UF1881: Resolución de incidencias de redes telemáticas

Elaborado por: Pedro Mora Pérez

Edición:6.0

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16424-13-9

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa

Bienvenido a la Unidad Formativa **UF1881: Resolución de incidencias de redes telemáticas**. Esta Unidad formativa pertenece al Módulo Formativo **MF0230_3: Administración de redes telemáticas**, que forma parte del Certificado de Profesionalidad **IFCT0410: Administración y Diseño de redes departamentales**, de la familia de **Informática y Comunicaciones**.

Presentación de los contenidos

La finalidad de esta Unidad Formativa es enseñar al alumno a atender las incidencias, diagnosticando las causas de disfuncionalidad del sistema y adoptando, a su nivel, las medidas oportunas para el rápido y fiable restablecimiento de la operatividad del mismo.

Para ello, se analizará la gestión y resolución de incidencias.

Objetivos de la Unidad Formativa

Al finalizar esta Unidad Formativa aprenderás a:

– Resolver las incidencias que se produzcan llevando a cabo el diagnóstico de las averías y efectuando su reparación en el tiempo adecuado y con el nivel de calidad esperado.

Área: informática y comunicaciones

Índice

Área: informática y comunicaciones

UD1

Gestión de incidencias

1.1. Definición del concepto de incidencia
1.2. Enumeración de los objetivos de la gestión de incidencias
1.3. Identificación y descripción de las actividades
    1.3.1. Identificación
    1.3.2. Registro
    1.3.3. Clasificación
    1.3.4. Priorización
    1.3.5. Diagnóstico inicial
    1.3.6. Escalado
    1.3.7. Investigación y diagnóstico
    1.3.8. Resolución y recuperación
    1.3.9. Cierre
1.4. Explicación y ejemplificación del flujo del proceso
1.5. Ejemplificación de indicadores y métricas
1.6. Recomendaciones básicas de buenas prácticas
1.7. Sistemas de gestión de incidencias
    1.7.1. Descripción de las funcionalidades
    1.7.2. Ejemplificación y comparación de herramientas comerciales y de código abierto

1.1. Definición del concepto de incidencia

Concepto de incidencia

El concepto de incidencia, tiene un componente absolutamente abstracto, en su vertiente general, y concreto y uniforme en el campo de las redes telemáticas.

El concepto de Incidencia es entendido en el sistema de gestión de calidad de la empresa, como todo aquel suceso que tiene relación directa o indirecta sobre la marcha normal de las actividades.

Entre las diferentes actividades que se pueden clasificar, podemos encontrar las sugerencias, quejas y reclamaciones relacionadas con los diferentes clientes, proveedores o el propio personal; Igualmente, quedan englobados los materiales que se han recibido en el almacén, que no se estén conformes con el mismo, etc.

Las incidencias pueden tener su origen en el incorrecto diseño de uno o varios procesos o en la incorrecta ejecución de los procesos establecidos e incluso en la falta de recursos necesarios.

Cuando se produce un suceso anómalo en el proceso natural de las comunicaciones a cualquier nivel, bien sea por las aplicaciones que gestionen servicios, o bien por las tecnologías subyacentes de la infraestructura que soportan esos servicios, se produce una incidencia concreta y precisa del fallo en el proceso operacional.

Por lo tanto, la incidencia, es aquel suceso espontáneo y puntual, por el cual provoca un mal funcionamiento de un servicio o proceso en concreto, cuyas consecuencias de su aparición, pueden ser tan graves como leves, dependiendo de la criticidad del servicio o proceso que ha quedado afectado por la incidencia.

El componente causa/efecto, consecuencia de la aparición de una incidencia, es un elemento elemental de la incidencia, el cual delimita el concepto

de incidencia, y lo diferencia de otras incidencias azarosas, que carecen del componente causa/efecto.

En el campo de TI, una incidencia es una interrupción del servicio no planificada, donde sus efectos se despliegan en una reducción del servicio TI, o en el peor de los casos, una interrupción total del servicio, provocando daños importantes en cuanto a calidad y operatividad, además de todos aquellos cuantificables que resulten vitales en las funciones del cliente receptor de dicho servicio.

Debido a esta interrupción del servicio, evidentemente no planificada, el problema que ha generado la incidencia, debe ser tratado con cierta diligencia y sobretodo, saber definir el problema para posteriormente ver las causas que lo originaron y como última instancia, elaborar un plan que defina las fases de resolución de la incidencia en base a la definición del problema que la originó.

El concepto de incidencia, está íntimamente relacionado con la operativa en la gestión de las mismas, enmarcado dentro de un proceso de operación de servicio, encargado de gestionarlas.

Las incidencias, pueden incluir fallos o reportes por parte de los usuarios, del equipo de servicio o de un sistema de monitorización.

Al definirse el concepto de incidencia como una interrupción o reducción de la calidad no planificada del servicio, está igualmente se relaciona con una serie de conceptos básicos, estrechamente ligados al concepto de incidencia.

Estamos hablando en este caso sobre:

– **La escala de tiempo.** A partir del SLA se establecen los tiempos máximos en los que se deben responder y resolver las incidencias reportadas.

  Las herramientas de gestión deben ser utilizadas para el cálculo y la asignación de estas escalas de tiempo, y para facilitar la respuesta/resolución de las incidencias dentro de dichas escalas utilizando alertas y escalados.

– **Modelos de incidencia.** Existen incidencias que no son nuevas, sino que ya se han producido anteriormente y que se volverán a producir en el futuro.

  Muchas empresas encuentran útil la definición de modelos de incidencia que se puedan aplicar a incidencias del servicio.

  Un modelo de incidencia debería incluir:

  · Los pasos a seguir para la resolución de la incidencia.

- El orden cronológico de estos pasos y sus dependencias si las hubiera.
- Responsabilidades: quién debe hacer qué.
- Plazos para la realización de las actividades.
- Procedimientos de escalado: quién debería ser contactado y cuándo.

El uso de los modelos de incidencia permite optimizar el proceso de resolución.

Incidencias Graves

Cada servicio debe definir cuáles son los criterios para que una incidencia se considere grave. La actividad de priorización, que veremos más adelante, debe tener en cuenta estos criterios.

Las incidencias graves deben tener asociado su propio procedimiento de resolución y escalado, y una escala de tiempos menor que el resto.

El concepto de incidencia, está inmersa dentro de otros conceptos y procesos, que están interrelacionados e interdependientes con la incidencia.

Estos son:

– **Detección.** Cuanto antes se detecte una incidencia, menor será su impacto en el negocio.

  Por lo tanto, es importante monitorizar los recursos con el objetivo de detectar las potenciales incidencias y normalizar el servicio antes de que se produzca un impacto negativo en los procesos de negocio o, si esto no es posible, que el impacto sea mínimo.

– **Registro.** Todas las incidencias del servicio deben ser registradas y cada incidencia debe registrarse de forma independiente.

  La información a registrar generalmente incluye:

  - Identificador único.
  - Categorización.
  - Urgencia, impacto y prioridad.
  - Fecha y hora.

- Persona/grupo que registra la incidencia.
- Canal de entrada.
- Datos del usuario.
- Síntomas.
- Estado.
- CIs (Configuration Items, elementos de configuración) asociados.
- Persona/grupo asignado para la resolución.
- Problema/Known error asociado.
- Actividades realizadas para la resolución.
- Fecha y hora de la resolución.
- Categoría del cierre.
- Fecha y hora de cierre.

– **Categorización.** En esta actividad se establece el tipo exacto de la incidencia.

  Generalmente se establece una categorización multinivel con dependencias entre niveles. El número de niveles dependerá de la granularidad con la que necesitemos tipificar las incidencias.

  A veces, no se categoriza adecuadamente una incidencia en el momento del registro. Si esto sucede, debemos asegurarnos de que en el momento del cierre la categorización queda correctamente establecida.

– **Priorización.** Generalmente, la prioridad de la incidencia nos va a determinar cómo se ha de gestionar.

  La prioridad de la incidencia suele depender de:

  - La urgencia: rapidez con que la incidencia necesita ser resuelta.
  - El impacto: generalmente se determina por el número de usuarios afectados, aunque lo realmente importante es la criticidad para el negocio de los usuarios afectados por la incidencia. Al final, lo que

realmente determina el impacto son los aspectos adversos que la incidencia tiene en el negocio.

Es muy conveniente que la herramienta de soporte utilizada sea capaz de calcular la prioridad en base a reglas.

En cualquier caso, el equipo de soporte debe conocer estas reglas para poder priorizar adecuadamente.

Normalmente la prioridad también determina la prioridad, aunque no tiene porqué ser así.

También podría depender de si el usuario es VIP, del departamento del usuario, etc.

– **Diagnóstico inicial.** Cuando se recibe una incidencia el personal de soporte de primer nivel, en base a los síntomas, diagnostica la incidencia y la resuelve si está capacitado para ello.

Criterios para la comprensión del problema
Reformulación del problema.
Consideración y cuestionamiento de los supuestos.
Descomposición del problema hacia arriba.
Descomposición del problema hacia abajo.
Emplear múltiples perspectivas al problema.
Uso del lenguaje efectivo.
Emplear una fuerte carga emotiva.
Invertir el problema.

– **Escalado.** Existen dos tipos de escalado:

· Funcional: el soporte de primer nivel se ve incapaz de resolver la incidencia y la asigna al grupo resolutor correspondiente.

· Jerárquico: en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA), éstas se deben notificar a los responsables del servicio correspondientes.

A pesar de que se produzca un escalado, la incidencia sigue perteneciendo al equipo de Service Desk, y es éste el responsable de hacer el seguimiento de la misma y mantener informados a los usuarios hasta su cierre.

– **Investigación y diagnóstico.** En la investigación y diagnóstico, cuando se produce un fallo en el sistema, lo más probable es que se deban investigar las causas más probables, que dieron lugar a tal fallo.

  Para establecer un procedimiento que derive en la investigación de las causas más probables, se deben tener en cuenta una serie de tareas, como son:

  La catalogación y determinación del impacto de la incidencia en los sistemas.

  Determinar con exactitud qué servicios han quedado afectados, y cuáles de ellos, requieren una serie de acciones especiales.

  Investigar la existencia de indicios registrados ya conocidos, para poder establecer similitudes, y acto seguido determinar las acciones pertinentes.

– **Resolución.** Cuando se detecta una solución potencial, ésta debería ser aplicada y testeada.

  Asimismo, todas las acciones realizadas para resolver la incidencia deben registrarse en el historial de la misma.

  Una vez comprobada la resolución, la incidencia se da por resuelta y se asigna al equipo de service desk para su cierre.

– **Cierre.** Antes de cerrar la incidencia, el equipo de service desk debería validar lo siguiente:

  · El usuario está satisfecho con la resolución de la incidencia.

  · El cierre ha sido categorizado.

  · Se han cumplimentado todos los datos necesarios.

  · Decidir si es un problema recurrente. En este caso, generar un problema.

1.2. Enumeración de los objetivos de la gestión de incidencias

En la gestión de incidencias, el objetivo principal del sistema de gestión es restaurar, cuanto antes, el fallo que se ha producido en el servicio, para que el impacto en el negocio, sea minimizado al máximo.

Referente a las incidencias, no todas deben ser fallos, también podemos encontrarnos con preguntas o consultas.

Por otro lado, la gestión de incidencias, incluye varios objetivos a tener en cuenta y a cumplir, ya que este sistema implica una multitud de elementos que hacen que su objetivo principal de restaurar el servicio lo antes posible ante cualquier fallo en la infraestructura, deba de dividirse en varios procesos o subobjetivos para cumplir con el fin del sistema, que abarca múltiples procesos.

La gestión de incidencias, incluye cualquier evento que pueda producir un fallo que interrumpa o tenga potencial suficiente para interrumpirlo.

Esto, también incluye los eventos generados por los clientes, ya sea procedente del control de servicio al usuario o de herramientas destinada para tal fin.

Este proceso de gestión de incidencias, se clasifica en:

- Identificación.
- Registro.
- Categorización.
- Priorización.
- Diagnóstico inicial.
- Escalado.
- Investigación y diagnóstico.
- Resolución y restauración.
- Cierre.

Un sistema de gestión de incidencias completo y eficaz, contiene muchos procesos y actividades, en las cuales debe centrar su atención.

Por lo tanto, en la diversidad de procesos y actividades que engloban un sistema de gestión de incidencias completo, existen varios objetivos que cuelgan jerárquicamente del objetivo principal de la gestión de incidencias.

Los objetivos a cubrir por parte del sistema de gestión de incidencias son:

– Gestión de eventos.

– Gestión de incidencias.

– Gestión de peticiones.

– Gestión de problemas.

– Gestión de acceso.

– Monitorización y control de actividad.

– Operaciones de TI.

También podemos incluir como objetivos del sistema de gestión, aunque a un nivel inferior de los nombrados, ya que estos pertenecen a subprocesos, ya que se pueden considerar así porque son procesos de apoyo a la operación del servicio.

Los objetivos de los subprocesos de apoyo son:

– Gestión del cambio.

– Gestión de la capacidad.

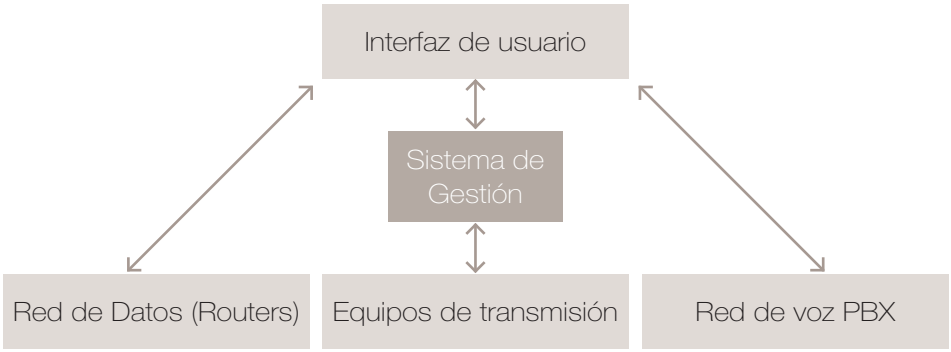
– Gestión de la disponibilidad.

– Gestión financiera.

– Gestión del conocimiento.

– Gestión de la continuidad del servicio.

– Medición y generación de informes del servicio.



Objetivos del Sistema de Gestión

El sistema de gestión tiene por objeto:

– Gestionar de forma centralizada y proactiva las alarmas procedentes de los routers del servicio.

– Proporcionar un diagnóstico de la avería producida, correlacionando la información de las diversas fuentes utilizadas.

– Proporcionar información adicional del cliente afectado por una determinada alarma.

– Definir un entorno de operación.

– Recolectar valores de rendimiento de los routers para la generación posterior de informes.

– Integración con el sistema de ticketing corporativo.

– Generación de informes.

Se ha expuesto los diferentes objetivos que pueden tener un sistema de gestión de incidencias, de una forma generalizada y sentando las bases, para establecer las líneas estratégicas de un sistema de gestión de incidencias.

1.3. Identificación y descripción de las actividades

A continuación, se hace un repaso de algunos aspectos relacionados con la operativa que se sigue en el tratamiento de tickets o actividades en la identificación y descripción de las diferentes actividades en el tratamiento de las incidencias.

Como premisa de actuación en el proceso de identificación y descripción de las actividades, todos **los técnicos asignados al área deberán entrar en el sistema, identificar las incidencias y describir las actividades del proceso, para su tratamiento completo, dentro de su ciclo de vida en el sistema de gestión de incidencias**.

Periódicamente se hará un seguimiento para comprobar si se han realizado las modificaciones solicitadas y en caso de que no se hayan hecho, se volverán a reclamar.

Todas las incidencias del servicio deben ser registradas y cada incidencia debe registrarse de forma independiente.

En todo sistema de gestión de incidencias, existe una serie de procesos o actividades, de los que se nutre el sistema de gestión de incidencias.

Estas actividades son:

- **La Gestión de Eventos.** Un evento, es un suceso que afecta directamente a la infraestructura IT subyacente. Estas notificaciones provienen por el propio servicio de IT, por los propios elementos configurables del servicio o por la herramienta de monitorización empleada para controlar los sistemas y el tráfico en la red.

  Con el fin de supervisar la infraestructura subyacente, la gestión de eventos tiene por misión la supervisión de todos los eventos que se producen en la infraestructura de TI.

  Estos eventos, como norma general, suelen estar automatizados para actuar en la incidencia y hacer un seguimiento y escalado de la misma, si fuese necesario.

  Esta gestión de eventos, puede ser implementado en cualquier parte de la gestión del servicio que tenga que ser monitorizado/gestionado.

- **La Gestión de incidencias.** Su principal cometido es restaurar cuanto antes, el servicio, el cual ha fallado o se ha visto seriamente dañado por el impacto negativo de una incidencia. Su misión es mitigar por completo o en caso contrario, minimizar los efectos adversos.