CLOUD COMPUTING: GESTIÓN DE EVENTOS, INCIDENCIAS Y PROBLEMAS

Máster Universitario en Dirección de Proyectos Informáticos

Presentado por:

D. Jorge Benítez Abad

Dirigido por:

D. José Carlos Ciria

Alcalá de Henares, a 11 de septiembre de 2020

UNIVERSIDAD DE ALCALÁ
Escuela Politécnica Superior

Máster en Dirección de Proyectos Informáticos

Trabajo Fin de Máster

Cloud Computing:
Gestión de eventos, incidencias y problemas.

Autor: Jorge Benítez Abad

Tutor/es: José Carlos Ciria

TRIBUNAL:

Presidente:

Vocal 1º:

Vocal 2º:

FECHA: 11 de septiembre de 2020

A mi prometida, por todo…

AGRADECIMIENTOS

Primero, quisiera dedicar unas palabras de agradecimiento a todos los profesores del máster de Dirección de Proyectos Informáticos toda su dedicación y apoyo, en especial al director del máster, Roberto Barchino Plata, y a mi tutor del TFM, José Carlos Ciria, su apoyo y orientación han hecho posible el desarrollo de este proyecto.

Quisiera agradecer todo su apoyo a todas aquellas personas que siempre han estado ahí, a mi lado o en la distancia, ya sean familia o amigos.

Además, quisiera hacer una mención especial a mis padres, Jose Luis y Sonsoles, y a mi hermano Jose Luis. Gracias a su apoyo incondicional he llegado hasta esta maravillosa etapa de mi vida.

Finalmente, agradecer todo su apoyo y ayuda a mi prometida María, pues de no ser por ella seguiría de siesta en lugar de haberme centrado en el desarrollo de este proyecto.

ÍNDICE REDUCIDO

RESUMEN *12*

SUMMARY *13*

PALABRAS CLAVE *14*

RESUMEN EXTENDIDO *15*

1. *Introducción* *18*
2. *Objetivo* *19*
3. *Ámbito* *20*
4. *Alcance* *21*
5. *Sistemas Cloud* *22*
6. *Alertas* *36*
7. *Estudio de campo* *39*
8. *Diseño de procedimientos* *49*
9. *Adaptación de los procedimientos para Cloud* *55*
10. *Cierres* *65*
11. *Resultados y conclusiones* *67*
12. *Trabajos futuros y mejoras* *69*
13. *Herramientas* *70*
14. *Bibliografía y enlaces de interés* *71*

ANEXOS *74*

ÍNDICE AMPLIADO

RESUMEN *12*
SUMMARY *13*
PALABRAS CLAVE *14*
RESUMEN EXTENDIDO *15*

1. Introducción *18*
2. Objetivo *19*
3. Ámbito *20*
4. Alcance *21*
5. Sistemas Cloud *22*
5.1. Descripción *22*
5.1.1. Fundamentos e historia *22*
5.1.2. Características *25*
5.1.3. Ventajas e inconvenientes *26*
5.2. Funcionamiento *27*
5.2.1. Servicios *28*
5.2.2. Tipos de nubes *29*
5.2.3. Controversia *30*
5.2.4. Aspectos de seguridad *31*
5.2.5. Limitaciones *32*
5.3. Principales proveedores *32*
6. Alertas *36*
6.1. Eventos *36*
6.2. Incidencias *37*
6.2.1. Incidencias, problemas y errores conocidos *37*
6.2.2. Incidencias y cambios *37*
6.3. Problemas *38*
7. Estudio de campo *39*
7.1. Cloud computing *39*
7.1.1. Infraestructura como servicio (IaaS) *40*
7.1.2. Plataforma como servicio (PaaS) *40*
7.1.3. Software como servicio (SaaS) *41*
7.2. Alertas *42*
7.2.1. Eventos *42*
7.2.2. Incidencias *43*
7.2.3. Problemas *47*
8. Diseño de procedimientos *49*
8.1. Procedimiento para la gestión de eventos *49*
8.1.1. Gestión de eventos en ITIL *49*
8.1.2. Procedimiento para la gestión de eventos Cloud *49*
8.1.3. Flujograma *50*
8.2. Procedimiento para la gestión de incidencias *51*
8.2.1. Gestión de incidencias en ITIL *51*
8.2.2. Procedimiento para la gestión de incidencias Cloud *51*
8.2.3. Flojugrama *52*
8.3. Procedimiento para la gestión de problemas *53*
8.3.1. Gestión de problemas en ITIL *53*
8.3.2. Procedimiento para la gestión de problemas Cloud *53*
8.3.3. Flujograma *54*

9. Adaptación de los procedimientos para Cloud *55*
9.1. Fase inicial *56*
9.2. Fase resolución *57*
9.2.1. Eventos *57*
9.2.2. Incidencias *58*
9.2.3. Problemas *59*
9.3. Fase retroalimentación *59*
9.3.1. Retroalimentaciones internas *60*
9.3.2. Retroalimentaciones externas *61*
9.4. Fase final *64*
10. Cierres *65*
11. Resultados y conclusiones *67*
12. Mejoras y trabajos futuros *69*
13. Herramientas *70*
14. Bibliografía y enlaces de interés *71*
14.1. Bibliografía *71*
14.2. Enlaces de interés *73*

ANEXOS *74*
ANEXO I: Procedimiento de gestión de eventos *74*
ANEXO II: Procedimiento de gestión de incidencias *75*
ANEXO III: Procedimiento de gestión de problemas *76*
ANEXO IV: Procedimiento de gestión de alertas *77*
ANEXO V: Escalado de alertas *78*

ÍNDICE DE FIGURAS

Imagen - 1: Conceptos generales *14*
Imagen - 2: Cronograma Cloud *24*
Imagen - 3: Cloud computing *28*
Imagen - 4: Capas Cloud *29*
Imagen - 5: Físico VS Cloud *30*
Imagen - 6: AWS *33*
Imagen - 7: Azure *33*
Imagen - 8: IBM *34*
Imagen - 9: Google *34*
Imagen - 10: Oracle *34*
Imagen - 11: VmWare *35*
Imagen - 12: iCloud *35*
Imagen - 13: Comparativa alertas *36*
Imagen - 14: Niveles Cloud *39*
Imagen - 15: IaaS *40*
Imagen - 16: PaaS *40*
Imagen - 17: SaaS *41*
Imagen - 18: Proceso ITIL gestión de Eventos *42*
Imagen - 19: Proceso de gestión de Incidencias *43*
Imagen - 20: Proceso ITIL gestión de Incidencias *45*
Imagen - 21: Proceso ITIL gestión de Problemas *47*
Imagen - 22: Proceso ITIL gestión de Eventos *49*
Imagen - 23: Flujograma gestión de Eventos *50*
Imagen - 24: Proceso ITIL gestión de Incidencias *51*
Imagen - 25: Flujograma gestión de Incidencias *52*
Imagen - 26: Proceso ITIL gestión de Problemas *53*
Imagen - 27: Flujograma gestión de Problemas *54*
Imagen - 28: Fases gestión de Alertas *56*
Imagen - 29: Fase inicial *56*
Imagen - 30: Fase resolución de Eventos *57*
Imagen - 31: Fase resolución de Incidencias *58*
Imagen - 32: Fase resolución de Problemas *59*
Imagen - 33: Retroalimentación Eventos *60*
Imagen - 34: Retroalimentación Incidencias *60*

Imagen - 35: Retroalimentación Problemas *61*
Imagen - 36: Retroalimentación Problemas graves *61*
Imagen - 37: Retroalimentación externa Eventos I *62*
Imagen - 38: Retroalimentación externa Incidencias I *62*
Imagen - 39: Retroalimentación externa Problemas I.a *62*
Imagen - 40: Retroalimentación externa Problemas I.b *63*
Imagen - 41: Retroalimentación externa Eventos II *63*
Imagen - 42: Retroalimentación externa Incidencias II *63*
Imagen - 43: Retroalimentación externa Problemas II *64*
Imagen - 44: Fase final *64*
Imagen - 45: Cierres *65*
Imagen - 46: Flujograma gestión de Eventos *74*
Imagen - 47: Flujograma gestión de Incidencias *75*
Imagen - 48: Flujograma gestión de Problemas *76*
Imagen - 49: Flujograma procedimiento de gestión de Alertas *77*
Imagen - 50: Escalado de alertas *78*

RESUMEN

La gestión de los eventos, de las incidencias y de los problemas resulta esencial a la hora de asegurar el correcto mantenimiento de los sistemas informáticos y la continuidad de la actividad laboral en los ámbitos públicos y privados.

Los avances en tecnología y la aparición de nuevos sistemas, como la computación en la nube, suponen un trabajo de revisión y mejora permanente de los procedimientos que afectan a estas gestiones.

El presente trabajo se encuadra dentro de esta tarea y plantea una serie de procedimientos, basados en ITIL, para la mejora de estas gestiones en entornos Cloud.

SUMMARY

The management of events, incidents and problems is essential to ensure the availability, capacity and performance, security and continuity of information systems supporting any type of organization.

Disruptive technologies, methodologies and models such as Cloud computingspur the need of continuous improvement of, among others, processes and procedures.

The present work is set withing this framework. We propose a serial of ITIL-inspirated processes to be applied in Cloud environments.

PALABRAS CLAVE

En este apartado se pretende introducir una serie de términos para conseguir proporcionar una mejor comprensión de este trabajo.

Más adelante, se profundizará en cada uno de estos términos.

- **Evento**: cualquier cambio de estado que tenga importancia para la gestión de un servicio u otro elemento de configuración. [1]
- **Incidencia**: una interrupción no planificada a un servicio o una reducción en la calidad de un servicio. [1]
- **Problema**: una causa o posible causa de uno o más incidentes. [1]
- **Alerta**: una notificación de que se ha alcanzado un umbral, se ha producido un error o algo ha cambiado. [1] Este término se utilizará para englobar el conjunto de eventos, incidencias y problemas.

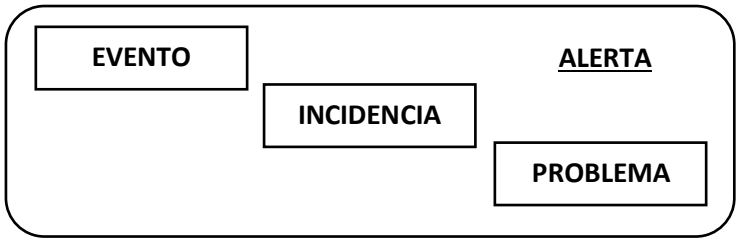


Imagen - 1: Conceptos generales

RESUMEN EXTENDIDO

Tanto en las empresas privadas como en las sociedades públicas, la necesidad de almacenamiento de datos e información importante es constante.

Hace no muchas décadas, los archivos físicos eran el principal mecanismo de almacenamiento de datos e información. Las empresas consumían grandes superficies para almacenar todos estos archivos, llegando al punto de ampliar las propias oficinas únicamente para guardar dichos archivos.

Toda información es importante y, se debe guardar y cuidar con mucho recelo. En innumerables ocasiones se producía el denominado espionaje industrial, que consistía en conseguir obtener todos los datos importantes de las empresas competidoras para conseguir ponerse a la vanguardia de su sector. Esta práctica, sobra decir, era y sigue siendo ilegal.

Con el avance de la tecnología y la aparición de la informática, todo esto sufrió una brusca revolución. La información empezaba a tratarse de forma digital, empezaba a dejarse de lado el almacenaje de papeles. Empezaron a aparecer los distintos sistemas de almacenamiento que conocemos hoy en día, que conseguían guardar en espacios mucho más reducidos una mayor cantidad de datos.

Además, se ganó en durabilidad de la información, ya que los documentos físicos podrían sufrir desperfectos únicamente con el paso del tiempo, mientras que, con los nuevos sistemas y la digitalización, los datos se podrían llegar a mantener intactos durante años o décadas. Pero este sistema tampoco es perfecto, ya que se debe renovar y actualizar progresivamente.

Con estos avances, se ganó en seguridad e integridad, ya que no sería tan sencillo realizar espionaje industrial. No obstante, sigue existiendo esta práctica, pero se ha vuelto mucho más compleja de realizar y, en el caso de enfrentarse a una situación de estas, es muy probable que se descubra el culpable de esta filtración de información.

El espionaje industrial ya no sólo se podía dar de forma física, entrar en una empresa y sacar información de sus bases de datos o de sus gestores de archivos, ahora también aparece la figura del hacker, quien puede realizar estas mismas actividades, pero ya no es necesario que las realice estando presencialmente en la organización. La informática e Internet se han convertido en otro riesgo a tener en cuenta, ya que lo único que no se puede hackear es un papel.

Los avances tecnológicos no solo revolucionaron el almacenamiento y el tratamiento de los datos, además provocaron grandes cambios a la hora de realizar las tareas. Ya no era necesario tener un montón de herramientas destinadas a realizar distintas tareas para llegar a un fin, ahora se consigue desarrollar un sinfín de aplicaciones que se pueden destinar a la realización de una o varias tareas.

La disponibilidad de esta información también se vio afectada por la aparición de la informática. Ya no era necesario rebuscar entre todos los papeles para localizar algún dato de hace meses o, incluso, años, lo cual podría suponer una gran pérdida de tiempo. Con la informática, todos los datos quedan guardados y la capacidad de consulta de estos es más rápida y eficaz.

Pero, finalmente, con el avance de los sistemas y las nuevas necesidades que han surgido, aparece en escena un nuevo competidor, que será capaz de rivalizar en todos y cada uno de estos aspectos, y con éxito indiscutible, los sistemas Cloud.

Este nuevo competidor destacó en todos los sentidos. Por primera vez, los clientes de los sistemas Cloud podían adquirir el almacenamiento a medida, arrancando de raíz el problema del espacio físico. Además, los sistemas Cloud estaban orientados a todo tipo de servicios, desde guardar fotos o documentos personales hasta alojar máquinas o servidores. Pero, no todo es perfecto en estos nuevos sistemas, ya que se dependía totalmente de la administración de los proveedores de estos sistemas. A estos nuevos servicios se les conoce como Cloud computing, computación en la nube o simplemente Cloud.

Una gran discrepancia que da este nuevo sistema está relacionada con la seguridad. Por primera vez desde la aparición de la informática, la seguridad pasa a ser competencia única y exclusiva de los proveedores de los sistemas Cloud, aunque el cliente siempre podrá elegir los niveles de seguridad que desea contratar, ya que no se necesitaría el mismo nivel de seguridad para una u otra cosa.

Hay que tener en cuenta que todo avance tiene sus dificultades. Al igual que cualquier otro sistema, el Cloud computing tiene sus eventos, sus incidencias y sus problemas. Por este motivo, se crean una serie de procedimientos cuyo fin es hacer frente a cada una de estas dificultades. Cada procedimiento, aunque puedan parecer similares, tienen diferencias fundamentales, dichas diferencias se orientan al correcto tratamiento de cada una de ellas.

Para hacer frente a esta necesidad de creación de procedimientos, ITIL definió las pautas que deberían seguirse a la hora de hacer frente a estas alertas, pero en ocasiones estas pautas necesitan mejoras para adaptarse a los sistemas que se intentan gestionar. Esto se puede traducir en pequeños pasos que permitan la mejora de los procedimientos de gestión o en otros más revolucionarios como la creación de nuevos procedimientos y la adaptación o unificación de los ya existentes.

Los procedimientos de gestión debían ser distintos para cada tipo de alerta, ya que, si no es lo mismo un evento que una incidencia que un problema, tampoco deberá ser el mismo procedimiento el destinado para gestionar cada una de estas alertas. Esto lo contempla de forma muy estricta ITIL, ya que define tres procedimientos distintos y claramente diferenciados para la gestión individual de cada una de estas alertas.

También se debe tener en cuenta el sistema al que se le quieran aplicar estos procedimientos. No es lo mismo gestionar una alerta de un sistema rudimentario como puede ser, por ejemplo, una calculadora o un sistema más innovador como pueden ser los entornos Cloud.

Indagando un poco más en el ejemplo de la calculadora, se puede ver con claridad la independencia entre estos tres tipos de alertas:

- Se localiza claramente la diversidad de eventos que pueden aparecer, como los que pueden causarse al pulsar cualquier botón.

- También puede aparecer algún tipo de problema, como puede ser que se acabe la pila o la batería. Pero estos problemas son, en definitiva, problemas físicos, ajenos al sistema de la calculadora.

- Pero en muy raras ocasiones aparecerán algún tipo de incidencia, ya que el sistema que lleva una calculadora es cerrado y no se va a interferir de ninguna forma en él. En la mayoría de las incidencias que pueda tener una calculadora puede darse por la inexperiencia del usuario en su uso.

Pero esto ya no ocurre en los nuevos sistemas que están surgiendo o que acaban de surgir, como puede ser la IA (Inteligencia artificial), la minería de datos o el sistema que se pretende mostrar en este trabajo, Cloud computing.

Estos sistemas más complejos se caracterizan por su innovación y actualización continua. Por este motivo, las definiciones individuales de gestión de las distintas alertas definidas por ITIL deben adaptarse, ya que puede llegar el supuesto de que una alerta a su vez cause otra distinta o que la respuesta aplicada para solventar una alerta provoque otra alerta distinta.

En este trabajo se pretende mostrar una visión en profundidad del Cloud computing, llegando a analizar las distintas arquitecturas que se manifiestan, los diversos servicios que pueden llegar a ofrecer y la complejidad que existe tras de este sistema. Además, se pretende mostrar una posible adaptación de los procesos de gestión de eventos, incidencias y problemas de forma individual, y como se podrían adaptar para crear una serie de procedimientos que puedan llegar a gestionar con eficacia estas alertas, teniendo en cuenta la posible correlación que puedan existir entre ellas, sin dejar de lado la definición estándar proporcionada por ITIL.

Hay que mencionar que los procedimientos individuales plasmados en este trabajo están basados en ITIL y no corresponden con ningún procedimiento existente definido por una tecnología en concreto. Además, hay que aclarar que el procedimiento que engloba la gestión de los tres tipos de alertas, tampoco se corresponden con ningún procedimiento definido por cualquier tipo de tecnología, únicamente está basado en las definiciones proporcionadas por ITIL y únicamente pretende ser un ejemplo de una de las posibles creaciones o modificaciones de procedimiento de gestión de eventos, incidencias y problemas destinado a entornos Cloud, basado en un estudio teórico desarrollado en este trabajo.

1. Introducción

En la actualidad, tanto en el mundo laboral como en el personal, se utiliza con mucha frecuencia los servicios que ofrecen los sistemas Cloud, ya sea para funciones comerciales (alojamiento de servidores, virtualización, aplicaciones…) o para uso personal (almacenamiento de documentos, imágenes, vídeos…).

A lo largo de este proyecto, se pretende profundizar en los sistemas Cloud (funcionamiento, utilidad, principales proveedores…) hasta llegar a la creación de distintos procedimientos a seguir en el caso de percibir algún tipo de evento, incidencia y/o problema.

2. Objetivo

Estudio en profundidad de los entornos Cloud y de la gestión de eventos, incidencias y problemas descritos por los procesos definidos por ITIL.

Además, se procederá con la creación de los procedimientos necesarios para conseguir abordar satisfactoriamente el tratamiento de los eventos, incidencias o problemas que puedan surgir, adaptando los procesos de ITIL definidos para cada una de estas alertas de forma individual y creando un procedimiento para abordar estas tres alertas de forma conjunta.

3. Ámbito

El estudio teórico estará orientado en entornos Cloud y en ITIL, mientras que el desarrollo de posibles nuevos procedimientos se orientará para sistemas poco complejos (en el caso de los procedimientos individuales) y para entornos Cloud (en el caso de un procedimiento destinado para gestionar sistemas más completos y complejos).

4. Alcance

Este trabajo pretende conseguir una visión más amplia de los sistemas Cloud y de la creación de procedimientos de gestión. Además de mostrar los factores a tener en cuenta a la hora de crear distintos procedimientos para gestionar eventos, incidencias y problemas en un sistema determinado, y los diversos escenarios que pueden llegar a surgir dependiendo del alcance que se busque a la hora de crear el procedimiento.

En este trabajo, se orientará a la gestión de eventos, incidencias y problemas por la complejidad que puede tener su gestión en entornos tan completos y complejos como pueden ser los sistemas Cloud, ya que habrá situaciones en que su gestión sea competencia de los proveedores o administradores y no de los usuarios finales.

5. Sistemas Cloud

5.1. Descripción

Cloud computing es un nuevo sistema que permite ofertar un catálogo de servicios estandarizados y satisfacer con ellos las necesidades de un negocio, de forma adaptativa y flexible, en caso de existir periodos de picos de trabajo o de demanda no previsible, consumiendo únicamente lo necesario. Se puede acceder a la información o servicios mediante una conexión a Internet desde un dispositivo móvil o fijo, independientemente de su localización.

La computación en la nube permite aumentar la cantidad de servicios basados en la red. Esto es un factor muy positivo tanto para los proveedores (pueden ofrecer un mayor número de servicios de una forma más rápida y eficiente) como para los clientes (reciben total transparencia y velocidad en el sistema, además de realizar únicamente el pago por el consumo realizado).

Estos sistemas cuentan con un gran número de ventajas, como, por ejemplo:

- Alto grado de automatización.
- Rápida movilización de recursos.
- Gran capacidad de adaptación a la demanda.
- Virtualización avanzada.
- Precio flexible sujeto únicamente al consumo.
- Etc.

El concepto de "Cloud computing", nube informática o nube, abarca la inmensa mayoría de todos los tipos de servicios en línea, pero generalmente se refiere a una de las siguientes modalidades o a su posible combinación:

- Software como servicio.
- Plataforma como servicio.
- Infraestructura como servicio.

5.1.1. Fundamentos e historia

El concepto de Cloud computing tiene sus raíces en los años sesenta. En esa década, JCR Licklider aportó la idea de una "red de computadoras intergaláctica". Esta idea aportaba una nueva visión en la que todo el mundo pudiera estar interconectado y que pudieran acceder a los datos o herramientas desde cualquier lugar.

En 1960, John McCarthy propuso la idea de que la computación, en un futuro, podrá ser organizada como un servicio público.

No fue hasta los años noventa que Internet no podía ofrecer un ancho de banda significativo para poder desarrollar la computación en la nube. En 1999 llegó Salesforce, quien fue pionera en la en la entrega de aplicaciones empresariales a través de simples páginas web, allanando el camino para futuras publicaciones de aplicaciones en Internet.

El siguiente avance lo realizó Amazon Web Services en 2002, lanzando un conjunto de servicios basados en la nube. Incluyó computación, almacenamiento e inteligencia artificial. En 2006 lanzó Elastic Compute Cloud (EC2), un servicio comercial que permitía a los particulares y a las pequeñas empresas alquilar equipos en los que pudieran ejecutar sus propias aplicaciones.

Ese mismo año, Google presentó su Google Docs, poniendo al Cloud computing a la vanguardia, pero no sería hasta un año después que IBM y Google, junto a universidades de Estados Unidos, colaborarían para su avance.

En 2008, Eucalyptus lanzó la primera plataforma de código abierto para el despliegue de nubes privadas, compatible con API-AWS, y Open Nebula lanza el primer software de código abierto para las nubes híbridas y privadas.

En 2009, Google, entre otros, comenzó a ofrecer aplicaciones basadas en navegador.

Otros factores que han permitido el desarrollo del Cloud computing, según Jamie Turner, han sido:

- El desarrollo universal de alta velocidad del ancho de banda.
- Las tecnologías de virtualización.
- La creación de las normas universales de interoperabilidad de software.

En 2010, el concepto de Cloud computing era muy amplio, por lo que se organizó en las tres capas que existen actualmente (IaaS, PaaS y SaaS).

Finalmente, en el año 2011, Apple inició su camino en este gran mundo lanzando iCloud.

- ***Cronograma***

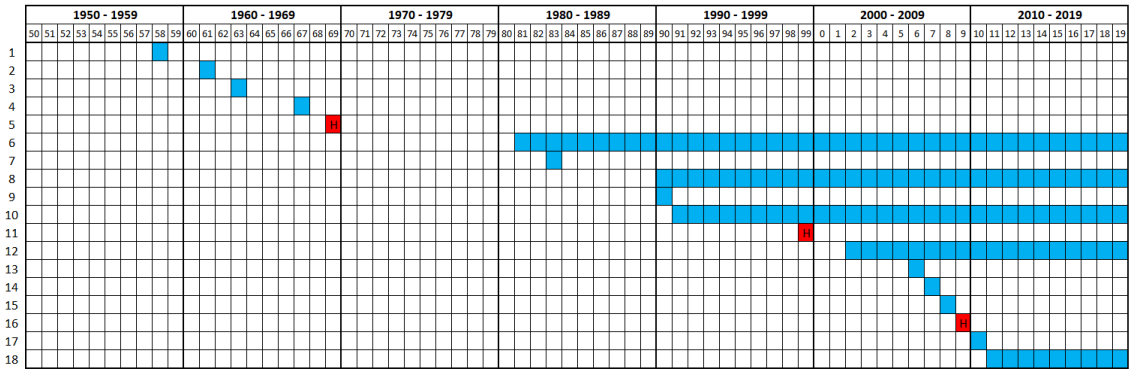


Imagen - 2: Cronograma Cloud

1. Creación del primer modem (1958).
2. Primera teoría de utilización de paquetes para transferir datos. Se empieza a sugerir el concepto de la computación en la nube (1961).
3. Aparece el concepto de la red intergaláctica (1963).
4. Primera conferencia de ARPANET (1967).
5. HITO: Conexión de las primeras 4 computadoras entre sí (1969).
6. Definición del protocolo TCP/IP y de la palabra "Internet" (1981).
7. Primer servidor de nombres de sitios (1983).
8. El aumento del ancho de banda comienza a ser significativo (años 90).
9. ARPANET llega a su fin (1990).
10. Se anuncia públicamente la World Wide Web (1991).
11. HITO: Llegada de Salesforce.com (1999).
12. Aparece AWS (2002).
13. Aparece EC2 de Amazon. La llegada de Google Docs trajo a la computación en la nube a la vanguardia (2006).
14. IBM, Google y universidades de Estados Unidos, colaboran en el avance de la computación en la nube (2007).
15. Aparecen Eucalytus y Open Nebula (2008).
16. HITO: Google, entre otros, presenta aplicaciones basadas en navegador (2009).
17. Se organiza el concepto en distintas capas (2010).
18. Aparece iCloud de Apple (2011).

5.1.2. Características

La computación en nube presenta las siguientes características clave:

- Agilidad: el proveedor tiene la capacidad de mejorar para ofrecer recursos tecnológicos.
- Coste: los recursos físicos, en general, tienen costes más elevados que los recursos en la nube. La naturaleza bajo demanda de la nube contrarresta el desembolso inicial que provoca el aprovisionamiento local.
- Escalabilidad y elasticidad: sin necesidad de cargas que acarreen una gran cantidad de tiempo, proporciona aprovisionamiento de recursos sobre una base de autoservicio casi a tiempo real.
- Independencia entre el dispositivo y la ubicación: permite a los usuarios acceder a los sistemas utilizando un navegador web, sin necesidad de estar en un lugar o de utilizar un dispositivo determinado (por ejemplo, PC o teléfono móvil).
- La virtualización permite compartir servidores y dispositivos de almacenamiento. Las aplicaciones se pueden migrar fácilmente entre servidores.
- Rendimiento: los sistemas en la nube son capaces de controlar y optimizar el uso de los recursos por sí mismos. Esta característica permite el seguimiento y el control de esta, proporcionando una mayor transparencia tanto al proveedor como al usuario final.
- Seguridad: debido a que los datos se encuentran centralizados, se puede mejorar. La seguridad en este tipo de sistemas se igual o mejor a la seguridad existente en los sistemas tradicionales, ya que los proveedores tienen en su mano la posibilidad de destinar recursos para solventar cualquier los problemas de seguridad que puedan aparecer, estos recursos en muchas ocasiones no están al alcance de los clientes. Los usuarios de Cloud son los responsables de la seguridad a nivel de la aplicación, pero es el proveedor el responsable de la seguridad de la infraestructura y de la seguridad física. [1]
- Mantenimiento: es más sencillo la instalación y el mantenimiento de aplicaciones en la computación en la nube, ya que no es necesario instalarlo ni mantenerlo de forma individual en el ordenador de cada uno de los usuarios.

5.1.3. Ventajas e inconvenientes

- ***Ventajas***

    - Integración de servidores Red. Los sistemas Cloud se pueden integrar con mayor facilidad y rapidez con el resto de las aplicaciones (tanto con software tradicional como con sistemas Cloud basados en infraestructura), ya estén desarrolladas internamente o de forma externa.

    - Cloud computing permite la prestación de servicio a nivel mundial, ya que es fácilmente adaptable, permite la recuperación total de pérdida de datos (mediante la utilización de backups) y reducen al máximo los tiempos de inactividad.

    - Una infraestructura totalmente integrada en Cloud permite a los proveedores del servicio evitar la instalación de cualquier tipo de software, ya que es proporcionado por el proveedor de la infraestructura Cloud. Los sistemas Cloud necesitan una inversión mucho menor para empezar a trabajar con ella, además de constar de una gran simplicidad.

    - Existen menos riesgos a la hora de la implementación, la cual es más rápida. Las aplicaciones de los sistemas Cloud suelen estar disponibles en un periodo de tiempo reducido, al contrario que en los sistemas tradicionales, incluso se puede aportar un gran nivel de personalización e integración de cara al cliente.

    - Las actualizaciones automáticas no afectan de forma negativa a los recursos de IT. Normalmente, a la hora de realizar una actualización a una nueva versión de las aplicaciones, los usuarios están obligados a destinar tiempo y recursos a volver a integrar y personalizar las aplicaciones. Con los sistemas Cloud no es necesaria la decisión entre conservar el trabajo o realizar la actualización, ya que todas esas integraciones y personalizaciones se mantienen de forma automática durante el periodo de la actualización.

    - Los sistemas Cloud contribuyen con el uso sostenible de la energía. Estos sistemas no necesitan la utilización de energía extra para el funcionamiento de la infraestructura, al contrario de lo que ocurría con los centros de datos tradicionales, que necesitan consumir una mayor cantidad de energía de la que en realidad necesitan. Con estos sistemas, el consumo de energía es el justo y necesario para su funcionamiento, reduciendo en gran medida el gasto innecesario de la energía.

- ***Inconvenientes***

    - La total centralización de las aplicaciones y del almacenamiento generan una total dependencia hacia el proveedor del servicio.

    - Sin acceso a Internet, la disponibilidad de las aplicaciones es nula.

    - La "salud" tecnológica y financiera de los proveedores de los sistemas Cloud condicionan la confiabilidad de los servicios. Algunos tipos de empresas o alianzas entre estas pueden causar un ambiente propicio para el monopolio, además de provocar un crecimiento desproporcionado en los servicios. [1]

    - Los servicios altamente especializados podrían tardar demasiado tiempo en ser desplegados en la nube, haciendo peligrar seriamente su disponibilidad.

    - La curva de aprendizaje en sociedades no tecnológicas es muy pronunciada, así como su consumo automático por aplicaciones, ya que la actualización continua de las aplicaciones y su madurez funcional provocan la continua modificación de sus interfaces.

    - Seguridad. La información debe recorrer una serie de canales y nodos para alcanzar su destino. Estos nodos son un foco de inseguridad. Mediante la utilización de protocolos seguros, como el protocolo HTTPS, se solventan estas inseguridades, pero disminuye la velocidad total debido a la sobrecarga que requieren.

    - Futura escalabilidad. A medida que el número de usuarios que compartan la infraestructura Cloud aumente, la sobrecarga de los servidores aumentará. Si la empresa no posee un esquema de crecimiento adecuado, se pueden producir degradaciones en el servicio.

5.2. Funcionamiento

Existen 3 elementos clave para entender cómo funciona el Cloud Computing: [2]

- Front end: el lado "cliente", desde el cual se interactúa con los servidores alojados en Cloud. Puede utilizarse a través de un navegador web o a través de una aplicación, en cualquier caso, se puede interactuar con él desde cualquier dispositivo. Se tratará de una interfaz que permita realizar peticiones o acciones, pero la ejecución real se realizará en el servidor Cloud.

- Conexión a Internet: el canal desde el que se acceder a los servidores de Cloud desde el lado del cliente (Front end). Puede tratarse de una conexión mediante una web o mediante una aplicación que, en ocasiones, permiten trabajar fuera de línea y, al restablecerse la conexión a Internet, sincronizar el trabajo realizado con el servidor de la nube.

- Back end: el lado "servidor", equipos informáticos que ejecutan las acciones o peticiones en el entorno de Cloud. Suelen estar distribuidos en varios centros de datos. Se suele contar con un servidor central encargado de gestionar el tráfico y las peticiones entrantes. A este servidor central se le denomina "Middleware".

En resumen, al utilizar los entornos Cloud, los usuarios interactúan con el Front end que, a través de una conexión a Internet, se conecta con el Back end, donde se procesan y ejecutan las peticiones, se ejecutan las aplicaciones y los procesos necesarios, y envía una respuesta al Front end, utilizando la misma conexión.

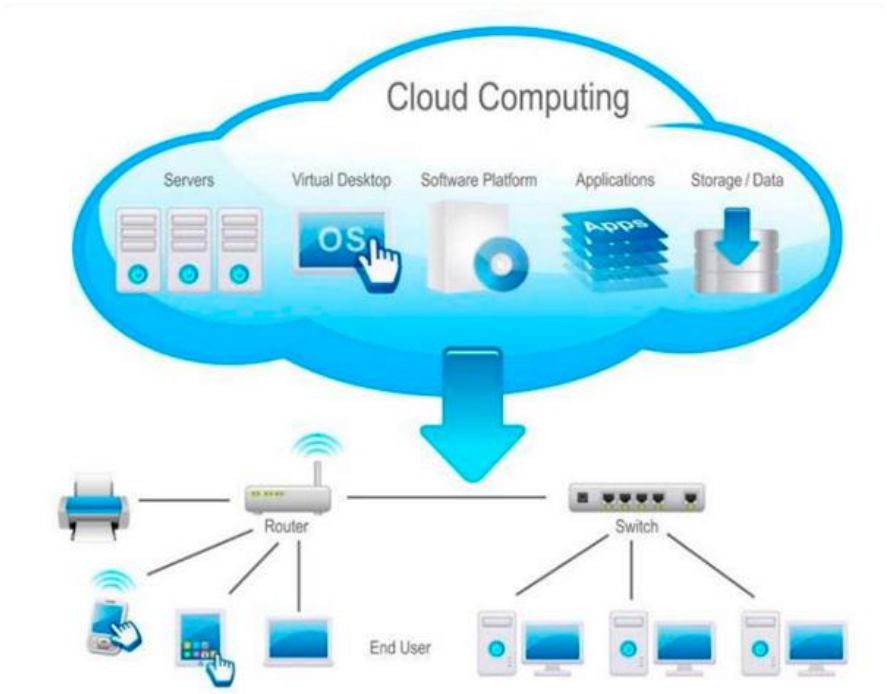


Imagen - 3: Cloud computing

5.2.1. Servicios

La amplia gama de servicios ofrecidos por las empresas de Cloud computing se puede clasificar en tres tipos básicos, coincidiendo con sus tres capas: [3]

- Infraestructura como servicio (IaaS):
  - Proporciona a los usuarios acceso a los recursos informáticos básicos.
- Plataforma como servicio (PaaS):
  - Orientadas al desarrollo de software.

- Software como servicio (SaaS):
    - Ofrece servicios de nivel de aplicación adaptados a las necesidades empresariales.

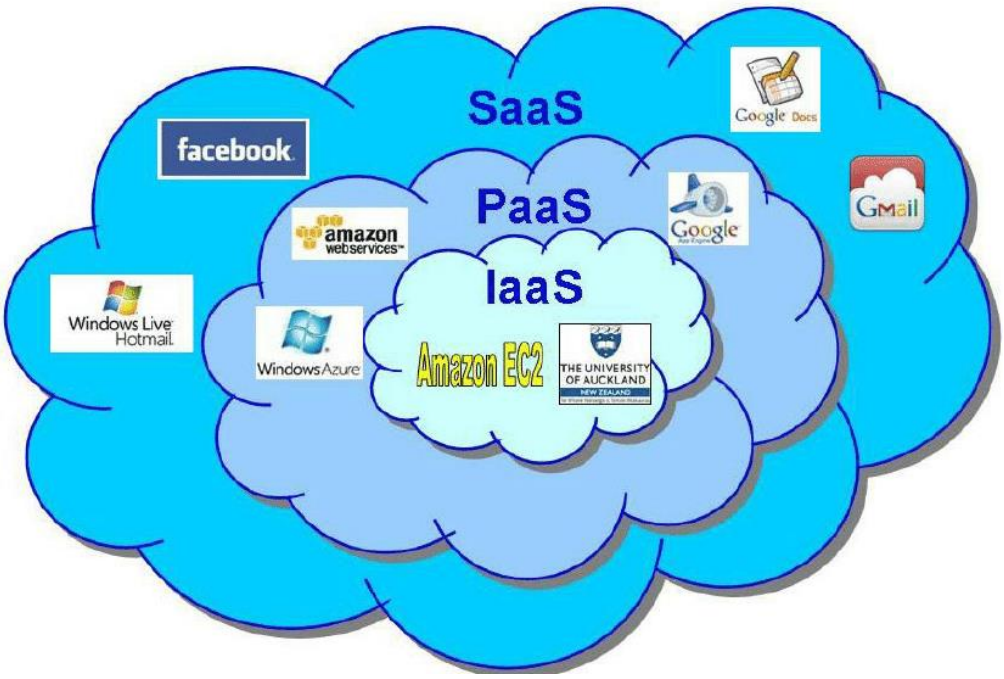


Imagen - 4: Capas Cloud

5.2.2. Tipos de nubes

- Nubes públicas: es una nube mantenida y gestionada por personas ajenas a la organización. Los datos, las aplicaciones y los procesos se mezclan con los de otros clientes en los servidores, en los sistemas de almacenamiento y en otras infraestructuras. Los clientes no conocen qué otros clientes están utilizando el mismo servidos, la misma red, los mismos sistemas de almacenamiento, etc. Todos estos recursos están disponibles al público a través del proveedor del servicio y que ofrece acceso a estos de forma remota a través de internet. [6]

- Nubes privadas: la mejor opción para las compañías que necesiten una protección de sus datos muy alta y que permita las ediciones a nivel de servicio. Se trata de una infraestructura bajo demanda y gestionada para un único cliente, el cual controla que aplicaciones se deben ejecutar y donde se debe realizar dicha ejecución. Estos clientes son los propietarios del servidor, de la red y de los discos, y pueden decidir qué usuarios pueden utilizar esta infraestructura. Las empresas, al poder administrar internamente estos servicios, tienen la ventaja de mantener la total privacidad de sus datos y pueden unificar el acceso de sus usuarios a estos o a las aplicaciones. [6]

- Nubes híbridas: se trata de una combinación de las nubes públicas y privadas. El usuario es propietario de parte de la nube, aunque, de forma controlada, comparte otras partes. Este tipo de nubes permiten el escalado aprovisionado externamente, según la demanda necesaria, pero permite la posibilidad de definir como distribuir las aplicaciones entre la parte pública y la privada. Inicialmente, es un modelo atractivo para las empresas, pero únicamente serían utilizadas para albergar aplicaciones simples, que no estén condicionadas por ninguna sincronización o que necesiten alguna base de datos compleja. Un ejemplo de este tipo de nubes serían los sistemas de correo electrónico empresarial. [6]

- Nubes comunitarias: según Joyanes Aguilar en 2012, el Instituto Nacional de Estándares y Tecnologías define la nube comunitaria a aquella que se organiza con el fin de alcanzar una función o propósito común. Son administradas por organizaciones constituyentes o por terceras partes. [6]

5.2.3. Controversia

La responsabilidad del almacenamiento de los datos y su control recae sobre los proveedores, dado que los sistemas Cloud no permiten a los clientes poseer físicamente los dispositivos necesarios para su almacenamiento, a no ser que los usuarios realicen copias de estos datos en unidades de almacenamiento externo.

Los sistemas Cloud han sido el foco de numerosas críticas, ya que los clientes pasan a depender de los proveedores y limitan su libertad. Además, numerosas críticas señalan que únicamente es posible la utilización de servicios y de aplicaciones que el proveedor esté dispuesto a proporcionar, algo muy similar a lo que ocurría con los antiguos sistemas centralizados. A esto, se le une la imposibilidad que tienen los usuarios de instalar nuevas aplicaciones, necesitando la aprobación de determinados administradores, dependiendo de la tarea que desempeñen. Por lo tanto, numerosos expertos consideran que este tipo de sistemas limitan tanto la libertad como la creatividad, los clientes dejan su privacidad y sus datos en manos de terceros, y se está consiguiendo un retorno a los antiguos sistemas centralizados. [7]

Imagen - 5: Físico VS Cloud

5.2.4. Aspectos de seguridad

La seguridad de la computación en la nube es un pilar fundamental que los proveedores de estos sistemas deben afrontar. Con respecto a los sistemas tradicionales, esta seguridad es igual o superior, ya que permite a los clientes obtener mecanismos de seguridad que antes no eran capaces de afrontar. Pero, aún sigue siendo un punto a mejorar, esto perjudica y retrasa la implantación de los sistemas Cloud seriamente.

- Seguridad como servicio [6]
    - La seguridad es proporcionada por los proveedores. Los servicios de seguridad están clasificados en categorías:
        - Gestión de identidades y acceso.
        - Prevención de pérdida de datos.
        - Seguridad en la web.
        - Seguridad para el correo electrónico.
        - Evaluación de la seguridad.
        - Gestión de instrucciones.
        - Seguridad de la información y gestión de eventos.
        - Cifrado.
        - Continuidad del negocio y recuperación de desastres.
        - Red de seguridad. [4]

- Seguridad del navegador [6]
    - En los entornos Cloud, se utilizan servidores o máquinas remotas. Los nodos de los clientes se utilizan únicamente como entrada o salida de ejecuciones, y para autenticar o autorizar a los usuarios en la información residente en la nube. Una de las plataformas más utilizadas por los usuarios para acceder a los entornos Cloud son los navegadores web. Esto se puede dividir en 2 tipos: SaaS (Software como servicio) y Web 2.0 (aplicaciones web). Para la encriptación de datos y para la autenticación se suele utilizar TLS (Transport Layer Security).

- Autenticación o identificación [6]
    - En los sistemas Cloud, el control de acceso principal es la autentificación. Es muy importante mantener estos controles de acceso, ya que los datos pueden ser visualizados por cualquiera desde Internet. Uno de los controles de acceso más utilizados es TPM (Trusted Platform Module), ya que es mucho más fuerte que la típica autentificación mediante usuario y contraseña.

- Pérdida de gobernanza [6]
    - En los entornos Cloud, los clientes pierden completamente el control frente a los proveedores en varios aspectos, influyendo de forma negativa sobre la seguridad. Por otro lado, el nivel de servicio, por defecto, no complace estas necesidades de seguridad, por lo que produce una brecha de seguridad.

- Protección de los datos [6]
    - Los sistemas Cloud ponen en riesgo la protección de datos para los usuarios de la nube y sus proveedores. Ocasiona dificultades a los proveedores del servicio como controladores de la información, dificultan la efectividad del manejo de los datos del proveedor y asegurar que los datos van por el camino adecuado. En el caso de múltiples transferencias de datos entre sistemas federados, este problema se agrava considerablemente. Por lo contrario, algunos proveedores ofrecen información de sus prácticas con esos datos, además de ofrecer una serie de certificaciones para el procesamiento de datos, actividades de seguridad y controles de datos.

5.2.5. Limitaciones

Algunas limitaciones que están retrasando un poco a la computación en la nube son las siguientes:

- Pérdidas de datos/fuga [6]
    - Los datos en la nube pueden comprometerse de diversas maneras, llegando a ser modificados, borrados sin backups, sacados de contexto o visualizados por personal no autorizado.

- Dificultad de valorar la fiabilidad de los proveedores [6]
    - Por estadística, algún empleado de un proveedor o algún empleado subcontratado no es de fiar, lo que podría traducirse en fuga de información. Por lo que se deben implementar buenos procedimientos de investigación de recursos humanos, además de políticas y procedimientos para fortalecer la seguridad de la información.

- Fuerza de los mecanismos de autentificación [6]
    - El punto débil de los entornos Cloud son los mecanismos de autentificación. Un atacante puede hacerse con la cuenta de usuario de un cliente y acceder a las máquinas virtuales, consiguiendo acceder a aplicaciones, recursos almacenados y datos sensibles.

5.3. Principales proveedores

En este apartado se enumera una serie de proveedores de sistemas Cloud, junto con una pequeña introducción de cada uno de ellos:

- ***Amazon Web Services (AWS):***

  AWS tiene significativamente más servicios y más funciones dentro de esos servicios que cualquier otro proveedor de la nube. Con unos costes más reducidos, mover las aplicaciones existentes a la nube de forma más rápida y sencilla.

  AWS también tiene la funcionalidad más profunda dentro de esos servicios. Por ejemplo, AWS ofrece la más amplia variedad de bases de datos diseñadas específicamente para diferentes tipos de aplicaciones para que pueda elegir la herramienta adecuada para el trabajo y obtener el mejor coste y rendimiento. [6]

Imagen - 6: AWS

- ***Microsoft Azure:***

  Microsoft es uno de los principales proveedores globales de servicios informáticos en la nube para empresas de todos los tamaños. Es un servicio de computación en la nube creado para construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centros de datos. Proporciona software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS) y es compatible con muchos lenguajes, herramientas y marcos de programación diferentes, incluidos software y sistemas específicos de Microsoft y de terceros. [7]

Imagen - 7: Azure

- ***IBM Cloud:***

  Es un conjunto de servicios de computación en la nube para empresas que ofrece la compañía de tecnología de la información IBM. IBM Cloud incluye infraestructura como servicio (IaaS), software como servicio (SaaS) y plataforma como servicio (PaaS) ofrecidos a través de modelos de entrega en la nube públicos, privados e híbridos, además de los componentes que componen esas nubes. [8]

Imagen - 8: IBM

- ***Google Cloud:***

  Google Cloud reúne todas las aplicaciones que Google ofrecía por separado en una misma plataforma. Destaca por su infraestructura rápida y fácilmente escalable, destinada para crear soluciones mediante la tecnología que alberga la nube.

  Google Cloud utiliza la nube como un espacio virtual que engloba el acceso, el almacenamiento y la gestión de los datos sin necesidad de realizar las tareas en hardware o software adicional.

  Google ofrece una variedad de servicios basados en la nube. Google Cloud Print permite imprimir sin necesidad de un sistema operativo, simplemente desde la web desde cualquier dispositivo. Simplemente bastaría con enviar el archivo a cualquier impresora que se encuentre conectada a la nube. Google también ofrece espacio en la nube para desarrolladores de bases de datos SQL para crear aplicaciones, así como para los usuarios de Microsoft Office que deseen editar colaborativamente documentos de Word, PowerPoint y Excel, sin necesidad de la utilización de un cliente local. [9]

Imagen - 9: Google

- ***Oracle Cloud:***

  Combina la plataforma como servicio (PaaS) de Oracle con la infraestructura en la nube, con lo que podrá ofrecer innovación más rápido que nunca y disfrutar de la escalabilidad y la fiabilidad que se espera de Oracle.

  Oracle demuestra avances en la tecnología de plataforma en la nube al extender Oracle Autonomous Cloud en toda la plataforma. Los servicios de autonomía dentro de la plataforma aprovechan la inteligencia artificial (IA) y el machine learning para ayudar a las organizaciones a reducir costes, reducir riesgos, acelerar la innovación y obtener información predictiva. [10]

Imagen - 10: Oracle

- ***VMware:***

  Proporciona software de virtualización disponible para ordenadores compatibles X86. Entre este software se incluyen VMware Workstation, y los gratuitos VMware Server y VMware Player. VMware funcionar en plataformas de cualquier sistema operativo que utilicen procesadores Intel (VMware Fusion). [11]

Imagen - 11: VmWare

- ***iCloud:***

  iCloud es un sistema de almacenamiento nube o Cloud computing de Apple Inc. Se basa en Amazon AWS y Microsoft Azure.

  El sistema basado en la nube permite a los usuarios almacenar música, videos, fotos, aplicaciones, documentos, enlaces favoritos de navegador, recordatorios, notas, iBooks y contactos, además de servir como plataforma para servidores de correo electrónico de Apple y los calendarios. [12]

Imagen - 12: iCloud

6. Alertas

En este trabajo, se utilizará el término alerta para referirse a un conjunto de eventos, incidencias y problemas, ya que, al detectar a cualquiera de ellos, se recibiría una alerta.

En la siguiente tabla se muestra una pequeña comparativa, la cual se desarrollará más adelante:

	Evento	*Incidencia*	*Problema*
DEFINICIÓN	Es una acción que se puede utilizar dándole una respuesta correcta.	Evento que afecte al desarrollo normal de la actividad.	Incidente que imposibilita el desarrollo de la actividad.
GRAVEDAD	No afecta a la continuidad de la actividad.	Afecta a la continuidad de la actividad de forma leve.	Pone en riesgo la continuidad de la actividad.
EJEMPLO	Clic de un ratón.	Buzón de correo lleno.	Destrucción de discos duros de forma inesperada.

Imagen - 13: Comparativa alertas

6.1. Eventos

De acuerdo con el diccionario de la RAE (Real Academia Española), el término evento tiene 3 grandes usos:

- Un evento es un suceso de importancia que se encuentra programado. Este suceso puede ser deportivo, artístico o social. [14]
- El segundo uso contradice al primero. Evento hace referencia a algo imprevisto o que puede acaecer, aunque no haya seguridad al respecto. Se trataría de una eventualidad, algo que escapa de la planificación.
- En tercer lugar, este uso engloba los 2 anteriores: un evento es un acaecimiento, una cosa que sucede. Esta definición proporciona una nueva perspectiva, ya que un evento puede ser planificado o darse de forma imprevista.

Para la ciencia, un evento es un fenómeno o un acontecimiento que se da en un momento y en un lugar determinado.

En las matemáticas, al subconjunto de un espacio muestral se le conoce como evento estadístico y se trataría de los posibles resultados que se pueden obtener al realizar un experimento aleatorio.

Para la informática, se define evento como la acción que detecta un programa, que puede hacer uso de él o ignorarlo. Normalmente, una aplicación cuenta con varios hilos de ejecución destinados a atender los distintos eventos que se le presenten. Una de las fuentes más habituales de origen de eventos son las acciones de los usuarios con los periféricos de entrada (teclado, ratón, etc.). Además, cualquier programa puede disparar sus propios eventos, como puede ser la de comunicar la finalización de una tarea o una función en concreto.

6.2. Incidencias

La terminología ITIL define un incidente como:

- Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción de este o una reducción de la calidad de dicho servicio. El objetivo de ITIL es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible. [1]

6.2.1. Incidentes, problemas y errores conocidos

Un incidente puede tratarse de un "problemas conocidos", es decir, puede coincidir con un fallo del que se desconoce su origen. También puede tratarse de un "error conocido" bajo el control de la gestión de problemas y registrado como un error conocido, es decir, un fallo del cual se conoce la causa y para el que existe una solución.

Se conseguirá una mayor velocidad a la hora de resolver estos incidentes si previamente se ha definido alguna estrategia de resolución. Cuando una incidencia no es el resultado de un error conocido o de un problema, puede tratarse de un fallo puntual o puede ser necesario iniciar una gestión de problemas, de tal forma que dicho incidente quede registrado para futuras ocasiones.

6.2.2. Incidentes y cambios

Las incidencias son la consecuencia de errores o fallos en la infraestructura IT. Estas incidencias pueden tener una causa aparente cuya resolución no necesitaría inversiones a largo plazo. Esta resolución podría tratarse de una reparación o de una petición de cambio que solventase el error.

Se podrá crear el registro de un problema cuando un incidente es considerado grave o se tiene constancia de múltiples casos de incidentes similares. Dicho problema no podrá ser registrado hasta que no se haya repetido varias veces el mismo incidente. Un problema y una incidencia se gestionan de distinta forma, se desarrolla en otro equipo de trabajo y se controla mediante la gestión de problemas. Un problema se convierte en un "problema conocido" cuando se ha identificado el problema, pero no se conoce la solución, por otro lado, pasa a ser en un "error conocido" tras identificarse las causas del problema. Para finalizar, se podrá realizar una petición de cambio para solventar el error y, en ese preciso momento, el proyecto pasará a ser competencia de la gestión del cambio.

Una solicitud de un nuevo servicio se clasifica como una solicitud de cambio y no como un incidente.

6.3. Problemas

De acuerdo con el diccionario de la Real Academia Española (RAE), un problema sería una cuestión que se trata de aclarar. Conjunto de hechos o circunstancias que dificultan la consecución de algún fin.

Según ITIL, un problema es la causa subyacente a uno o más incidentes. [1]

En general, un problema puede ser un hecho puntual o ser derivado de un incidente. Cuando un problema es conocido, es decir, se conoce su origen, sus posibles consecuencias y, además, se conoce la mejor forma de solventarlo, ese problema pasa a ser un incidente. Por lo contrario, si un incidente desconocido no es un hecho recursivo y es completamente desconocido, pasaría a clasificarse como problema.

De acuerdo con esto, se puede concluir que cualquier incidente que sea totalmente desconocido o que interrumpa en su totalidad el desarrollo esperado de alguna tarea, se tratará de un problema. Los problemas son las alertas más graves y los que ponen en gran riesgo la continuación de la actividad.

7. Estudio de campo

7.1. Cloud computing

Este tipo de sistemas evita que los ordenadores de los usuarios asuman una alta carga de trabajo en el momento de ejecutar aplicaciones necesarias para el desarrollo del trabajo de los usuarios. Pero, gracias al almacenamiento en la nube, toda esta carga de trabajo la soporta la red de equipos que forman el sistema Cloud, agilizando el trabajo y facilitando la accesibilidad sin afectar a los equipos de los usuarios.

Lo único realmente necesario para el usuario no es una aplicación instalada en su equipo, sino ejecutarlo a través del navegador de internet como si se tratara de cualquier otra web. Los sistemas Cloud realizarán el resto del trabajo.

En conclusión, los sistemas Cloud cuentan con una serie de ventajas respecto a los sistemas tradicionales. Multiplica los recursos a los cuales el usuario puede tener acceso de una forma rápida y sencilla, además de evitar el coste de licencias de las aplicaciones y de los softwares para cada equipo, un gasto muy significativo para las empresas que los sistemas Cloud reducen considerablemente.

Cloud computing se divide en tres niveles o capas de servicio: [6]

Imagen - 14: Niveles Cloud

7.1.1. Infraestructura como servicio (IaaS)

La infraestructura como servicio es el nivel más inferior de Cloud computing. Ofrece la infraestructura hardware como un servicio en red (almacenamiento o capacidad de procesamiento). Se pone a disposición del usuario servidores, enrutadores, sistemas de almacenamiento, conexiones y otros sistemas para manejar cargas de trabajo (procesamiento en batch o aumento de servidor o de almacenamiento durante los picos de carga de trabajo). [6]

Ejemplos conocidos son: Amazón Web Services (AWS), Joyent.

Imagen - 15: IaaS

7.1.2. Plataforma como servicio (PaaS)

Se trata de la capa intermedia de Cloud computing. Ofrece la plataforma como servicio. Aquí, se puede encontrar un entorno de trabajo que permite tener un ambiente de desarrollo mediante una serie de herramientas y módulos. Ofrece al usuario una representación de una plataforma de desarrollo disponible en la red.

Facilita la implementación de aplicaciones, reduciendo el coste y la complejidad de administrar hardware y/o software obtenido de un proveedor específico. [6]

Un ejemplo conocido: Azure de Microsoft.

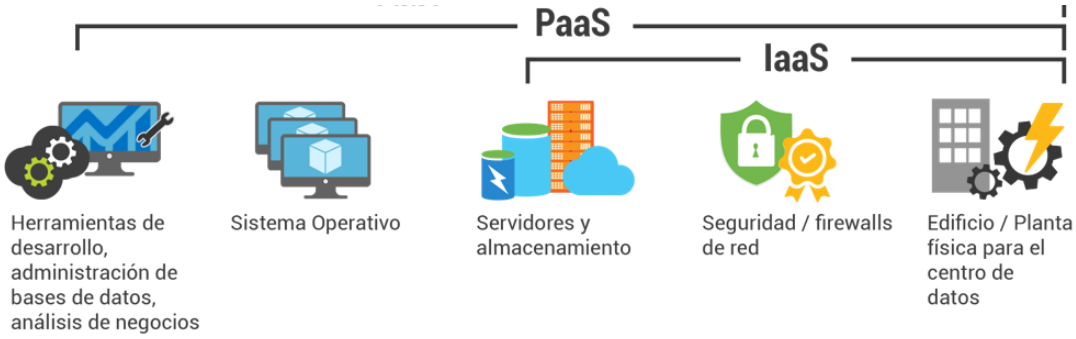


Imagen - 16: PaaS

7.1.3. Software como servicio (SaaS)

El software como servicio es la capa de más externa/alta de la nube y ofrece aplicaciones como servicios a los que pueden acceder múltiples usuarios de forma simultánea. Estas aplicaciones se encuentran instaladas en los servidores del proveedor, de forma que cada aplicación se ejecuta en una sola instancia y ofrece acceso múltiple bajo demanda, para todos los usuarios que lo necesiten.

El software en la nube elimina la necesidad de instalación y ejecución de aplicaciones en los equipos de los usuarios finales y elimina la carga del mantenimiento y del soporte técnico del software. [6]

Ejemplos de SaaS más conocidos son: Salesforce, Google Apps, Microsoft Office 365

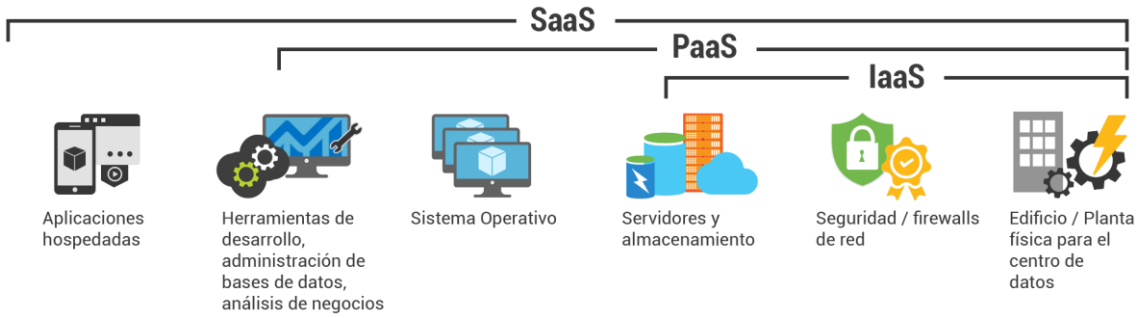


Imagen - 17: SaaS

7.2. Alertas

7.2.1. Eventos

La Gestión de Eventos estaba incluida en ITIL v2 dentro de la Gestión de la Infraestructura. En ITIL v3, los objetivos y las actividades de la Gestión de Eventos son idénticas a las de ITIL v2.

Además, en ITIL v3 la Gestión de Eventos es considerado como un desencadenante para las actividades en la Gestión de Incidentes y la Gestión de Problemas.

El proceso de Gestión de Eventos en ITIL v3 contiene los siguientes subprocesos [18]:

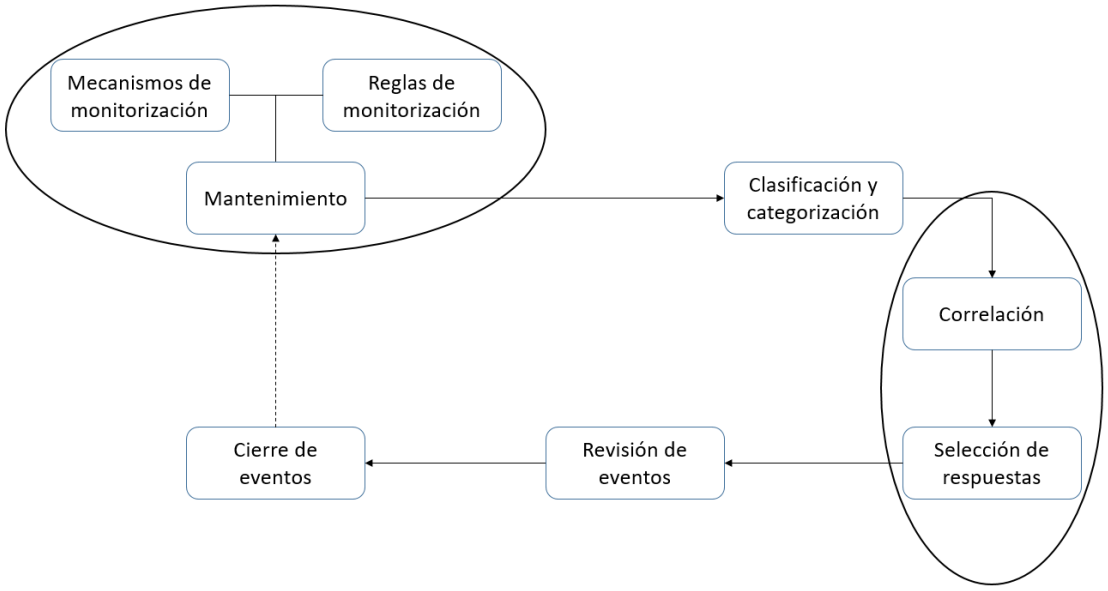


Imagen - 18: Proceso ITIL gestión de Eventos

- ***Mantenimiento de Mecanismos y Reglas de Monitorización de Eventos***

  Establecer y mantener los mecanismos para generar reglas efectivas para los procesos de descarte y correlación de Eventos.

- ***Clasificación y Categorización de Eventos***

  Clasificar aquellos eventos que se pueden obviar, y asignar categorías a los que son significativos.

- ***Correlación de Eventos y Selección de Respuestas***

  Interpretar el significado de un Evento y elegir una respuesta apropiada.

- ***Revisión y Cierre de Eventos***

  Verificar que la respuesta elegida para el Evento sea adecuada y verificar si se puede cerrar dicho Evento. Además, hay que asegurar que se analicen los registros de los eventos de forma que se identifiquen patrones y/o tendencias que puedan indicar medidas correctivas necesarias.

7.2.2. Incidencias

El proceso habitual de gestión de incidentes es el siguiente:

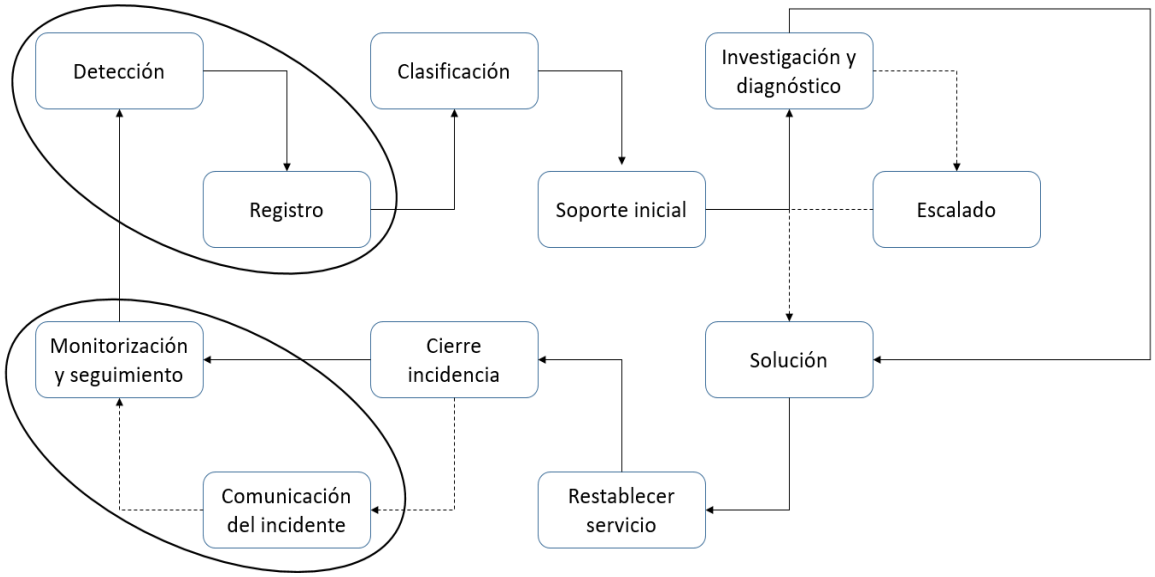


Imagen - 19: Proceso de gestión de Incidencias

- ***Detección y registro del incidente***

  Mediante la detección de un sistema de monitorización o mediante la afectación a uno o más usuarios, se crea una nueva incidencia en un sistema de solicitud de tickets, por ejemplo, Help Desk.

- ***Clasificación y soporte inicial***

  Como pueden recibirse varias incidencias de forma simultánea, a continuación, habrá que determinar el nivel de prioridad, para poder enviarlo al nivel de soporte correspondiente.

La mayoría de las aplicaciones de tickets, permiten realizar la asignación de incidencias de forma automática, consiguiendo reducir los tiempos de atención, según las reglas de negocio, creando los criterios necesarios.

La prioridad de las incidencias se asigna según:

- Impacto: afectación a la actividad y/o al número de usuarios afectados.
- Urgencia: tiempo máximo para su resolución y/o nivel de servicio o SLA (Service Level Agreement).

- ***Investigación y diagnóstico***

  Para comenzar, se debe identificar, analizar y documentar todos los síntomas relacionados con la incidencia.

- ***Escalado***

  Es un mecanismo que permite obtener, de una forma más temprana, una resolución apropiada que se hubiera podido aplicar en etapas más avanzadas de este proceso. Esto se da cuando el personal de un nivel de soporte determinado transfiere el incidente hacia un nivel de soporte superior. Esto ocurre por:

  - Falta de conocimientos.
  - Poca experiencia.
  - Falta de recursos requeridos.

- ***Solución y restablecimiento del servicio***

  Es importante conseguir una resolución temprana, pero lo principal es conseguir restablecer el servicio.

  Una vez restablecido el servicio, se podrá agregar la solución a la base de conocimiento (KB – Knowledge Base), que ayudará con la reducción de los tiempos de respuesta cuando se vuelva a producir esta incidencia o una similar.

- ***Cierre del incidente***

  Una vez restablecido el servicio y que el usuario confirme que el problema se encuentra solucionado, se realiza el cierre de la incidencia realizando una documentación detallada.

  Si se tiene conocimiento de la causa de la incidencia, se añadirá a la base de conocimiento.

  Si, por lo contrario, no se conoce la causa de la incidencia, se generará un caso donde se realizará un análisis de toda la documentación y se realizarán las acciones necesarias para encontrar la causa.

- ***Monitorización, seguimiento y comunicación del incidente***

  Es importante medir el rendimiento del área de soporte. Esto se consigue mediante el análisis de la incidencia, el tiempo empleado en resolverla y la propia resolución.

En ITIL v3, los objetivos y las actividades de la Gestión de Incidencias son idénticas a las de ITIL v2.

En ITIL v3 se establece una diferencia entre "Incidentes" (interrupciones del servicio) y "Solicitudes de Servicio" (consultas básicas de los usuarios como, por ejemplo, restablecer contraseñas, etc.). De las solicitudes de servicio ya no se encarga la Gestión de Incidentes, pasa a ser competencia del proceso de "Cumplimiento de la Solicitud".

En ITIL v3 se ha añadido un proceso para tratar los casos urgentes, también llamados "Incidentes Graves".

El proceso ITIL v3 Gestión de Incidentes abarca los siguientes subprocesos [19]:

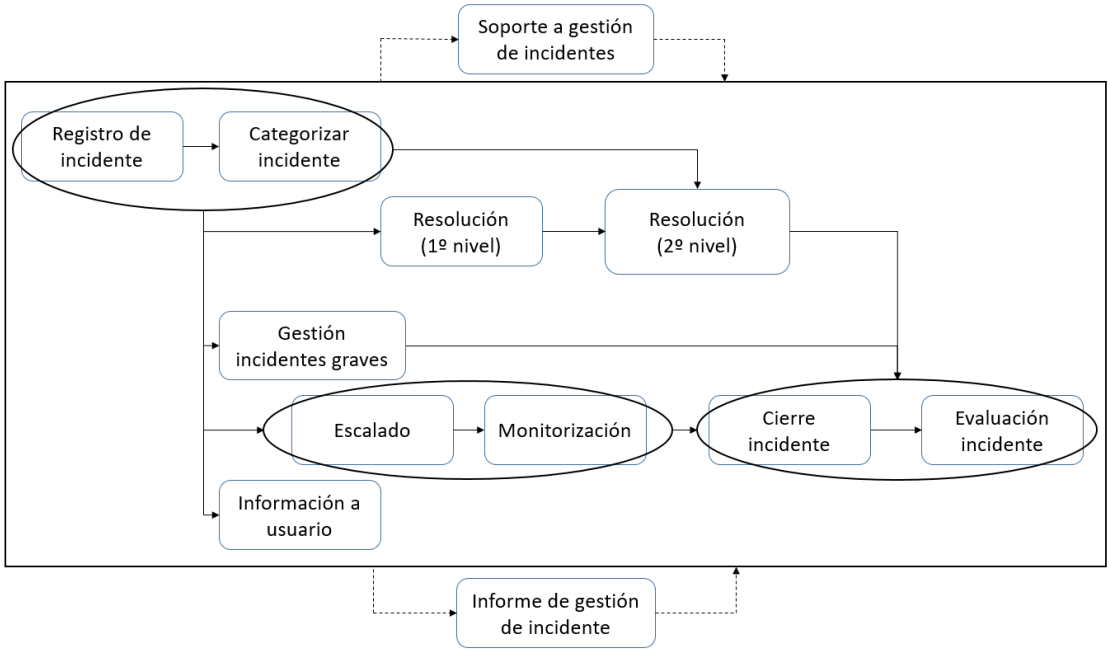


Imagen - 20: Proceso ITIL gestión de Incidencias

- ***Soporte a Gestión de Incidentes***

  Proveer y mantener las herramientas, las reglas y los procesos para conseguir un manejo de Incidencias efectivo y eficiente.

- ***Registro y Categorización de Incidentes***

  Registrar y asignar prioridades a las incidencias, de forma que se faciliten soluciones efectivas e inmediatas.

- ***Resolución de Incidentes por el Soporte de Primera Línea***

  Resolver una Incidencia (interrupción del servicio) en un periodo reducido de tiempo acordado por este nivel de resolución. La finalidad es conseguir el restablecimiento del servicio IT de una forma temprana, o aportar alguna solución temporal en el caso de ser necesario. Una vez que se verifique que el soporte en primera línea o primer nivel no puede resolver la Incidencia o cuando se exceda el periodo máximo propuesto por este nivel, la Incidencia será transferida al soporte en segunda línea o segundo nivel.

- ***Resolución de Incidentes por el Soporte de Segunda Línea***

  Resolver una Incidencia (interrupción del servicio) en un periodo reducido de tiempo acordado por este nivel de resolución. La finalidad es conseguir el restablecimiento del servicio IT de una forma temprana, o aportar alguna solución temporal en el caso de ser necesario. En el caso de ser necesario, se podrán involucrar grupos de soporte especiales o proveedores externos (soporte de tercera línea o de tercer nivel). Si no es posible corregir la Incidencia, se creará un Registro de Problema y se transferirá el caso a la Gestión de Problemas.

- ***Gestión de Incidentes Graves***

  Las Incidencias Graves provocan interrupciones considerables en el servicio y en las actividades de la sociedad, y se deben resolver con mayor urgencia. La finalidad es conseguir el restablecimiento del servicio IT de una forma temprana, o aportar alguna solución temporal en el caso de ser necesario. Si es necesario, podrán involucrarse grupos de soporte especiales o proveedores externos (soporte de tercera línea o de tercer nivel). Si no es posible corregir la Incidencia, se creará un Registro de Problema y se transferirá el caso a la Gestión de Problemas.

- ***Monitorización y Escalado de Incidentes***

  Realizar una monitorización constante del estado del procesamiento de las Incidencias pendientes, para tomar inmediatamente medidas que corrijan los efectos adversos en el caso de que peligre el nivel de servicio.

- ***Cierre y Evaluación de Incidentes***

  Antes de realizar el cierre de la Incidencia, es necesario someter el Registro de Incidente a un control de calidad final. Su finalidad es asegurar que la incidencia se haya resuelto y que toda la información necesaria para describir exhaustivamente el ciclo de vida de la incidencia haya sido recopilada con suficiente detalle. Además, esto se guardará para futuras referencias.

- ***Información Pro-Activa a Usuarios***

  Avisar e informar a los usuarios afectados de los fallos existentes en el servicio tan pronto como se conozca en el Service Desk, de forma que los usuarios sean capaces de realizar ajustes ante las posibles interrupciones del servicio. Informar a los usuarios conseguirá reducir las solicitudes de incidencias presentadas por estos.

- ***Informes de Gestión de Incidentes***

  Recopilar información relativa a los Incidentes para su posible futura utilización en otros procesos de Gestión de Servicios, y para conseguir potenciar las mejoras.

7.2.3. Problemas

La Gestión de Problemas estaba incluida en ITIL v2. En ITIL v3, los objetivos y las actividades de la Gestión de Problemas son idénticas a las de ITIL v2.

En ITIL v3 se ha añadido un nuevo subproceso (Revisión de problemas graves). Este nuevo subproceso, se ocupa de comprobar la solución de un problema para evitar que se vuelva a producir, además, de ganar experiencia para futuros casos.

El proceso ITIL v3 Gestión de Problemas abarca los siguientes subprocesos [20]:

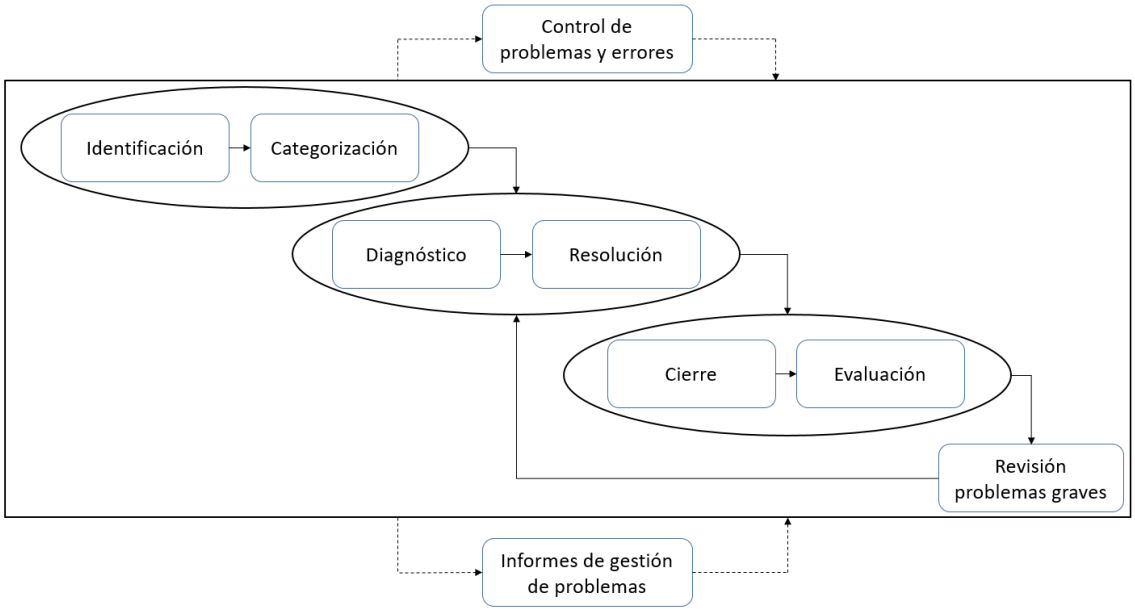


Imagen - 21: Proceso ITIL gestión de Problemas

- ***Identificación y Categorización de Problemas***

  Registrar y determinar la prioridad de los Problemas con la diligencia adecuada, de forma que se consiga que una solución rápida y efectiva sea viable.

- ***Diagnóstico y Resolución de Problemas***

  Identificar el origen de los Problemas e iniciar la solución más adecuada. Si fuera posible, se proporcionarán soluciones temporales.

- ***Control de Problemas y Errores***

  Realizar una monitorización constante de los Problemas más destacados a la luz del estatus de su procesamiento, para introducir, siempre que sea necesario, medidas correctivas.

- ***Cierre y Evaluación de Problemas***

  Es necesario asegurar que, tras solucionar de una forma exitosa un Problema, se realice una descripción histórica completa en el Registro de Problemas. Además, es necesario realizar la actualización del Registro de Errores Conocidos.

- ***Revisión de Problemas Graves***

  Como se ha mencionado anteriormente, este subproceso se encarga de comprobar la solución de un problema para evitar que se vuelva a producir, además, de ganar experiencia para futuros casos.

- ***Informes de Gestión de Problemas***

  Hay que asegurar que los otros procesos de Gestión de Servicios y la dirección de IT estén debidamente informados de los Problemas pendientes, el estado de su procesamiento y las soluciones temporales aplicadas.

8. Diseño de procedimientos

Los siguientes procedimientos se han desarrollado teniendo en cuenta el marco de trabajo ITIL que se ha visto anteriormente.

8.1. Procedimiento para la gestión de eventos

8.1.1. Gestión de eventos en ITIL

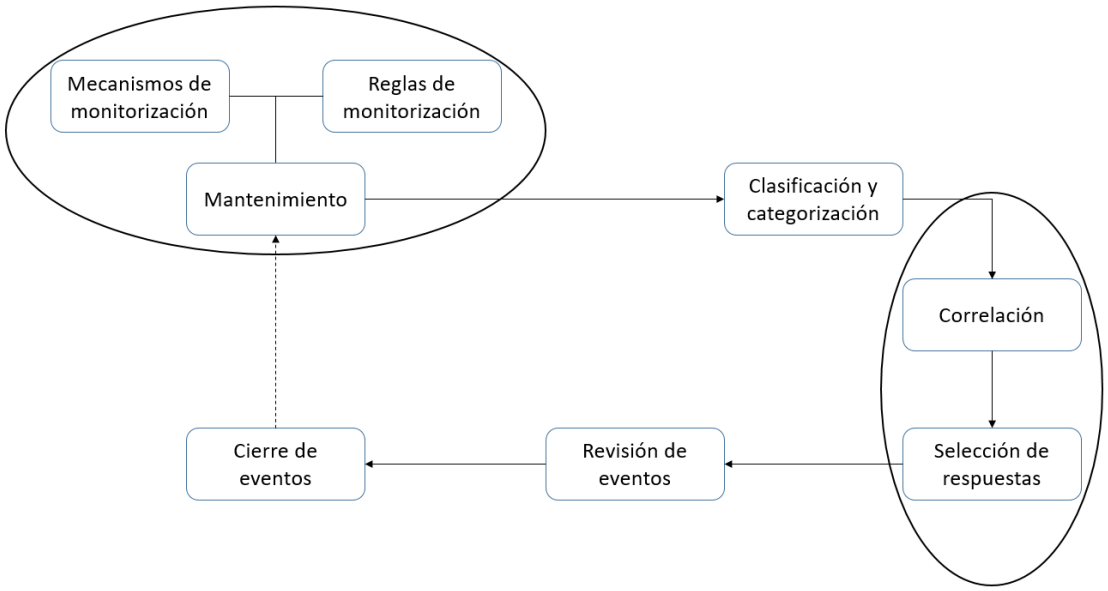


Imagen - 22: Proceso ITIL gestión de Eventos

8.1.2. Procedimiento para la gestión de eventos Cloud

i. **Inicio**
ii. **Mantenimiento de mecanismos y reglas de monitorización:** mantener los mecanismos y las reglas de monitorización actualizadas correctamente, permitirá detectar eventos de una forma más eficaz.
iii. **¿Se han realizado las tareas de mantenimiento?**
iv. **Detección de eventos**
v. **¿Se ha detectado algún evento?:** en el caso que no se haya detectado ningún evento, se volverían a realizar las tareas de mantenimiento, para evitar que se produzcan eventos que los mecanismos y las reglas actuales son incapaces de detectar.
vi. **Clasificación y categorización:** dependiendo del evento que se detecte, deberá ser solventado de una forma u otra.

vii. **¿Existe más de un evento?:** en el caso que se hayan detectado más de un evento, se procedería a investigar si existe alguna relación entre ellos, ya que un evento puede provocar otro distinto.
viii. **Correlación**
ix. **Selección de respuesta**
x. **¿Se ha aplicado una respuesta adecuada?:** se puede seleccionar alguna respuesta que solvente el evento. Es recomendable aplicar respuestas que solvente el evento y todos los posibles eventos que estén relacionados a este y que esa solución sea eficaz a corto y largo plazo.
xi. **Revisión de eventos:** se debe comprobar que, a la hora de solventar los eventos detectados, no se produzcan otros eventos inesperados.
xii. **¿Se ha solventado?:** se considerará que un evento está solventado siempre y cuando se haya solventado este evento y la totalidad de eventos que estén relacionados a este.
xiii. **Cierre de evento**
xiv. **Fin**

8.1.3. Flujograma

En el Anexo I se podrá visualizar el siguiente flujograma más ampliado:

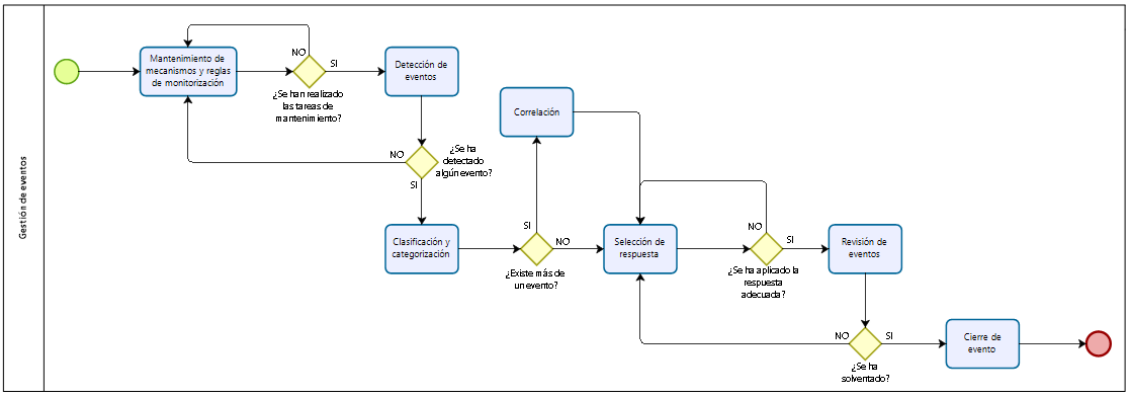


Imagen - 23: Flujograma gestión de Eventos

8.2. Procedimiento para la gestión de incidencias

8.2.1. Gestión de incidencias en ITIL

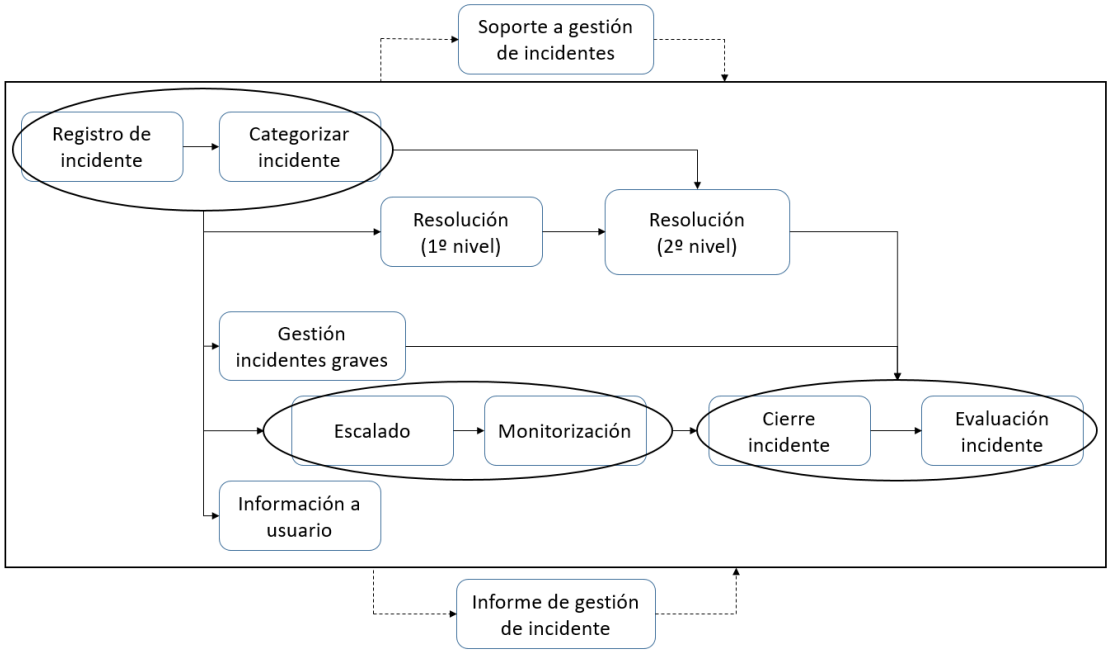


Imagen - 24: Proceso ITIL gestión de Incidencias

8.2.2. Procedimiento para la gestión de incidencias Cloud

i. **Inicio**
ii. **Detección de incidencia**
iii. **Registro:** una vez detectada o notificada una incidencia, es imperativo su registro, ya que será de gran importancia para la resolución de esta incidencia o de incidencias futuras.
iv. **Categorización:** dependiendo del incidente y de su naturaleza, se deberá tratar de una forma o de otra, o por unos especialistas o por otros.
v. **¿La incidencia es grave?:** los incidentes graves se abordarán aparte. No pasarán por los distintos niveles de gestión, sino que, para priorizarlo, se gestionará directamente por los niveles más altos de gestión e, incluso, llegar a escalarlo con rapidez.
vi. **Resolución en primer nivel**
vii. **¿Se ha solucionado?**
viii. **Cierre de incidencia**
ix. **Evaluación de la incidencia:** siempre que se le aplique una resolución a un incidente, la aplique el nivel que la aplique, se deberá hacer una evaluación exhaustiva para garantizar la resolución total del incidente.
x. **Gestión de incidentes graves:** es importante priorizar los incidentes graves, ya que su resolución es fundamental para que no derive en un problema y pueda llegar a afectar a la continuidad de la actividad. Por este motivo, tiene conexión directa con el escalado,

ya que, si no se encuentra una resolución rápido, es imperativo notificarlo a los proveedores del servicio para que entren en acción.

xi. **¿Se ha solucionado?**

xii. **Escalar incidencia:** el escalado se debe realizar siempre que un incidente, ya sea grave o no, no reciba una resolución rápida y apropiada.

xiii. **Monitorización de la incidencia:** una vez escalado el incidente, es importante seguir su progreso, para notificar a los encargados de su resolución, cualquier cambio que pueda surgir.

xiv. **Resolución en segundo nivel**

xv. **¿Se ha solucionado?**

xvi. **Fin**

8.2.3. Flujograma

En el Anexo II se podrá visualizar el siguiente flujograma más ampliado:

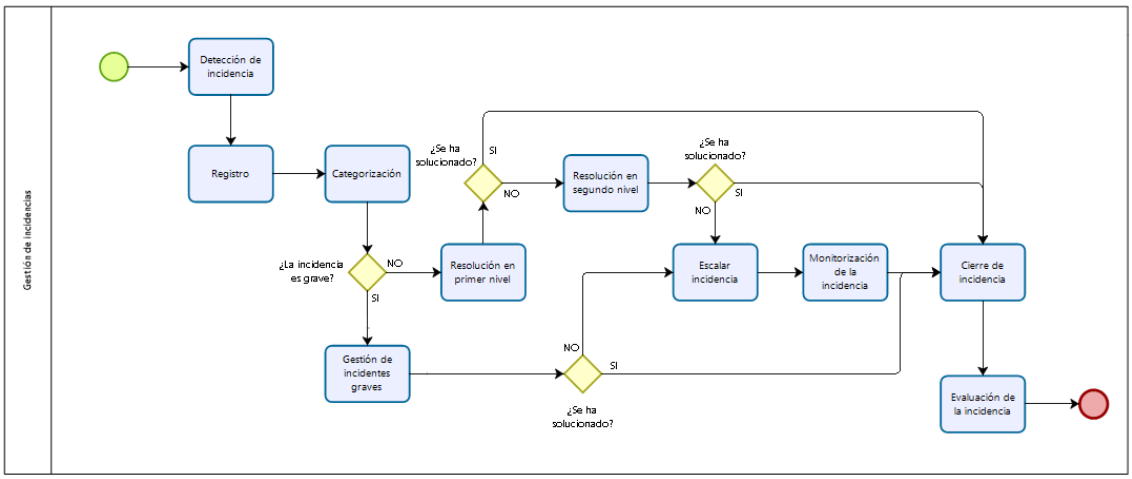


Imagen - 25: Flujograma gestión de Incidencias

8.3. Procedimiento para la gestión de problemas

8.3.1. Gestión de problemas en ITIL

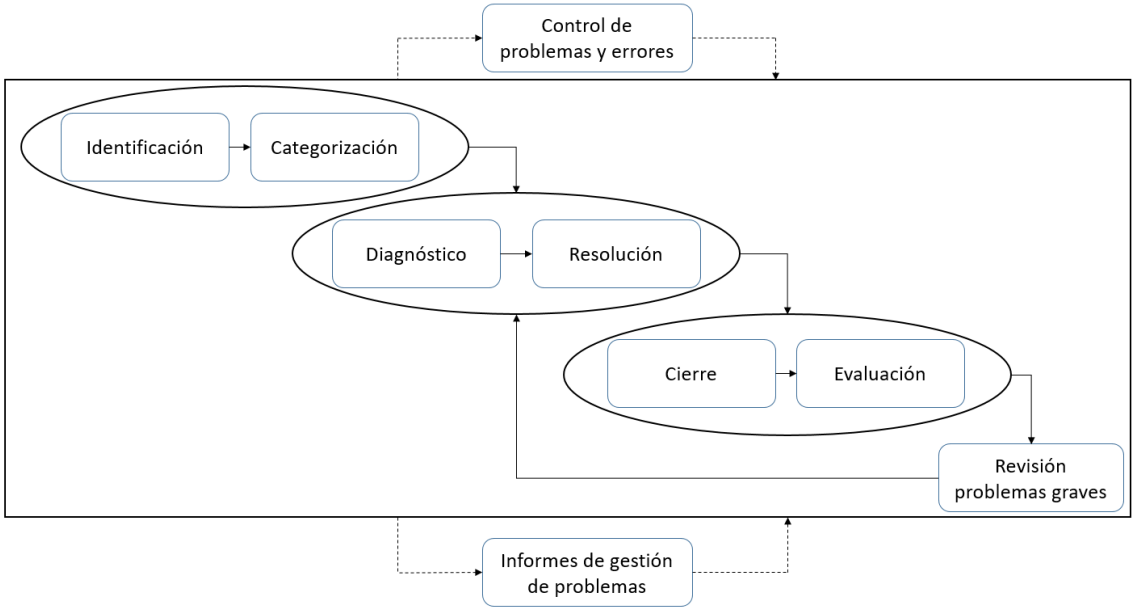


Imagen - 26: Proceso ITIL gestión de Problemas

8.3.2. Procedimiento para la gestión de problemas Cloud

i. **Inicio**
ii. **Detección de problemas**
iii. **Identificación:** es muy importante identificar el problema correctamente, ya que puede haber ocurrido otro similar anteriormente que, su solución, pueda ayudar el presente problema.
iv. **¿Es un problema conocido?:** en el caso que el problema no sea conocido, habría que proceder a categorizar el nuevo problema.
v. **Categorización**
vi. **Diagnóstico:** hay que investigar minuciosamente los motivos por los que ha surgido dicho problema, y descubrir el alcance que haya tenido.
vii. **¿Se conocen las causas y las consecuencias?**
viii. **Resolución**
ix. **¿Se ha solucionado?:** se considerará que el problema está solucionado siempre y cuando se haya solventado tanto el problema como las causas que lo hayan provocado, además de confirmar que los posibles efectos que haya podido causar el problema se hayan solventado correctamente.
x. **Cierre problema**
xi. **Evaluación:** una vez solucionado el problema, se realizará una evaluación minuciosa, la cual permitirá evaluar no solo el estado del problema, sino también el estado de las causas que lo han provocado y el estado de las consecuencias que hayan podido surgir a raíz de él.

xii. **¿Ha sido un problema grave?:** es importante tener claro si el problema ha sido grave o no, ya que habrá que tener más en consideración los problemas graves porque pueden llegar a afectar significativamente a la continuidad de la actividad laboral.

xiii. **Revisión de problemas graves**

xiv. **¿Se ha solventado correctamente?:** al igual que con los problemas menos graves, se considerará el problema grave solventado siempre y cuando se haya solventado este, las causas que lo hayan provocado y las consecuencias que haya podido causar.

xv. **Cierre de problemas graves.**

xvi. **Fin**

8.3.3. Flujograma

En el Anexo III se podrá visualizar el siguiente flujograma más ampliado:

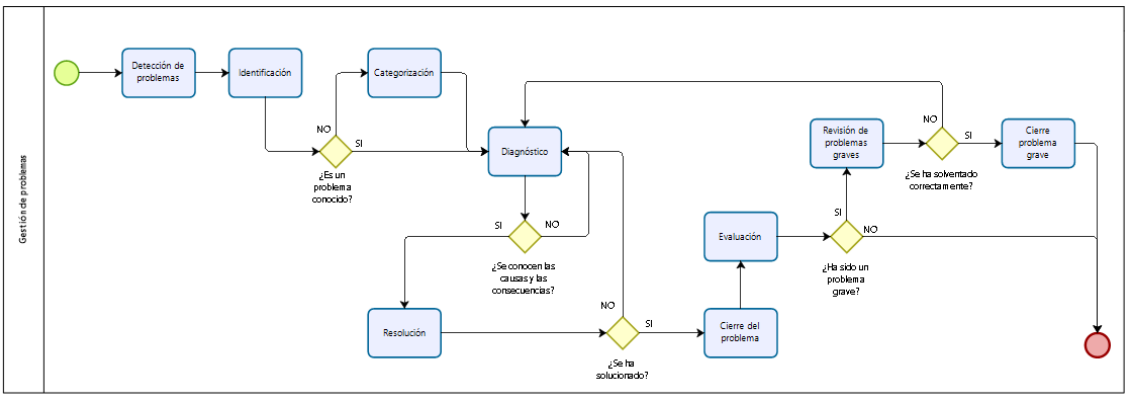


Imagen - 27: Flujograma gestión de Problemas

9. Adaptación de los procedimientos para Cloud

Los procedimientos que se acaban de ver sobre la gestión de eventos, incidencias y problemas, son muy necesarios, pero solo aplicables a casos aislados entre sí.

Si se dividen las posibles alertas detectadas por el cliente o usuario final en 2 tipos diferenciados, se verá claramente esta relación. Estos 2 tipos serías:

- Alertas relacionadas con su propia infraestructura: el usuario detectará eventos, incidencias y problemas que estén relacionados únicamente con la infraestructura que haya implantado el propio cliente en Cloud, es decir, detectará las alertas en sus propias máquinas virtuales, servidores, bases de datos, etc.

- Alertas relacionadas con la infraestructura de Cloud: el usuario únicamente detectará incidencias que serán causadas por la infraestructura de Cloud. Aunque el usuario las detecte y trate estas alertas como incidencias, a la hora de su escalado a los proveedores de los sistemas Cloud, estos los clasificarán como eventos, incidencias o problemas, y las tratarán como tales.

La infraestructura propia del cliente se ve influida directamente por la infraestructura propia de Cloud, por este motivo, el cliente detectaría las alertas de Cloud como incidentes.

Por ejemplo, se pueden producir perdida de información de unas bases de datos desplegadas por los clientes. La mejor forma de recuperar dicha información es mediante la utilización de un backup anterior de dichas bases de datos. Estos backups son creados y administrados por los proveedores de los sistemas Cloud, los cuales se encargarían de resolver este incidente.

Por otro lado, el cliente puede detectar un incidente por la recepción de numerosos correos no deseados o fraudulentos, pero, al escalarlo a los proveedores de Cloud, se podría detectar una falla en la seguridad y procederían a solventar este problema.

Hay otras alertas competencia de los proveedores de Cloud que son detectadas por los clientes como incidencias, como es el caso de la latencia. La latencia es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de una red (depende del tamaño de los paquetes transmitidos o por el tamaño de los búferes dentro de los equipos de conectividad). En Cloud, depende de las zonas en las que se encuentren las máquinas y hacia donde quieran llegar. Al igual que con las fallas de seguridad, la competencia de la latencia es del proveedor de Cloud, por lo que el usuario detectaría estos retrasos de transmisión como incidencias y lo escalarían para su resolución.

Finalmente, en cualquier sistema, donde se pueden incluir los sistemas Cloud, un evento, una incidencia o un problema, puede causar la aparición de “daños colaterales”, que se traduce en apariciones de otros eventos, incidencias o problemas. Es decir, un evento puede causar o estar causado por otro evento, una incidencia o un problema, y del mismo modo puede llegar a ocurrir con las incidencias o los problemas.

Para solventar estos marcos, es recomendable adaptar estos procedimientos, llegando al punto de unificarlos. En este apartado se pretende realizar un procedimiento para poder controlar de una forma ordenada y coordinada estas posibles situaciones.

Este procedimiento se puede generalizar en cuatro fases:

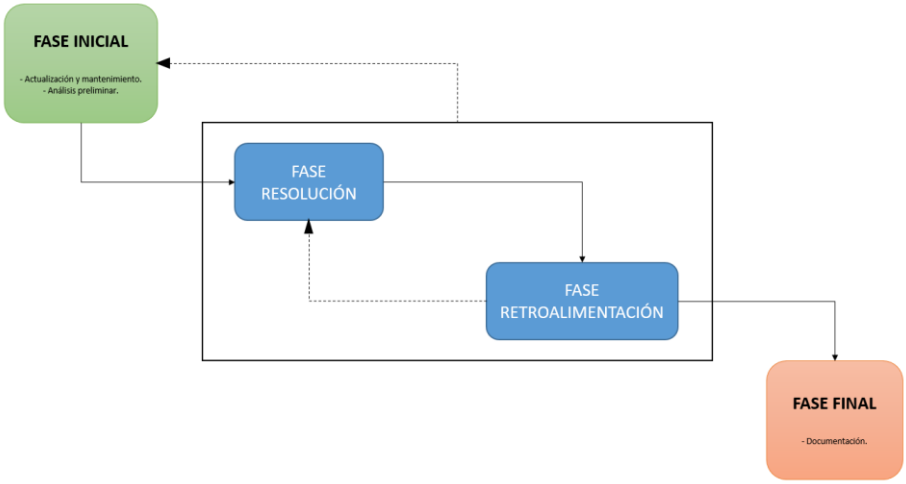


Imagen - 28: Fases gestión de Alertas

En el Anexo IV, se puede visualizar el diagrama desarrollado para hacer frente a estos supuestos y del que, a continuación, se mostrará su explicación.

9.1. Fase inicial

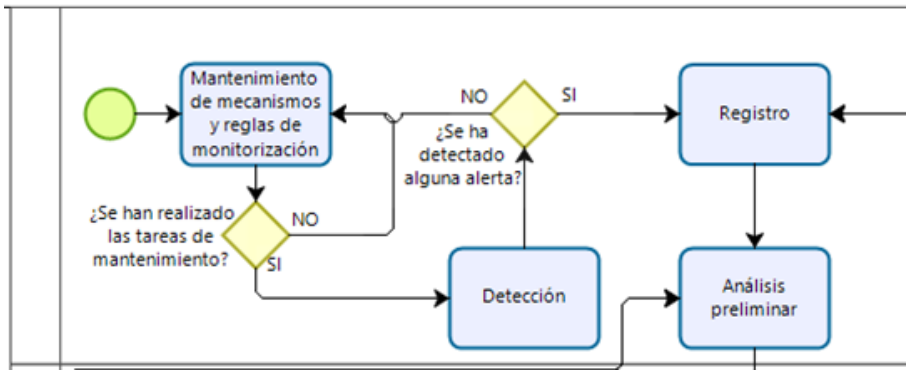


Imagen - 29: Fase inicial

Posiblemente, la fase más importante del procedimiento de gestión de alertas por dos factores esenciales:

- Mantenimiento de mecanismos y reglas de monitorización y/o detección: al igual que un antivirus cuanto más actualizado esté más eficaz es, los mecanismos y reglas de monitorización deben mantenerse actualizados en todo momento. Al ritmo que avanza la tecnología, pueden darse, por ejemplo, eventos que los mecanismos y las reglas no sean capaces de detectar en ese momento, ya que es muy posible que puedan ser desconocidos para ellos.

- Análisis preliminar: se deberá realizar un análisis inicial para conseguir una clasificación más exacta y un futuro diagnóstico más eficaz, y así conseguir una gestión de las alarmas mucho más ágil y, una resolución más eficiente y temprana. En este mismo paso, se estudiará la capacidad de actuación ante cada alerta, ya que habrá situaciones en que su resolución será únicamente cometido de los proveedores de los sistemas Cloud.

9.2. Fase resolución

Ya sea para la resolución de un evento, una incidencia o un problema, el procedimiento a seguir para la resolución de cualquiera de estas tres alertas es muy similar a sus respectivas metodologías ITIL, únicamente se añade una serie de pasos que servirán para comprender como se ha originado la alerta y evitar o reducir, en la medida de lo posible, el "daño colateral" de generación de otras alertas a la hora de aplicar una u otra respuesta.

A continuación, se profundizará en estos pasos adicionales relativos a cada una de las tres alertas que se están estudiando, además de realizar relaciones entre los pasos de gestión de cada alerta y los entornos Cloud.

9.2.1. Eventos

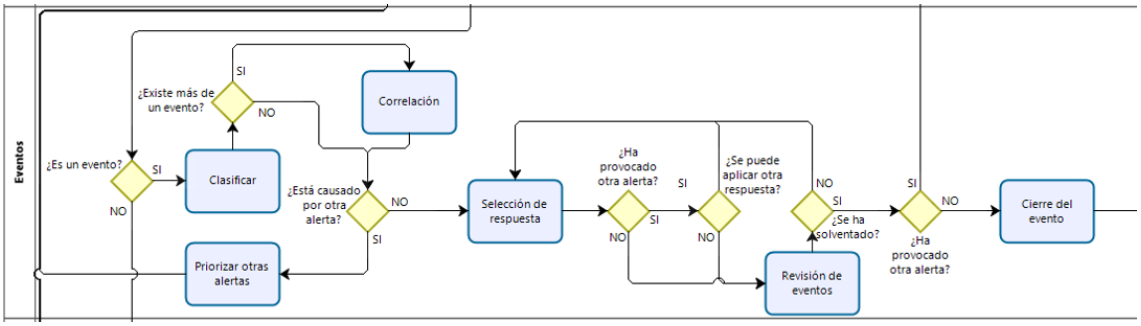


Imagen - 30: Fase resolución de Eventos

La primera diferencia que se visualiza con respecto a ITIL vista anteriormente, es la comprobación de si el evento se ha generado por culpa de cualquier otra alerta o no. En caso afirmativo, se pasará a priorizar esa alerta, volviendo al análisis preliminar de la fase inicial.

Si el evento no ha sido consecuencia de otra alerta, se continuará con el procedimiento de gestión del evento, hasta llegar a las comprobaciones de retroalimentación, que se explicará más adelante.

Con respecto a los entornos Cloud y como se ha mencionado anteriormente, se debe concretar la naturaleza del evento y si la respuesta que se debe aplicar para solventarlo es una de las funciones que únicamente puede realizar el proveedor del sistema Cloud que, a su vez, seguirá este mismo procedimiento para asegurar una respuesta adecuada.

9.2.2. Incidencias

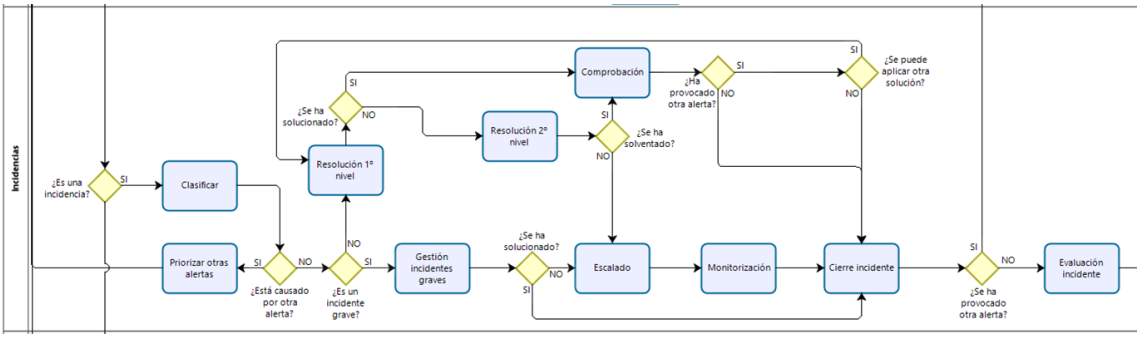


Imagen - 31: Fase resolución de Incidencias

Comparando la nueva gestión de incidencias con la vista anteriormente en ITIL. Se ve claramente un progreso similar en la gestión, pero se añaden una serie de ampliaciones para abordar las posibles causas de su origen:

- La incidencia es nueva: dicha incidencia se ha provocado por causas ajenas a la gestión de otras alertas. En este caso, se procederá con la gestión normal de la incidencia.

- La incidencia ha sido causada por otra alerta: otra alerta ha podido repercutir de algún modo en el sistema, generando esta incidencia u otras alertas. En este caso, se priorizará la alerta que haya generado esta incidencia, volviendo al análisis preliminar. Se retomaría la gestión de esta incidencia en el momento que se gestionara la alerta principal, en el caso de persistir.

- La incidencia ha sido un daño colateral: al aplicar una resolución o una respuesta para tratar de solventar un evento, una incidencia y/o un problema, dicha resolución o respuesta ha generado esta incidencia. Al originarse por este motivo, se entiende que no quedaban más opciones para solventar una alerta determinada, por lo que se deberá tratar esta incidencia inmediatamente después de la aplicación de la respuesta.

Con respecto a los entornos Cloud, existirán incidencias que no puedan resolverse ni en el 1º nivel ni en el 2º nivel de la gestión de la incidencia, por lo que se procedería al escalado de la incidencia y pasaría a ser responsabilidad de los proveedores del sistema Cloud, los cuales, al igual que en el caso anterior, deberán seguir este mismo procedimiento para asegurar una gestión adecuada y correcta de la incidencia.

En la gestión de las incidencias se produce lo que se mencionaba anteriormente. El usuario final puede detectar una incidencia de su arquitectura y procedería a su resolución, pero podría detectar una incidencia en su arquitectura que no fuera capad de solventar, por lo que se escalaría a los proveedores del servicio Cloud, ya que se tratará de una alerta que está directamente relacionada con la arquitectura Cloud y que el usuario final no tiene los medios ni la capacidad de hacerle frente.

Se pasaría al registro de esta alerta por parte de los administradores de la arquitectura Cloud, ya que, posteriormente, se necesitaría realizar un análisis preliminar de la alerta y su posterior clasificación, dependiendo de tratarse de una alerta causada por un evento, una incidencia o un problema. En el Anexo V se puede visualizar un diagrama de gestión de alertas, en el cual se

relaciona el "escalado" por parte del usuario final con el "registro" por parte de los administradores del servicio Cloud y la relación entre "informar" de la fase final por parte de los administradores de Cloud y la "monitorización" de la incidencia por parte del usuario final.

9.2.3. Problemas

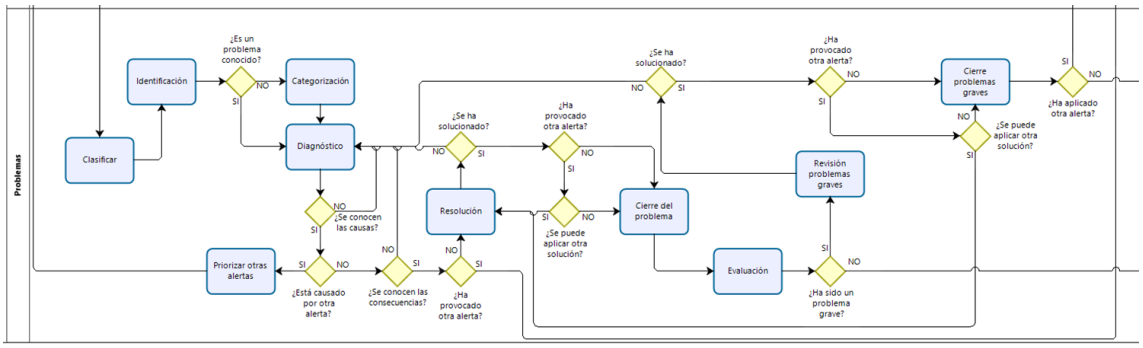


Imagen - 32: Fase resolución de Problemas

En el procedimiento de gestión de problemas, de nuevo ocurre lo mismo que en los casos anteriores. Se realiza una ampliación con respecto a ITIL para comprobar el posible origen de este problema.

En este caso, el procedimiento a seguir sería igual que en los casos anteriores:

- Si el problema es nuevo o se ha originado como un daño colateral, se continúa con normalidad por el procedimiento de gestión del mismo. En el caso de tratarse de un daño colateral, se procederá a la resolución del problema inmediatamente después del cierre de la alerta origen.

- Si el problema ha sido causado por otra alerta, se deberá priorizar la alerta que lo ha causado (volviendo al análisis preliminar) y volver a gestionar este problema una vez se haya solventado dicha alerta y si el problema persiste.

En este caso, habría que tener en cuenta lo mismo mencionado anteriormente. Existirán problemas que sean competencia exclusiva de los proveedores de Cloud, por lo que se les informará de este problema y ellos deberán encargarse de solucionarlo. Para ello utilizaría el procedimiento que se ha explicado anteriormente.

9.3. Fase retroalimentación

Se podría decir que tenemos 2 tipos de retroalimentaciones: internas y externas.

- Retroalimentaciones internas: como ya se ha podido ver en los procedimientos mostrados anteriormente, están destinadas a afrontar las posibles alertas causadas por una resolución o respuesta en concreto, e intentar darle otros puntos de acción antes del cierre de la alerta.

- Retroalimentaciones externas: en el momento de aplicar una respuesta, esta puede generar otras alertas. Si no existen otras respuestas que puedan evitar esta situación, esta retroalimentación permite abordar esas nuevas alertas antes del cierre completo de la alerta original.

En este apartado, se pretenderá dar una visión más en profundidad a cada una de las retroalimentaciones definidas en el proceso de gestión de cada una de las alertas.

9.3.1. Retroalimentaciones internas

Retroalimentación en la gestión de eventos: en este caso se realiza una retroalimentación muy sencilla para intentar evitar futuras alertas generadas por la respuesta que se aplique.

Simplemente, se comprueba si la respuesta ha generado alguna otra alerta. En caso negativo, se procedería con la revisión del evento. Si, por lo contrario, esa respuesta a generado otra alerta, se comprobaría si se puede aplicar otra respuesta para evitar este inconveniente. Si se puede aplicar otra respuesta, se volvería a la selección de respuesta, pero si no existe otra posibilidad, se continuaría a la revisión del evento y más adelante se realizará otra retroalimentación para gestionar la alerta que se haya provocado. Esto se tratará más en profundidad según se avance en el presente documento.

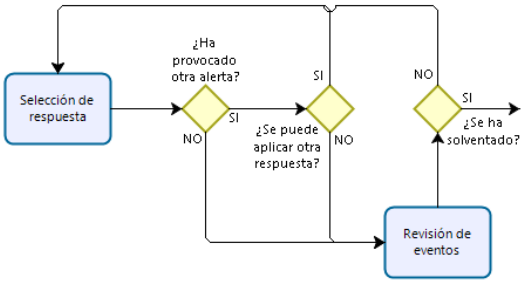


Imagen - 33: Retroalimentación Eventos

Retroalimentación en la gestión de incidencias: aquí se pretende conseguir lo mismo que en el caso anterior, la diferencia radica en que, si se puede aplicar otra resolución, se pasaría al 1º nivel, pudiendo llegar hasta el 2º nivel e incluso, proceder al escalado de la incidencia, si fuera necesario, para que intervengan los proveedores del sistema Cloud.

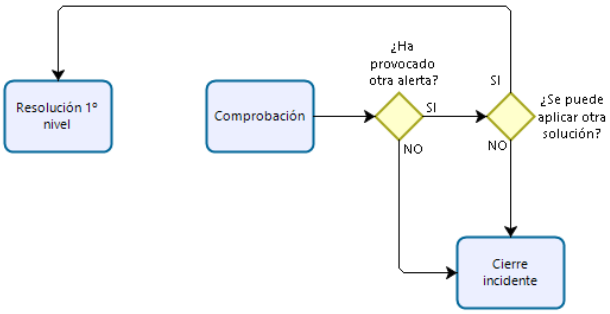


Imagen - 34: Retroalimentación Incidencias

Retroalimentación en la gestión de problemas: aquí se pueden realizar hasta dos retroalimentaciones diferenciadas por el tratamiento que haya recibido el problema con respecto a su gravedad.

Se procede a realizar las comprobaciones pertinentes a los problemas una vez se les haya aplicado su resolución, para evitar, en la medida de lo posible, posibles "daños colaterales" producidos por la misma.

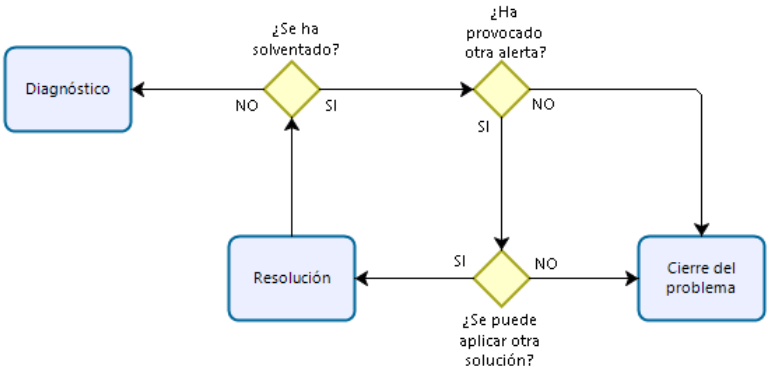


Imagen - 35: Retroalimentación Problemas

Una vez comprobado, se pasa a la parte de gestión de problemas graves que, del mismo modo, intentará evitar cualquier generación de alarmas adicionales.

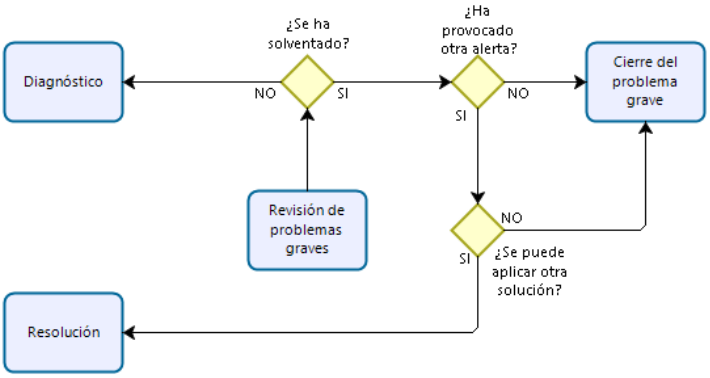


Imagen - 36: Retroalimentación Problemas graves

9.3.2. Retroalimentación externa

Esta retroalimentación está destinada esencialmente a reiniciar el procedimiento completo en el caso que se produzca uno de los siguientes escenarios:

- Como se ha mencionado anteriormente, es posible que la respuesta o resolución aplicada genere otras alertas. Por lo tanto, no se considerará la alerta inicial cerrada hasta que se hayan cerrado las alertas que hayan surgido por este motivo. A continuación, se muestran estas retroalimentaciones:

- Eventos:

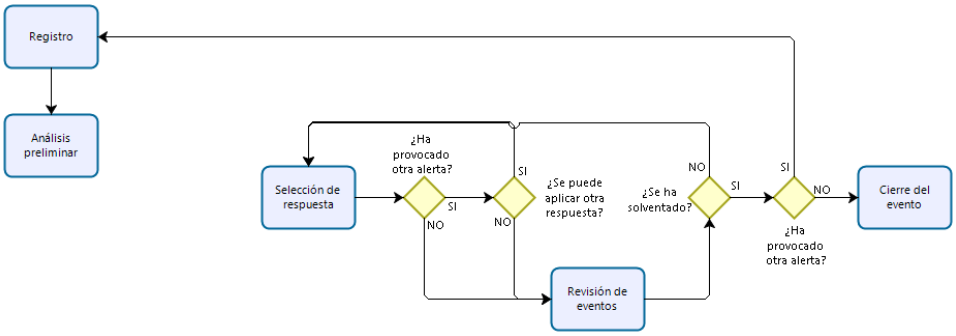


Imagen - 37: Retroalimentación externa Eventos I

- Incidencias:

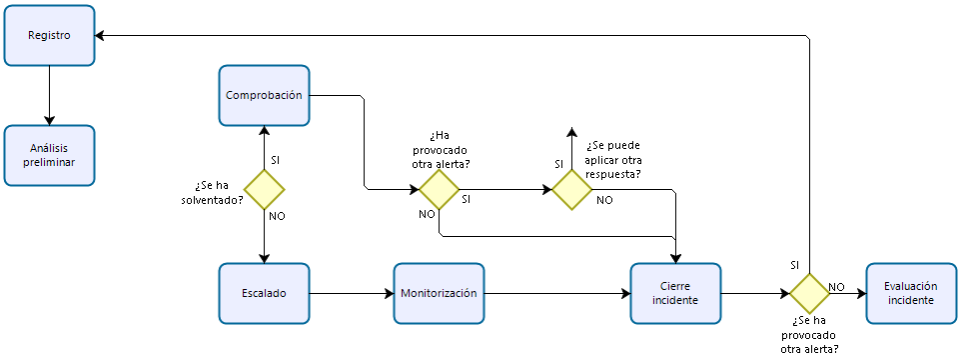


Imagen - 38: Retroalimentación externa Incidencias I

- Problemas:

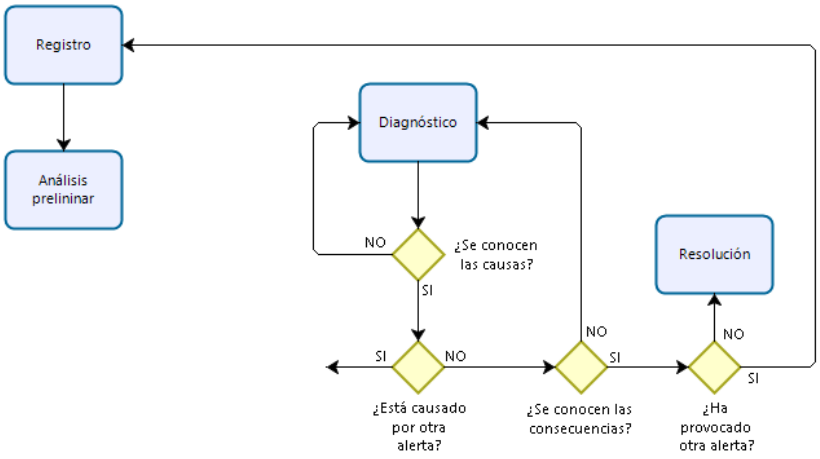


Imagen - 39: Retroalimentación externa Problemas I.a

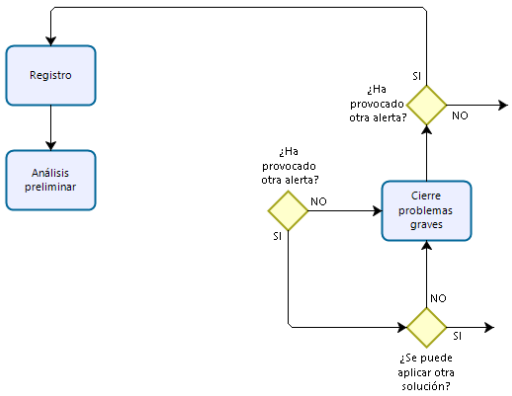


Imagen - 40: Retroalimentación externa Problemas I.b

- La alerta que se está gestionando es consecuencia de otra alerta. Por lo tanto, se deberá gestionar la alerta "origen" y en el momento que se solventase, volver a esta alerta, en el caso de que persistiese. A continuación, se muestra esta retroalimentación:

    - Eventos:

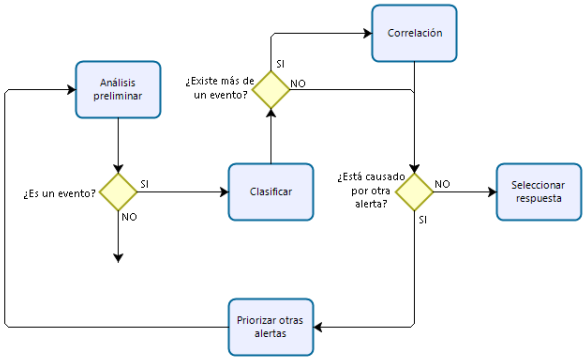


Imagen - 41: Retroalimentación externa Eventos II

    - Incidencias:

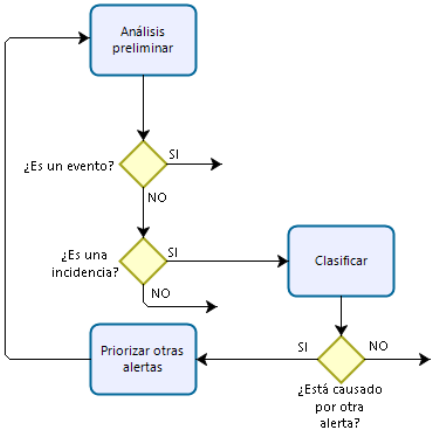


Imagen - 42: Retroalimentación externa Incidencias II

- Problemas:

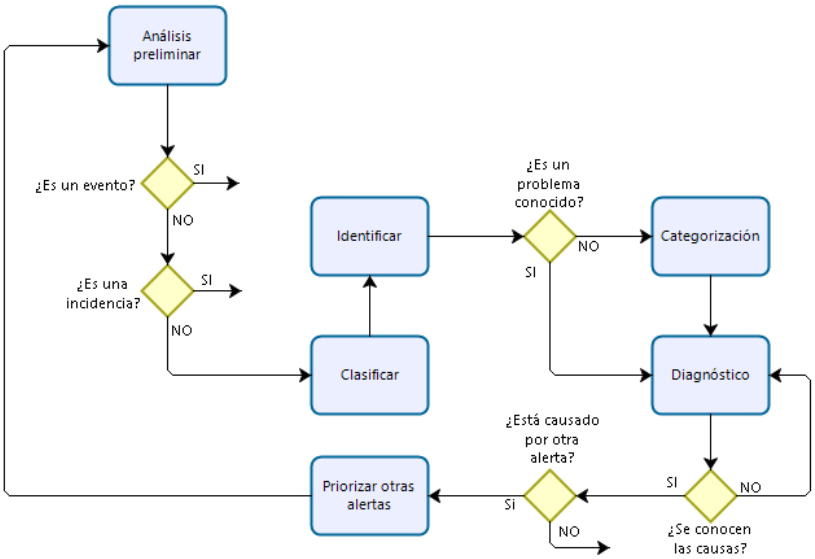


Imagen - 43: Retroalimentación externa Problemas II

Con esta retroalimentación, se consigue un orden imprescindible para gestionar las alertas, ya que nunca se debe dejar un procedimiento sin finalizar e iniciar otro distinto.

9.4. ***Fase final***

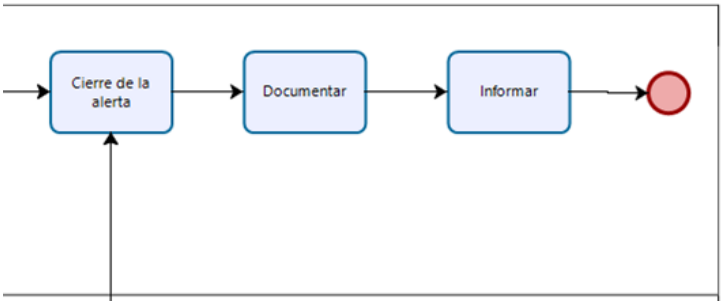


Imagen - 44: Fase final

En esta última fase, es importante centrarse en la documentación completa de la alerta: detección, causas, consecuencias, resolución y cierre.

Es imprescindible la realización de esta documentación, ya que facilitará la gestión de alertas similares o iguales que puedan aparecer en un futuro, además de ayudar a la compresión de la alerta y de las acciones tomadas para su gestión.

Una vez completada esta documentación, habrá que informar a todos los implicados o que se han visto afectados por esta alerta.

10. Cierres

En este apartado se pretende aclarar las diferencias fundamentales que existen entre un cierre de eventos, incidencias o problemas, y un cierre las alertas.

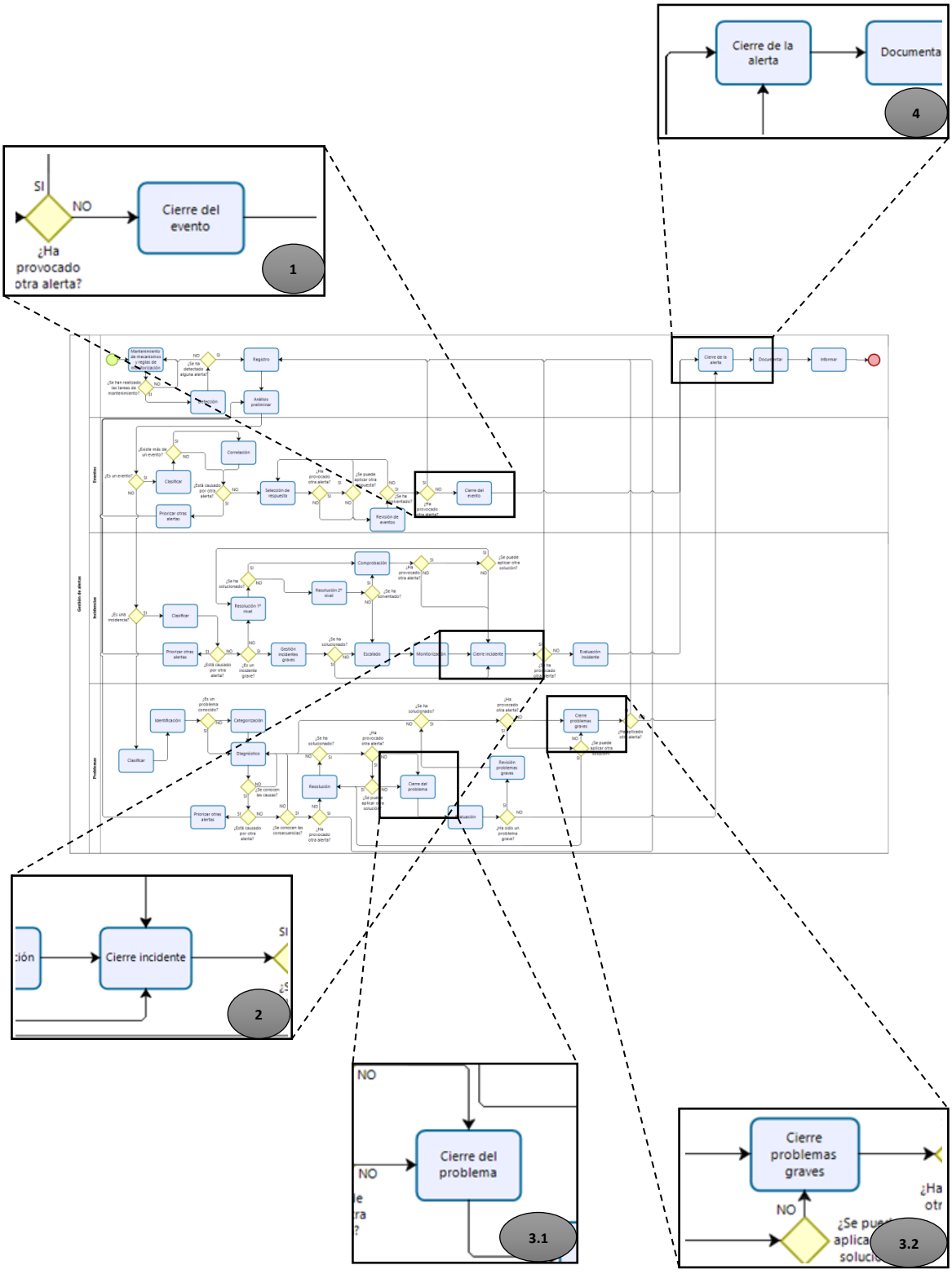


Imagen - 45: Cierres

Como se puede ver, existen cinco cierres diferenciados, los cuales deben seguir una serie de pautas para su ejecución:

- **Cierre 1:** corresponde al cierre del evento. Un evento se considera cerrado cuando dicho evento se haya solventado y se haya solucionado cualquier otra alerta que haya generado el propio evento o la respuesta que se le haya aplicado.

- **Cierre 2:** corresponde con el cierre de las incidencias. Una incidencia se considera cerrada siempre y cuando se haya aplicado una resolución que haya solventado la incidencia y que no haya generado otra alerta al aplicar dicha resolución. También se considerará la incidencia cerrada cuando se haya solventado dicha incidencia y la resolución haya generado otra alerta, siempre y cuando no se pueda aplicar otra resolución. Este cierre tiene la peculiaridad de llegar a él mediante el escalado de la incidencia, ya que, como se ha mencionado anteriormente, habrá incidencias que deban intervenir los proveedores de Cloud para su gestión y tratamiento.

- **Cierre 3.1:** se corresponde con el cierre de los problemas. Al igual que en el caso de las incidencias, un problema se considera cerrado siempre y cuando se haya aplicado una resolución que haya solventado el problema y que no haya generado otra alerta al aplicar dicha resolución. También se considerará el problema cerrado cuando se haya solventado dicho problema y la resolución haya generado otra alerta, siempre y cuando no se pueda aplicar otra resolución.

- **Cierre 3.2:** al igual que el cierre 3.1, este cierre se corresponde con la gestión de los problemas, pero, en este caso, de los problemas graves. Las condiciones que se deben cumplir para realizar el cierre de los problemas graves son idénticas a las condiciones de cierre de los problemas.

- **Cierre 4:** este cierre corresponde al cierre de las alertas. Dicho cierre engloba a los cierres vistos anteriormente. La diferencia principal que radica en este cierre con respecto a los anteriores es la siguiente:
    - En los cierres correspondientes a la gestión de los eventos, las incidencias y los problemas, la principal condición es la resolución de los mismos.
    - El cierre de la alerta únicamente se puede llevar a cabo mediante el cumplimiento de las siguientes condiciones:
        - El cierre de cada una de las alertas.
        - El cierre de todas las alertas adicionales que haya causado la alerta principal.
        - El cierre de todas las alertas que se hayan podido generar al aplicar una determinada resolución o respuesta.

11. Resultados y conclusiones

Como se ha podido ver a lo largo de este trabajo, los procedimientos son esenciales para la gestión de los eventos, de las incidencias y de los problemas, ya que se debe construir una serie de procedimientos perfectamente adaptados, que consigan reflejar cualquier situación que se pueda dar.

En los procedimientos vistos en ITIL para la gestión de estas alertas de forma individual, se puede comprobar cómo se adaptan perfectamente a cualquier escenario que se pueda dar, por ejemplo:

- En la gestión de los eventos se tiene en cuenta la aparición de varios eventos y se busca la relación entre ellos para poder gestionarlos de forma conjunta.

- En la gestión de las incidencias se considera que una incidencia pueda no solventarse y para ello se ponen varios niveles de resolución e, incluso, se contempla la posibilidad del escalado de las incidencias.

- En la gestión de los problemas realiza una clasificación entre problemas graves y no graves, para tener una mayor atención a aquellos problemas graves.

Por separado, estos procedimientos definidos por ITIL están orientados a asegurar la eficiencia en la gestión de cada una de estas alertas.

El problema surge cuando se intenta adaptar estos procedimientos a entornos o sistemas como los sistemas Cloud. En estos sistemas entran en juego diversos factores (arquitectura, proveedores, etc.). Al tratarse de sistemas más complejos, aparece la necesidad de unificar estos procedimientos sin dejar de lado la definición inicial de ITIL, es decir, aparece la necesidad de unir estos tres procedimientos de gestión en uno, ya que se produce la aparición de los siguientes factores esenciales a tener en cuenta:

- El origen de la alerta:
    - La alerta se puede dar por primera vez: en este caso, los procedimientos a seguir serán, inicialmente, los definidos por ITIL.
    - La alerta puede estar causada por otra alerta.
    - La alerta puede ser un daño colateral producido por la respuesta aplicada a otra alerta.

- Respuesta: este factor no lo contemplan los procedimientos definidos por ITIL en su totalidad. ITIL comprueba que la respuesta que se haya aplicado sea correcta y eficaz, pero no contempla la posibilidad de que, al aplicar una respuesta correcta y eficaz, pueda causar otra alerta e intentar evitarlo eligiendo otra posible respuesta igualmente válida.

No hay que confundir unir los tres procedimientos definidos por ITIL con fusionarlos. No se busca crear un procedimiento genérico para la gestión total de los tres tipos de alertas, se pretende mantener la definición básica de gestión de cada uno de los tipos de alertas, adaptándolos para conseguir crear un procedimiento que compruebe todos los factores que se puedan dar en cada uno de ellos.

Además, se muestra la importancia de tener perfectamente definidos los cierres de cada una de las alertas, ya sea por separado o en conjunto.

- Por separado, cada procedimiento se debe cerrar individualmente, teniendo en cuenta que en cada una de las alertas se ha aplicado una respuesta adecuada.

- En conjunto, los eventos, las incidencias y los problemas se deben cerrar, como se ha mencionado anteriormente, no solo cuando se haya aplicado una respuesta adecuada, además hay que tener en cuenta las posibles alertas que hayan podido surgir de ella o de su resolución. Una vez cerrada cada una de las alertas involucradas, se considerará la alerta cerrada.

En conclusión, hay que estudiar muy detenidamente los procedimientos que se van a adaptar para gestionar unas determinadas alertas y para que sistemas se van a adaptar, ya que es muy posible que se deban introducir una serie de mejoras para contemplar cualquier escenario que pueda surgir, de principio a fin.

12. Mejoras y trabajos futuros

- Creación de equipos de trabajo destinados a estas funciones.
- Adaptación más exhaustiva y diferenciada para cada proveedor de entornos Cloud.
- Estudio exhaustivo de los eventos, incidencias y problemas que debe abordar el proveedor.
- Estudio de las herramientas existentes para abordar cada fase de este procedimiento en relación con un proveedor Cloud determinado.
- Estudio y análisis de herramientas destinadas al modelado de procedimientos.
- Creación de una herramienta específica destinada a la monitorización de las alertas y su situación en el procedimiento de gestión.
- Desarrollo de otros procedimientos basados en ITIL.

13. Herramientas

En este apartado se pondrá una serie de herramientas destinadas a la realización de procedimientos. En este trabajo se ha utilizado la herramienta “Bizagi Process Modeler”.

- DRAW.IO
- CACOO
- CREATELY
- Diagramas BPMN
- Bonita BPM
- ADONIS
- ARIS
- Modelio

El mercado actual ofrece un gran catálogo de herramientas destinadas a la creación o modelado de diagramas UML, bases de datos y flujogramas. En esencia, no existe gran diferencia a la hora de utilizar cualquiera de ellos.

14. Bibliografía y enlaces de interés

14.1. Bibliografía

[1] V. H. L. S. A.O., ITIL 4 Foundation Courseware (Spanish edition), ISBN: 978 94 018 0463 9, 2019.

[2] M. Armbrust, A. Fox, R. Griffith, A. Konwinski, G. Lee y D. Patterson, «A view of cloud computing,» de *A view of cloud computing*, ISSN 0001-0782. doi:10.1145/1721654.1721672., 2010, pp. 50-58.

[3] R. Stallman, "Cloud computing is a trap," *The Guardian,* p. 1, 29 Sep 2008.

[4] beServices, «beServices,» beServices Cloud computing y servicios IT, 12 09 2018. [En línea]. Available: https://www.beservices.es. [Último acceso: 26 10 2019].

[5] Administrador, «profitline,» profitline business outsourcing, 14 02 2019. [En línea]. Available: https://profitline.com.co. [Último acceso: 26 10 2019].

[6] Administrador, «Nube Computing Blog,» Wordpress, [En línea]. Available: https://nubecomputingblog.wordpress.com/tipos-de-nubes/. [Último acceso: 12 11 2019].

[7] Administrador, «Wikipedia,» Wikipedia, 05 07 2018. [En línea]. Available: https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_nube. [Último acceso: 07 11 2019].

[8] L. Joyanes Aguilar, «Computación en la nube: Notas para una estrategia española en cloud computing,» *Revista del Instituto Español de Estudios Estratégicos,* p. 1, 14 11 2018.

[9] Administrador, «aws,» Amazon, [En línea]. Available: https://aws.amazon.com. [Último acceso: 15 02 2020].

[10] Administrador, «azure,» Microsoft, [En línea]. Available: https://azure.microsoft.com. [Último acceso: 15 02 2020].

[11] Administrador, «ibm,» IBM, [En línea]. Available: https://www.ibm.com. [Último acceso: 15 02 2020].

[12] Administrador, «google,» Google, [En línea]. Available: https://cloud.google.com. [Último acceso: 15 02 2020].

[13] Administrador, «oracle,» ORACLE, [En línea]. Available: https://www.oracle.com/. [Último acceso: 15 02 2020].

[14] Administrador, «vmware,» vmWare, [En línea]. Available: https://www.vmware.com. [Último acceso: 15 02 2020].

[15] Administrador, «icloud,» Apple, [En línea]. Available: https://www.icloud.com. [Último acceso: 15 02 2020].

[16] Administrador, «blogspot.com,» Blogspot, 09 02 2018. [En línea]. Available: http://creacioneventos.blogspot.com. [Último acceso: 25 01 2020].

[17] A. Celaya Luna, Cloud: Herramientas para Trabajar en la Nube, ISBN: 978-84-9021-385-8, 2017.

[18] Administrador, «wiki,» Process maps, [En línea]. Available: https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Eventos. [Último acceso: 02 03 2020].

[19] Administrador, «wiki,» Process maps, [En línea]. Available: https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Incidentes. [Último acceso: 05 03 2020].

[20] Administrador, «wiki,» Process maps, [En línea]. Available: https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Problemas. [Último acceso: 05 03 2020].

14.2. Enlaces de interés

https://aws.amazon.com/es/

https://azure.microsoft.com/es-es/

https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Eventos

https://Cloud.google.com/

https://www.ibm.com/es-es/Cloud

https://www.iCloud.com/

https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Incidentes

https://wiki.es.it-processmaps.com/index.php/Portada

https://www.oracle.com/es/Cloud/

https://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_de_Problemas

https://Cloud.vmware.com/es

ANEXOS

ANEXO I: Procedimiento de gestión de eventos

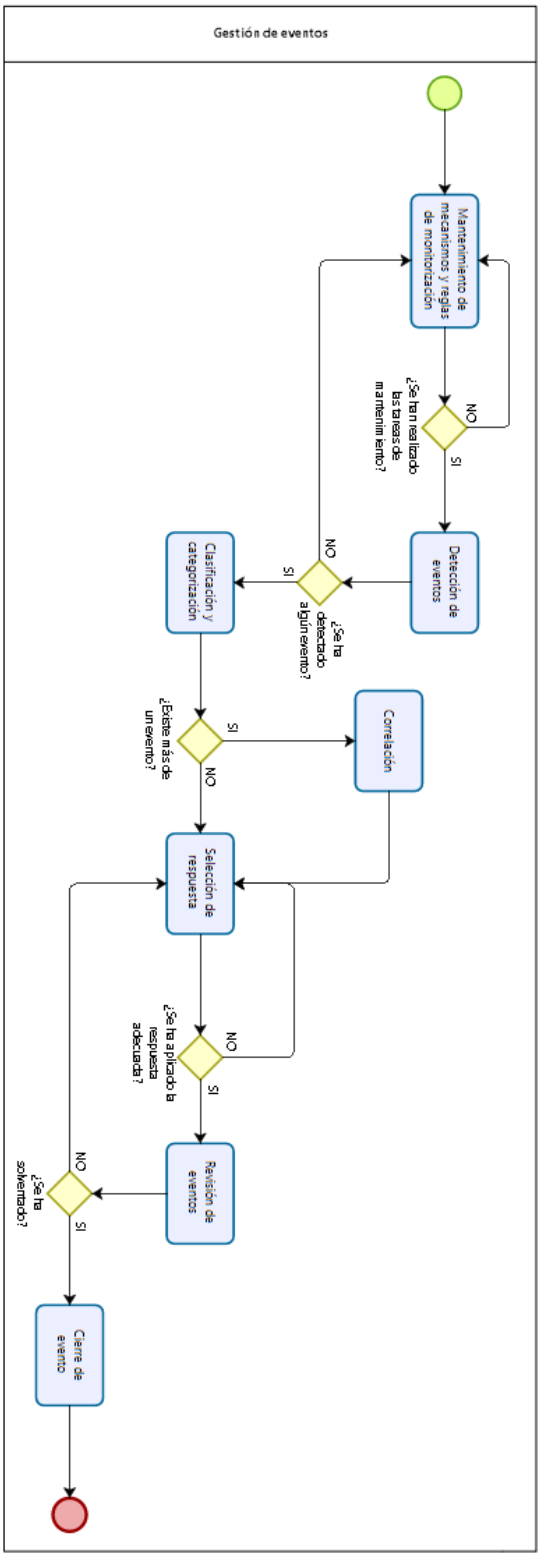


Imagen - 46: Flujograma gestión de Eventos

ANEXO II: Procedimiento de gestión de incidencias

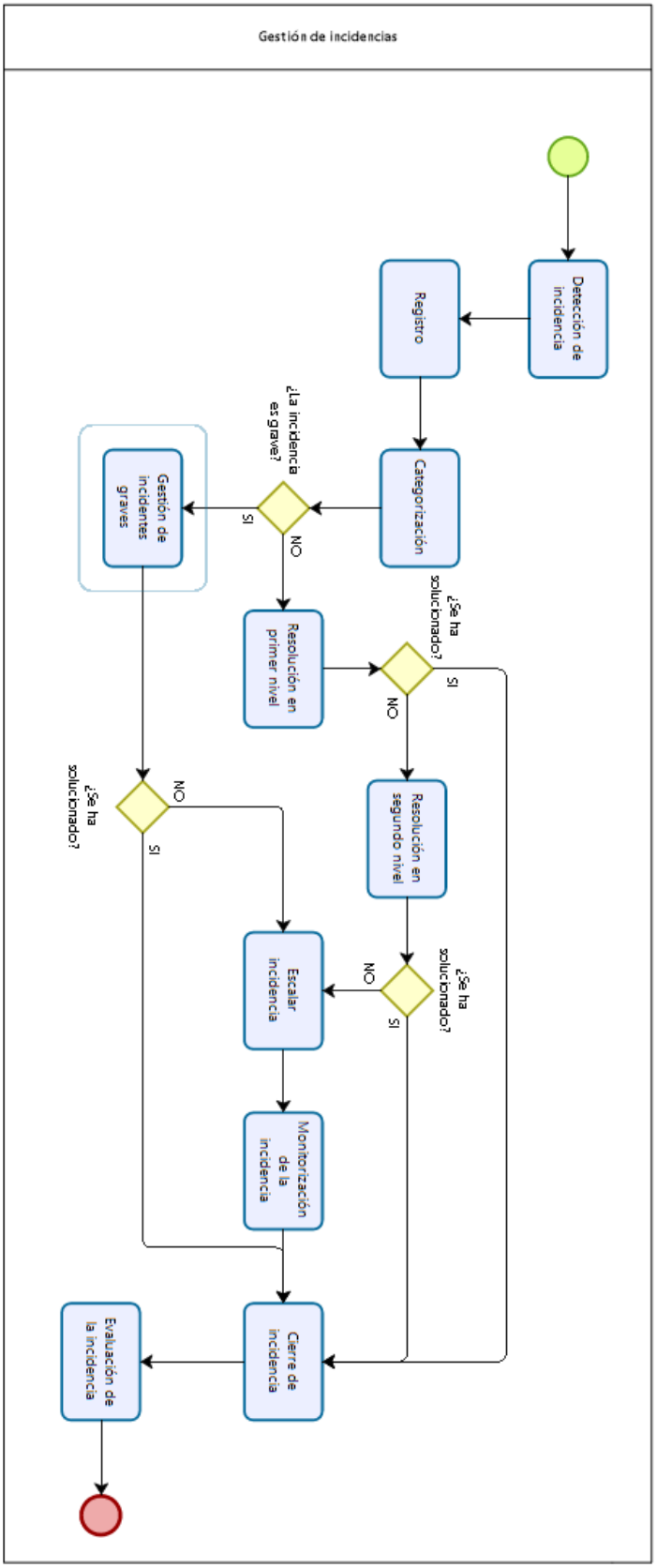


Imagen - 47: Flujograma gestión de Incidencias

ANEXO III: Procedimiento de gestión de problemas

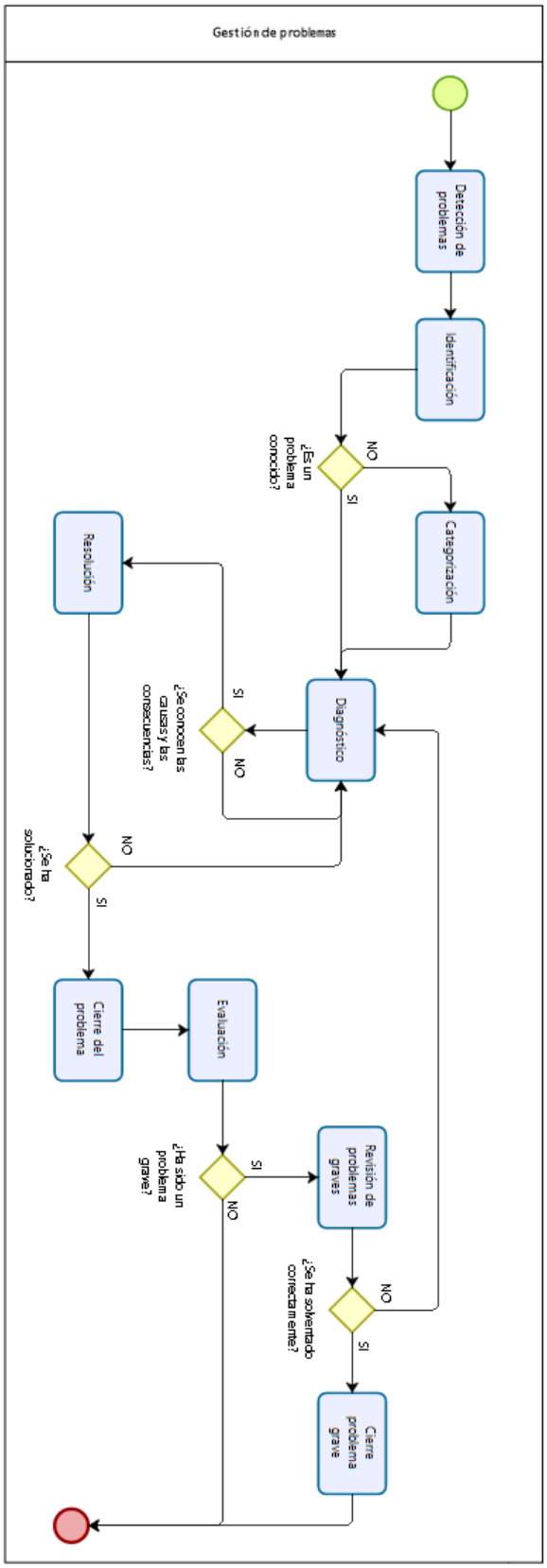


Imagen - 48: Flujograma gestión de Problemas

ANEXO IV: Procedimiento de gestión de alertas

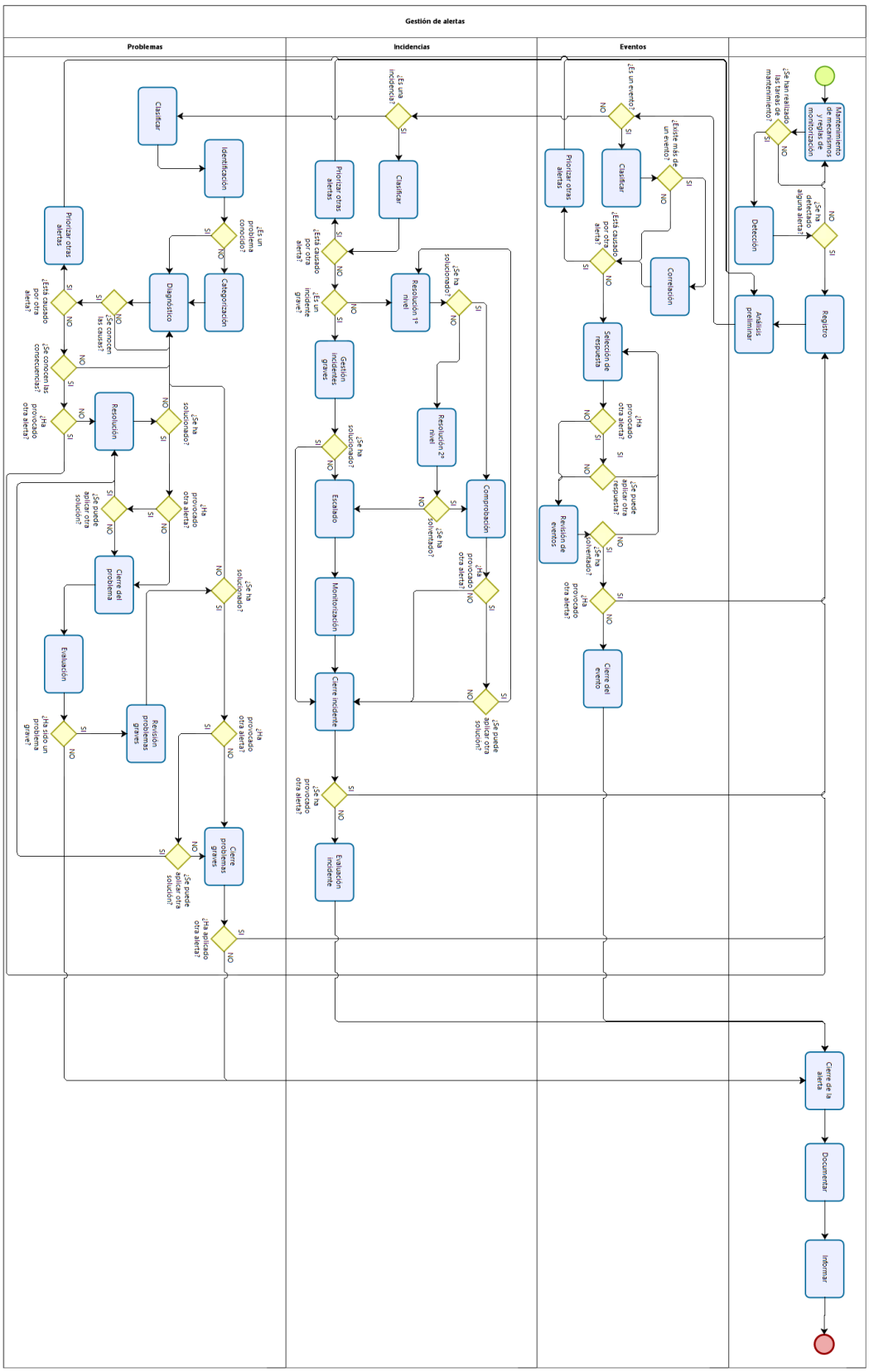
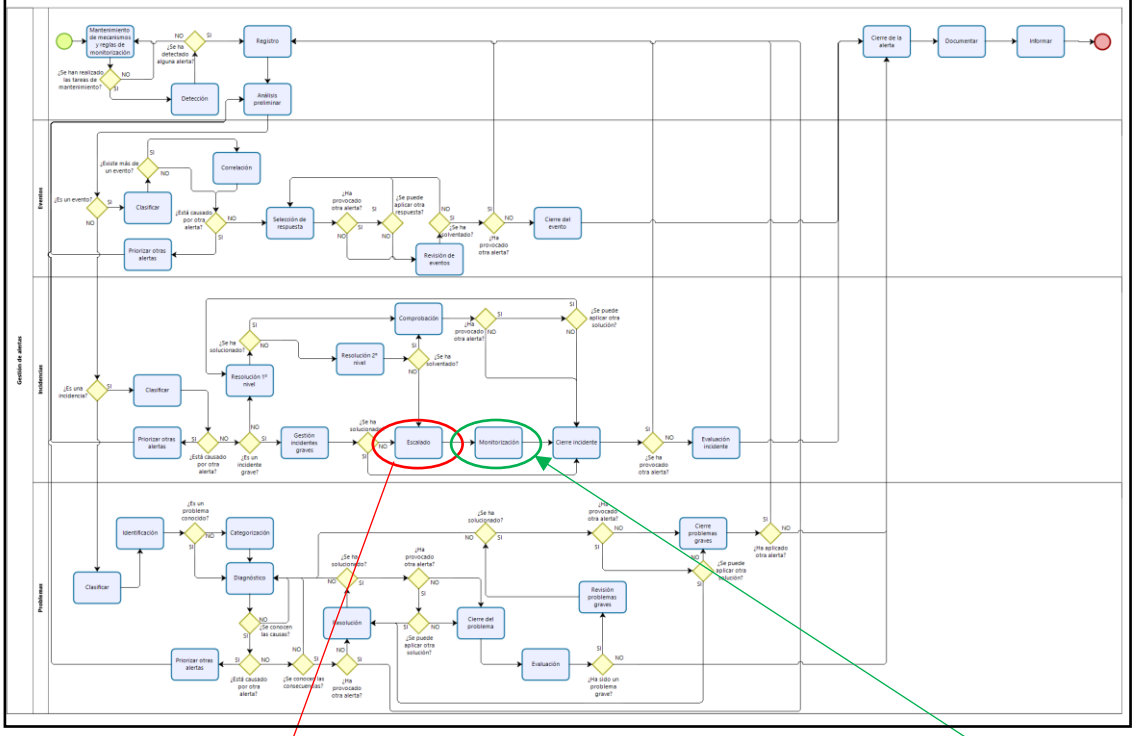
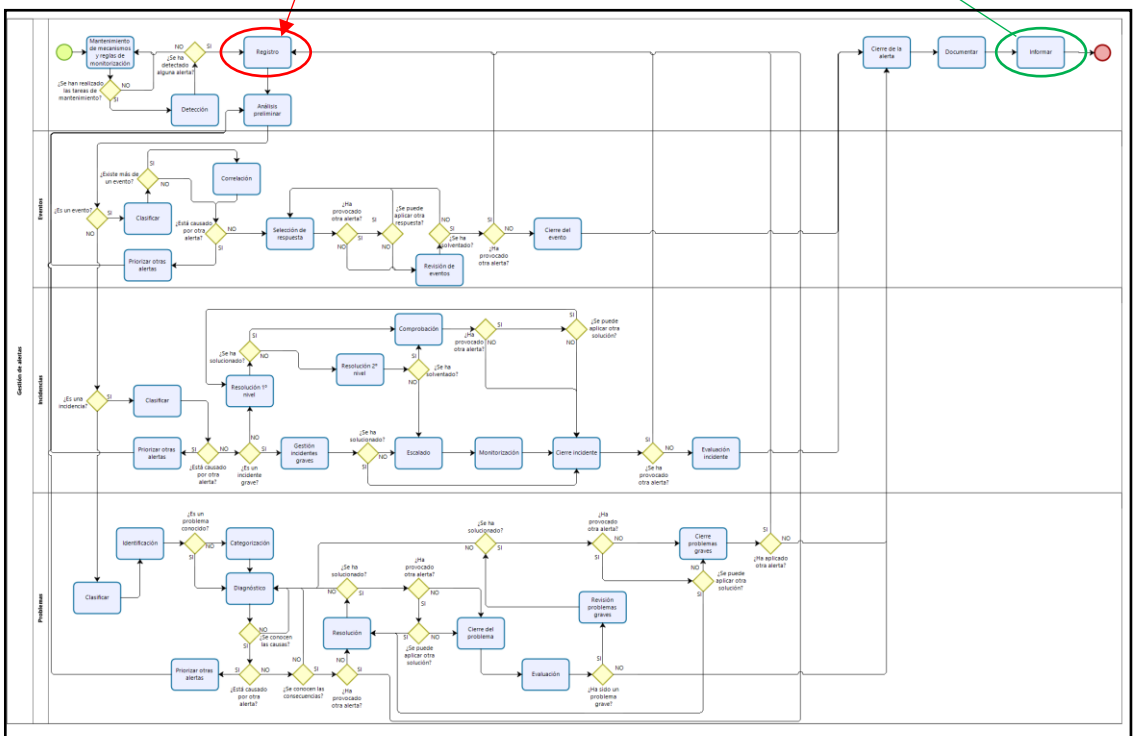


Imagen - 49: Flujograma procedimiento de gestión de Alertas

ANEXO V: Escalado de alertas

Procedimiento para usuario final.





Procedimiento para administradores de Cloud.

Imagen - 50: Escalado de alertas

2020

ESCUELA POLITECNICA SUPERIOR

Universidad de Alcalá