Gestión de Incidentes

La **gestión de incidentes** es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan.

Los incidentes que no pueden ser resueltos rápidamente por el equipo de ayuda al usuario, son asignados a un especialista del equipo de soporte técnico. La resolución del incidente debe ser ejecutada lo antexs posible para restaurar el servicio rápidamente.

Índice

Definición

La terminología ITIL 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.

Incidentes, problemas y errores conocidos

Un incidente puede coincidir con un “problema conocido” (fallo sin un origen conocido) o con un “error conocido” (fallo con origen conocido) bajo el control de la gestión de problemas y registrado en la base de datos de errores conocidos.

En el caso de que se hayan determinado algunas estrategias de resolución de problemas, el acceso a ellas por parte del servicio técnico permitirá una mayor velocidad a la hora de resolverlas. Cuando un incidente no es el resultado de un problema conocido o un error conocido, puede ser un fallo puntual o puede ser necesario comenzar una gestión de problemas, de forma que este incidente quede registrado para futuras referencias.

Incidentes y cambios

Los incidentes son el resultado de fallos o errores en la infraestructura TI. La causa de los incidentes puede ser aparente y puede ser solucionada sin necesidad de inversiones futuras, mediante una reparación o una petición de cambio para solventar el error.

Cuando un incidente es considerado como grave, o se observan múltiples casos de incidentes similares, puede crearse el registro de un problema (el problema puede no ser registrado hasta que se haya repetido varias veces el mismo incidente). La gestión de un problema es diferente a la gestión de incidentes, se desarrolla en otro equipo de trabajo y se controla mediante la gestión de problemas. Cuando un problema se ha identificado y no se conoce la solución, el problema se convierte en un “problema conocido”. Tras identificar la causa del problema, este pasa a ser un “error conocido”. Finalmente una petición de cambio puede ser realizada para solventar el error. A partir de este punto, el proyecto es competencia de la gestión del cambio.

Una petición de un nuevo servicio no se clasifica como incidente, si no como una petición de cambio.

Procesos de gestión de incidentes

El proceso habitual de gestión de incidentes es el siguiente:

Detección y registro del incidente

Con la afectación a uno o varios usuarios, o la detección de un sistema de monitoreo, se crea una nueva incidencia, en general, en un sistema de solicitud de tickets (Ticket Request System o Help Desk)

Clasificación y soporte inicial

Como pueden recibirse múltiples incidencias al mismo tiempo, el paso siguiente es determinar el nivel de prioridad, para enviarse al personal de soporte correspondiente.

La mayoría de aplicaciones permite automatizar la asignación de incidencias para reducir los tiempos de atención, conforme a reglas de negocio, creando los criterios necesarios.

La prioridad se asigna según:

Impacto : Afectación del negocio y/o número de usuarios afectados

Urgencia : Tiempo máximo para solución y/o nivel de servicio o ANS (en inglés Service Level Agreement o SLA)

Investigación y diagnóstico

Inicialmente se deben identificar, analizar y documentar todos los síntomas. Esto ayuda a determinar la ubicación y posibles correcciones.

Escalamiento

Mecanismo para agilizar la solución oportuna que puede darse en cualquier etapa del proceso. Ocurre cuando el personal de un Nivel de Soporte transfiere el incidente hacía el siguiente nivel, por:

- Falta de conocimientos
- Poca experiencia
- Falta de recursos requeridos

Solución y restablecimiento del servicio

La rápida solución es crítica, lo importante es restablecer el servicio y mejorar la satisfacción del usuario.

Después de lo cual, se puede agregar la solución a la base de conocimiento (Knowledge Base - KB), que ayudará a disminuir los tiempos de respuesta cuando se repita una incidencia igual o similar.

Cierre del incidente

Después de restablecer el servicio y que el usuario confirme la solución del problema, se cierra la incidencia documentando detalladamente.

Si se conoce la causa, ésta se agrega a la base de conocimiento con las evidencias, análisis, descartes y solución.

Si se desconoce la causa, se genera un caso donde se analice toda la documentación y se realicen acciones tendientes a encontrala.

Monitorización, seguimiento y comunicación del incidente

El análisis de repetición de incidencias, tiempos de respuesta y solución medirán el rendimiento del área de soporte como el nivel de satisfacción del usuario

--

Ejemplos

Los incidentes deben clasificarse a medida que son reportados. Algunos ejemplos de incidentes según su clasificación son los siguientes:

- Aplicaciones
    - Servicio no disponible
    - Fallo de la aplicación
    - Capacidad del disco duro excedida
- Hardware
    - Caída del sistema
    - Alerta automática
    - Impresión