Uruguay Presidencia | agesic

Proceso de Gestión de Incidentes

Infraestructura y Operaciones de TI

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

Contenido

1. Tabla del proceso

<table>
<tr><td colspan="2">Proceso: Gestión de Incidentes</td></tr>
<tr><td colspan="2">Objetivo:
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 en encontrar y analizar las causas raíz de un determinado incidente sino exclusivamente en restaurar el servicio lo más rápidamente posible.
Se define Incidente de acuerdo a la metodología ITIL: “Una interrupción no planificada de un servicio de IT o una reducción en la calidad de un servicio de IT. Una falla de un ítem de configuración que aún no ha impactado el servicio también es un incidente”.</td></tr>
<tr><th>Entradas</th><th>Salidas</th></tr>
<tr><td>• Identificación de un Incidente: puede ser una alerta del sistema de monitoreo o una llamada telefónica, un e-mail o un ticket ingresado en el sistema.</td><td>• Incidente resuelto
• Registro de Problema</td></tr>
<tr><th colspan="2">Roles y Responsabilidades</th></tr>
<tr><td>Rol</td><td>Descripción</td></tr>
<tr><td>Cliente</td><td>Usuario que reporta el incidente.</td></tr>
<tr><td>Ejecutor del proceso</td><td>Todas las personas del área que ejecutan actividades del proceso periódicamente, y tienen un perfil basado en lo operativo.</td></tr>
<tr><td>Gestor del proceso</td><td>Se encarga de que todo lo definido se esté haciendo, y tiene un perfil basado en lo operativo.</td></tr>
<tr><td>Dueño del proceso</td><td>Se encarga de que todo lo relativo al proceso esté definido, y tiene un perfil basado en la calidad.</td></tr>
<tr><th colspan="2">Recursos materiales o sistemas</th></tr>
<tr><td colspan="2">• ManageEngine Service Desk Plus – Sistema de tickets utilizado por el área</td></tr>
</table>

Actividades
Las principales actividades de este proceso son: • Realizar el registro del incidente en el sistema de gestión de tickets. • Clasificar el incidente para determinar la urgencia, impacto y prioridad, y el técnico que debe atender el incidente. • Realizar un diagnóstico del incidente y determinar una solución que permita restaurar el servicio rápidamente. • Validar la resolución del incidente. • Determinar si se debe invocar a la gestión de problemas. • Cerrar el ticket del incidente asegurándose que la información registrada sea completa.

Procesos relacionados	
Proceso Relacionado	**Relación**
Gestión de Problemas	Cuando la prioridad de un Incidente es registrada como Alta o Crítica se invoca al proceso de Gestión de Problemas para realizar un Análisis de la Causa Raíz del mismo, a efectos de determinar soluciones más estables que las que puedan haber surgido para resolver el Incidente. En otros casos puede ser que el Incidente no se logre resolver y se necesite realizar el Análisis de la Causa Raíz para poder obtener una solución al Problema y por lo tanto al Incidente también.
Gestión de Cambios	Un Cambio puede llegar a derivar en un nuevo Incidente ya que realiza modificaciones sobre un activo o elemento de configuración. Por otro lado, un Incidente puede llegar a precisar de un Cambio o Cambio Urgente para que se restaure el servicio.

Referencias / documentos relacionados

2. Métricas del proceso

Se definen las siguientes métricas para medir la eficacia y eficiencia de este proceso.

Métricas de Demanda

Incidentes por mes

Nombre:	Cantidad de Incidentes Cerrados
Descripción:	Cantidad de Incidentes que fueron cerrados -y por lo tanto clasificados íntegramente en el sistema de tickets- el mes pasado.
Frecuencia:	Mensual
Interesado(s):	Equipo de Dirección, Divisiones IOTI

Incidentes críticos por mes

Nombre:	Cantidad de Incidentes Críticos Cerrados
Descripción:	Cantidad de Incidentes con prioridad Crítica que fueron cerrados -y por lo tanto clasificados íntegramente en el sistema de tickets- el mes pasado.
Frecuencia:	Mensual
Interesado(s):	Equipo de Dirección, Divisiones IOTI

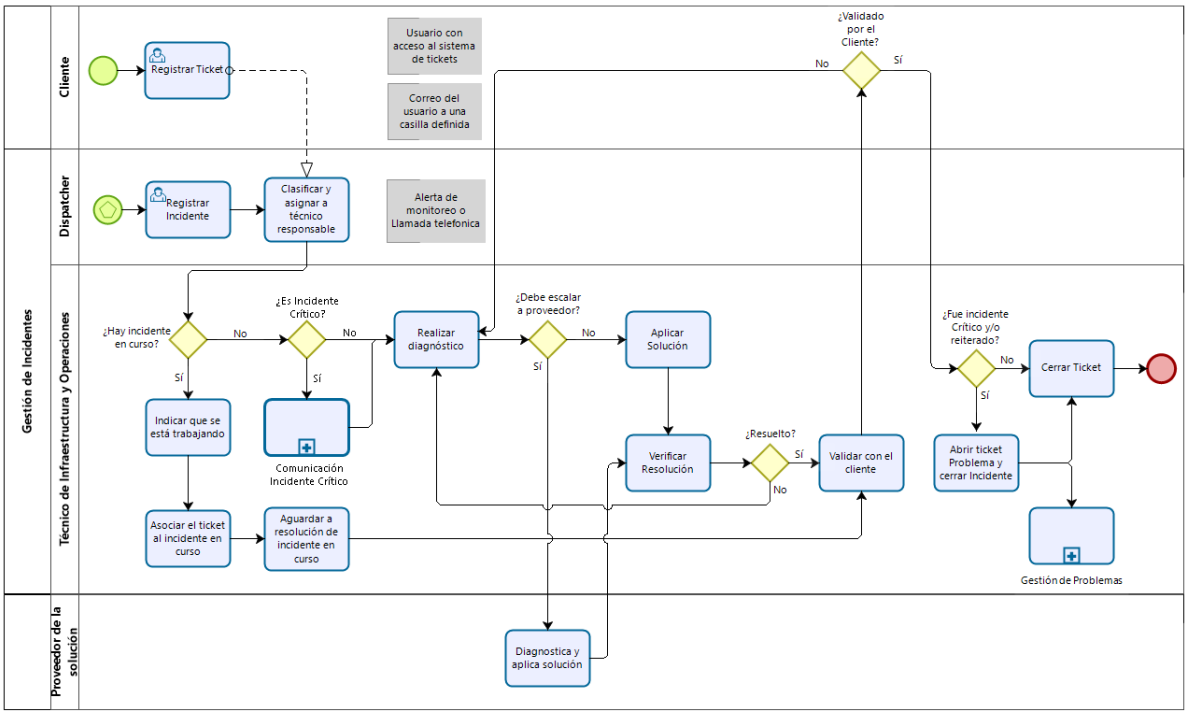
Métricas de Eficiencia

Tiempo de resolución

Nombre:	Tiempo de ejecución promedio hasta el cierre del Incidente.
Descripción:	Se mide el tiempo transcurrido desde el momento en que se crea el ticket de Incidente en el sistema hasta que el Incidente se cierra tras la aprobación del cliente, para luego calcular el promedio de los tiempos de todos los tickets registrados durante el mes.
Frecuencia:	Mensual
Interesado(s):	Equipo de Dirección, Divisiones IOTI

3. Descripción del proceso

3.1. Diagrama



3.2. Procedimiento

1. Registrar Incidente

Los incidentes se deben registrar apenas se reciba la primera notificación. Al registrar un incidente se debe completar la siguiente información en el sistema de tickets:

a) Quién informa sobre el incidente (si es un usuario se debe registrar toda la información para poder contactarlo, si es por un evento el incidente quedará ingresado a nombre de la persona de Mesa de Servicios que lo registra).

b) Breve descripción del incidente a modo de título.

c) Información detallada sobre el síntoma del incidente. Por ejemplo, servicios o sistemas afectados, cantidad de usuarios afectados, hora de comienzo del incidente.

Los incidentes también pueden ser ingresados por usuarios que tengan acceso a la vista web del sistema de gestión de tickets o también puede darse el caso en que los clientes manden un mail a una casilla determinada y el sistema de gestión de tickets tome la información contenida en el mail y abra el ticket del incidente.

2. Clasificar

Para clasificar el incidente se debe registrar la siguiente información:

a. Categoría y/o subcategoría, lo que permite clasificar el incidente según la solución afectada.

b. Prioridad, la que va a estar dada por el Impacto y la Urgencia. La Urgencia la establece el cliente, y el técnico establece el Impacto. Este último estará determinado por el daño que está ocasionando el incidente en el negocio del cliente.

3. ¿Hay Incidente en curso?

Para evitar trabajar sobre el mismo incidente en más de un ticket a la vez, se debe verificar si ya no existe un registro abierto con características similares. Para ello se buscará en la base de Incidentes tomando palabras claves de la descripción del Incidente y luego analizando la lista de Incidentes devuelta por la búsqueda.

4. ¿Pertenece al dominio de Mesa de Servicios?

Si en el paso anterior no se encontraron incidentes similares, entonces se debe analizar la información preliminar del Incidente para determinar si es un Incidente que pueda resolver el equipo de Mesa de Servicios o no. Si de este análisis se entiende que no es un Incidente que pueda resolver el equipo de Mesa de Servicios, entonces se deberá reasignar al equipo que se considere más adecuado para resolver el Incidente.

5. ¿Es un Incidente Crítico?

Una vez asignado al grupo correspondiente, y en caso de que sea un Incidente Crítico, se debe invocar al procedimiento de Comunicación de Incidente Crítico. De esta manera se notifica al equipo de Dirección sobre lo ocurrido.

6. Indicar que se está trabajando

Si existe un incidente similar en curso se debe indicar al Cliente que reportó el Incidente sobre dicha situación y en la medida de lo posible brindarle un tiempo estimado de resolución.

7. Asociar el ticket al incidente en curso

Cuando existe un incidente similar, en el nuevo ticket simplemente se mantendrá informado al cliente en el ticket original vinculado. Toda la información y tareas realizadas para solucionar el Incidente quedarán registradas en el primer ticket abierto para el mismo.

8. Realizar diagnóstico preliminar

Se realiza un análisis e investigación del Incidente a partir de la información registrada para el propio incidente, así como consultando la Base de Conocimiento (incidentes anteriores, errores conocidos, problemas abiertos, etc.), la Base de Configuraciones (para determinar todos los componentes asociados con el incidente) y la información que pueda observarse en las herramientas de monitoreo. Todos los hallazgos y posibles soluciones deben quedar debidamente registrados como parte de la información del Incidente.

9. Brindar soporte inicial

Cuando se tenga un indicio de una posible solución para el Incidente se le brindará soporte inicial al Cliente con el fin de restablecer el servicio a su estado normal lo más rápidamente posible.

10. Validar resolución

Una vez que se asume que el incidente está resuelto, y si el incidente había sido notificado por el Cliente, se notificará al cliente vía telefónica en caso de incidentes de severidad Alta o vía email en los demás casos, para que el Cliente confirme si el incidente está resuelto o no.

Una vez notificado el Cliente de la resolución del incidente se deberá esperar a que el Cliente confirme que el mismo ha quedado resuelto. En caso que el Cliente no responda en un tiempo acordado, se deberá volver a contactar al Cliente. El tiempo acordado para volver a contactar al Cliente depende del Cliente y de la Severidad del Incidente.

11. Cerrar ticket

Una vez que el Cliente confirma que el incidente está resuelto se podrá dar por finalizado el ticket. En caso de incidentes registrados a partir de los sistemas de monitoreo bastará con que el chequeo asociado al incidente en los sistemas de monitoreo vuelva a su estado normal para poder cerrar el ticket.

4. Definiciones

Evento

Es un cambio de estado que tiene importancia para la gestión de un ítem de configuración o de un servicio. El termino Evento también es utilizado para indicar una Alerta o Notificación creada por un Servicio de IT o un ítem de configuración o una herramienta de monitoreo. Un evento requiere del personal de Mesa de Servicios para tomar una acción e iniciar el proceso de registro del Incidente.

Problema

Es la causa subyacente, aún no identificada, de una serie de incidentes o un incidente aislado de importancia significativa.

Error conocido

Un problema se transforma en un error conocido cuando se han determinado sus causas.

Severidad del Incidente

Una de las clasificaciones que se realiza para los incidentes corresponde al impacto que los mismos tienen sobre la operativa del negocio del Cliente. Para esta clasificación se definen las siguientes categorías de severidad.

Impacto	Descripción
Crítico	Es un incidente que impacta de forma severa al negocio o clientes. Principalmente incidentes de disponibilidad, caídas de servicios (backend) o cortes de conectividad en Servicios o Soluciones clasificadas con Prioridad 0 o 1.
Alto	Es un incidente que está impactando toda la operativa del negocio del Cliente. Un gran número de usuarios está afectado por el incidente y les es imposible realizar su trabajo. Es una situación crítica para el negocio.
Medio	Un sistema no está funcionando correctamente y afecta severamente la operativa de una parte del negocio del Cliente.
Bajo	Un usuario o un grupo muy reducido de usuarios se ven afectado por el incidente. La operativa del negocio del Cliente no se ve afectada.