



# Gestión de Incidentes

## ESTRUCTURA DE CONTENIDOS

1. Definición.
2. Procesos para la gestión de incidentes.
  - 2.1. Identificación y Registro.
  - 2.2. Clasificación y Priorización.
    - 2.2.1. Tipos de Incidencias.
  - 2.3. Diagnóstico Inicial y Escalado.
  - 2.4. Investigación y diagnóstico.
  - 2.5. Resolución y recuperación.
  - 2.6. Cierre.

Recursos Bibliográficos.

Glosario.

## INTRODUCCIÓN

Cuando la calidad en un servicio se reduce considerablemente o se produce una interrupción no controlada, es necesario contar con las herramientas o metodologías apropiadas para afrontar la situación y proporcionar una solución rápida y eficaz a la situación.

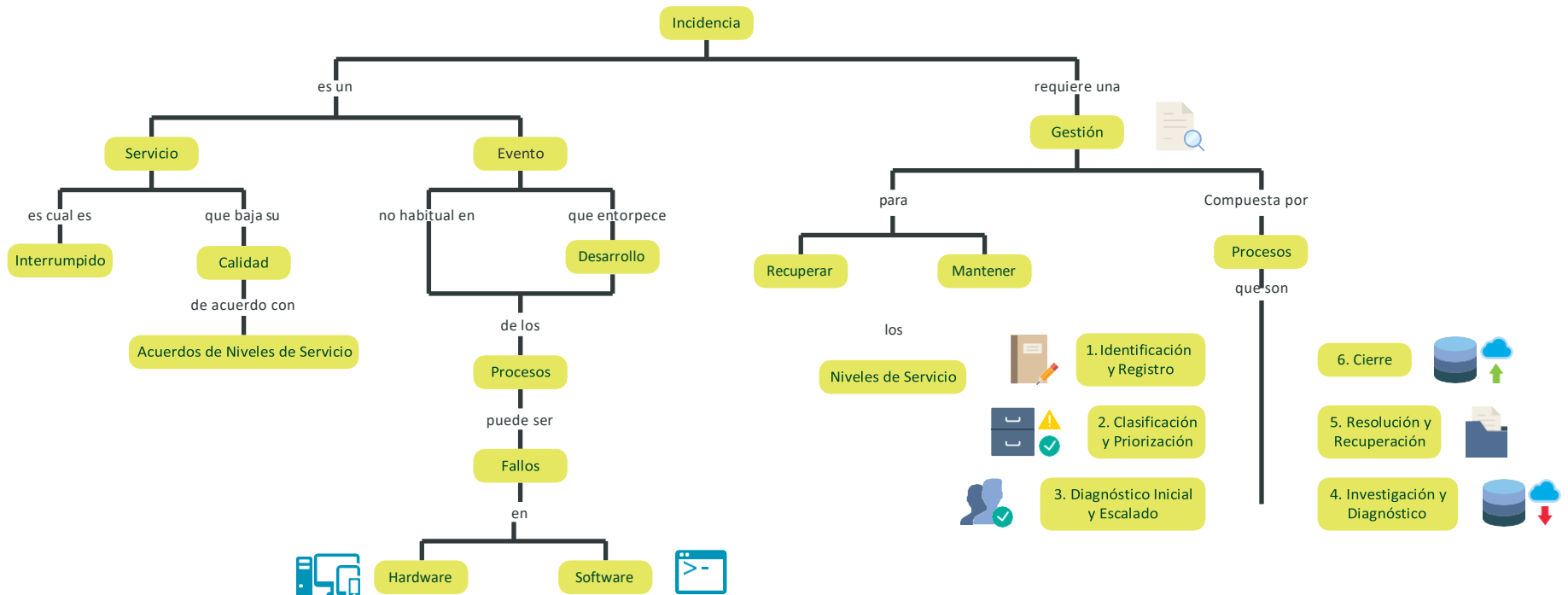
Para afrontar este tipo de eventualidades, se requiere tener claras las actividades que como técnico de soporte, permitirán dar respuesta efectiva a los diferentes tipos de situaciones que se puedan presentar.

Si se realiza una correcta Gestión, se está garantizando el cumplimiento de los Niveles de Servicios establecidos, propendiendo por la productividad de los usuarios, optimizando recursos y aprovechando los procesos de monitorización y control.

En caso contrario, se crearía un clima de insatisfacción con los usuarios, desperdicio de recursos tratando de solucionar incidentes.



## MAPA CONCEPTUAL



## 1. DEFINICIÓN



La terminología de la Biblioteca de Infraestructura de Tecnologías de Información (denominada ITIL por sus siglas en inglés), define un incidente como: "Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. El objetivo de ITIL es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible."<sup>1</sup>

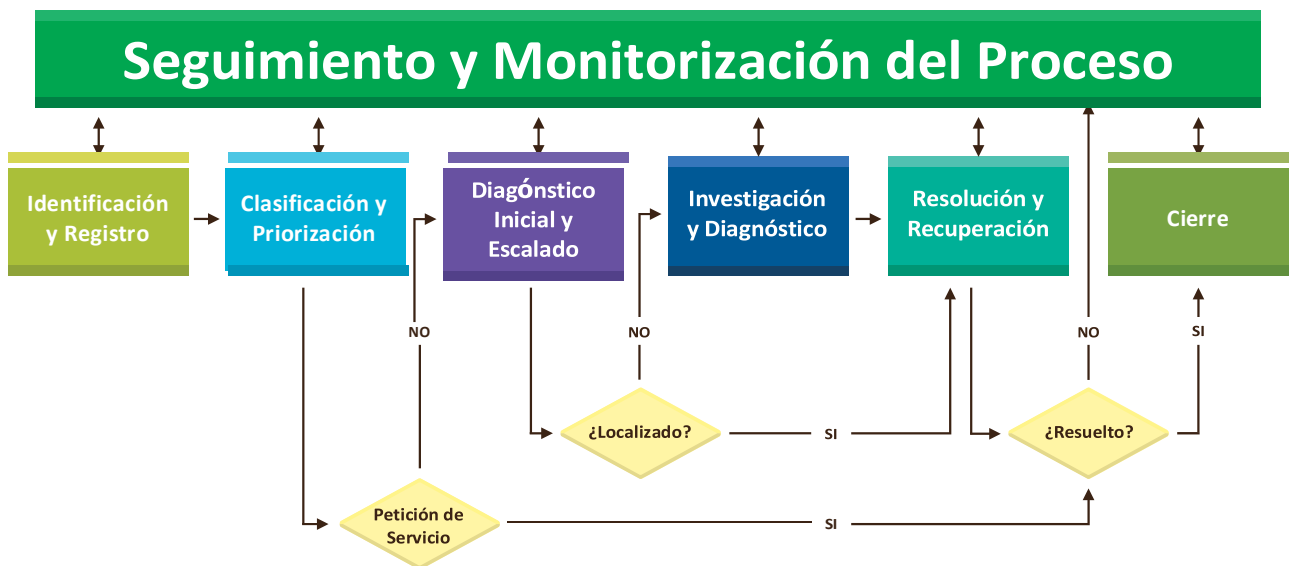
La Gestión de Servicios de Tecnologías de la Información incluye dentro de sus áreas de procesos la gestión de incidentes, que busca recuperar o mantener los niveles de servicio acordados, garantizando la disponibilidad y calidad en los servicios.

<sup>1</sup> ITIL Incident Management - The ITIL Open Guide



## 2. PROCESOS PARA LA GESTIÓN DE INCIDENTES.

Los procesos presentados por ITIL para realizar la gestión de incidentes se resumen en la siguiente gráfica que muestra el ciclo de vida de la gestión de incidentes:



### 2.1. IDENTIFICACIÓN Y REGISTRO



Las incidencias pueden ser reportadas a partir de diferentes fuentes como son: usuarios, operaciones de monitoreo o soporte técnico. Al recibir un reportese debe hacer el registro de forma inmediata con la información básica requerida para procesar el incidente tal como: fecha y hora, descripción del incidente y usuarios afectados (dependiendo del tipo de incidente es posible que se haga necesario notificar a otros usuarios).

Es común que varios usuarios reporten la misma incidencia, así que este proceso requiere verificar que el incidente no haya sido registrado aún y además que este incluido dentro de los Acuerdos de Niveles de Servicio.

La identificación y registro debe generar un número de referencia que identifique el incidente, facilite su consulta, seguimiento y las comunicaciones con los usuarios, también se debe asignar un estado inicial (registrado, activo u otro).

## 2.2. CLASIFICACIÓN Y PRIORIZACIÓN



Se deben clasificar los incidentes para lo cual es importante definir un nivel de prioridad el cual estará basado en el impacto que tiene sobre los procesos funcionales y el número de usuarios que afecta, otro factor clave para la clasificación es el tiempo máximo en que espera el usuario sea resuelto el incidente, esto dependiendo de los acuerdos de niveles de servicio pactados.

Los recursos asignados a la atención y solución del incidente dependerán de la clasificación que se le haya determinado.

Se requiere entonces definir los niveles de clasificación de los incidentes y asignarles un plan de atención donde se especifique rango de tiempo y recursos, así como un posible cambio de estado (activo, en proceso, suspendido, resuelto, cerrado, etc.).

## TIPOS DE INCIDENTES

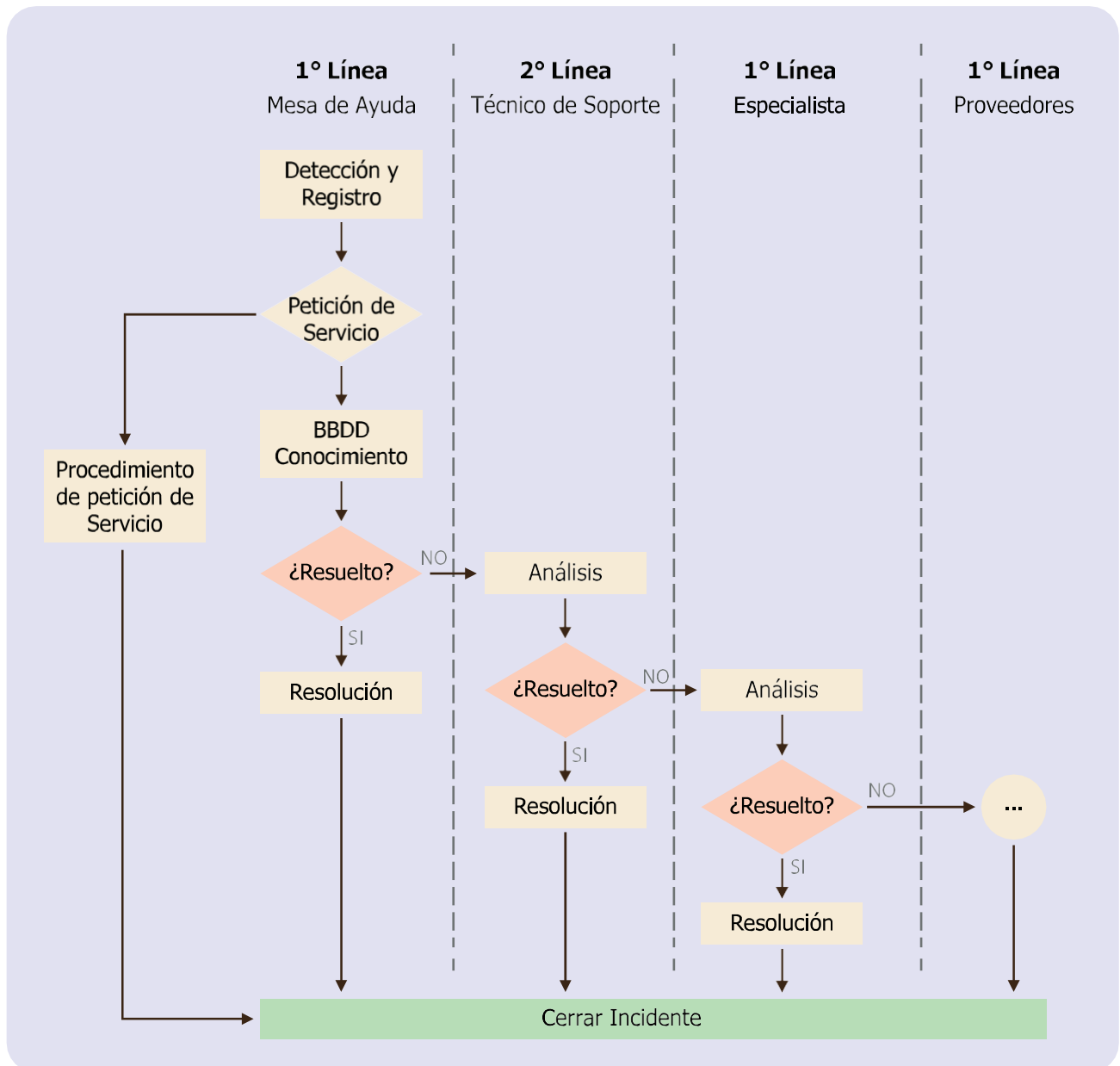
- A nivel de Software.
  - ❖ Error de ingreso al sistema operativo.
  - ❖ Fallo al cargar la aplicación.
- Hardware.
  - ❖ Dispositivos no funcionan correctamente.
  - ❖ Problemas de fluido eléctrico en el equipo de cómputo.

## 2.3. DIAGNÓSTICO INICIAL Y ESCALADO

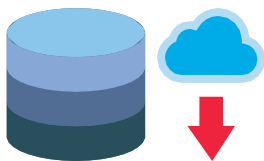


Una vez que el incidente fue clasificado y priorizado, se procede a realizar un diagnóstico inicial del incidente, teniendo en cuenta si es una actividad que puede ser atendida desde los técnicos de soporte técnico.

En algunos casos no se puede resolver en primera instancia, así que se procede a realizar el escalado, bien sea funcional o jerárquico. El escalado funcional corresponde a la necesidad de atención por parte de un especialista de más alto nivel; el escalado jerárquico es aquel en el que se requiere de un responsable con mayor autoridad para la toma de decisiones que corresponden a la solución del incidente.



## 2.4. INVESTIGACIÓN Y DIAGNÓSTICO



La base de datos de conocimiento KB (Knowledge DataBase, por sus siglas en Inglés) es el lugar donde reside la información respecto a los posibles incidentes y su método de solución, allí se busca el incidente y se define la gestión para lograr su solución. En caso de no encontrar la solución en la KB se consulta a un experto o si es necesario se realiza el escalamiento a un nivel superior de acuerdo con los protocolos establecidos para esto.

La KB debe ser actualizada con los datos de seguimiento a los incidentes presentados, así como el registro de nuevos procedimientos adoptados para la resolución de incidentes nuevos o ya registrados. Esto a futuro evitará escalamientos innecesarios y permitirá aprovechar el conocimiento adquirido durante la solución de un incidente. Es recomendable tener también una base de datos donde se registren las configuraciones actuales con los incidentes registrados para poder establecer el efecto que esto tenga en la solución del incidente.

Es necesario mantener al usuario informado del progreso o estado de la incidencia o petición de servicio y en caso que se afecten los niveles de servicio establecidos, establecer de común acuerdo las acciones a realizar.

## 2.5. RESOLUCIÓN Y RECUPERACIÓN



La base de conocimiento (KB) debe contener información sobre los procedimientos a seguir para cada tipo de incidente registrado allí. La información allí almacenada debe incluir:

- Errores conocidos.
- Gestión de la configuración.
- Resolución de problemas.
- Gestión de Impacto.

En ocasiones la solución al incidente se centra en cambios en infraestructura, lo cual debe informarse a las instancias correspondientes. En estos casos se hace necesario también analizar y planificar el proceso de cambio para garantizar que se realice en condiciones óptimas que permiten asegurar la calidad y niveles de servicio establecidos.

Cuando el incidente se presenta continuamente y no se ha encontrado una solución definitiva, debe ser informado para realizar una investigación más detallada de las causas y posible corrección.

## 2.6. CIERRE



Una vez que se haya solucionado el incidente se espera realizar las siguientes actividades:

- Confirmar con los usuarios la atención y solución del incidente.
- Actualizar la KB con el proceso utilizado para resolver el incidente y en caso de ser necesario reclasificar el incidente.
- Cerrar incidente.



Parte fundamental del cierre del incidente, es la realización de informes que permitan evaluar y controlar el proceso mismo.

Los objetivos a cubrir con la realización de informes son:

- Presentar a los Usuarios la información sobre el cumplimiento de los acuerdos de servicios.
- Determinar acciones correctivas en caso de incumplimiento de los Acuerdos de niveles de Servicios no justificados.
- Monitorear las actividades administrativas relacionadas con el "Centro de Soporte".
- Controlar los procesos, determinando si se han seguido los protocolos establecidos y se han asignado correctamente los recursos.
- Identificar errores en la definición de procesos o protocolos para aplicar las medidas correctivas.
- Obtener información que sirva de soporte para identificación de costos asociados al servicio, necesidades de infraestructura, recursos utilizados, etc.
- Dentro de las posibles métricas a incluir en los informes están:
  - ✓ Número total de incidentes
  - ✓ Tiempo promedio de resolución de incidentes
  - ✓ Tipos de incidentes más recurrentes.
  - ✓ Porcentaje de tiempo fuera de servicio
  - ✓ Número de incidentes resueltos satisfactoriamente
  - ✓ Número de incidentes reabiertos

## RECURSOS BIBLIOGRÁFICOS

ITIL (Information Technology Infrastructure Library) (2012). Glosario de Términos ITIL, Definiciones y Acrónimos. Consultado en mayo de 2012 en: [www.itil-officialsite.com](http://www.itil-officialsite.com)

ITIL (Information Technology Infrastructure Library) (2012). Open Guide. Consultado en mayo de 2012 en: <http://www.itlibrary.org/index.php?page=ITIL>

Osiatis (2012). ITIL-Gestión de Servicios TI. Consultado en mayo de 2012 en: [http://itil.osiatis.es/Curso\\_ITIL/Gestion\\_Servicios\\_TI/gestion\\_de\\_incidentes/vision\\_general\\_gestion\\_de\\_incidentes/vision\\_general\\_gestion\\_de\\_incidentes.php](http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php)

## GLOSARIO

**Aceptación:** Acuerdo formal que indica que un Servicio de TI, Proceso, Plan, u otro Entregable se han completado, es preciso, Confiable y cumple con los Requisitos especificados.

**Alerta:** Advertencia de que se ha superado un umbral, de que algo ha cambiado, o de que hubo un Fallo.

**Base de Conocimiento [Knowledge Base]:** Base de datos lógica que contiene los datos empleados por el Sistema de Gestión del Conocimiento del Servicio.

**Diagnóstico:** Una etapa en Ciclo de vida de Incidentes y Problemas. El propósito de Diagnóstico es identificar un Alternativa (solución temporal) para un Incidente o la Causa Raíz de un Problema.

**ITIL:** Del inglés Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información.

**Monitorear:** Acción que permite supervisar o controlar las operaciones realizadas utilizando medios físicos o a través de aplicaciones de software

## CONTROL DE DOCUMENTO

## GESTIÓN DE INCIDENTES

**Desarrollador  
de contenido  
Experto temático**

Ana Yaqueline Chavarro  
Joselin Sanabria

**Asesor Pedagógico**

Rafael Neftalí Lizcano Reyes  
Claudia Milena Hernandez Naranjo

**Productor Multimedia**

Luis Gabriel Urueta Alvarez

**Productor de Audios**

Victor Hugo Tabares Carreño

**Programador**

Daniel Martínez Díaz

**Líder Expertos  
Temáticos**

Hugo García Calderón

**Líder Línea  
de Producción**

Santiago Lozada Garces

## Atribución, no comercial, compartir igual

Este material puede ser distribuido, copiado y exhibido por terceros si se muestra en los créditos. No se puede obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.



**Creative Commons**