



Uruguay
Presidencia

<>agesic

Política de Gestión de Problemas

Infraestructura y Operaciones de TI

Importante: El presente documento es para trabajo interno; no para su difusión fuera del ámbito de Agesic.



Contenido

1. Introducción	1
2. Metas y objetivos del Proceso de Gestión de Problemas	1
3. Apertura de problemas	2
4. Valor y beneficio esperado	2-3
4.1 Valor y beneficio esperado	3
5. Actividades y dedicación	3-5
5.1 Registro, priorización, escalamiento y seguimiento	3
5.2 Investigación, análisis y actualización del caso.....	3-4
5.3 Diagnóstico y resolución de problemas.....	4-5
6. Roles y responsabilidades.....	5-7
6.1 Dueño y Gestor del Proceso de Problemas	5
6.2 Dueño del servicio	5
6.3 Analista de Problema (referente técnico)	6
6.4 Gestor de Problema.....	6
6.5 Mesa de Servicios - Service Desk.....	6-7
6.6 Equipo de Dirección.....	7
7. Factores críticos de éxito.....	7
8. Indicadores (KPIs)	8
9. Dificultades y desafíos	8-9
9.1 No adoptar un proceso formal para la Gestión de Problemas resulta en.....	8
9.2 Casos en los que no se puede resolver un problema o se opta por cerrarlo	8
9.3 Desafíos comunes: Gestión de conocimiento y configuración	8-9



1. Introducción

Con la finalidad de habilitar una entrega de las operaciones con las garantías y/o calidad esperada es necesario lograr una eficaz gestión de problemas. Para ello resulta clave asumir el compromiso con estas actividades. Se debe conceder recursos para dedicar a la gestión de problemas, garantizando que se cumplan las actividades asociadas.

El presente documento define la política para la Gestión de Problemas en el Área de Infraestructura y Operaciones de TI y otorga un marco en cuanto a:

- Metas y objetivos de la Gestión de Problemas
- Criterios para la apertura de Problemas
- Determinar el valor y beneficio esperado
- Determinar las actividades y dedicación
- Establecer roles y responsabilidades
- Establecer métricas
- Desafíos de la Gestión de Problemas

2. Metas y objetivos del Proceso de Gestión de Problemas

- Prevenir la ocurrencia de incidentes
- Erradicar los incidentes recurrentes
- Minimizar el impacto de incidentes que no puedan ser prevenidos

Para evitar la ocurrencia de incidentes hay que anticipar problemas en forma proactiva, es decir problemas potenciales, antes de que causen incidentes.

Los principales objetivos del proceso consisten en asegurar que:

- se registran correctamente los problemas
- se escalan y reportan en forma correcta y precisa
- se priorizan y gestionan en la secuencia adecuada
- existe una lista de problemas visible y reportada
- la resolución alcanza para cumplir requerimientos de SLA con clientes

3. Apertura de problemas

¿Cuándo existe un problema?

Por definición estándar problema es la causa raíz, oculta, subyacente a uno o más incidentes.

Solo deberían mantenerse problemas abiertos cuando hay recursos para trabajarlos y se entiende que hay razones de negocio que lo justifican.

Cuando no existan los recursos para trabajar un problema o bien tenga baja prioridad por un período prudencial (por ejemplo 120 días) deberá cerrarse el problema luego de aceptarse "convivir" con el mismo, dejándose constancia en la base de conocimiento. El caso pasa al ámbito de la gestión de riesgos.

En el contexto de las operaciones de Agestic, se debe abrir un problema cuando así lo entienda el **referente técnico del activo** en cuestión y exista el apoyo por parte del dueño del servicio. Son estos quienes en última instancia deben determinar que corresponde abrir un problema. Para esto podrá valerse de distintas fuentes, reportes, monitoreo o solicitud proveniente de otras áreas, grupos técnicos o del negocio.

Una vez que se ha identificado/reconocido un problema y por tanto registrado, es un factor crítico de éxito respetar que se cumplan las actividades asociadas a su correcta gestión.

4. Valor y beneficio esperado

Pensar en términos de causa y efecto con el fin de identificar causas de potenciales incidentes y empujar la mejora continua. Es fundamental identificar el valor/beneficio aportado a la Organización al anticipar la resolución de un problema. Significa entender las razones que justifiquen invertir recursos en su prevención e identificar el potencial riesgo de no atender su resolución a tiempo.

El equipo de gestión de problemas debe procurar entonces **trabajar en modalidad proactiva**. Se trata de capitalizar la experiencia e involucrar su knowhow en las **fases de diseño y transición del servicio** con el fin de identificar y erradicar problemas antes de que alcancen a los ambientes de producción. Para ello debe ser **apoyado por la dirección pues necesita de recursos adicionales** pudiendo en ocasiones retrasar tiempos de salida en producción a fin de que el beneficio en el mediano plazo sea mayor.

La gestión de problemas soporta la Gestión de Incidentes críticos y proporciona entrada a la Gestión de Cambios para la ejecución de cambios tendientes a resolver incidentes que estén afectando entornos de producción. Para conseguir resultados **es esencial demostrar** a las partes interesadas, las relaciones entre incidentes, causas raíces y acciones realizadas, a fin de que se comprenda la forma en que contribuye al beneficio general del servicio. Los problemas deben ser enfocados y priorizados en su contexto y conjunto considerando sus implicaciones y relaciones.

4.1. Valor y beneficio esperado

Reducción de Riesgos

- Reduce incidentes por lo que los servicios TI resultan más confiables aumentando la calidad de los servicios.

Reducción de Costos

- Reducción en el número de incidentes lleva a una ocupación más eficiente del tiempo del personal técnico de soporte.

Aumento de capacidades

- Consolidar información sobre problemas, errores conocidos y acciones correctivas facilitan el aprendizaje de la organización capitalizando conocimiento y habilidades.

5. Actividades y dedicación

5.1. Registro, priorización, escalamiento y seguimiento

La gestión de problemas no es un proceso que funcione aislado. No puede existir sin la gestión de Incidentes y hay una fuerte correlación entre la madurez de gestión de incidentes y la eficiencia y resultados de la gestión de problemas. **La gestión de Incidentes debe asegurar que los problemas sean detectados y documentados correctamente.**

A su vez la gestión de Incidentes trabaja en comunión con la gestión de Eventos. Anomalías en alarmas o tendencias de incidentes son entradas imprescindibles para la gestión de problemas.

La gestión de Incidentes debe asegurar que en paralelo a la restauración del servicio durante e inmediatamente posterior a un incidente se capte y registre toda la información relevante. *Por ej. El volcado de memoria del servidor antes de un reinicio para tener información para el análisis de la causa raíz.*

Posteriormente la Gestión de Problemas se encarga de dar curso a las actividades de priorización, escalamiento y seguimiento y **debe asegurar que se ejecuten dichas actividades** o escalar oportunamente cuando detecta que estas no se están llevando a cabo.

5.2. Investigación, análisis y actualización del caso

Las **principales tareas se basan en la investigación y análisis** preventivos para lograr anticipar causas de potenciales incidencias y el análisis reactivo para identificar la causa raíz de incidente(s) y su definitiva resolución capitalizando experiencia y conocimiento para la futura prevención.

Deben utilizarse técnicas, herramientas y metodologías estándar de análisis acorde a las mejores prácticas de la industria. Debe ser posible relacionar un registro de problema a todas las partes interesadas. Ej: lista de problemas/incidentes relacionados a un proyecto más grande.

Es fundamental registrar en un repositorio centralizado toda la información relevante, así como el progreso y acciones o actividades realizadas. De igual modo se deben relacionar (vincular) los tickets de eventos e incidentes con el ticket de problema en la herramienta de gestión.

5.3. Diagnóstico y resolución de problemas

Es fruto del trabajo de las actividades en el punto anterior. El resultado de la investigación de un problema será un diagnóstico de su causa raíz = informe de RCA (Root Cause Análisis).

Hay varias técnicas útiles para la resolución de problemas que se pueden utilizar para ayudar a diagnosticar y resolver problemas:

- Verificar la Base de datos: busca de errores conocidos (KEDB) y si existen antecedentes de incidencias similares en el pasado, de ser así, una resolución ya debería haber sido utilizada.
- Análisis cronológico: los eventos que provocaron el problema serán verificados en orden cronológico para tener una línea de tiempo de eventos. El objetivo es ver qué evento desencadena el siguiente evento, etc.

Fases de investigación y diagnóstico

- definiendo el problema
- describiendo el problema en términos de identificación, ubicación, duración e impacto
- estableciendo posibles causas
- probando la causa más probable
- verificando la verdadera causa

Una vez completada la investigación y encontrada una solución temporal (o incluso una permanente), se debe generar un Registro de error conocido y guardarlo en la Base de datos de errores conocidos o conocimiento para luego servir de ayuda a identificar y resolver otros problemas/incidentes similares.

Para dar lugar a la ejecución de las actividades anteriores:

- Los **dueños de problema / dueños de solución (negocio)** deben asegurar los **recursos** para realizar dichas actividades.
- Ellos deben priorizar la carga de trabajo para gestionar los problemas en línea con los objetivos del servicio y del negocio.

- También **deben asegurar que los contratos con sus proveedores** explicitan las actividades de gestión de problemas.

6. Roles y responsabilidades

6.1. Dueño y Gestor del Proceso de Problemas

Se encargan de la salud y adopción del proceso y les corresponde monitorear la efectividad sobre la ejecución de las actividades.

Responsabilidades:

- Asegurar definición de una **política/proceso documentado** acorde a las necesidades.
- Asegurar su **adopción** y recoger devoluciones.
- Revisión periódica para la integración y mejora agregando valor a las partes.
- Asegurar una relación coherente entre problemas, incidentes, cambios.
- Monitorear los problemas existentes y encaminar acciones cuando no se conducen las actividades definidas.

6.2. Dueño del servicio

Para asegurar que los servicios se gestionan con foco en el negocio debe haber un único punto de rendición de cuentas. El **dueño de servicio/solución** es el responsable por su servicio dentro de la organización con independencia de los componentes tecnológicos, capacidades profesionales o procesos que lo sustentan.

Responsabilidades:

- **Es el responsable del servicio a lo largo de su ciclo de vida.**
- Iniciación, transición y soporte de servicios.
- Alta/baja en el catálogo de servicios (información, contactos, componentes, SLAs).
- Mejora continua y gestión de cambio de los servicios.
- Representar el servicio en la organización.
- Punto de escalamiento y notificación para incidentes mayores.
- Representar el servicio en CABs.
- Asistir al Gestor de Problemas en la identificación, priorización y resolución.
- **Asegurar los recursos necesarios y que las partes interesadas sean involucradas en las actividades de Gestión de Problemas según prioridad del negocio.**
- Comprometer el soporte requerido desde otras organizaciones, proveedores, etc.
- Asegurar que el personal de soporte en la organización posee las habilidades y entrenamiento necesarios.

6.3. Analista de Problema (referente técnico)

Provee habilidades y conocimientos en un dominio en particular (técnico, operativo, aplicación, etc.). Puede pertenecer a otra área.

Responsabilidades:

- **Asistir al gestor de problemas en el análisis** de datos, identificar posibles problemas y su solución.
- Facilitar desarrollo de workarounds y acciones correctivas.
- Registrar y actualizar problemas y errores conocidos con información adecuada y relevante.
- **Asistir al gestor de problemas en validar** que la causa raíz ha sido erradicada luego de implementarse la solución recomendada.

6.4. Gestor de Problema

Pertenece al **equipo de Infraestructura y Operaciones de TI** y es el responsable de empujar, facilitar, dar seguimiento y ejecutar las propias actividades de gestión de los problemas coordinando con las partes involucradas.

Responsabilidades:

- **Asegurar** el correcto **registro** de problemas y su relación con los incidentes.
- Capturar los datos e información durante las tareas de soporte y restauración de incidentes críticos.
- **Asegurar el análisis** de datos e identificar posibles causas encaminando su solución con los responsables técnicos.
- Asegurar correcta priorización, **escalamiento y seguimiento** con los proveedores y terceras líneas de soporte facilitando los flujos de información, envíos de logs, etc.
- Orquestar/coordinar las actividades para diagnóstico y resolución.
- Gestionar y coordinar las actividades necesarias para desarrollar los Workaround, acciones preventivas y soluciones definitivas.
- Validar que la causa raíz ha sido erradicada luego de implementarse la solución recomendada.
- Cuando la resolución sea mediante un cambio (es habitual) **asegurar** que exista el correspondiente RFC.
- **Enviar actualización** a las partes interesadas sobre el estado de situación.
- **Divulgar** la lista de problemas.

6.5. Mesa de Servicios - Service Desk

La función principal de la Mesa de Servicios es proveer el punto único de contacto y comunicación para usuarios, clientes, grupos de TI y procesos.

Responsabilidades:

- **Colaborar** con el gestor de problemas en documentar todo lo relevante a incidentes/solicitudes/eventos relacionadas con información detallada y exacta.
- Registrar y **relacionar** incidentes con problemas (**vincular tickets en sistema de tickets**)
- **Comunicar** avisos y acciones relevantes a todas las partes interesadas.
- Elaborar y **enviar** regularmente **reportes** relacionados.

6.6. Equipo de Dirección

Se encarga de soportar la **priorización y escalamiento de Problemas y de asegurar los recursos** para la ejecución de las actividades definidas.

En caso de dificultades con los recursos se encarga de obtener el compromiso del dueño de solución, proveedor, etc.

7. Factores críticos de éxito

- **Asegurar los recursos** para ejecutar un proceso formal y adoptado, separado de la gestión de incidentes y la gestión de cambios para registrar, clasificar, priorizar y determinar acciones correctivas.
- Tener **criterio claro de aceptación** sobre cuando existe un problema en términos técnicos y de negocio.
- **Ejecutar las actividades** de detección de problemas mediante el análisis de datos históricos y actuales de incidentes, problemas, eventos, release notes y monitoreo de demanda, capacidad y disponibilidad.
- Asegurar que todos los problemas, errores conocidos, información relevante y de resolución son registrados en un repositorio común con enlaces a incidentes, cambios, y demás sistemas y fuentes de información relacionadas (ej: Tickets en sistemas de proveedores).
- **Implementar** formalmente otros procesos de gestión de Servicios TI como Gestión de Configuración, Conocimiento y Catálogo de servicios.
- Evitar que el grupo de gestión de problemas a fin de cumplir un KPI tienda rápidamente a establecer un diagnóstico en una situación compleja, aun cuando se haya descubierto un elemento que contribuya significativamente, pues finalmente esto solo llevará en los hechos a detener el análisis.

8. Indicadores (KPIs)

1. Número de incidentes críticos repetidos.
2. Número de incidentes asociados a un problema.
3. Número de problemas abiertos.
4. Tiempo promedio de diagnóstico de problemas.
5. Tiempo promedio de resolución de problemas por prioridad

9. Dificultades y desafíos

9.1. No adoptar un proceso formal para la Gestión de Problemas resulta en:

- Incidentes recurrentes, clientes insatisfechos y pérdida de confianza en la organización.
- Uso ineficiente de recursos (recursos senior utilizados en reaccionar a los incidentes en **vez de proactivamente gestionar diseño, transición y soporte de los servicios**).
- Disminuida motivación de los empleados que repetidamente deban atender y gestionar incidentes con las mismas características.

9.2. Casos en los que no se puede resolver un problema o se opta por cerrarlo:

Hay situaciones en las que aun cuando se identifica la causa raíz, se decide no implementar una resolución por cuanto debido a costos u otras razones de negocio la gerencia opta por aceptar los riesgos de recurrencia de incidentes. A discreción del dueño de servicio la gestión del problema puede pausarse o cerrarse como no resuelto.

9.3. Desafíos comunes: Gestión de conocimiento y configuración

La Gestión formal del conocimiento y configuración son factores críticos de éxito para una eficaz y eficiente Gestión de problemas.

Con frecuencia se da la falta de práctica de los técnicos involucrados en compartir su experiencia y conocimiento. Fallan en registrar en el repositorio central y en documentar o comunicar lo sucedido, por lo tanto, en hacer disponible y accesible donde sea necesario un conocimiento que pertenece a la organización.

Se deben registrar las actividades de seguimiento, horas de trabajo dedicadas a análisis de logs, histórico de incidentes, reuniones técnicas, escalar con proveedores, análisis de eventos, registros de avances, comunicación al área sobre los avances.

La función de Mesa de Servicios debe madurar para colaborar todo lo posible en dichas gestiones.

Las Bases de Datos creadas por estos procesos (sistema de gestión de conocimiento, sistema de gestión de configuración y base de datos de errores conocidos) pueden quedar incompletas o desactualizadas, por lo tanto, sistemas de gestión no maduros o informales son un factor de riesgo.

