República Bolivariana de Venezuela

Ministerio del Poder Popular para la Educación

Instituto Universitario de Tecnología Mario Briceño Iragorry

Valera, estado Trujillo.

**Recolección de datos y clasificación de incidentes**

Gabriel Torres  
C.I: 30.047.646

Informática

Kerly Hernández

Julio de 2022**Introducción**

Todas las acciones con el fin de obtener un beneficio emprendidas por una persona, empresa o grupo de personas, llevan a cabo diferentes actividades previas como la recolección de datos y su posterior clasificación, para definir un plan y conseguir el mejor resultado posible. El departamento de gestión de incidencias en una empresa, cuyo fin es reducir al mínimo cualquier problema emergente, no está exento de ello, pues para tener una mejor aproximación a la resolución de un incidente, necesita recolectar datos y clasificar esos datos en orden de crear una respuesta eficiente y viable. Pero, ¿de qué formas se pueden recolectar datos? ¿qué sistemas ayudan en este proceso? ¿qué beneficios brinda clasificar los incidentes? ¿cómo se pueden clasificar los incidentes? y ¿cuál es la respuesta dependiendo de la clasificación?

**Recolección de Datos**

La recolección de datos es un enfoque sistemático con el fin de obtener información relacionada a un objeto de interés cuya finalidad es ganar algo de ello. En el caso de la gestión de incidentes, se realiza para obtener un mejor panorama y hallar la solución más eficiente a la incidencia.

**Tipos de recolección de datos**

La recolección de datos se puede realizar de distintas maneras para detectar un incidente en el sistema, las cuales pueden ser:

1. Encuestas: se realizan encuestas a los clientes con el objetivo de determinar qué tipo de problemas han tenido.
2. Observación: es la forma más clásica de obtener información sobre lo que está ocurriendo en el sistema pues simplemente necesita estar al tanto de lo que ocurre observándolo.
3. Tickets de los usuarios: son los problemas reportados por los usuarios.
4. Sistemas de monitoreo: se pueden usar sistemas informáticos que se encarguen de monitorear el sistema y detectar irregularidades que luego son reportadas.

Los sistemas de monitoreo usados para recolectar datos sobre las incidencias pueden ser los siguientes:

* Sistemas de notificación de incidentes: son softwares cuya función principal es detectar y notificar de incidentes que afecten el funcionamiento normal del sistema en la empresa.
* Sistemas de informes de cuasi accidentes: se definen como sistemas con el propósito de realizar informes relacionados a incidentes que fueron solucionados antes de provocar algún tipo de daño.
* Sistemas de análisis de causa raíz: son sistemas informáticos que tratan de encontrar la causa raíz de un incidente con el fin de solucionarlo y aprender de él en pro de reducir las incidencias de este tipo en el futuro.

**Clasificación de los incidentes**

Normalmente, cuando ocurre un incidente, el departamento de gestión de incidencias necesita clasificarlo con el objetivo de dar una respuesta óptima y eficaz, y mantener ordenada la información sobre el mismo por una posible reincidencia.

**Beneficios de la Clasificación**

1. Clasificar los incidentes según su relevancia mejora la eficiencia a la hora de abordarlos, puesto que el enfoque recae en aquellos cuya severidad es mucho más grave.
2. Se obtiene una mejor organización de la información sobre los incidentes.
3. Al clasificarlo, es más fácil encontrar su solución, debido a que se pueden buscar otros incidentes de características similares y usar las soluciones aplicadas a ellos.
4. Ahorrar recursos que pueden ser mal invertidos.

**¿Cómo clasificar los incidentes?**

La clasificación de incidentes en una compañía depende de varias cosas, pues no todas las compañías tienen los mismos problemas; pero, en resumen, los tres parámetros principales con los que se puede clasificar un incidente son:

1. La severidad del incidente que corresponde al impacto que puede tener.
2. La prioridad que se refiere a la urgencia de responder al incidente.
3. La categoría con la que más comparte características esa incidencia.

Cabe destacar que, aunque la prioridad interviene en la forma de clasificar los incidentes, simplifica mucho las cosas categorizar los incidentes usando solo el parámetro de severidad combinado con la prioridad, debido a que tal vez el impacto de un problema a la compañía sea bajo, pero es prioridad solucionarlo rápido y, por tanto, un incidente de bajo impacto, pero de alta prioridad puede ser categorizado con severidad media.

**¿Qué tipos de respuestas se requieren?**

La respuesta a un incidente va a variar dependiendo de su severidad. Por ejemplo:

Si es un incidente de alta severidad, se envía el problema directamente al departamento encargado de la categoría del incidente para solucionarlo lo antes posible. En el caso de que el problema sea de severidad media, en efecto, se escalará al departamento encargado de esa categoría para estar alerta y solucionar el problema, sin la necesidad de que su resolución sea inmediata. Y si la severidad del incidente es baja, se creará un ticket para atender el problema cuando sea posible, pues no tiene un gran impacto en la compañía.

Ejemplos de cómo sería la respuesta de un sistema a la severidad de un incidente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severidad | Categoría | Incidente | Impacto | Respuesta |
| Alta | Servidores | La página no carga | El servicio web no puede ser usado por los usuarios. Pérdida de clientes, etc. | Comunicación inmediata con el departamento de servidores, encargado de mantener la página en línea |
| Media | Servidores | La carga de la página es un 50% más lento de lo normal | El acceso al servicio web se vuelve molesto y los clientes se quejan | Se comunica con el equipo de servidores para que estén alerta y solucionen el problema. |
| Baja | Front-end | Una pequeña animación de la página web no funciona apropiadamente | Poco perceptible para los usuarios | Creación de ticket para que se resuelva, sin la necesidad de resolverlo inmediatamente |

**Conclusión**

Finalmente, la información expuesta, permitió entender las formas en las que se pueden recolectar datos para gestionar una incidencia, que van desde el uso de sistemas informáticos como los sistemas de notificación de incidentes, hasta la realización de entrevistas. Además de eso, se exponen los beneficios de clasificar incidentes y los parámetros más comunes por los que el equipo de gestión de incidencias se guía para hacer esto y, a su vez, se facilitan ejemplos que ayudan a sintetizar la información relacionada al tipo de respuesta de acuerdo al nivel de severidad de una incidencia.

Claramente, existe mucha más información en la red que habla sobre los temas tocados previamente y, como recomendación al lector, sería maravilloso que los leyera para aclarar dudas que no hayan sido resueltas durante el desarrollo de este informe.

**Bibliografía**

Tableau. El análisis de la causa raíz, explicado con ejemplos y métodos. Tableau. Consultado el 21 de julio de 2022 <https://www.tableau.com/es-mx/learn/articles/root-cause-analysis>

Atlassian. El camino hacia una mejor gestión de incidentes empieza aquí. Atlassian. Consultado el 22 de julio de 2022 <https://www.atlassian.com/es/incident-management/incident-response>

Safety Culture (28 de abril de 2022). Notificación de cuasi accidentes: Una guía de seguridad. Safety Culture. Consultado el 22 de julio de 2022 <https://safetyculture.com/es/temas/cuasi-accidente/>

Recolección de información para una auditoria informática. Auditoria en Informática CUN. Consultado el 21 de julio de 2022 <https://sites.google.com/site/auditoriaeninformaticacun/recoleccion>

Pugh, A. (8 de julio de 2022). How to Classify Security Incidents for Easier Response. Tandem. Consultado el 22 de julio de 2022 <https://tandem.app/blog/how-to-classify-security-incidents-for-easier-response>

Hunt, J. Incident Classification. GitLab. Consultado el 22 de julio de 2022 <https://about.gitlab.com/handbook/engineering/security/security-operations/sirt/severity-matrix.html>

Culver, H. (9 de julio de 2020) How to Classify Incidents. DZone. Consultado el 22 de julio de 2022 <https://dzone.com/articles/how-to-classify-incidents>