ManageEngine
Analytics Plus

# MITIGUE LAS INTERRUPCIONES Y MANTENGA LA PRODUCTIVIDAD CON ANÁLISIS DE TI UNIFICADO

Las interrupciones son la peor pesadilla de un profesional de TI. Descubra cómo mitigar las interrupciones utilizando el marco de tres pasos que se analiza en nuestro último e-book.

# Introducción

Las interrupciones son la peor pesadilla de un profesional de TI. Los asombrosos efectos de las interrupciones se dejan sentir en todos los niveles financieros y operativos, incluyendo pérdidas de ingresos, pérdidas de productividad y daños a la reputación.

Dependiendo del tamaño de la organización, las pérdidas financieras derivadas de una interrupción pueden variar. Los tiempos de inactividad cuestan entre:

**De 137 a 427 dólares**[1]
por minuto *para las pequeñas empresas*

**$16,000 dólares**[1]
por minuto *para las grandes empresas*

Las pérdidas de productividad y los daños a la reputación no son tan fáciles de cuantificar, ya que a veces pueden superar con creces las pérdidas económicas directas.

La clave para ser proactivo y mitigar las interrupciones es identificar a tiempo los indicadores de fallo y tomar medidas para evitar dichas interrupciones. Tradicionalmente, los responsables de TI han recurrido a aplicaciones de monitoreo y gestión de mercados verticales de TI específicos para predecir o pronosticar interrupciones inminentes. Sin embargo, la realización de análisis unificados facilita el cotejo de datos procedentes de múltiples aplicaciones de monitoreo y gestión de TI que abarcan todos los mercados verticales de TI. Esto le ayuda a comprender los eventos o cambios que precedieron a una interrupción de TI, lo que le permite obtener información exhaustiva que puede proporcionar una visibilidad de 360 grados de las interrupciones.

En este e-book, exploraremos un marco de tres pasos que puede ayudarle a detectar los primeros síntomas de fallo, así como la forma de identificar y mitigar las interrupciones.

Paso
01

# Selección y supervisión de indicadores fiables de fallos

Las interrupciones pueden paralizar las operaciones del negocio. Sin embargo, la buena noticia es que las interrupciones rara vez son el resultado de una interrupción brusca de los servicios, y en la mayoría de los casos siguen una secuencia específica de eventos que conducen al fallo. La supervisión de estas señales o síntomas puede ayudarle a predecir con bastante exactitud cuándo es probable que se produzcan fallos e interrupciones.

Por ejemplo, una interrupción debida a la congestión de la red podría haber tenido varios síntomas antes de su manifestación, como velocidad lenta de Internet, pérdida de paquetes, latencia, tiempos de espera de la conexión, aplicaciones que no responden, mayor tiempo de ida y vuelta, fluctuaciones de la red, escasa velocidad de transferencia de la red o mayor longitud de las colas.

Identificar los indicadores de fallo y supervisar el comportamiento histórico de estos indicadores puede ayudarle a establecer patrones de comportamiento normales. Una vez establecidas las líneas de base, le resultará más fácil identificar comportamientos anómalos y establecer un sistema de alarmas y notificaciones para interrupciones inminentes. Hacerlo puede ayudar mucho a evitar interrupciones. Para ayudar a delimitar los indicadores, vamos a examinar cuatro grandes categorías de fallos que provocan interrupciones:

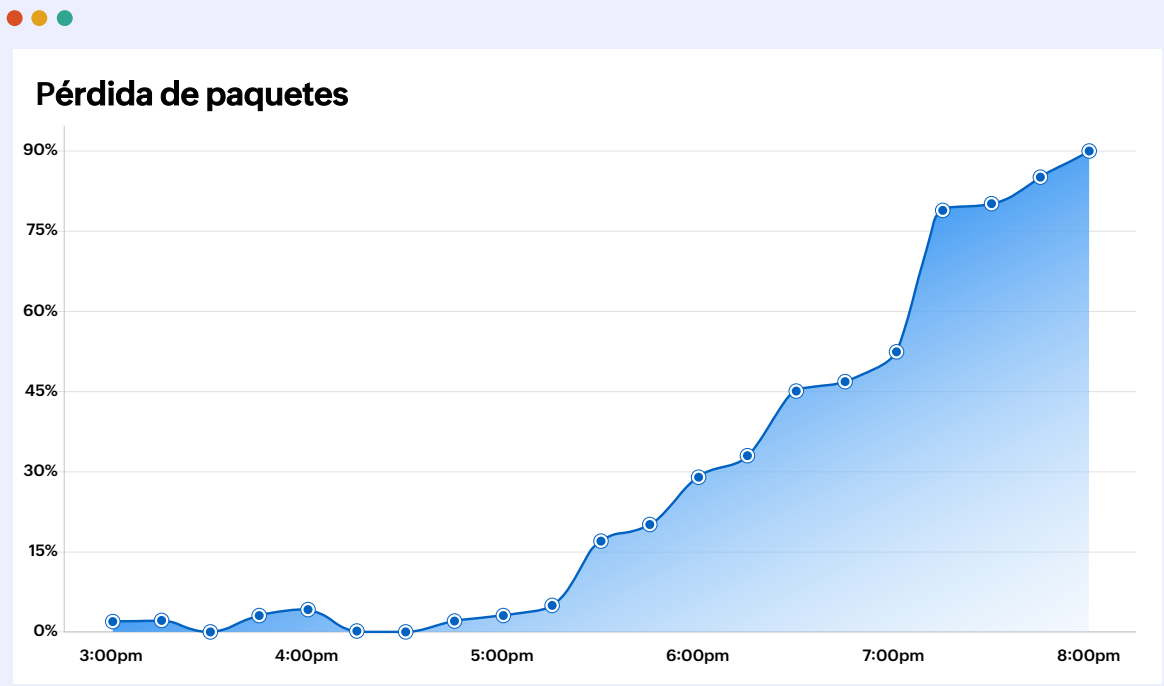
- Interrupciones debidas a fallos de los componentes
- Interrupciones debidas a limitaciones de capacidad
- Interrupciones debidas a errores humanos
- Interrupciones debidas a causas naturales

## Interrupciones debidas a fallos de los componentes

Los componentes de hardware y software fallan a menudo, o no funcionan como se esperaba, lo que provoca interrupciones. Los componentes de hardware, como switches, routers o servidores, pueden degradarse o quedar obsoletos, lo que provoca un rendimiento deficiente y, en última instancia, el cierre del sistema. Los componentes de software pueden desarrollar errores o fallos en su código con el tiempo o durante las actualizaciones que pueden provocar un mal funcionamiento de las aplicaciones de software. El seguimiento de la disponibilidad y el rendimiento de los componentes de hardware y software, y la vigilancia de los cambios en los niveles de rendimiento pueden ayudar a predecir cuándo es probable que fallen estos componentes. He aquí algunos ejemplos:

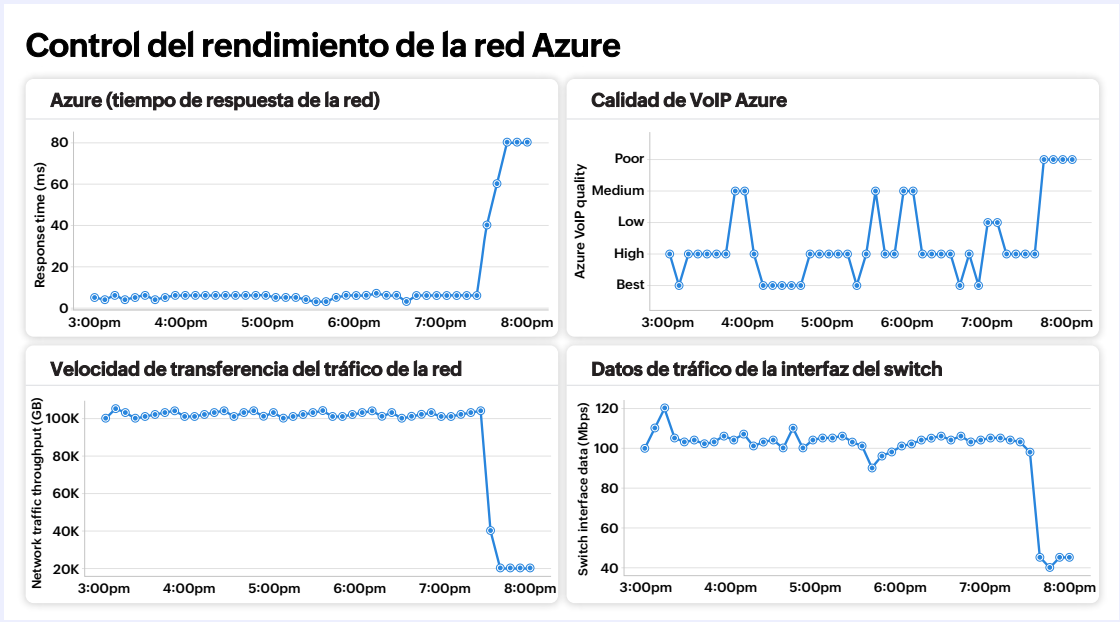
**Ejemplo A:** Considere las interrupciones de la red resultantes del fallo de uno o más componentes de la red. La supervisión de la **latencia y la pérdida de paquetes** puede indicar cuándo ha bajado el rendimiento de la red, y servir como señal de alerta temprana de que es probable que la red se caiga.

El siguiente informe de ejemplo muestra la pérdida de paquetes (en porcentaje) de un servicio de **VoIP**[2] en el plazo de unas horas. Una pérdida de paquetes del 1 al 5% puede ser aceptable. Cualquier porcentaje superior al 5% es motivo de preocupación y puede afectar a las cargas, las descargas y la velocidad de reproducción de los vídeos. Una pérdida de paquetes del 20% o superior indica que es probable que la red se caiga en unos minutos.



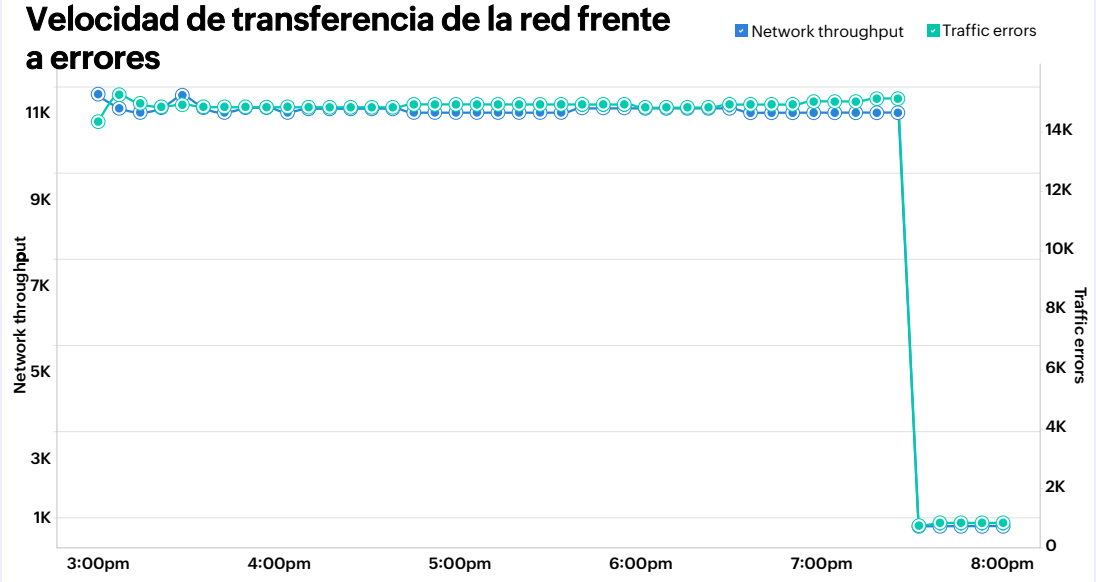

Aunque el aumento de la pérdida de paquetes es un indicio de que el rendimiento de la red se está degradando, un análisis en profundidad de la **velocidad de transferencia de la red** o del **volumen de tráfico** que fluye a través de dispositivos de red específicos, como routers, switches, servidores, dispositivos de almacenamiento y endpoints relacionados con la red en cuestión, puede ayudar a identificar el componente de red que está fallando.

El dashboard de muestra que aparece a continuación ofrece una imagen en tiempo real del tráfico que pasa por dispositivos de red como routers, switches, dispositivos de almacenamiento y endpoints.

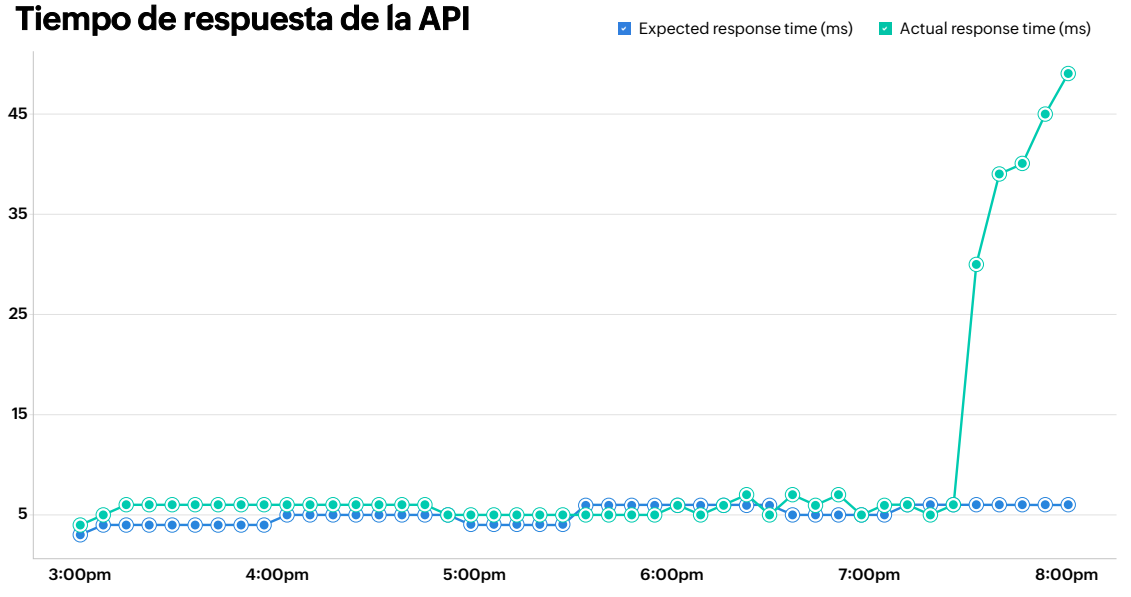



**Ejemplo B:** Considere los problemas relacionados con el software, como los fallos de la API. Las API esenciales para la comunicación entre dos o más aplicaciones pueden fallar por multitud de motivos, desde parches de actualización defectuosos hasta cambios de configuración involuntarios incompatibles con la API. El control del **número de errores de tráfico y del tiempo que tarda el objetivo en obtener respuestas** de los endpoints del cliente puede revelar cuándo es probable que fallen las API.

## Velocidad de transferencia de la red frente a errores




## Tiempo de respuesta de la API



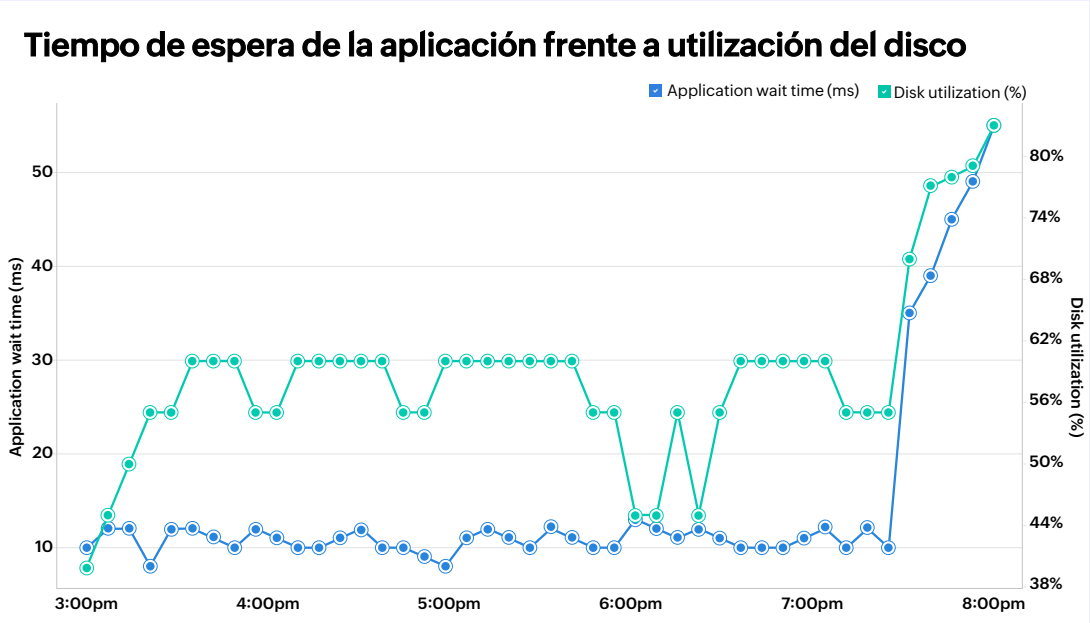
Las llamadas a la API que tardan mucho en responder indican problemas con la llamada a la API que pueden afectar al rendimiento de los servicios que dependen de las respuestas de la API.

El seguimiento de métricas críticas de disponibilidad y rendimiento, como el tiempo de respuesta, el tráfico de red, la latencia y la pérdida de paquetes, resulta útil para identificar fallos de hardware o software que puedan provocar una interrupción.

## Interrupciones debidas a limitaciones de capacidad

Cuando la demanda de un recurso supera la carga que puede soportar, se producen limitaciones de capacidad. Una demanda cada vez mayor de ese recurso podría ralentizar su rendimiento y, finalmente, apagarlo por sobrecarga. Algunos ejemplos de limitaciones de capacidad son los servidores que se quedan sin CPU o capacidad de almacenamiento, las redes que se quedan sin ancho de banda o las aplicaciones que tienen muy pocos hilos para procesar en paralelo. Las mejores métricas para hacer un seguimiento de las limitaciones de capacidad son las relacionadas con el uso. El control de las métricas de uso de los recursos frente a su capacidad disponible puede revelar cuándo los recursos se dirigen hacia una sobrecarga. He aquí algunos ejemplos:

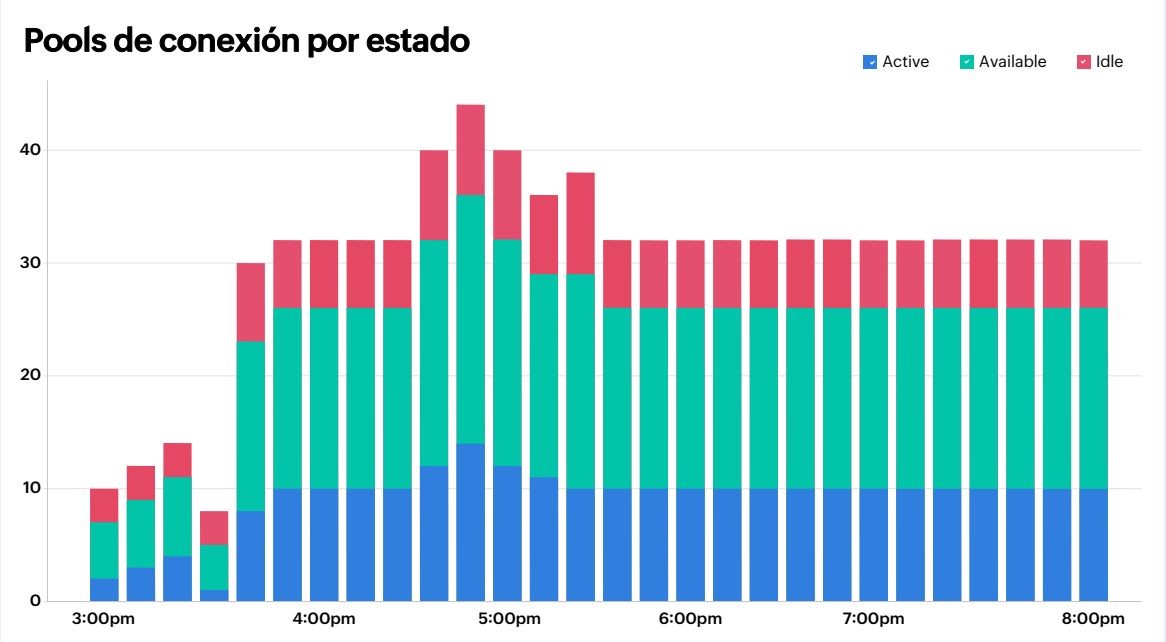
**Ejemplo A:** A veces, la lentitud o indisponibilidad de una aplicación por falta de capacidad puede deberse a la utilización de los discos. El informe ilustra que, a medida que aumenta la utilización del disco y se acerca al pico de utilización, aumenta el tiempo de espera de las aplicaciones.




Cuando la utilización del disco aumenta más allá de su pico, el sistema no podrá cargar datos adicionales ni seguir brindando funcionalidad a la aplicación, que dejará de estar disponible.

**Ejemplo B:** Otro ejemplo de limitaciones de capacidad son los pools de conexiones insuficientes que crean un interbloqueo, haciendo que las aplicaciones no estén disponibles para los usuarios. Cuando el tamaño del pool de conexiones es demasiado pequeño, la latencia aumenta y el tiempo de espera de las aplicaciones se incrementa, lo que acaba provocando su indisponibilidad.

Aquí hay un informe que muestra el número de pools de conexión para un servidor Tomcat por su estado.



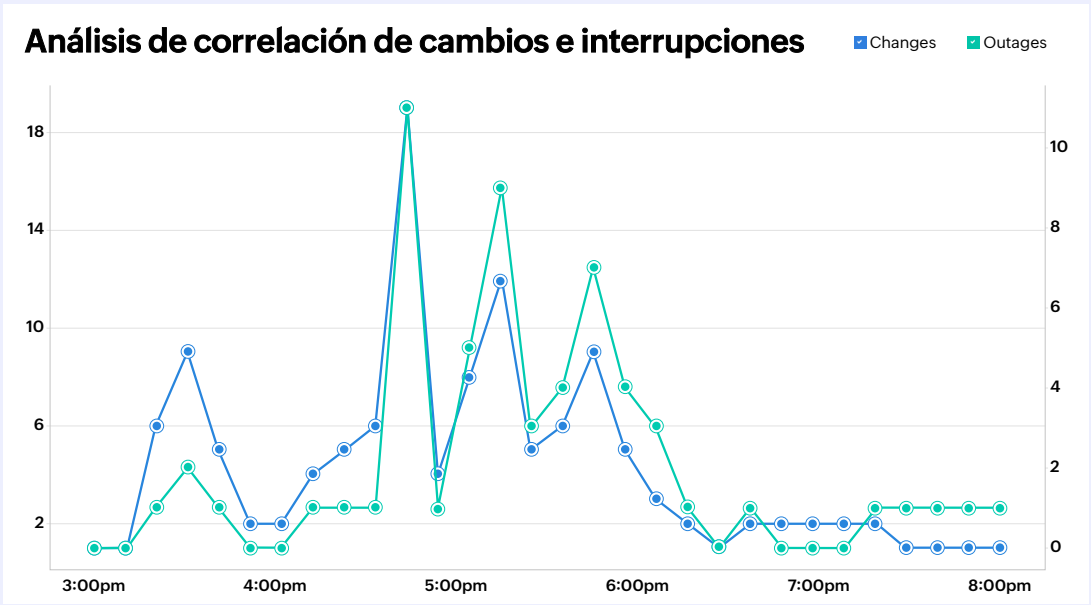

El control de las métricas de uso como las comentadas anteriormente son indicadores fiables de fallos inminentes por limitaciones de capacidad.

## Interrupciones debidas a errores manuales

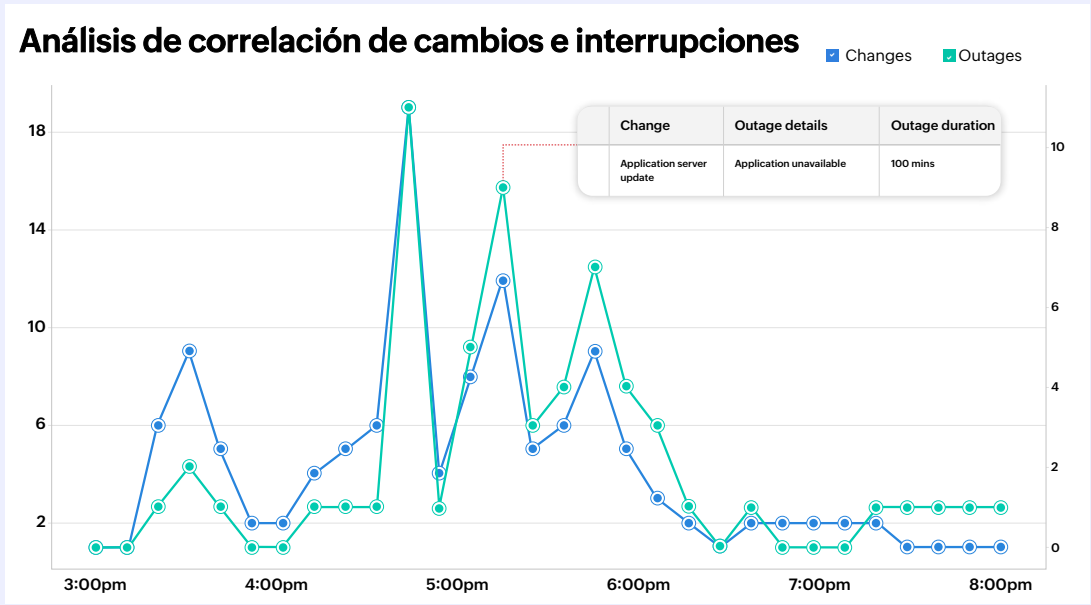
Las interrupciones debidas a errores humanos, como la implementación de cambios no planificados, la instalación de actualizaciones no probadas o la modificación de configuraciones de red sin la planificación adecuada, pueden afectar profundamente a la disponibilidad de redes y sistemas. En **Enero de 2023**[3], los servicios en la nube de Microsoft, incluidos Azure, Teams y Outlook, experimentaron una interrupción global debido a una actualización de la WAN. Esta interrupción afectó a usuarios de todo el mundo y causó importantes trastornos en la productividad y la comunicación. Exactamente un mes después, Amazon AWS sufrió una importante interrupción que afectó a varios sitios web y aplicaciones como Netflix, Spotify y Reddit. Casi al mismo tiempo, Google Cloud Platform (GCP) también experimentó una interrupción parcial que afectó a algunos de sus productos, como Gmail, YouTube y Drive. El origen de ambas interrupciones se remonta a un error de configuración de la red introducido durante un mantenimiento rutinario.

Teniendo en cuenta que los errores humanos son consecuencia de los cambios implementados o introducidos, el control del volumen de cambios y la correlación de los fallos con los cambios implementados pueden servir como indicadores fiables de las interrupciones relacionadas con los cambios.

He aquí un informe que compara la tendencia de las interrupciones en los dos últimos años y el volumen de cambios implementados.




Si se examina detalladamente en una de las interrupciones, es evidente que existe una fuerte correlación entre un cambio implementado (una actualización del servidor de aplicaciones) y una interrupción que duró hora y media.



## Interrupciones debidas a causas naturales

Incluso cuando los departamentos de TI funcionan a las mil maravillas, pueden producirse interrupciones. Las causas que escapan al control humano, como las interrupciones de electricidad, las inclemencias del tiempo o las catástrofes naturales, pueden afectar enormemente a la continuidad del negocio. La mejor defensa, y posiblemente la única defensa contra las causas naturales que pueden adoptar las organizaciones, es comprender los patrones y prepararse. Por ejemplo, analizar el patrón histórico de interrupciones de una organización puede revelar unidades de negocio u oficinas propensas a sufrir interrupciones relacionadas con catástrofes naturales.

A continuación se muestra un mapa que ilustra el historial de interrupciones de una organización de ejemplo. Está claro que Florida ha sido testigo del mayor número de interrupciones en el pasado. Es bien sabido que las regiones costeras, sobre todo a lo largo del Golfo de México, son propensas a huracanes e inundaciones. Esta información puede utilizarse para crear dispositivos de seguridad para estas regiones cuando se produzcan catástrofes naturales.

**Interrupciones relacionadas con catástrofes naturales**

Las causas naturales son uno de los principales motivos de las interrupciones imprevisibles. Aunque no se puede detener a la madre naturaleza, siempre hay medidas que puede tomar para proteger sus servidores y garantizar que sus servicios estén siempre disponibles.

- Diseñe estratégicamente planes de recuperación en caso de catástrofe para garantizar la continuidad del negocio. En primer lugar, analice los tipos de catástrofe que suponen un mayor riesgo para la continuidad de los negocios en regiones específicas. A continuación, audite todos los recursos de TI de sus redes y servidores para conocer las necesidades de capacidad y uso. Luego, elabore planes sobre la cantidad de almacenamiento de datos, red y otras infraestructuras que se necesitarían para continuar las operaciones en caso de catástrofe.

- Establezca sitios de recuperación en caso de catástrofe y garantice que se realicen copias de seguridad periódicas de los datos en estos sitios/servidores. Disponer de una copia de seguridad le garantiza poder cambiar rápidamente sus servicios de los servidores primarios a los de respaldo casi al instante, mientras que la copia de seguridad de los datos garantiza que los datos disponibles sean recientes y estén actualizados para que sus empleados y usuarios finales puedan utilizarlos. Opte por las copias de seguridad en la nube y haga copias de seguridad de los datos en función de la geografía y las operaciones para una recuperación en caso de catástrofe sin inconvenientes.

- Cree roles y responsabilidades específicas para las personas de su equipo de TI durante las catástrofes. Disponer de recursos específicos para hacer frente a necesidades de TI especiales durante las catástrofes infunde orden y claridad en medio del caos.

- Haga un simulacro una vez que haya planificado su infraestructura y el personal para hacer frente a las catástrofes. Realice una prueba de recuperación completa o una prueba de simulación para comprobar si su plan es preciso y sostiene a su negocio cuando sea necesario.

Paso
02

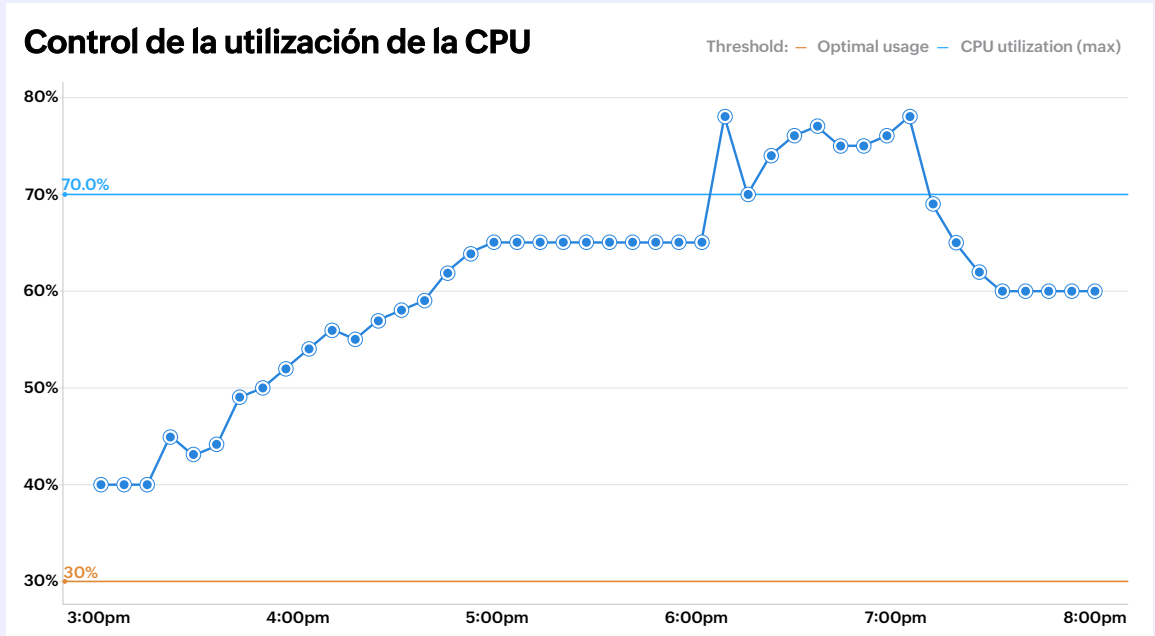
# Establezca alertas basadas en reglas para detectar infracciones

Determinar las métricas y los indicadores críticos adecuados es el paso crucial para mitigar las interrupciones. El resto, es decir, establecer umbrales y monitorear y ajustar los umbrales, es fácil de conseguir una vez que se han decidido los indicadores.

En uno de nuestros ejemplos anteriores, exploramos la falta de disponibilidad de los pools de conexión. Se pueden establecer umbrales para el número mínimo y máximo de pools de conexiones necesarios para una disponibilidad de la aplicación sin inconvenientes.

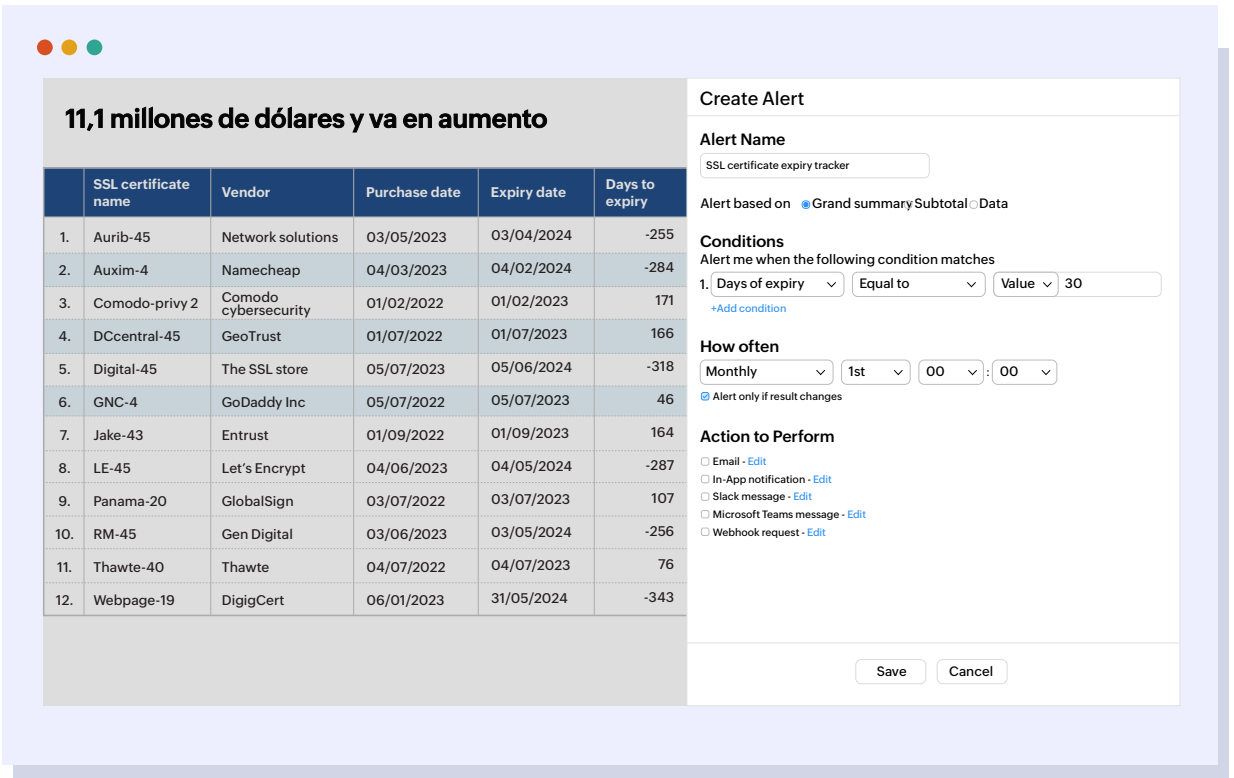
Una vez que el número de pools de conexiones necesarios cae por debajo de los límites permitidos (es decir, el umbral creado), se puede alertar a los responsables de TI afectados para que aumenten el número de conexiones disponibles.

Alternativamente, también se pueden establecer umbrales para realizar un control del rendimiento de base y máximo. El siguiente informe muestra el uso de la CPU para una instancia de Azure. Los niveles básicos se fijan en el 30%, mientras que los niveles máximos se fijan en el 70%.




El control de la utilización del disco mediante niveles básicos y máximos lleva la predicción de interrupciones al siguiente nivel al proporcionarle una ventana para evaluar y planificar la utilización del disco, con la posibilidad de evitar una situación en la que tenga una alta utilización del disco. Identificar y comprender las ocasiones en las que la utilización del disco desciende y alcanza su punto máximo le proporcionará el margen suficiente para equilibrar los requisitos de capacidad del disco entre el uso y las necesidades.

También se pueden establecer umbrales basados en reglas para detectar la caducidad y el final de la vida útil de activos de software como certificados SSL o licencias. La falta de un sistema de alerta adecuado para la caducidad de licencias y certificados ha provocado el cierre de varias empresas importantes en el pasado. **Microsoft**[4] sufrió una interrupción embarazosa en 2020 debido a un certificado SSL caducado. Un año después, **Epic Games**[5]creador de Fortnite, Rocket League y Houseparty, sufrió una interrupción masiva debido a certificados SSL caducados. El costo medio anual de las interrupciones debidas a la caducidad de los certificados ronda los **$11.1 11,1 millones de dólares y va en aumento**[6].




| | SSL certificate name | Vendor | Purchase date | Expiry date | Days to expiry |
|---|---|---|---|---|---|
| 1. | Aurib-45 | Network solutions | 03/05/2023 | 03/04/2024 | -255 |
| 2. | Auxim-4 | Namecheap | 04/03/2023 | 04/02/2024 | -284 |
| 3. | Comodo-privy 2 | Comodo cybersecurity | 01/02/2022 | 01/02/2023 | 171 |
| 4. | DCcentral-45 | GeoTrust | 01/07/2022 | 01/07/2023 | 166 |
| 5. | Digital-45 | The SSL store | 05/07/2023 | 05/06/2024 | -318 |
| 6. | GNC-4 | GoDaddy Inc | 05/07/2022 | 05/07/2023 | 46 |
| 7. | Jake-43 | Entrust | 01/09/2022 | 01/09/2023 | 164 |
| 8. | LE-45 | Let's Encrypt | 04/06/2023 | 04/05/2024 | -287 |
| 9. | Panama-20 | GlobalSign | 03/07/2022 | 03/07/2023 | 107 |
| 10. | RM-45 | Gen Digital | 03/06/2023 | 03/05/2024 | -256 |
| 11. | Thawte-40 | Thawte | 04/07/2022 | 04/07/2023 | 76 |
| 12. | Webpage-19 | DigiCert | 06/01/2023 | 31/05/2024 | -343 |

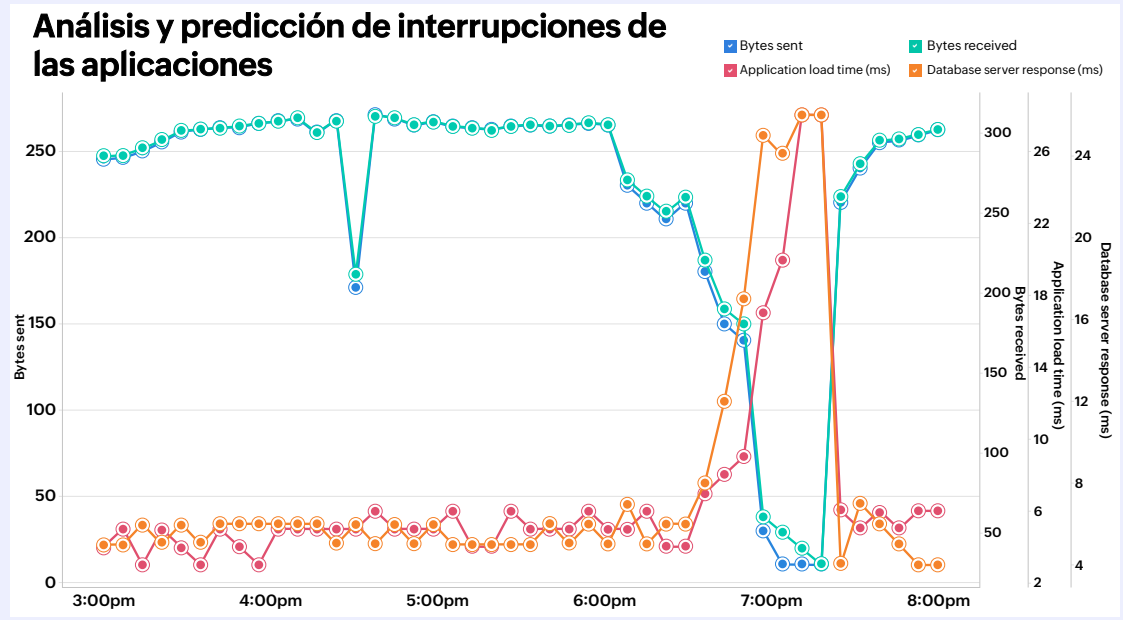
Controlar cuándo caducan los certificados o las licencias es importante para detectar las infracciones antes de que se produzcan. Así dispondrá del tiempo y la información necesarios para solucionar los problemas y evitar interrupciones.

Paso
03

# Unificar los indicadores de fallos

La deconstrucción de una interrupción revelaría que el fallo se produjo debido a un cambio en el funcionamiento normal de los sistemas y componentes de TI. Identificar estos puntos de fallo mediante indicadores y configurar alertas basadas en umbrales puede ayudarle a detectar estos problemas a medida que avanzan hacia una interrupción. Sin embargo, es probable que estos umbrales cambien a medida que maduren los procesos operativos y la organización. Analizar continuamente los datos y actualizar estos umbrales garantizará que su sistema siga siendo funcional y efectivo a largo plazo.

Aunque establecer y ajustar los umbrales y estar atento a los cambios ayuda a detectar los activadores de las interrupciones o los indicadores de interrupciones en una fase temprana, estos indicadores también pueden agruparse para detectar fallos multipunto unificando la información de varios indicadores. Por ejemplo, los fallos de las aplicaciones no tienen por qué deberse siempre a fallos puntuales. También pueden ser el resultado de fallos en varios puntos, como dispositivos de red, servidores de aplicaciones y servidores de bases de datos; los tres componentes básicos que deben funcionar con eficiencia para que los usuarios puedan acceder a las aplicaciones de manera eficiente. Una aplicación puede dejar de responder ante el usuario final incluso si uno de estos componentes falla o no funciona eficientemente. El análisis permite a los usuarios ver todos los componentes subyacentes juntos para que los equipos de aplicaciones obtengan una visión holística del estado de las aplicaciones.




Esta superposición o unificación de la información permite registrar errores y alertas sin inconvenientes, lo que facilita la detección de fallos en tiempo real.

# Conclusión

Mientras que las aplicaciones de monitoreo y gestión de TI específicas del mercado vertical pueden dar una idea aproximada de las interrupciones y ayudar a preverlas, la unificación de todos los datos de TI se basa en indicadores y umbrales en tiempo real para predecir una interrupción, utilizando datos de un grupo de aplicaciones de monitoreo y gestión. Esto aumenta la precisión y fiabilidad de las predicciones de interrupciones de servicio al proporcionar una visibilidad completa y de 360 grados de los datos de TI.

En este e-book, hemos aplicado el marco de predicción de interrupciones en tres pasos y lo hemos aplicado a algunos casos de uso para comprender cómo predecir, prepararse y prevenir una interrupción de TI.

Para obtener más información sobre cómo aprovechar los análisis unificados para prevenir interrupciones, consulte algunos de nuestros otros recursos.

# Acerca de

ManageEngine Analytics Plus es una solución de análisis de TI de autoservicio basada en IA que ayuda a las organizaciones a implementar iniciativas complejas que abordan los requisitos de las empresas en expansión. Disponible on-premises y en la nube, Analytics Plus visualiza datos de TI de varias aplicaciones y se integra de forma out-of-the-box con varias aplicaciones de TI populares como ManageEngine ServiceDesk Plus, Jira, Service Now, Zendesk y ManageEngine Endpoint Central. Analytics Plus cuenta con un asistente de análisis basado en inteligencia artificial que responde a instrucciones de voz y texto para proporcionar visualizaciones significativas. Esto elimina la necesidad de que un analista de datos ayude a los gestores de la mesa de ayuda y reduce el tiempo de elaboración de informes, al tiempo que permite a las organizaciones tomar decisiones más rápidas y basadas en datos.

Inicie su viaje de análisis de TI con una prueba gratuita de Analytics Plus. ¿Quiere obtener más información sobre el producto antes de probarlo? Solicite una demo virtual gratuita con uno de nuestros expertos en soluciones.

**280**
clientes
en todo el mundo

**Más de 90**
productos
y herramientas gratuitas

**Más de 190**
países
atendidos

**Más de 20**
años de experiencia
en gestión de TI

## Referencias


1. https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/
2. https://www.ir.com/guides/what-is-network-packet-loss
3. https://www.linkedin.com/pulse/recent-cloud-platform-outages-2023-pankaj-kumar-mandal/
4. https://informationsecuritybuzz.com/experts-reaction-on-microsoft-teams-suffers-major-worldwide-outage-due-to-expire-certificate/
5. https://www.keyfactor.com/blog/the-enemy-of-uptime-an-expired-ssl-certificate/
6. https://devops.com/5-ways-to-prevent-an-outage/


Analytics Plus