology. (2015). *ITIL for Beginners: The Complete Beginner's Guide to ITIL*. NA: ClydeBank Media LLC.

CMMI Institute. (2013). CMMI® para Servicios (Versión 1.3) [software]. NA: CMMI Institute.

Computer Associates. (12 de 12 de 2016). *Agile Software - CA Technologies*. Obtenido de http://www.ca.com/us/products/ca-agile-central.html

Daine, G. (30 de 8 de 2016). *ITIL® Vs. DevOps! 25 Influential Experts Share Their Insights (Is ITIL® Agile Enough?)*. Obtenido de https://purplegriffon.com/blog/is-itil-agile-enough

De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A., & Tieneke Verheijen, T. (2008). ITIL® V3 Foundation Exam - The Study Guide. (J. v. editor), Ed.) NA: Van Haren Publishing, Zaltbommel.

Dimes, T. (2015). *Conceptos Básicos de Scrum: Desarrollo de software Agile y manejo de proyectos Agile*. NA: Babelcube Inc.

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2013). Fundamentals of Business Process Management. Berlin: Springer.

Strauss, K. (2016). *The World's Most Reputable Companies, 2016*. Obtenido de http://www.forbes.com/sites/karstenstrauss/2016/03/22/the-worlds-most-reputable-companies-2016/#49b39baf4f95

Hazzan, O., & Dubinsky, Y. (2009). *Agile Software Engineering*. Londres: Springer-Verlag.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2010). *Metodología de la Investigación*. México: McGraw-Hill.

Intel. (2016). Intel 2016 Corporate Overview. Recuperado de https://www.intel.com/content/www/us/en/company-overview/company-overview.html

Interbrand Best Global Brands. (2015). *Best Global Brands*. Recuperado de http://interbrand.com/best-brands/best-global-brands/2015/

ISACA. (2012). COBIT 5: *A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows: ISACA.

Kniberg, H., & Skarin, M. (2010). *Kanban y Scrum – Obteniendo lo mejor de ambos*. Obtenido de http://www.proyectalis.com/documentos/KanbanVsScrum_Castellano_FINAL-printed.pdf

Loukides, M. (2012). *What is DevOps?* NA: O'Reilly Media.

New Relic. (20 de 2 de 2017). *New Relic Kickstarting DevOps e-Book*. Obtenido de https://try.newrelic.com/rs/newrelic/images/NewRelic-Kickstarting-Devops-eBook.pdf

Schwaber, K., & Sutherland, J. (1 de 6 de 2016). *Download the official Scrum Guide*. Recuperado de http://www.scrumguides.org/download.html

ServiceNow. (2016). IT Service Management. Obtenido de https://www.servicenow.com/solutions/it-service-management.html

UCISA. (2 de 11 de 2016). *Service Operation*. Obtenido de https://www.ucisa.ac.uk/representation/activities/ITIL/serviceoperation

Walls, M. (2013). *Building a DevOps Culture*. NA: O'Reilly Media.