ATLASSIAN
Opsgenie

Las 5 fases de la gestión de incidentes y cómo mejorarlas

TSOFT

ATLASSIAN Platinum Solution Partner
ENTERPRISE

Agenda

Vamos a empezar

Para ponerlo de forma sencilla, la gestión eficaz de incidentes forma parte esencial de todos los sistemas empresariales. ¿Por qué? Debido a que las herramientas tecnológicas y los flujos de trabajo se vuelven cada vez más complejos e interconectados, los sistemas se vuelven cada vez más vulnerables a tiempos de inactividad no planeados, que pueden afectar a cualquier sistema en cualquier momento, impactando las operaciones de negocio externas e internas. Los costos de estos incidentes pueden llegar a sumar miles de dólares por minuto.

Con este impacto potencial por delante, las organizaciones buscan avanzar rápidamente sobre prácticas de respuesta a incidentes, para asegurarse de que puedan ser gestionados de forma efectiva lo más rápido posible. Esto significa adoptar un enfoque holístico para un incidente, entender cómo avanza y cómo mejorar de forma continua la resistencia de los sistemas. Desde la perspectiva académica, existen varias opiniones sobre cómo muchas fases están asociadas a un flujo de trabajo típico de respuesta a incidentes. Aunque esto puede ser distinto para cada organización, vamos a concentrarnos en las siguientes cinco etapas para representar el ciclo de vida de un incidente:

1. Preparación
2. Detección y Alerta
3. Contención
4. Reparación
5. Análisis

Sin considerar cada una de estas etapas, las organizaciones corren el riesgo de administrar mal los incidentes, generando retrasos innecesarios y altos costos. Abajo, vamos a analizar cada una de estas etapas y ofreceremos recomendaciones sobre prácticas que van a ayudar a los equipos a resolver incidentes de forma más eficiente.

Preparación

Incluso los profesionales de TI con más experiencia dirán que la preparación es una parte esencial de la gestión de incidentes. Es la fase donde los equipos exploran posibilidades hipotéticas y, entonces, definen procesos para resolverlas.

Las organizaciones líderes se enfocan en la preparación de la misma manera que los atletas practican un deporte. El objetivo es construir una memoria muscular alrededor de la respuesta a incidentes y, así, reaccionar de manera más rápida.

> Las metodologías de respuesta a incidentes normalmente destacan la preparación, no solamente estableciendo una capacidad de respuesta a incidentes, sino también para prevenirlos asegurando que los sistemas, redes y aplicaciones sean suficientemente seguros.”
>
> NIST

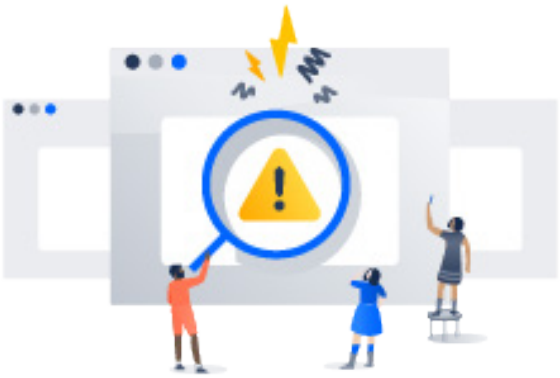
Ideas para mejorar

Esté siempre preparado.
El botiquín para quienes responden a los incidentes es un backup de información crítica que los equipos necesitan para solucionar problemas en el menor tiempo posible. Al centralizar este material en un único lugar, los equipos tienen el conocimiento a mano y no necesitan buscarlo. Esto puede incluir varias cosas, dependiendo de la estructura de los equipos y los sistemas de la organización:

· Planes de respuesta a incidentes
· Listas de contactos
· Plan de guardia
· Políticas de escalonamiento
· Links para herramientas de conferencia
· Códigos de accesos
· Documentos de póliza
· Documentación técnica y runbooks

· No le huyas a los runbooks.
Los runbooks ofrecen a los integrantes del equipo la orientación esencial sobre qué pasos dar en una determinada situación. Esto es especialmente importante para los equipos que trabajan en horarios rotativos y/o cuándo un experto no puede ser contactado rápidamente. Sin los runbooks disponibles, los responsables que no están familiarizados con algún sistema quedan perdidos al intentar determinar cuáles son los pasos necesarios para empezar la reparación. Un conjunto de runbooks actualizado permite que los equipos respondan rápidamente y también construye colectivamente una base de conocimiento que le da un soporte continuo al mejoramiento de las prácticas de respuesta a incidentes.

· Acoge el caos y fomenta la estabilidad.
El término “Ingeniería del Caos” hasta puede parecer un oxímoron, pero no lo es. En verdad, es la práctica de probar a través de la inserción de fallas en los sistemas para entender cómo ellos pueden ser construidos de una forma más robusta y segura. Un ejemplo es el Chaos Monkey. Originalmente desarrollado por Netflix, Chaos Monkey es una herramienta que prueba la resistencia de la red a través de apagones intencionales de sistemas de producción. Aunque parezca peligrosa, la práctica realmente ayuda a los ingenieros a probar continuamente los sistemas para asegurar su capacidad de recuperación. De este modo, el Chaos Monkey ayudó a los equipos de Netflix a construir una cultura alrededor de la resistencia del sistema. Con el éxito, muchas otras organizaciones siguieron el ejemplo de esta práctica.



Detección y Alerta

La detección de incidentes no se enfoca solamente en saber que algo está mal, también en cómo los equipos son informados sobre esto. Aunque estos dos pueden parecer procesos distintos, están muy conectados en verdad. El desafío es que si bien la proliferación de herramientas de monitoreo de TI disponibles ha mejorado la capacidad de los equipos en identificar anormalidades e incidentes, estas mismas herramientas también pueden crear una tormenta de alertas, o falsos positivos que complican la respuesta en el proceso.

Los mejores equipos de TI suman una capa al proceso de monitoreo para asegurarse de que los avisos sean gestionados correctamente. Esta capa actúa para centralizar el proceso de alertas, mientras también desarrolla una inteligencia extra para la forma en que se entregan las alertas.

> La detección debe conducir a la respuesta apropiada... Esto exige principalmente la necesidad de identificar y comunicar claramente los roles, las responsabilidades y el enfoque inicial para el tratamiento de los incidentes. Debe incluir la determinación de quién debe identificar el incidente y determinar su gravedad como un medio para manejar el incidente efectivamente dentro del contexto organizacional."
>
> MITA

Ideas para mejorar

· Piensa fuera del NOC.
Históricamente, los Centros de Operación de Red (en inglés, Network Operations Centers - NOCs) actuaban como un centro de alertas y monitoreos para sistemas de TI a gran escala. El desafío es que un ingeniero típico de NOC puede ser el responsable por la clasificación y escalonamiento de incidentes desde cualquier lugar del sistema. Las herramientas modernas de gestión de incidentes permiten que este proceso se optimice significativamente. Automatizando la entrega de alertas, los flujos de trabajo, las agendas de los equipos y las políticas de escalonamiento, el potencial de equívoco y/o retraso humano puede ser evitado.

· Agrega, no agraves.
No hay nada peor que recibir una ola continua de avisos que vienen de varias herramientas de monitoreo. Al centralizar el flujo de alertas a través de una única herramienta, los equipos son capaces de filtrar mejor el ruido y enfocarse rápidamente en los temas que necesitan atención.

· Conocimiento = poder.
Una alerta básica indica que algo está mal, pero no siempre expresa qué es lo que está mal. Esto genera retrasos innecesarios, ya que los equipos deben investigar y determinar la causa del problema. Al integrar las alertas con los detalles técnicos de la causa del problema, el proceso de reparación puede empezar más rápido.

· Quis custodiet ipsos custodes?
La frase latina “¿Quién vigilará a los vigilantes?” identifica un problema universal enfrentado por todos los equipos de TI. Esto es porque las herramientas de monitoreo que utilizan son igualmente vulnerables a los incidentes y apagones que los sistemas para los cuales fueron diseñadas para proteger. Sin tener como asegurarse de que las herramientas de monitoreo funcionen correctamente, los sistemas pueden apagarse fácilmente sin ningún aviso. Los procesos de avisos holísticos aseguran que tanto los sistemas como las herramientas que los monitorean sean chequeados constantemente.

Contención

El proceso de clasificación de un incidente de TI es similar a los procesos utilizados en el sector médico. El primer paso es identificar la extensión del incidente. Después, el incidente necesita contención, para que la situación no empeore. Todas las acciones tomadas en esa fase deben enfocarse en limitar y evitar que más daños ocurran.

> La contención a corto plazo no pretende ser una solución a largo plazo para el problema; solamente pretende contener el incidente antes de que empeore."
>
> R. BEJTLICH, INSTITUTO BROOKINGS

Ideas para mejorar

- **Detén el sangrado.**

Un médico de clasificación sabe que se está arriesgando a aumentar los daños si se queda atrapado intentando resolver todas las situaciones en el momento que llegan. Su enfoque son acciones de corto plazo que estabilizan al paciente lo suficiente para llevarlo a una atención más aguda. En el sector de tecnología, las acciones de contención se enfocan en soluciones temporarias (aislar una red, retraer una estructura, reiniciar los servidores, etc) que, mínimamente, limitan el alcance del incidente o, idealmente, reactivan los sistemas. Si los esfuerzos de gestión de incidentes se enfocan solamente en la reparación, y no en la contención, una interrupción puede extenderse innecesariamente mientras se busca la solución permanente.

- **No hagas todo solo.**

La cultura del héroe en los equipos de TI es una filosofía que está muriendo. No está más de moda ser el ingeniero solitario que trabaja horas y fines de semana interminables porque es la única persona que puede reactivar los sistemas. En vez de eso, los equipos están trabajando como equipos: colaborando en los problemas porque saben que los incidentes pueden ser reparados más rápido cuando el conocimiento es compartido. Las herramientas de conferencia y chat y feeds de video en vivo se convierten en elementos esenciales en la caja de herramientas de la gestión de incidentes, haciendo que los equipos puedan juntarse rápidamente y colaborar en tiempo real. También es muy común que los equipos integren herramientas de chat con herramientas de gestión de incidentes, así los incidentes pueden ser desencadenados, reconocidos y reparados desde una sola plataforma.

· Sé transparente.

La era digital tiene cantidades infinitas de información disponible en cualquier momento. Durante un colapso de TI, esto puede ser una ventaja o una desventaja. Si los usuarios encuentran una interrupción del servicio, es común que el incidente sea divulgado en un corto período de tiempo. Para estar preparado para esto, los equipos deben tener un plan de comunicación de incidentes listo. El objetivo es conquistar la confianza de los clientes reconociendo el problema públicamente y asegurandoles que las medidas necesarias para solucionarlo están siendo tomadas. Las herramientas como Twitter, StatusPage y los foros de usuarios son lugares perfectos para compartir esta información. Es importante que este proceso sea pensado para continuar en las fases de reparación y análisis, aumentando aún más la confianza de los usuarios, que, en caso contrario, pueden abandonar un sistema.

Reparación

Íntimamente ligado a la contención está la reparación. Aquí es donde las soluciones de largo plazo son implementadas para asegurar que el incidente se resolvió de forma completa y eficaz. Si en la fase de contención el objetivo es reactivar los sistemas, en la fase de reparación el objetivo es entender lo que generó el problema y cómo resolverlo de forma que los incidentes similares no vuelvan a afectar el sistema en el futuro.

> “Antes de la recuperación total del sistema, los esfuerzos de reparación deben enfocarse en arreglar el origen del problema. La fase final de recuperación no es solamente reactivar el sistema, sino hacerlo mejor y más seguro. El sistema debe tener la misma capacidad operacional, pero también la capacidad de protegerse de lo que causó el incidente corregido.”
>
> DEPARTAMENTO DE SEGURIDAD INTERNA DE E.E.U.U.

Ideas para mejorar

· Cynefin.
Un esquema de toma de decisiones, Cynefin (se pronuncia “KUN-iv-en”) proporciona una forma estructurada de abordar los problemas que ayuda a los encargados de los incidentes a determinar el mejor camino de acción en función de la naturaleza del problema en sí. Dependiendo del tipo de incidente (simple, complejo, complicado, caótico), se define un enfoque para resolverlo:

· ¿El incidente tiene causa y solución conocidas?
· ¿Necesito involucrar a otras personas para que me ayuden a resolver el incidente?
· ¿Hay tiempo para investigar el problema e identificar la mejor respuesta o la situación exige acción inmediata?

· ¿Qué tal automatizar?
Las herramientas de chat se han convertido en una solución ideal para que las organizaciones mejoren su comunicación y colaboración. No obstante, esas herramientas también avanzaron más allá de simplemente permitir que los equipos envíen mensajes. El equipo de desarrollo de software de GitHub fue pionero en el avance de las herramientas de chat cuando lanzaron la herramienta Hubot, de código abierto, que permite a los usuarios activar acciones y scripts directamente desde un entorno de chat. Esto permite a los equipos simplificar las operaciones, creando bots que automatizan procesos (iniciando una reinicio del servidor, implantando una parte de código, etc.).

Análisis

Los flujos de trabajo de gestión de incidentes no terminan cuando pasa la tormenta y los sistemas son restaurados. En ese momento, empieza una de las fases más importantes del ciclo de vida de la gestión de incidentes: el análisis. La intención de una “autopsia” es entender claramente las causas sistémicas de un incidente, junto con las medidas tomadas para hacerle frente.

Desde aquí, los equipos líderes trabajan para identificar oportunidades de mejoramiento alrededor de los sistemas y de los procesos definidos para mantenerlos. Evaluando esta información, los equipos pueden desarrollar nuevos flujos de trabajo que soportan sistemas con una mayor resistencia y una respuesta más rápida a los incidentes.

> “El análisis post-incidente debe ser escrito en forma de reporte para proporcionar una revisión paso a paso de todo el incidente; este reporte debe ser capaz de responder las preguntas quién, qué, dónde, por qué y cómo, que pueden surgir durante la reunión de lecciones aprendidas. El objetivo general es aprender de los incidentes dentro de una organización para mejorar el desempeño del equipo y proveerse de materiales de referencia en caso de un incidente similar.”
>
> INSTITUTO SANS

Ideas para mejorar

- **Aprende con el fracaso.**

Abrumadoramente, los equipos de TI dirán que solo tienen tiempo para revisar las “grandes interrupciones”. Aunque esto sea un buen comienzo, muchas veces los incidentes que pueden tener impactos persistentes son descuidados. Un reporte de “autopsia” detallado puede no ser necesario para todos los incidentes, pero una revisión resumida de los detalles siempre debe hacerse. De esta forma, la conciencia de una situación apoya el avance del conocimiento colectivo y la mejora continua.

· ¡No existe una causa raíz!

¿O existe? Al analizar un incidente, es poco común que se identifique solamente una causa. Según el modelo Cynefin, estos son clasificados en la categoría de incidentes “simples”, ya que la causa y la respuesta necesaria son conocidas y replicables. Pero nunca es así de fácil. Frecuentemente, los sistemas son más complejos e interdependientes para definir una única causa raíz del incidente. Aunque la causa raíz parezca evidente (como decir que un error de digitacion bloquea una aplicación), en general, hay motivos para pensar que factores externos pueden haber permitido que la aplicación se bloqueara (o no lo haya evitado).

· No culpes a nadie.

El objetivo de cada autopsia debe ser entender lo que salió mal y lo que se puede hacer para evitar problemas similares en el futuro. O sea, es importante que el proceso no sirva para culpar a las personas. Esto es porque los equipos que se enfocan en “quién” y no en “qué” afectan el análisis por las emociones y no entienden verdaderamente lo que sucedió.

Resumen

En los ambientes modernos de TI, el cambio es la única constante. Eso significa que los sistemas serán continuamente modificados de formas nuevas y distintas. Los equipos que entienden esto también entienden que no es una cuestión de que si los sistemas van a fallar sino de cuándo. Prepararse para estas fallas es esencial para el éxito continuo y debe formar parte del ADN de los equipos de ingeniería.

Sobre Opsgenie

Opsgenie es una moderna plataforma de gestión de incidentes para servicios always-on, que permite a los equipos de Dev&Ops planificar las interrupciones de servicio y mantener el control durante los incidentes. Con más de 200 integraciones profundas y un mecanismo de reglas altamente flexible, Opsgenie centraliza las alertas, notifica a las personas correctas de forma confiable y permite que colaboren y tomen acciones rápidamente. A lo largo de todo el ciclo de vida del incidente, Opsgenie rastrea todas las actividades y proporciona ideas para mejorar la productividad e impulsar una eficiencia operativa continua.

Mira Opsgenie en acción.
¡Arranca gratis ya!

TSOFT

ATLASSIAN Platinum Solution Partner ENTERPRISE

Estamos contigo en los desafíos más críticos de tu negocio

Con profesionales certificados y experiencia comprobada en DevOps, Business Agility, ITSM, Automatización y Trabajo Remoto, te ofrecemos:

Migración desde otras herramientas

Migración desde instancias server a la nube o data center

Entrenamiento con expertos certificados

Assesment sobre licenciamiento y consultoría sobre buenas prácticas en el uso

Upgrade de versiones de todas las soluciones Atlassian

Integraciones con otras herramientas

TSOFT

ATLASSIAN

Platinum
Solution Partner
ENTERPRISE