Gestión de Incidentes

La **Gestión de Incidentes** tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

La **Gestión de Incidentes** no debe confundirse con la **Gestión de Problemas**, pues a diferencia de esta última, no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas.

Las propiedades y funcionalidades de la **Gestión de Incidentes** se resumen sucintamente en el siguiente interactivo:

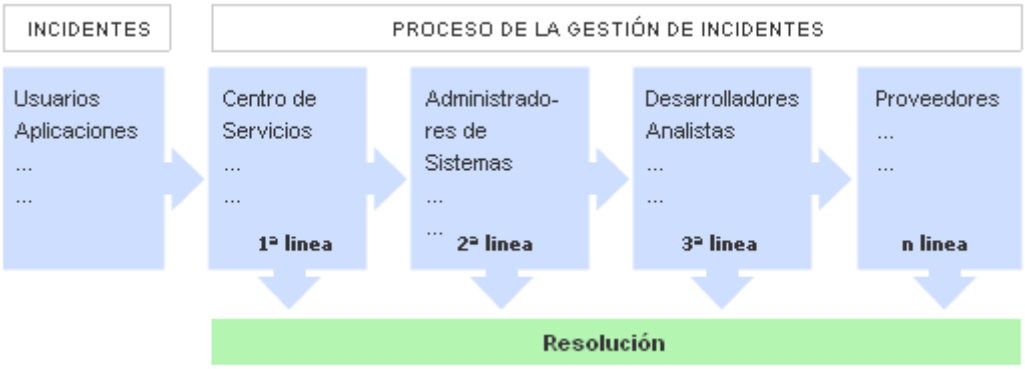
Introducción y Objetivos

Los objetivos principales de la **Gestión de Incidentes** son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el **SLA** correspondiente.

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el **Centro de Servicios** (**Service Desk**) debe jugar una papel esencial en el mismo.

El siguiente diagrama resume el proceso de gestión de incidentes:



Aunque el concepto de incidencia se asocia naturalmente con cualquier malfuncionamiento de los sistemas de hardware y software según el libro de Soporte del Servicio de ITIL un incidente es:

"*Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo*".

Por lo que casi cualquier llamada al **Centro de Servicios** puede clasificarse como un incidente, lo que incluye a las **Peticiones de Servicio** tales como concesión de nuevas licencias, cambio de información de acceso, etc. siempre que estos servicios se consideren estándar.

Cualquier cambio que requiera una modificación de la infraestructura **no** se considera un servicio estándar y requiere el inicio de una Petición de Cambio **(RFC)** que debe ser tratada según los principios de la **Gestión de Cambios**.

Los principales beneficios de una correcta **Gestión de Incidentes** incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio acordados en el **SLA**.
- Mayor control de los procesos y monitorización del servicio.
- Optimización de los recursos disponibles.

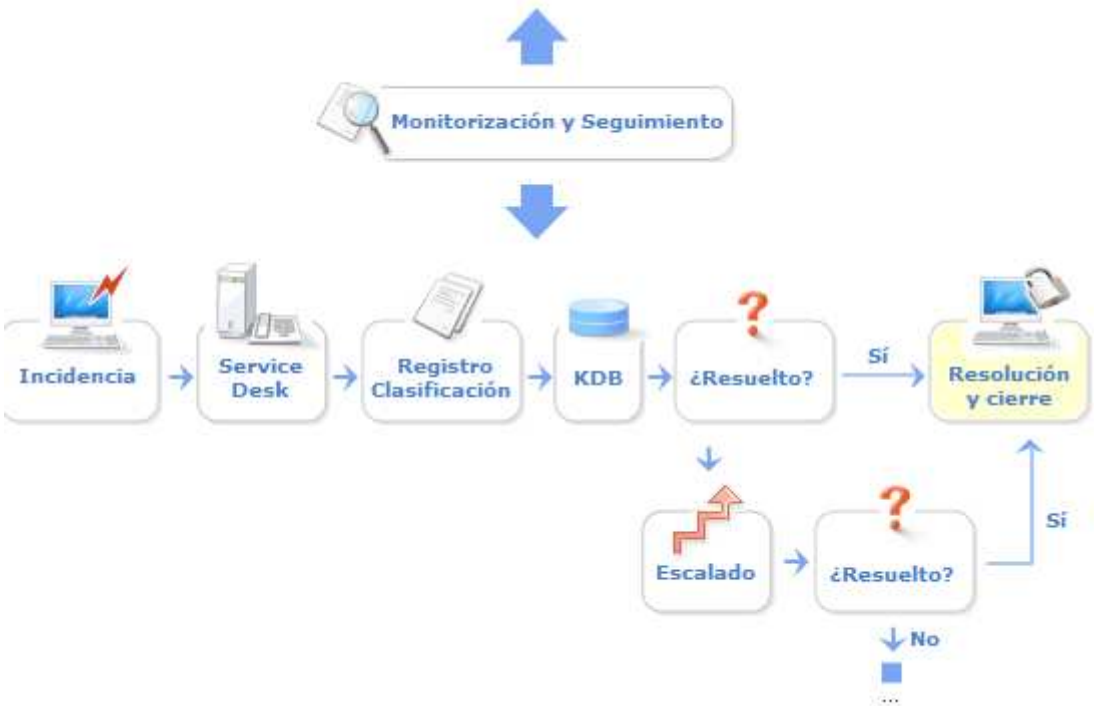
- Una **CMDB** más precisa pues se registran los incidentes en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

Por otro lado una incorrecta **Gestión de Incidentes** puede acarrear efectos adversos tales como:

- Reducción de los niveles de servicio.
- Se dilapidan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución del incidente.
- Se pierde valiosa información sobre las causas y efectos de los incidentes para futuras reestructuraciones y evoluciones.
- Se crean clientes y usuarios insatisfechos por la mala y/o lenta gestión de sus incidentes.

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

- No se siguen los procedimientos previstos y se resuelven las incidencias sin registrarlas o se escalan innecesariamente y/o omitiendo los protocolos preestablecidos.
- No existe un margen operativo que permita gestionar los "picos" de incidencias por lo que éstas no se registran adecuadamente e impiden la correcta operación de los protocolos de clasificación y escalado.
- No están bien definidos los niveles de calidad de servicio ni los productos soportados. Lo que puede provocar que se procesen peticiones que no se incluían en los servicios previamente acordados con el cliente.



Clasificación del Incidente

Es moneda frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basa esencialmente en dos parámetros:

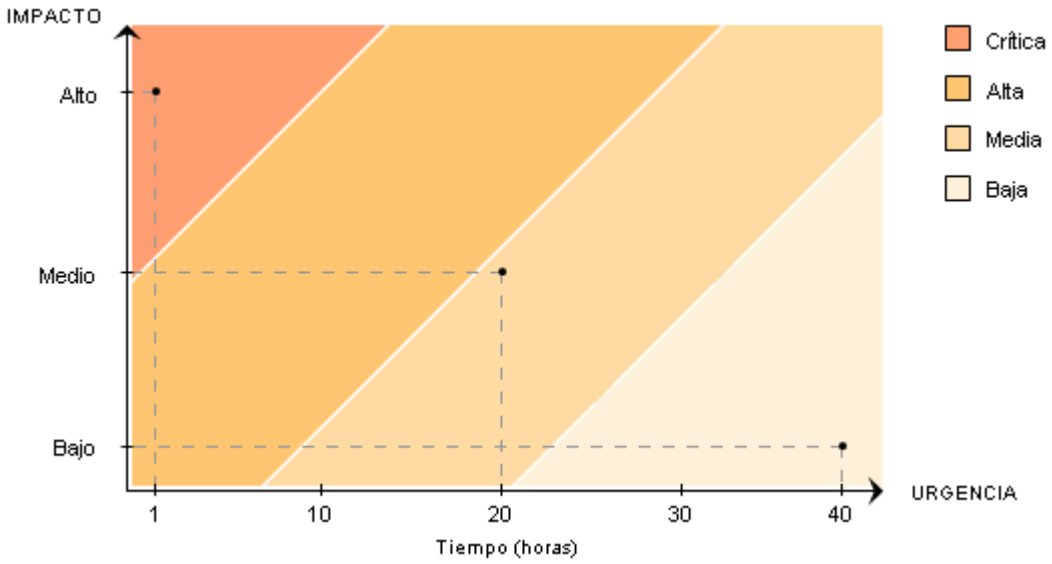
- **Impacto:** determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.
- **Urgencia:** depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio acordado en el **SLA**.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes "sencillos" se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente.

La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un posible "diagrama de prioridades" en función de la urgencia e impacto del incidente:



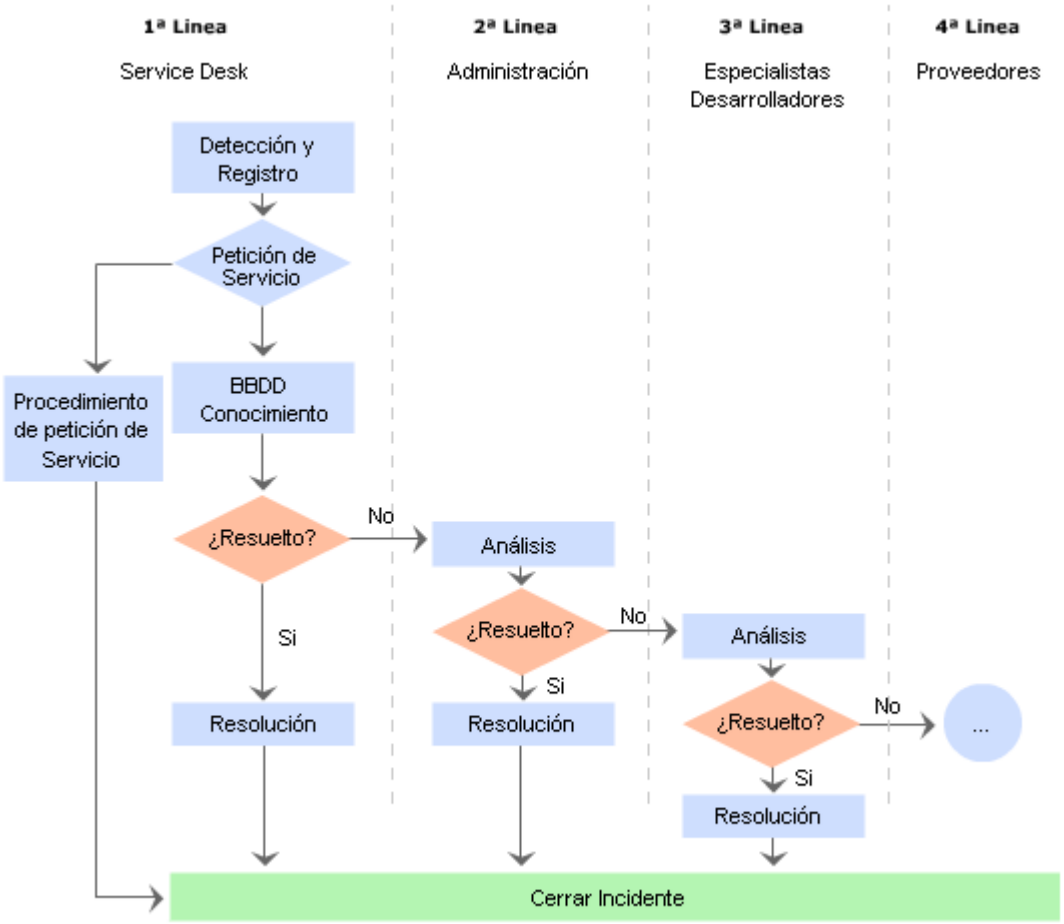
Escalado y Soporte

Es frecuente que el **Centro de Servicios** no se vea capaz de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina **escalado**.

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional**: Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.
- **Escalado jerárquico:** Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapen de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.

El proceso de escalado puede resumirse gráficamente* como sigue:



* El escalado puede incluir más niveles en grandes organizaciones, o por el contrario , integrar diferentes niveles en el caso de PYMES

Proceso

El siguiente diagrama muestra los procesos implicados en la correcta **Gestión de Incidentes**:

Nota: los botones del gráfico permiten acceder a información mas detallada sobre la interrelación con otros procesos TI

Registro y Clasificación de Incidentes

Registro

La admisión y registro del incidente es el primer y necesario paso para una correcta gestión del mismo.

Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, el mismo **Centro de Servicios** o el soporte técnico, entre otros.

El proceso de registro debe realizarse inmediatamente pues resulta mucho más costoso hacerlo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

- La admisión a trámite del incidente: el **Centro de Servicios** debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el **SLA** del cliente y en caso contrario reenviarlo a una autoridad competente.
- Comprobación de que ese incidente aún no ha sido registrado: es moneda corriente que más de un usuario notifique la misma incidencia y por lo tanto han de evitarse duplicaciones innecesarias.
- **Asignación de referencia**: al incidente se le asignará una referencia que le identificará unívocamente tanto en los procesos internos como en las comunicaciones con el cliente.
- **Registro inicial**: se han de introducir en la base de datos asociada la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados...).
- **Información de apoyo**: se incluirá cualquier información relevante para la resolución del incidente que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia **CMDB** (hardware interrelacionado), etc.
- **Notificación del incidente**: en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.

Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- **Categorización**: se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente.
- **Establecimiento del nivel de prioridad**: dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de prioridad.
- **Asignación de recursos**: si el **Centro de Servicios** no puede resolver el incidente en primera instancia designara al personal de soporte técnico responsable de su resolución (segundo nivel).
- **Monitorización del estado y tiempo de respuesta esperado**: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al **SLA** correspondiente y la prioridad.

Análisis, Resolución y Cierre de Incidentes

En primera instancia se examina el incidente con ayuda de la **KB** para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

Si la resolución del incidente se escapa de las posibilidades del **Centro de Servicios** éste redirecciona el mismo a un nivel superior para su investigación por los expertos asignados. Si estos expertos no son capaces de resolver el incidente se seguirán los protocolos de escalado predeterminados.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo.

Si fuera necesario se puede emitir una **Petición de Cambio (RFC)**. Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la **Gestión de Problemas** para el estudio detallado de las causas subyacentes.

Cuando se haya solucionado el incidente se:

- Confirma con los usuarios la solución satisfactoria del mismo.
- Incorpora el proceso de resolución a la **KB**.
- Reclasifica el incidente si fuera necesario.
- Actualiza la información en la **CMDB** sobre los elementos de configuración **(CI)** implicados en el incidente.
- Cierra el incidente.

Control del Proceso

La correcta elaboración de informes forma parte esencial en el proceso de **Gestión de Incidentes**.

Estos informes deben aportar información esencial para, por ejemplo:

- La **Gestión de Niveles de Servicio**: es esencial que los clientes dispongan de información puntual sobre los niveles de cumplimiento de los **SLAs** y que se adopten medidas correctivas en caso de incumplimiento.
- Monitorizar el rendimiento del **Centro de Servicios**: conocer el grado de satisfacción del cliente por el servicio prestado y supervisar el correcto funcionamiento de la primera línea de soporte y atención al cliente.
- Optimizar la asignación de recursos: los gestores deben conocer si el proceso de escalado ha sido fiel a los protocolos preestablecidos y si se han evitado duplicidades en el proceso de gestión.
- Identificar errores: puede ocurrir que los protocolos especificados no se adecuen a la estructura de la organización o las necesidades del cliente por lo que se deban tomar medidas correctivas.
- Disponer de Información Estadística: que puede ser utilizada para hacer proyecciones futuras sobre asignación de recursos, costes asociados al servicio, etc.

Por otro lado una correcta **Gestión de Incidentes** requiere de una infraestructura que facilite su correcta implementación. Entre ellos cabe destacar:

- Un correcto sistema automatizado de registro de incidentes y relación con los clientes
- Una Base de Conocimiento **(KB)** que permita comparar nuevos incidentes con incidentes ya registrados y resueltos. Una **(KB)** actualizada permite:

  Evitar escalados innecesarios.

  Convertir el "know how" de los técnicos en un activo duradero de la empresa.

  Poner directamente a disposición del cliente parte o la totalidad de estos datos (a la manera de **FAQs**) en una Extranet. Lo que puede permitir que a veces el usuario no necesite siquiera notificar la incidencia.
- Una **CMDB** que permita conocer todas las configuraciones actuales y el impacto que estas puedan tener en la resolución del incidente.

Para el correcto seguimiento de todo el proceso es indispensable la utilización de métricas que permitan evaluar de la forma más objetiva posible el funcionamiento del servicio. Algunos de los aspectos clave a considerar son:

- Número de incidentes clasificados temporalmente y por prioridades.
- Tiempos de resolución clasificados en función del impacto y la urgencia de los incidentes.

- Nivel de cumplimiento del **SLA**.
- Costes asociados.
- Uso de los recursos disponibles en el **Centro de Servicios**.
- Porcentaje de incidentes, clasificados por prioridades, resueltos en primera instancia por el **Centro de Servicios**.
- Grado de satisfacción del cliente.

Caso Práctico

El **Service Desk** de "Cater Matters" ha recibido una llamada del encargado de suministros del comedor de uno de sus clientes.

Dicho encargado informa de que a pesar de haber solicitado una nueva partida de helados hace unos días a través de la web ésta aún no se ha recibido y apenas quedan reservas en sus frigoríficos

El operador del **Service Desk** busca en la base de datos de pedidos y confirma que se realizó el pedido hace varios días pero también observa que éste se ha guardado defectuosamente.

El operador intenta desde su puesto repetir la orden pero el sistema sigue fallando.

El operador toma, basándose en los protocolos establecidos, las siguientes decisiones:

- Evalúa la prioridad: aunque el impacto es bajo, el incidente es urgente pues el cliente necesita rápidamente el suministro.
- Registra los datos del incidente.
- Consulta la **Base de Conocimiento** para investigar si el incidente es consecuencia de un **error conocido** y cuáles son las posibles soluciones temporales
- Propone una solución temporal al cliente: indica una zona reservada de la web desde la que se pueden realizar pedidos "urgentes" vía email.
- Contacta con el departamento de sistemas previendo que el incidente pueda repetirse a lo largo de la mañana.
- Consulta, mediante la aplicación que monitoriza las existencias de almacén, la disponibilidad de los helados solicitados.
- Tranquiliza al cliente asegurándole que mediante su servicio express recibirá los helados solicitados antes del mediodía.

Por otro lado el departamento de sistemas:

- Realiza una serie de pruebas y comprueba que, de manera general, el sistema funciona correctamente.
- No consigue identificar la causa del incidente.
- Contacta con el **Service Desk** y propone que se eleve el problema a la **Gestión de Problemas** pero pre-calificando su prioridad como baja.

El **Service Desk** recibe la información y determina que:

- Dado el bajo impacto del incidente y el hecho de que se haya proporcionado al cliente una solución temporal satisfactoria no se requiere un escalado superior.
- Registra la solución temporal del incidente junto a la información proporcionada por el departamento de sistemas.
- Da por cerrado el incidente.