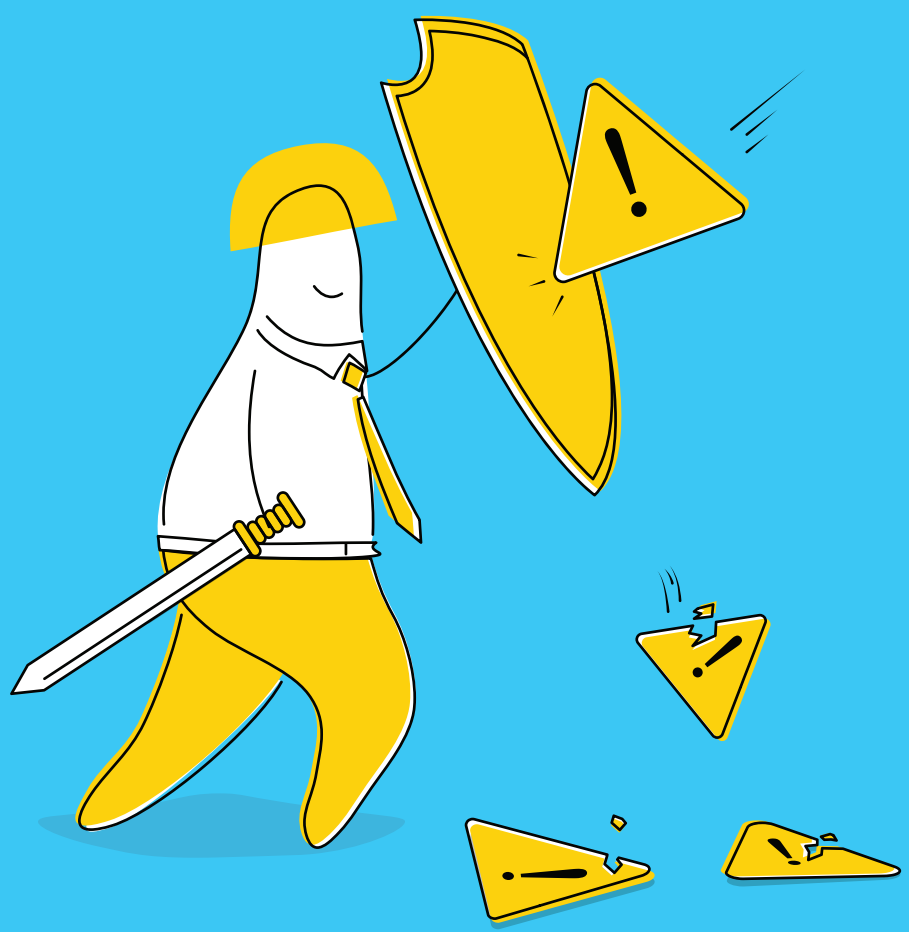
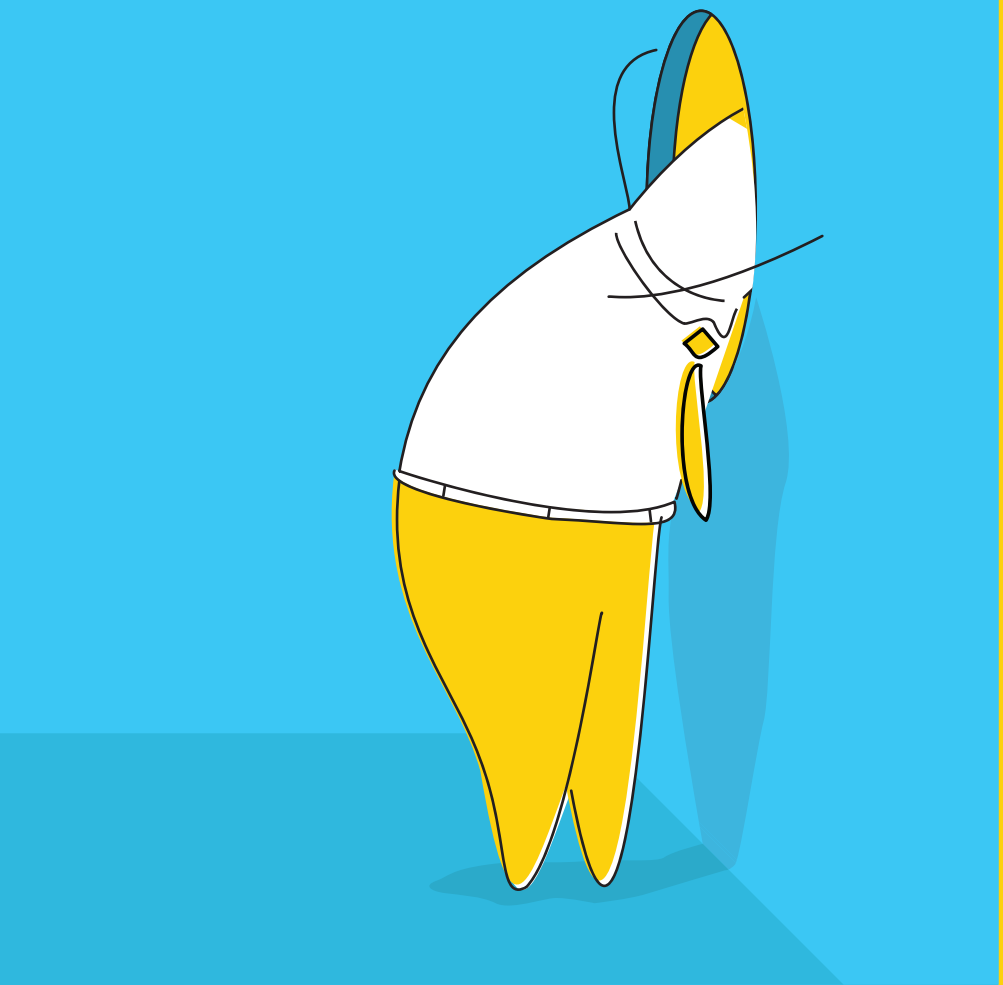
ManageEngine
ServiceDesk Plus



MANUAL DE GESTIÓN DE INCIDENTES

CÓMO ZOHO GESTIONA EL ESPECTRO DE INCIDENTES DE TI

¿QUÉ CONTIENE?



Introducción **01**

Contexto 01
¿A quién va dirigido esta guía? 03
¿Qué es un incidente? 03
¿Qué es la gestión de incidentes (IM)? 03
Los valores de nuestros incidentes 04
Nuestras herramientas de IM 05

Procesos de gestión de incidentes **09**

Iteración de desktop 10
Big bang 21
CyberSec 31

Análisis de la causa raíz (RCA) **42**

¿Qué es el RCA? 42
¿Por qué realizar el RCA? 42
Principios de RCA 42
Proceso de RCA 43
Reuniones de RCA 49

Conclusión **49**

"¡Uf! Eso estuvo cerca. ¡Esperemos que no vuelva a ocurrir!"

Introducción

En la última década, hemos combatido miles de incidentes.

Como pioneros, hemos experimentado incidentes de escasa repercusión que, por lo general, han necesitado menos técnicos, pero aun así han requerido un marco de gestión de incidentes (IM) bien establecido. En la mayoría de los incidentes del pasado, dependíamos de la resolución de problemas por parte de individuos. Sin embargo, a medida que nuestra infraestructura de TI crecía, nos enfrentábamos a incidentes más complejos y de mayor repercusión, lo que nos obligó a mejorar nuestra IM.

Pronto nos dimos cuenta de que no existe un proceso único para gestionar los distintos tipos de incidentes a los que se enfrenta nuestra organización. Así que tomamos los marcos más efectivos y añadimos, combinamos u omitimos pasos para gestionar cada tipo de incidente en función de su impacto y de nuestras operaciones empresariales. Esto garantiza que cada respuesta esté bien adaptada a los retos que plantea cada incidente.

¿El resultado? Nuestro proceso de incidentes va ahora más allá de los marcos establecidos en el sector. Nuestros marcos de IM se clasifican en función de la gravedad y el impacto que los distintos tipos de incidentes tienen en las operaciones de la empresa.

Marco de IM		Impacto	Escenarios
Iteración de desktop	• Incidentes de falla/ corrección que afectan a un usuario individual	• Afecta a un solo usuario • No hay servicios críticos afectados	• Restablecimiento de contraseñas • La conexión a Internet funciona con lentitud
	• Incidentes de impacto bajo o medio que afectan a grupos de usuarios o departamentos	• Afecta a un solo usuario VIP • Afecta a un pequeño grupo de usuarios finales • No hay riesgo de pérdidas económicas ni de pérdida de reputación	• El laptop del CEO no funciona y no puede enviar ni recibir comunicaciones • Una impresora no funciona en un piso determinado
Bing Bang	• Alta urgencia • Afecta al servicio	• Un determinado servicio, aplicación o componente de infraestructura crítico para el negocio no está disponible y el tiempo estimado para su recuperación es desconocido o excesivamente largo • El servicio no está disponible. Se espera el restablecimiento inmediato.	• Nuestra conexión de red de alta velocidad falla, y la comunicación hacia y desde fuera de nuestra organización se interrumpe • La funcionalidad principal de una aplicación no funciona, lo que afecta a varios clientes • Una de nuestras aplicaciones no funciona. Un ataque de denegación de servicio distribuido (DDoS)
Fallo crítico	• Urgencia inmediata • Situaciones críticas o de alerta roja que afectan a la empresa	• Afecta a los resultados de nuestra empresa • Impacto mayor en los ingresos, la reputación y los asuntos jurídicos	• Errores y vulnerabilidades del software • Malware • Amenaza persistente avanzada (APT) • Ransomware • Phishing e ingeniería social • Amenaza interna

En lo que respecta a la IM, no existe una solución única, ya que cada organización es diferente. Lo que funcione para su organización dependerá de su modelo de negocio, infraestructura, operaciones, la información que esté protegiendo, sus recursos, etc. Reconozca que algunas técnicas solo se consiguen con el tiempo y la experiencia. ¡Sin embargo, esto no debe disuadirle de empezar!

¿A quién va dirigida esta guía?

Este e-book está dirigido a líderes, directores y profesionales de TI desde la perspectiva de la gestión de servicios. Le guiaremos a través de nuestros procesos de IM con flujos de procesos ilustrados, roles y mejores prácticas. Esta guía está repleta de lecciones que hemos aprendido por ensayo y error, para que usted no tenga que hacerlo.

Antes de entrar en materia, vamos a aclarar los conceptos básicos.

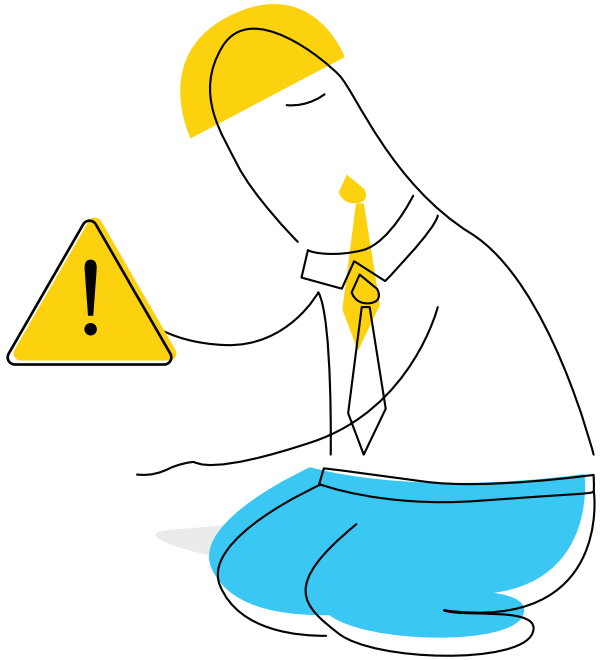
¿Qué es un incidente?

Un incidente es una interrupción no planificada que causa, puede causar o reduce la calidad de un servicio de TI. Algunos ejemplos clásicos son la lentitud de Internet, la caída de una aplicación empresarial o el mal funcionamiento de una impresora.

La verdad es que podemos definir un incidente de muchas maneras. Lo más importante es que cada incidente tenga una respuesta y una resolución bien estructuradas y oportunas.

¿Qué es la gestión de incidentes?

La gestión de incidentes es una forma de restablecer el funcionamiento normal del servicio lo antes posible, minimizando cualquier impacto adverso en las operaciones de la empresa o en el usuario.

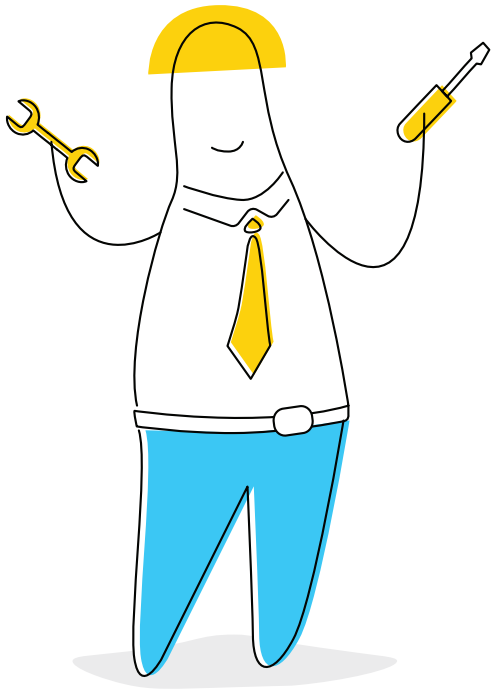


Los valores de nuestros incidentes

Principios de los incidentes	Enfoque
Ser proactivo, no reactivo	• Un enfoque proactivo: el mantenimiento preventivo se realiza regularmente para reducir la probabilidad de fallas, incluso antes de que los usuarios se vean afectados. • Las herramientas de monitoreo proporcionan visibilidad sobre la salud y el rendimiento de la red, y nos alertan de los problemas antes de que se conviertan en incidentes.
Ser abierto y comunicar apropiadamente	• Nos comunicamos con nuestros clientes desde el principio y a menudo, para que sepan que estamos al tanto de los problemas y trabajando en ellos. • Cuando se produce un incidente, se notifica automáticamente a un grupo predefinido de partes interesadas a través de sus métodos de contacto preferidos.
Alinear equipos, colaborar de manera efectiva	• Tenemos equipos distribuidos de varias zonas horarias trabajando juntos durante incidentes de gran impacto, marcando a un número de puente de conferencia telefónica y utilizando aplicaciones de comunicación o productividad para gestionar el incidente.
Recuperarse rápidamente	• La gestión de incidentes puede significar muchas cosas. Sin embargo, para nosotros se traduce en gestión del tiempo. • Utilizamos Site24x7, que nos avisa en cuanto algo falla. Adelantarse a los problemas es crucial para nuestra IM. A veces, nuestros empleados se convierten en un sistema de alerta. Utilizan nuestros sistemas a diario y probablemente sean los primeros en darse cuenta de que algo no va bien. • Tenemos un sistema de IM abierto, seguimos protocolos cuando es necesario y trabajamos en equipo para resolver el problema lo antes posible.
Documentar las lecciones	• A veces cometemos errores. ¿Y quién no? Sin embargo, nos aseguramos de aprender de esos errores documentando las lecciones aprendidas.
Mejorar continuamente	• Profundizamos en lo que salió mal para asegurarnos de no cometer el mismo error dos veces. • A veces, realizamos simulacros de incidentes para ver cómo se mantiene nuestra estrategia de IM. Y seguimos afinándola antes de que ocurra la situación real.

Nuestras herramientas de IM

Utilizamos varias herramientas para facilitar nuestros procesos de IM.



Incidentes de desktop

Control y gestión de incidentes:
ServiceDesk Plus Cloud está personalizado para adaptarse a nuestros procesos de gestión de incidentes.

Gestión de contraseñas:
Password Manager Pro es una bóveda segura para almacenar y gestionar información confidencial compartida, como contraseñas, documentos e identidades digitales de empresas.

Incidentes de disponibilidad mayores

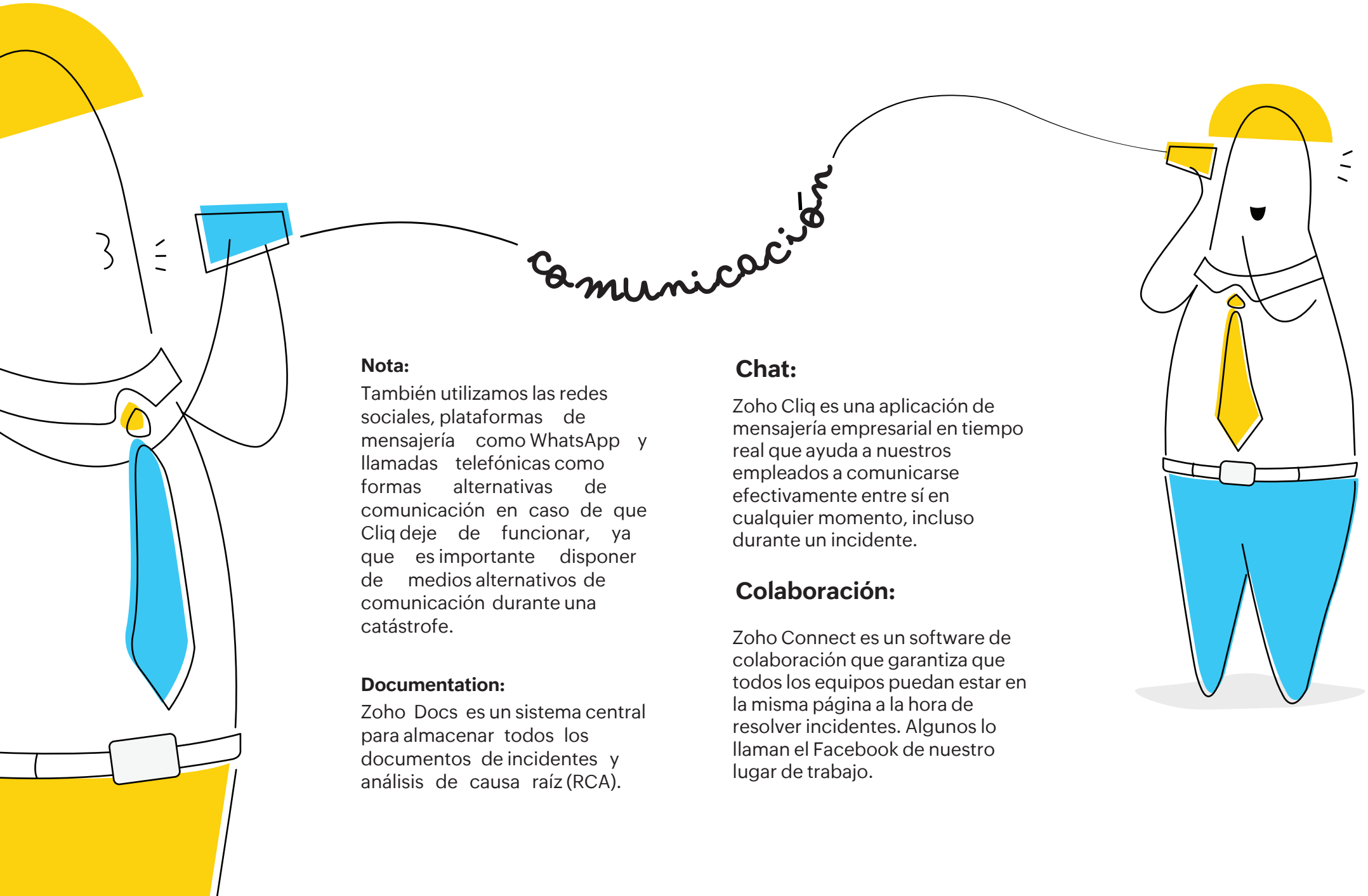
Herramienta de alerta:
ADManager Pluses una herramienta de autoservicio para restablecer contraseñas.

Restablecimiento de contraseñas:
ADManager Plus es una herramienta de autoservicio para restablecer contraseñas.

Gestión de endpoints:
Desktop Central, una solución unificada de gestión de endpoints, ayuda a gestionar servidores, laptops, desktops, smartphones y tablets desde una ubicación central.

Incidentes de seguridad

Programa Bug Bounty:
Bug Bountyes una herramienta de terceros para que empleados y particulares informen de fallos y errores (bugs), como exploits y vulnerabilidades.



Nota:

También utilizamos las redes sociales, plataformas de mensajería como WhatsApp y llamadas telefónicas como formas alternativas de comunicación en caso de que Cliq deje de funcionar, ya que es importante disponer de medios alternativos de comunicación durante una catástrofe.

Documentation:

Zoho Docs es un sistema central para almacenar todos los documentos de incidentes y análisis de causa raíz (RCA).

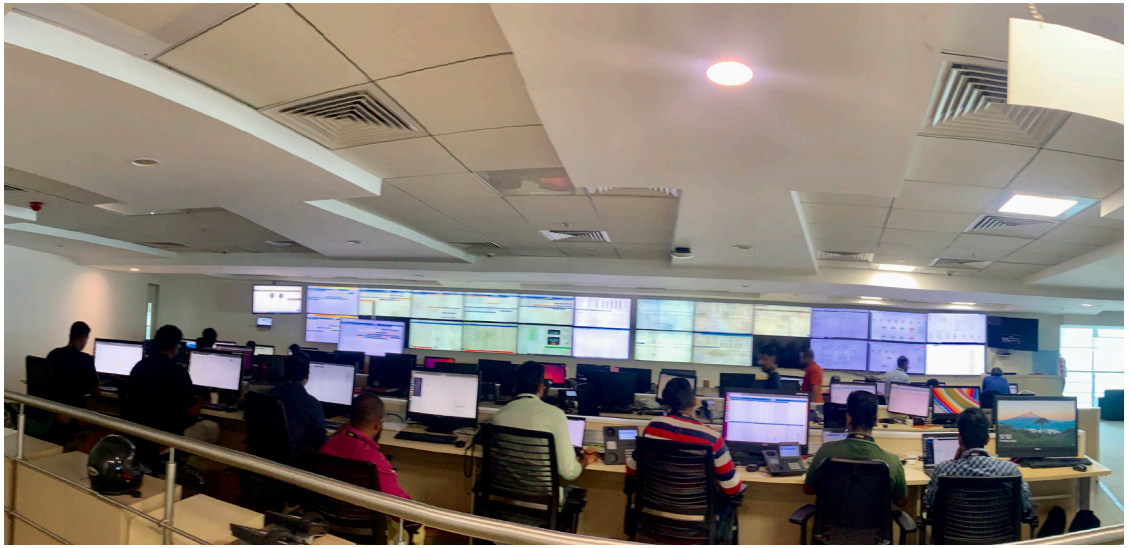
Chat:

Zoho Cliq es una aplicación de mensajería empresarial en tiempo real que ayuda a nuestros empleados a comunicarse efectivamente entre sí en cualquier momento, incluso durante un incidente.

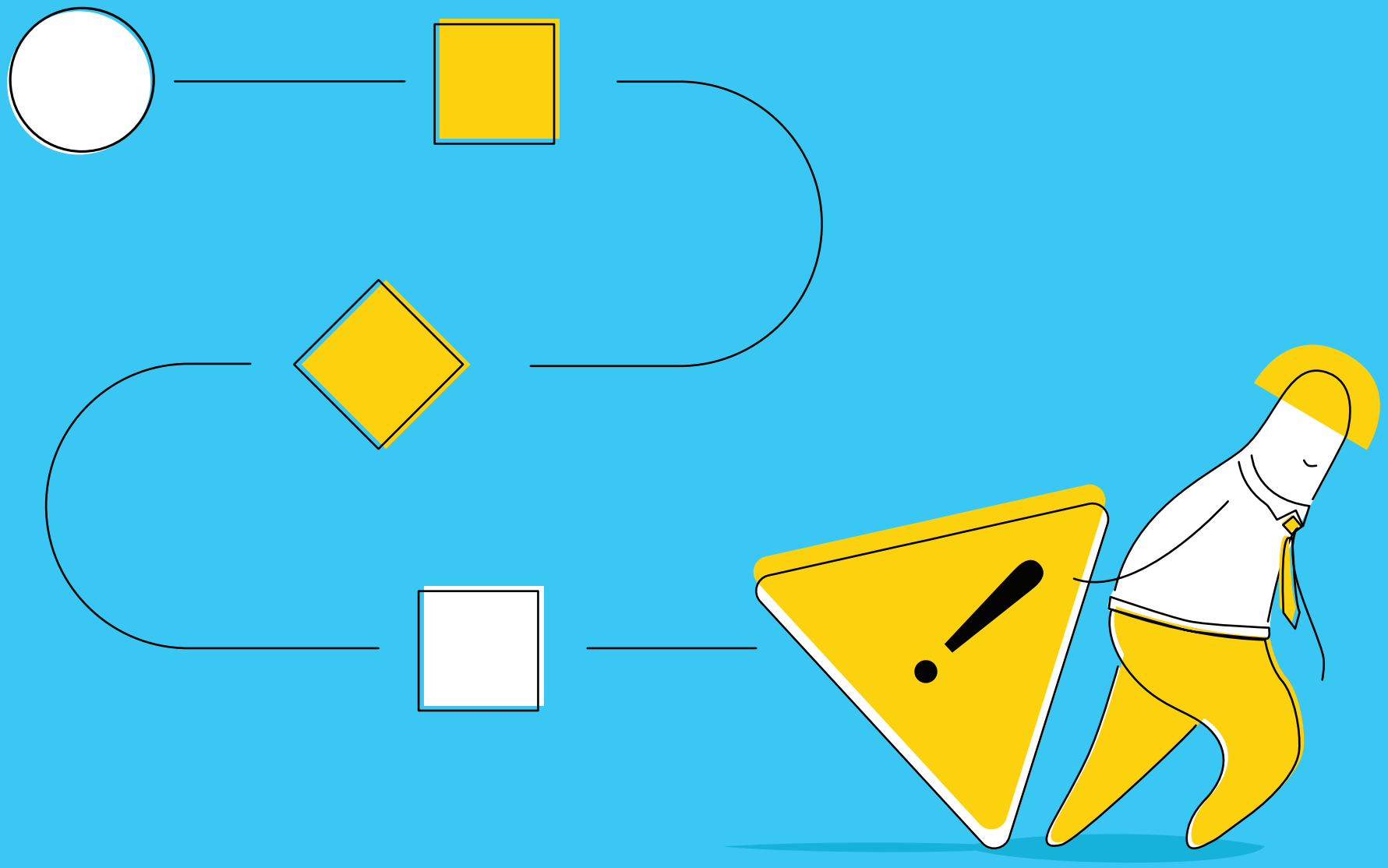
Colaboración:

Zoho Connect es un software de colaboración que garantiza que todos los equipos puedan estar en la misma página a la hora de resolver incidentes. Algunos lo llaman el Facebook de nuestro lugar de trabajo.

Nuestro centro de mando para la gestión de incidentes (IMCC)



Nuestro centro de mando para la gestión de incidentes (IMCC) es una gran sala segura con grandes pantallas, similares a las de la NASA, de dispositivos de monitoreo para proporcionar métricas detalladas y visibilidad, lo que permite a nuestros equipos de gestión de incidentes reaccionar con rapidez y solucionar los problemas efectivamente durante los incidentes. Esta sala alberga tres equipos principales: el equipo del centro de control de red (NOC), el equipo Zorro y el equipo de administración del sistema central. Disponemos de control de acceso dinámico en otros lugares de trabajo para realizar actividades de monitoreo.



PROCESOS DE GESTIÓN DE INCIDENTES

Iteración de desktop
(falla/corrección e incidentes menores)

Big bang
(incidentes de disponibilidad mayores)

CyberSec
(fallos críticos o incidentes críticos)

Iteración de desktop

(incidentes de desktop)

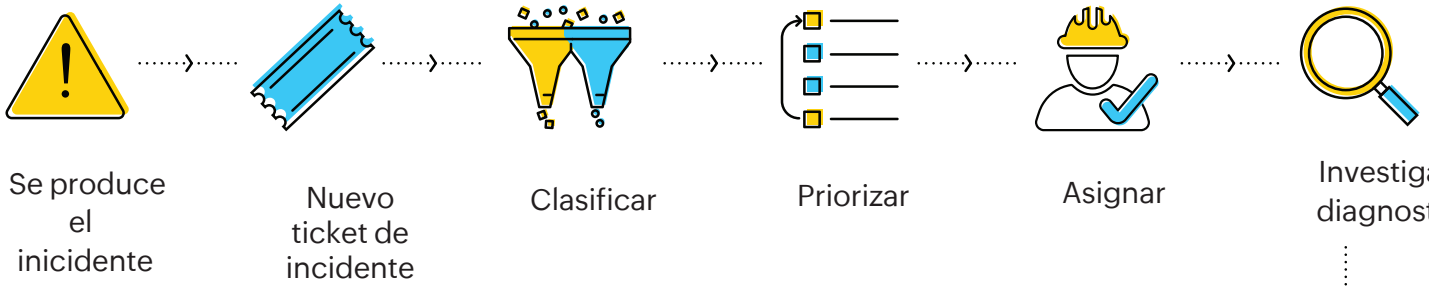
Equipos, roles y responsabilidades

Técnicos de PitStop:
Al igual que cualquier organización de TI, nuestro equipo de asistencia técnica de TI de primera línea gestiona los incidentes de desktop. Llamamos PitStop a nuestro centro de asistencia de TI.

Equipo central de administración de sistemas:

Tenemos un equipo central de administración de sistemas como parte de nuestro centro de mando de gestión de incidentes que supervisa todos los incidentes que llegan a nuestro edificio de 12 pisos. Colocamos un PitStop con un técnico en cada piso; en ausencia de un técnico PitStop en una piso, el equipo central de administración del sistema se encarga de los incidentes de desktop de ese día concreto.

En la mayoría de los casos, los incidentes son enviados a los técnicos por el coordinador de incidentes, que supervisa todos los incidentes de desktop entrantes mediante reglas de negocio en nuestra herramienta de gestión de servicios de TI (ITSM). Los técnicos de PitStop también pueden auto-asignarse tickets en caso de que el coordinador de incidentes esté ausente.

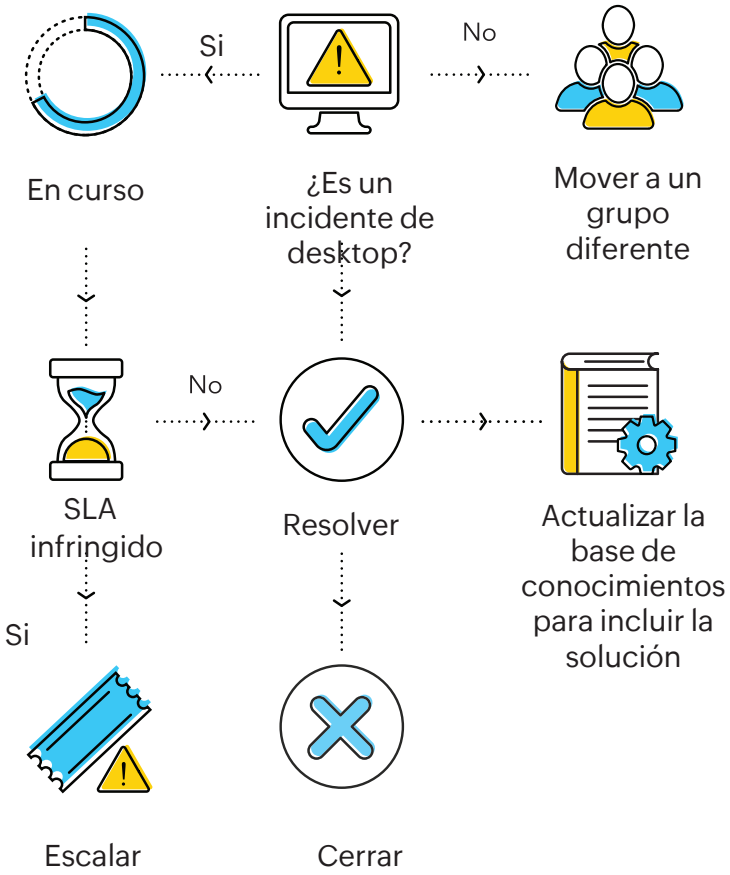


El proceso

En un día normal, nuestros técnicos de PitStop solucionan incidentes de impacto bajo a medio, como restablecimiento de contraseñas, problemas con impresoras y problemas de red, y realizan diversas tareas, entre ellas:

- Comunicar las interrupciones del servicio a todos los usuarios finales.
- Abrir la comunicación con los usuarios finales para investigar y recopilar toda la información posible sobre los incidentes para su rápida resolución.
- Crear solicitudes de cambios o registros de problemas.
- Respetar los acuerdos de nivel de servicio (SLA) de los incidentes y escalarlos según sea necesario.
- Resolver y cerrar incidentes.
- Proporcionar actualizaciones de estado a los usuarios finales durante todo el ciclo de vida del incidente.

Para gestionar los incidentes cotidianos, utilizamos un modelo de resolución de alta velocidad con el que probablemente usted esté familiarizado. Es un proceso sencillo y directo que resuelve los obstáculos y garantiza un flujo continuo.



Nuevo incidente

Un incidente suele comenzar cuando nuestros empleados comunican un problema a través de un correo electrónico, una llamada telefónica, un chat en tiempo real o el portal de autoservicio de nuestra herramienta ITSM. El incidente se registra como un ticket de incidente y llenamos los siguientes datos de manera predeterminada.

Título	Resumen del incidente
Descripción	Proporcione tantos detalles como sea posible para ayudar a los técnicos a diagnosticar el incidente y proporcionar una resolución más rápida.
Impacto	¿A quién afecta: a un solo usuario o a toda la empresa?
Urgencia	¿Con qué rapidez debe resolverse el incidente?
Prioridad	¿Cuál es la importancia del incidente en función del impacto y la urgencia?
Grupos	¿Qué grupo de resolución gestiona el incidente? Por ejemplo, creamos grupos para temas específicos como hardware, software, impresoras, etc.
Activos	¿Cuáles son los activos y servicios afectados por el incidente notificado? ¿Se trata de un único activo o de varios?

Tras el registro, el incidente pasa al estado abierto, que es el primer estado de nuestro flujo de trabajo de incidentes.

Categorización

Nuestro coordinador de incidentes empieza por asignar los incidentes a las categorías y subcategorías adecuadas para facilitar su clasificación. Sin categorización, el gestor de incidentes no sabrá cuántos problemas de sistemas operativos y aplicaciones hemos experimentado, ni qué medidas hay que tomar para reducir esos incidentes.
Clasificamos los incidentes por las siguientes razones.

- Para agrupar incidentes similares en un bucket común para acelerar el ciclo de vida del
- incidente. Para enrutar y asignar automáticamente los incidentes a los equipos adecuados para su rápida resolución.
- Por ejemplo, asignar automáticamente los problemas relacionados con Linux al equipo
- adecuado. Para el análisis de problemas.
- Para generar un informe bien estructurado.

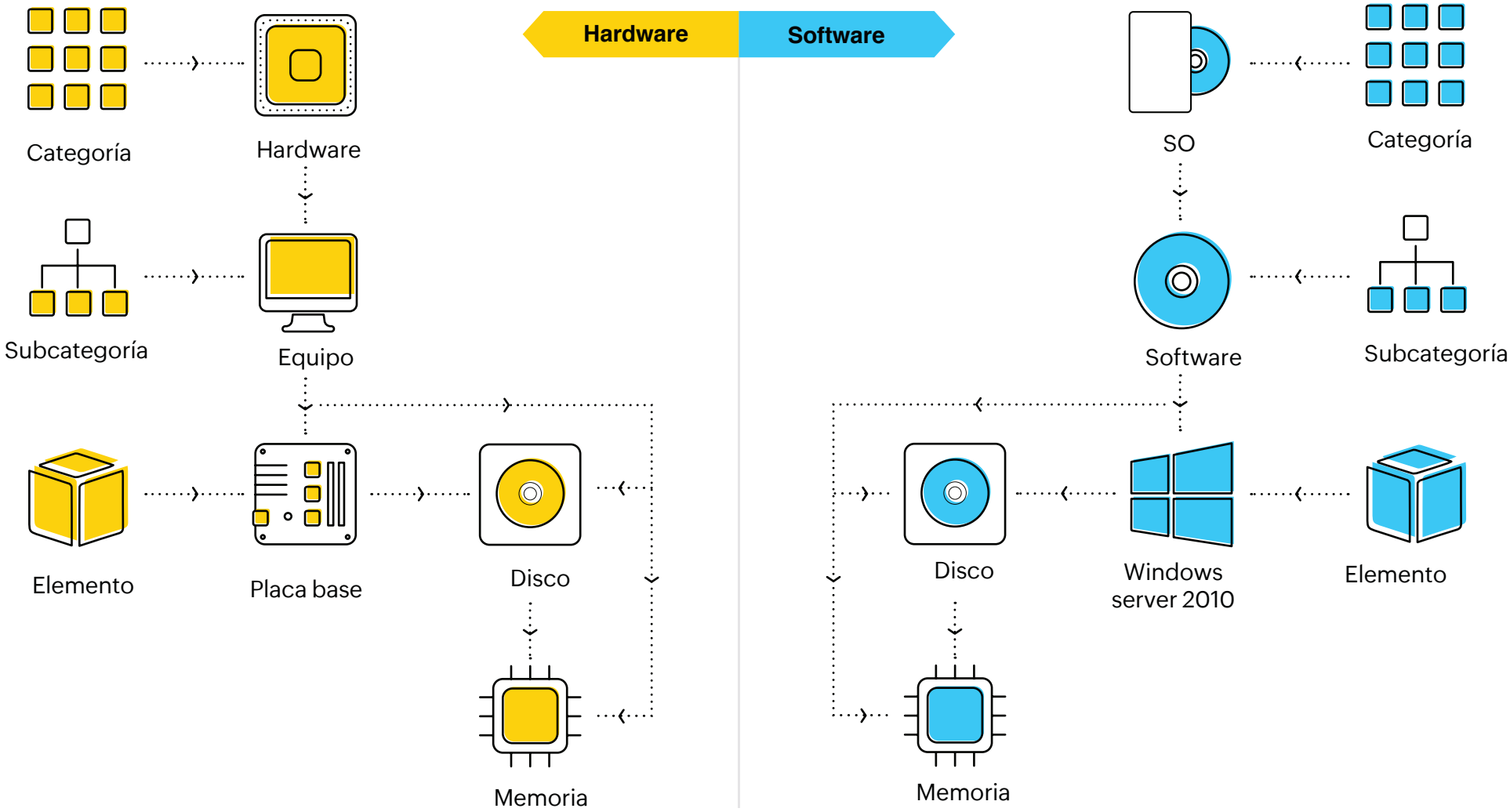
Como mejor práctica para una categorización efectiva, nos ceñimos a tres niveles de categorización. Demasiados niveles pueden complicar el proceso, y muy pocos podrían frustrar el propósito. La categorización suele comenzar con la categoría principal, luego una subcategoría y, por último, el elemento de configuración afectado.

Limitamos las categorías principales a unas 10-15 para que sean amplias pero gestionables. Cada tres o seis meses, nuestro coordinador de incidentes comprueba los registros históricos y clasifica los incidentes según las categorías principales para comprobar si los incidentes entran dentro de esas categorías. Se analiza el log de incidentes y se determina la categoría preguntando:

- ¿Cómo se distribuyen los incidentes en el árbol de categorías?
- ¿Están bien definidas las categorías y subcategorías principales?
- ¿Los niveles de categorización aceleran la resolución de incidentes?
- ¿Cuántos incidentes entran en la categoría "Otros"?
- ¿Se ven comprometidos los informes debido a una categorización ineficiente?

En función de las respuestas y de nuestras necesidades empresariales, el coordinador de incidentes afina la profundidad del árbol de categorías.

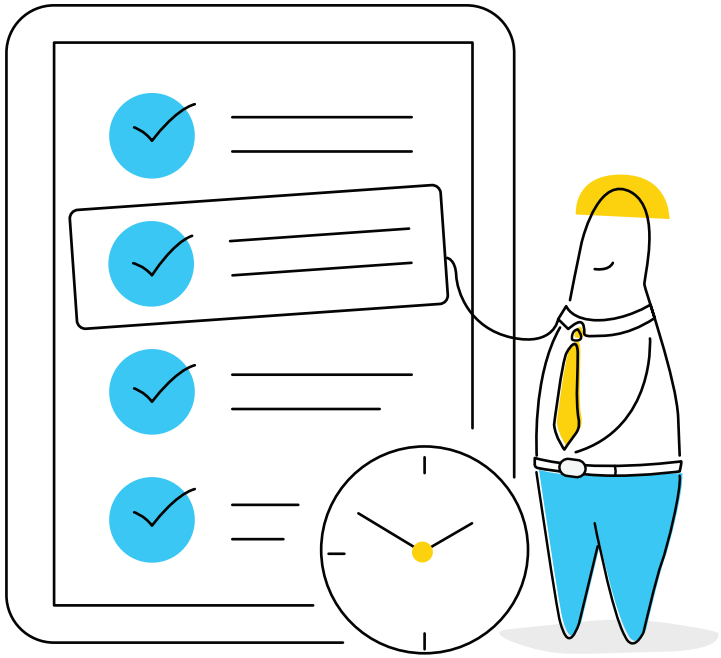
Aquí hay un ejemplo típico del árbol de categorías que utilizamos para gestionar problemas de hardware y software.



Priorización

Nuestro coordinador de incidentes empieza por asignar los incidentes a las categorías y subcategorías adecuadas para facilitar su clasificación. Sin categorización, el gestor de incidentes no sabrá cuántos problemas de sistemas operativos y aplicaciones hemos experimentado, ni qué medidas hay que tomar para reducir esos incidentes.

Aunque todos los incidentes deben resolverse, algunos tienen un mayor impacto en nuestro negocio y requieren un mayor sentido de la urgencia para resolverlos. Determinamos la prioridad de un incidente mediante una matriz de priorización de incidentes (impacto x urgencia) para garantizar la satisfacción del usuario final, el uso óptimo de los recursos y la mínima afectación de nuestras operaciones comerciales.



Para asignar nuestra matriz de prioridades, nos preguntamos:

- ¿Cómo se ve afectada la productividad?
- ¿Cuántos usuarios están afectados? ¿Se trata de un solo usuario o de un grupo? ¿Están afectados los usuarios VIP?
- ¿Cuántos sistemas o servicios están afectados?
- ¿Hasta qué punto son críticos estos sistemas/servicios para la organización?
- ¿Se ven afectados los clientes? ¿Hay un impacto significativo en los ingresos?
- ¿Tiene un impacto importante en los ingresos/la reputación de la empresa?

La matriz de prioridades define automáticamente la prioridad de un incidente específico en función de las entradas proporcionadas (impacto y urgencia) por los usuarios finales al registrar un ticket en nuestra herramienta ITSM. En nuestra matriz de prioridades, el impacto aparece en el eje "y" y la urgencia en el eje "x". Agrupamos los impactos por: usuario, grupo, departamento y negocio. En cuanto a la urgencia, los cuatro niveles son bajo, medio, alto y crítico.

La matriz de prioridades ofrece un resumen general de cada incidente y garantiza que los incidentes mayores se prioricen y aborden con rapidez; también garantiza que los incidentes de baja prioridad, como los de desktop, se gestionen en un plazo aceptable.

Aquí hay algunos casos de uso que muestran cómo utilizamos nuestra matriz de prioridades:

Urgencia	Impacto	Escenarios
Falla/corrección (afecta a individuos y pequeños grupos)	• Afecta a un solo usuario • No hay servicios críticos afectados	• Restablecimiento de contraseñas • La conexión a Internet funciona con lentitud
Menor impacto (afecta a incidentes de grupo/impacto medio)	• Afecta a un solo usuario VIP • Afecta a un pequeño grupo de usuarios finales • No hay riesgo de pérdidas económicas ni de pérdida de reputación	• El laptop del CEO no funciona y no puede enviar ni recibir comunicaciones • Una impresora no funciona en un piso determinado
Big bang (afecta al servicio)	• Un determinado servicio, aplicación o componente de infraestructura crítico para el negocio no está disponible y el tiempo estimado para su recuperación es desconocido o excesivamente largo • El servicio no está disponible. Se espera el restablecimiento inmediato del servicio	• Nuestra conexión de red de alta velocidad falla, y la comunicación hacia y desde fuera de nuestra organización se interrumpe • Una de nuestras principales aplicaciones no funciona, lo que afecta a varios clientes • Ataque DDoS
Situaciones críticas, de emergencia o de alerta roja (afecta a los negocios)	• Afecta a los resultados de nuestra empresa • Impacto mayor en los ingresos, la reputación y los asuntos jurídicos	• Errores y vulnerabilidades del software • Malware • APT • Ransomware • Phishing e ingeniería social • Amenazas internas •

Asignación y enrutamiento

El incidente se asigna ahora a un técnico de PitStop para su investigación y diagnóstico. Para ello, utilizamos reglas de incidentes proporcionadas por nuestra aplicación ITSM que definen el orden de enrutamiento y asignan los incidentes a los grupos seleccionados. Supongamos que una impresora del tercer piso no funciona y se registra un incidente. Nuestra herramienta ITSM registra la ubicación del usuario en el formulario de incidentes y, debido a dónde se originó el mismo, se enruta automáticamente al técnico de PitStop del tercer piso. También se envía una notificación al técnico de PitStop poco después de que se enrute el incidente, para que el técnico sepa que debe empezar a trabajar en el problema.

Comunicaciones abiertas

Una vez asignado un incidente, un técnico de PitStop abre la comunicación con el usuario final afectado. Los técnicos formulan y responden preguntas, y proporcionan a los usuarios finales actualizaciones periódicas antes, durante y después del incidente. Es importante que los técnicos de PitStop se comuniquen bien con los usuarios finales en cada paso.
Utilizamos principalmente tres métodos de comunicación:

- Un hilo de correo electrónico se inicia poco después de que el técnico inicie una conversación con el usuario final dentro de la herramienta ITSM, lo que garantiza que todas las comunicaciones estén en un mismo lugar. Se envían notificaciones y actualizaciones periódicas a los usuarios finales afectados hasta que se resuelva y cierre el incidente
- Utilizamos anuncios en nuestra herramienta ITSM para publicar información relacionada con la mesa de ayuda en toda la organización, o para determinados grupos de usuarios finales en relación con problemas del servidor, actualizaciones del servicio, renovación de licencias, etc. Es importante que los técnicos de PitStop y los usuarios finales de nuestra empresa estén al tanto de los detalles de los incidentes.
- Para una resolución más rápida y más detalles sobre el incidente, el técnico de PitStop llama a los usuarios finales a sus teléfonos en su desktop o sus móviles.

Escalamiento

El incidente pasa ahora al estado en curso y muestra la fase del ciclo de vida del ticket. El técnico de PitStop actualiza el estado para mantener informado al usuario final y atenerse a los SLA aplicables. Si el técnico de PitStop no es capaz de resolver el ticket, este se remite al coordinador de incidentes, que lo reasigna a un técnico con conocimientos más avanzados.

Para los incidentes de desktop con prioridad baja, el SLA suele fijarse en tres o cinco días y los usuarios finales deben recibir una respuesta en cuatro horas, y para un incidente de prioridad media, se fija en un día y los usuarios finales deben recibir una respuesta en dos horas.

Cierre

Cuando no es necesario escalar, el técnico de PitStop puede cerrar el ticket; este es el último paso en el ciclo de vida del incidente. Esto implica registrar la resolución en la herramienta ITSM para futuras referencias antes de cerrarlo. Una vez cerrados, los incidentes siguen siendo accesibles para los técnicos de PitStop y para el coordinador de incidentes, de modo que si el usuario final vuelve a llamar, el técnico puede consultar el historial y reabrir el incidente si es necesario.

Las mejores prácticas en caso de incidentes de desktop

- HDisponga de varios canales de creación de tickets para que los usuarios finales puedan generar tickets fácilmente por correo electrónico, chat, portal y llamada
- telefónica.
  Anime a los usuarios finales a encontrar respuestas incluso antes de dirigirse a un
- técnico en busca de ayuda con el autoservicio.
  Haga que los técnicos utilicen aplicaciones móviles para gestionar su mesa de
- ayuda y responder a las solicitudes de los empleados, incluso cuando no estén en su puesto de trabajo. Automatice la gestión de usuarios mediante la integración
- con Active Directory de la empresa.
  Clasifique a sus usuarios finales en grupos basados en su departamento y
- gestionados por la mesa de servicio.
  Gestione de forma proactiva los incidentes que se repiten con frecuencia, como el restablecimiento de contraseñas, utilizando herramientas de restablecimiento automático de contraseñas que permitan a los administradores de sistemas proporcionar a los empleados acceso a un portal de autoservicio basado en web
- para que puedan restablecer sus contraseñas de forma segura.
  Automatice las actividades que mejoran la eficiencia y la productividad del
- equipo, incluidos los incidentes rutinarios del desktop, como la categorización, la priorización y la asignación. Disponga de una base de conocimientos que permita
- a los técnicos buscar las soluciones existentes para resolver los problemas
- eficientemente.
- No haga esperar interminablemente a sus usuarios finales. Cumpla sus SLA.
  Mantenga informados a los usuarios finales en cada fase del ciclo de vida del incidente. Automatice las actividades de notificación para ahorrar tiempo.

Big bang

(incidentes de disponibilidad mayores)

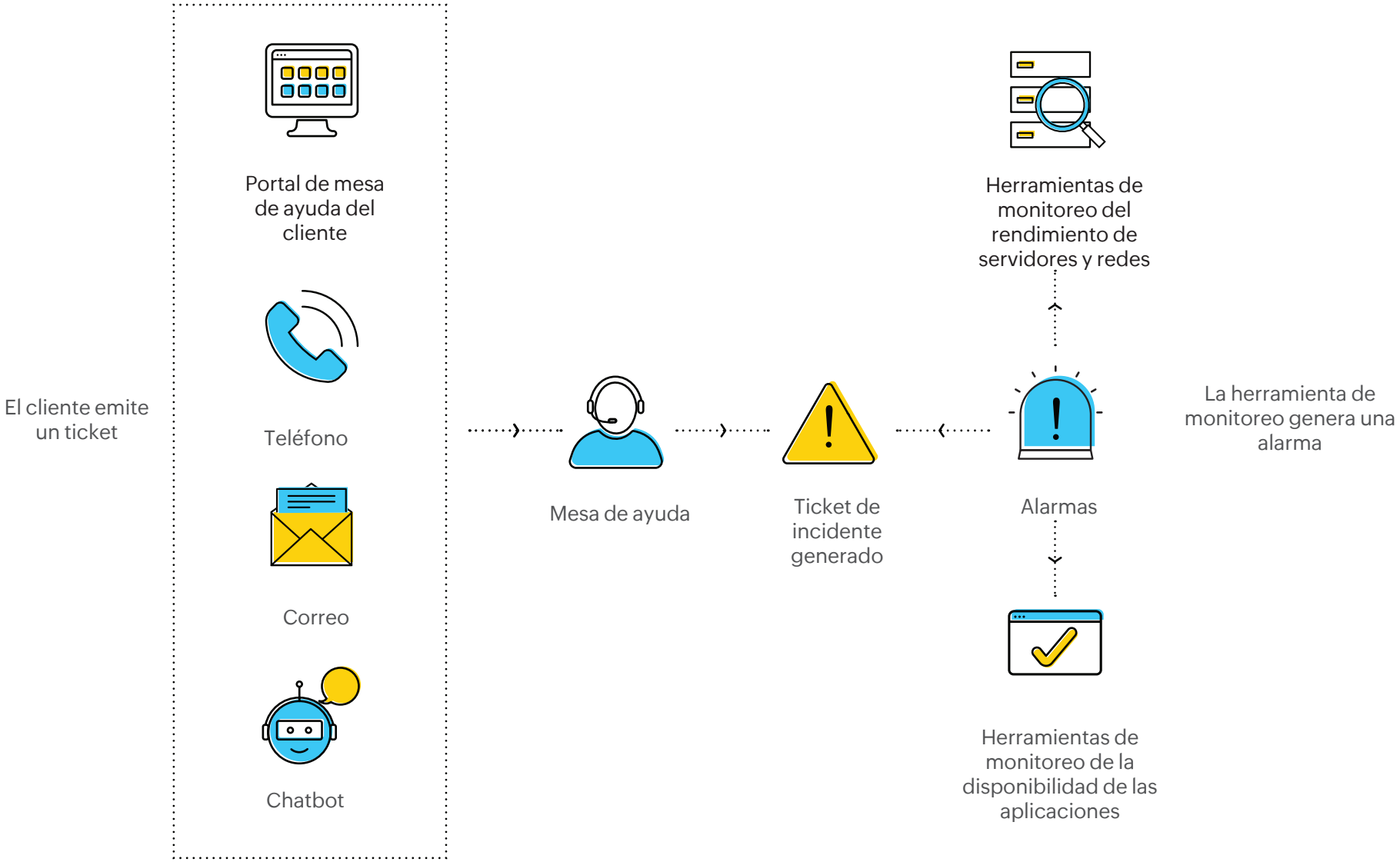
Cualquier incidente que afecte a muchos usuarios, prive a la empresa de uno o varios servicios cruciales y exija una respuesta rápida y eficiente se considera un incidente mayor. En el mundo de la tecnología en la nube, alcanzar una disponibilidad del 99,99 por ciento se ha convertido en la norma. En Zoho, nuestro compromiso con nuestros clientes es garantizar una disponibilidad del 99,99 por ciento.

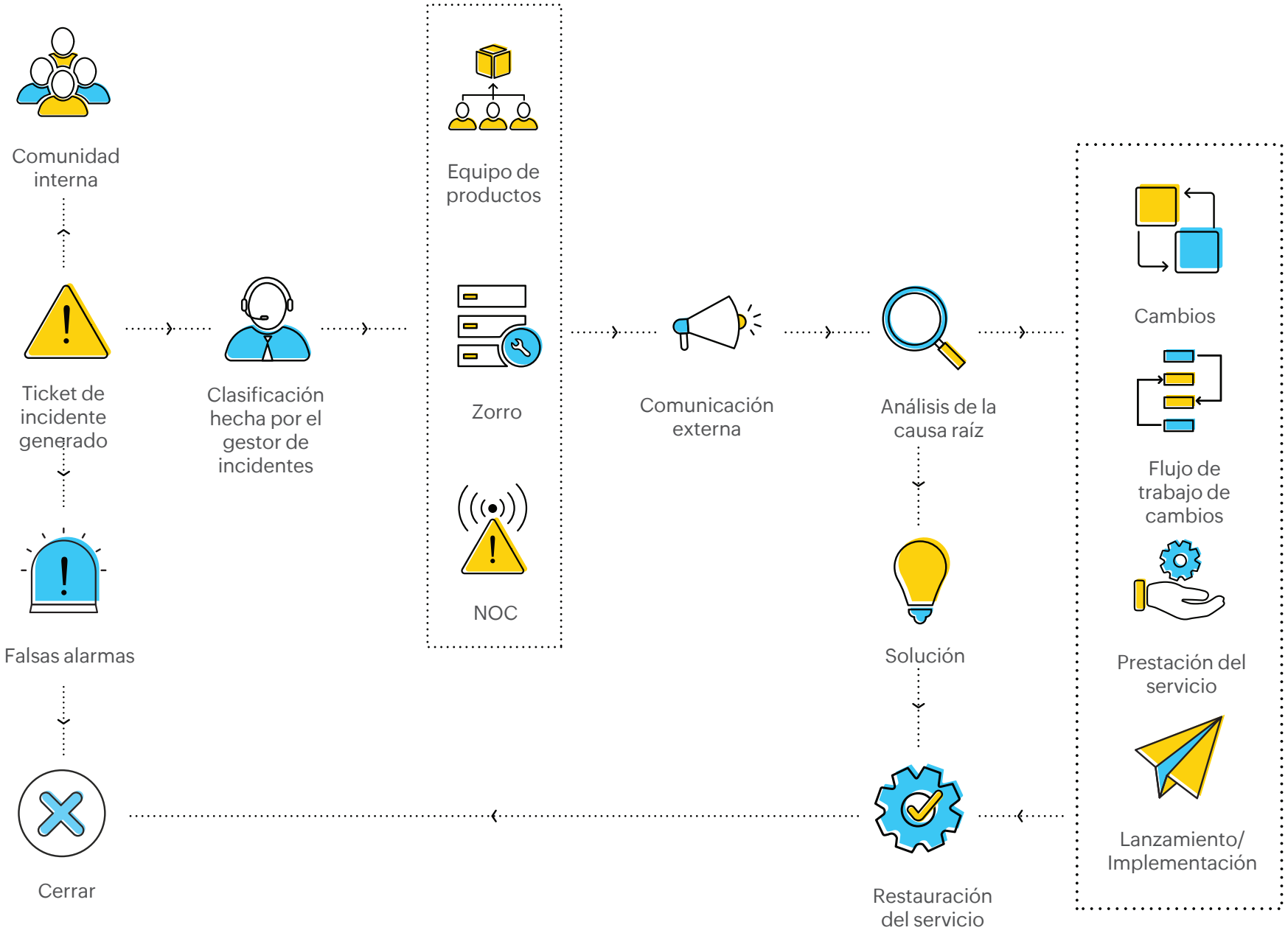
Los clientes pueden comprobar la disponibilidad de nuestros servicios en nuestra Página de Estado de Zoho. Cuando se produce un incidente de disponibilidad mayor, seguimos el proceso de IM llamado big bang, que incluye facilitar la colaboración, alinear a las partes interesadas, informar a los clientes y, en última instancia, trabajar en el incidente de forma continua hasta su resolución.

En esta sección se abordan tres problemas de disponibilidad diferentes:

- Problemas con la red
- Problemas con el servidor
- físico Problemas con la aplicación

La siguiente figura muestra el proceso que seguimos durante un incidente de disponibilidad.



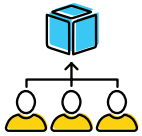

Comunidad interna
Ticket de incidente generado
Falsas alarmas
Cerrar
Clasificación hecha por el gestor de incidentes
Equipo de productos
Zorro
NOC
Comunicación externa
Análisis de la causa raíz
Solución
Restauración del servicio
Cambios
Flujo de trabajo de cambios
Prestación del servicio
Lanzamiento/ Implementación

Equipos, roles y responsabilidades

Equipo de respuesta a incidentes (IRT)

Gestor de incidentes:

Como capitán del barco que supervisa el incidente, el gestor de incidentes trabaja con el NOC, Zorro y los equipos de producto, así como con sus respectivos coordinadores de incidentes, para resolver los problemas y mantener los SLA.



Ingeniería y desarrollo (equipos de producto):

Para un incidente relacionado con una aplicación, el equipo de producto individual es el principal punto de contacto para el gestor de incidentes. Los ingenieros del equipo de producto suelen ser el grupo que resuelve los problemas durante los incidentes de disponibilidad.

Equipo de software como servicio (SAS):

Gestiona el inventario de los activos del centro de datos.

Centro de control de red (NOC):

Gestiona los incidentes de disponibilidad de la red.

Coordinador de incidentes:

A cada equipo de producto se le asigna un coordinador de incidentes que es responsable de evaluar y coordinar un incidente de disponibilidad.

Servidores y mantenimiento (Zorro):

Cuando se identifica un incidente relacionado con el servidor, el equipo Zorro presta asistencia. El equipo Zorro se encarga del aprovisionamiento y mantenimiento de los servidores en los centros de datos.

Equipo de prestación de servicios (SD):

Gestiona el envío de actualizaciones a todas las aplicaciones Zoho.

Gestor de las comunicaciones externas:

El gestor de incidentes actúa como nuestro gestor de las comunicaciones externas, proporcionando a los clientes actualizaciones frecuentes sobre las interrupciones.

Detectar

Site24x7 es una herramienta de monitoreo de disponibilidad que utilizamos para monitorear la disponibilidad de nuestras aplicaciones en varias ubicaciones. Esta aplicación se integra de manera eficiente con nuestra herramienta ITSM, reconoce la indisponibilidad de las aplicaciones y envía alertas proactivas para crear incidentes en nuestra herramienta ITSM. En caso de falsa alarma, se cierra el incidente.

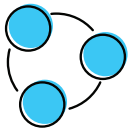
Nuevo incidente

Hemos configurado nuestro principal proceso de IM en nuestra herramienta de mesa de ayuda utilizando un ciclo de vida de la solicitud (RLC). Cada vez que se crea un incidente, se envían notificaciones al gestor de incidentes y a los coordinadores de incidentes de los equipos Zorro, NOC y de los productos afectados. Estas notificaciones incluyen el número de incidente, la descripción y la prioridad del incidente. Una vez que el incidente se registra como un ticket en nuestra herramienta ITSM, se encuentra en estado abierto, el estado inicial en nuestro RLC.

Comunicarse con las partes interesadas

El gestor del incidente, tras recabar la información necesaria de la alerta y del coordinador del incidente, abre la comunicación con las partes interesadas internas.

Herramienta ITSM:
Desde el ticket de incidente, se envía un correo electrónico a los equipos de gestión de incidentes, NOC, Zorro y producto para comenzar la investigación inicial.



Zoho Connect:
Connect es un software de colaboración en equipo, como una aplicación interna similar a Facebook, que conecta a todas las partes interesadas y permite mantener conversaciones abiertas durante un incidente. Contamos con un grupo llamado Incidentes que incluye a más de 1.200 miembros, entre ellos personal para brindar respuestas, principales interesados y responsables de la toma de decisiones, para garantizar una mayor transparencia y coordinación.

Zoho Cliq:
Un software de chat de colaboración empresarial que permite al gestor de incidentes, a los coordinadores de incidentes, a los equipos de producto y a otras partes interesadas ofrecer actualizaciones rápidas, compartir archivos y buscar un contacto o una conversación del pasado. El chat en grupo nos permite ponernos en contacto y añadir más personal para brindar respuestas y de resolución según sea necesario para trabajar más rápidamente en los incidentes

Documentar la interrupción:
Una teleconferencia o un hilo de debate no bastan para que todos sepan lo que está pasando y lo que les espera. Las partes interesadas y los clientes necesitan informes de progreso significativos, garantías de que el incidente puede solucionarse y que no haya ninguna sorpresa. El gestor de incidentes mantiene un documento de estado del incidente en Zoho Writer para proporcionar un lugar claro para ver cómo, por qué y cuándo se produjo el incidente, las medidas adoptadas o en curso, los datos compartidos, y una comprensión del camino claro hacia la resolución.

Este documento puede editarse, comentarse y compartirse en toda la organización. El gestor de incidentes comparte este documento en el hilo Connect correspondiente al incidente, y también lo utiliza para el análisis de la causa raíz (RCA). También es una buena forma de que el gestor de incidentes registre las observaciones y decisiones clave que se producen en conversaciones no grabadas en otros medios, como el chat y los hilos de discusión.

Evaluar

Nos ocupamos de muchos tipos de incidentes de disponibilidad importantes y contamos con varios equipos para corregirlos. La respuesta dada a estos incidentes depende de muchos factores, como la coordinación, la comunicación y la gestión. Para que la respuesta a un incidente tenga éxito, todos estos factores deben funcionar conjuntamente. Para optimizar la respuesta, necesitamos un lenguaje común para comunicarnos, y hay que definir bien el orden en que deben intervenir los equipos y ejecutarse las tareas.

Una vez que un incidente de disponibilidad proviene de Site24x7, comienza la clasificación entre equipos. Nuestro gestor de incidentes actúa como responsable de la clasificación, reuniendo a los equipos NOC, Zorro y de producto. Se crea en Cliq un canal que incluye NOC, Zorro y el equipo de producto para identificar si el problema está relacionado con la red (NOC), el servidor (Zorro) o un producto, de modo que el ticket pueda delegarse a los equipos adecuados y resolverse.

El gestor de incidentes empieza por evaluar el incidente formulando algunas preguntas para comunicar la información correcta a las partes interesadas y a los clientes.

- ¿Cuándo se produjo la interrupción?
- ¿La interrupción es visible para los clientes?
- ¿A cuántos clientes afecta?
- ¿Cuántos tickets de asistencia hay?
- ¿Qué equipo (NOC, Zorro o producto) se encarga de la corrección?
- ¿Dispone el equipo de los recursos adecuados ese día en particular?
- ¿Acuerda el equipo de resolución sus horarios y protocolos de
- comunicación antes de ponerse a trabajar?

Una vez que se ha identificado la titularidad del incidente, y recibe una prioridad que se ha considerado un incidente mayor, lo que significa que el incidente es urgente y tiene un impacto en la organización, el gestor de incidentes envía la comunicación externa inicial.

Comunicación externa

El gestor de incidentes tiene ahora razonablemente claro el incidente y la implicación del equipo, y tiene que comunicarlo a los clientes lo antes posible. El gestor del incidente recibe ayuda del equipo de comunicación para actualizar el blog sobre la indisponibilidad

Durante una interrupción, hacemos un anuncio en el blog que incluye detalles como la fecha y hora de ocurrencia, la naturaleza del incidente y las medidas correctivas con actualizaciones frecuentes. Cada vez que los clientes intentan acceder al servicio durante una interrupción, se les redirige al anuncio del blog para que puedan mantenerse al día de lo sucedido.

Además del blog, durante una interrupción también se publica un anuncio en la comunidad en el que ofrecemos actualizaciones frecuentes y respondemos a las preguntas de los clientes. Los clientes también pueden comprobar la disponibilidad del servicio en nuestra página de estado.

Delegar

El gestor de incidentes trabaja con el coordinador de incidentes en el NOC, Zorro y los equipos de productos para gestionar todas las operaciones de incidentes, la aplicación de recursos y las responsabilidades de todos los implicados. Una vez que el NOC, Zorro y los respectivos equipos de producto reciben la respuesta a través del canal Cliq y se ha identificado el equipo propietario, se activa automáticamente un conjunto de tareas a través del ciclo de vida de la solicitud para el equipo propietario del incidente, como se muestra a continuación.

Enviar seguimiento

El gestor de incidentes envía regularmente pings al equipo de resolución para recibir actualizaciones rápidas sobre el progreso del incidente, que transmitirá al cliente. En el foro y el blog se actualizan con frecuencia datos breves y concisos, como el inicio del periodo de inactividad, una breve descripción de la causa conocida del periodo de inactividad, el tiempo estimado de restablecimiento y la hora prevista para la próxima actualización del estado, para mantener informados a los clientes..

Resolver y cerrar

Cuando el incidente deja de afectar a los clientes, se considera resuelto y, o bien un técnico cierra manualmente el ticket, o bien, transcurrido el tiempo suficiente, el estado del ticket cambia automáticamente a cerrado. El gestor del incidente envía las últimas comunicaciones internas y externas, e inicia el RCA utilizando como base el documento de estado del incidente.

Esta es nuestra lista de control para resolver (y cerrar) los tickets:

- ✓ ¿Se ha resuelto el incidente a satisfacción de los propietarios de los tickets?
- ✓ ¿Se encarga el personal de resolución de las tareas de limpieza?
- ✓ ¿Se han cerrado todas las tareas relacionadas y se ha notificado a los usuarios pertinentes?
- ✓ ¿Ha notificado el gestor del incidente a todas las partes?
- ✓ Y lo que es más importante, ¿se ha notificado la resolución a los clientes?
- ✓ ¿Han aceptado todas las partes interesadas el cierre del incidente mayor?
- ✓ ¿Se ha registrado e iniciado el RCA?
- ✓ ¿Se ha enviado el orden del día de la reunión de RCA a los grupos de resolución? ¿Se ha notificado el cierre a la mesa de servicio?

Las marcamos para completar el proceso de incidentes mayores de la forma más clara posible y asegurarnos de que no se nos ha pasado nada por alto.

Las mejores prácticas en caso de incidentes mayores

Defina claramente un incidente mayor:

Lo llamamos incidente mayor cuando afecta a muchos usuarios, priva a la empresa de uno o más servicios cruciales y exige una respuesta que va más allá del proceso rutinario de gestión de incidentes. A veces, un incidente de desktop de alta prioridad puede percibirse como un incidente mayor. La falla del laptop de un VIP durante una conferencia de usuarios es un incidente de alta prioridad, pero desde luego no es un incidente mayor. Para evitar cualquier confusión, usted debe definir claramente un incidente mayor basándose en factores como la urgencia, el impacto y la gravedad.

Disponga de un plan de comunicación:

El plan de comunicación debe incluir los detalles del evento (cómo, cuándo, plan de acción, hora estimada de corrección y tiempo de intervalo de actualización), las partes implicadas y la frecuencia de la comunicación.

Establezca SLA:

Establezca SLA de respuesta y resolución independientes con vías de escalamiento claras. Si el equipo tiene poco personal ese día, no dude en recurrir a los recursos necesarios de otros equipos para trabajar en la resolución y garantizar que el SLA no se vea afectado.

Tenga un proceso de IM exclusivo:

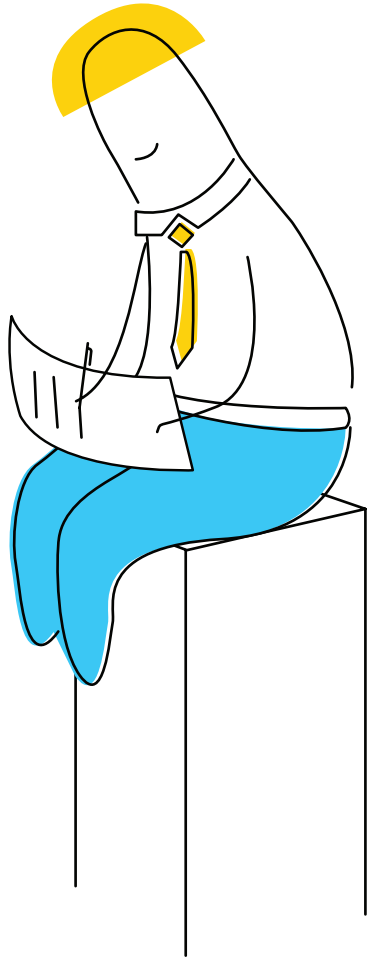
Los flujos de trabajo o procesos independientes para la gestión de incidentes mayores le ayudarán a tratar eficientemente los distintos tipos de incidentes, como la indisponibilidad del servicio o los problemas de rendimiento y fallos de hardware o software, para que pueda garantizar una resolución sin inconvenientes.

Incorpore los recursos y equipos adecuados:

Asegúrese de que el equipo y los recursos adecuados trabajen en los incidentes con roles y responsabilidades claramente definidas.

Documente el proceso de mejora continua del servicio:

Como práctica recomendada, nuestro gestor de incidentes recopila detalles como el número de personas implicadas en el proceso, sus roles y responsabilidades, los canales de comunicación, las herramientas utilizadas para la corrección, los flujos de trabajo de aprobación y escalamiento, y el plan de acción general utilizado para la respuesta y la resolución en el documento de estado del incidente. Las partes interesadas, incluida la alta dirección, evalúan este documento para garantizar la mejora continua del servicio.



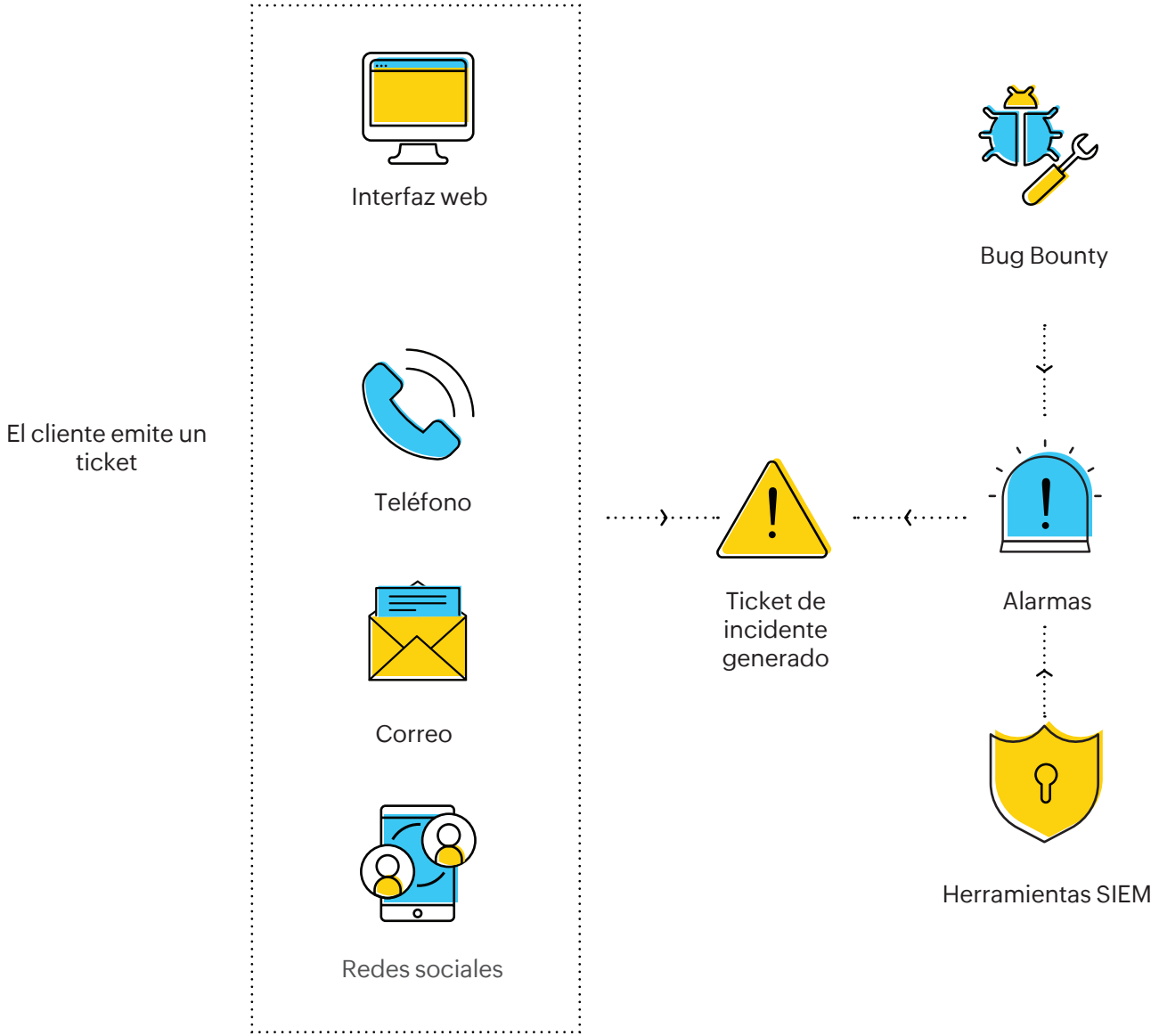
CyberSec

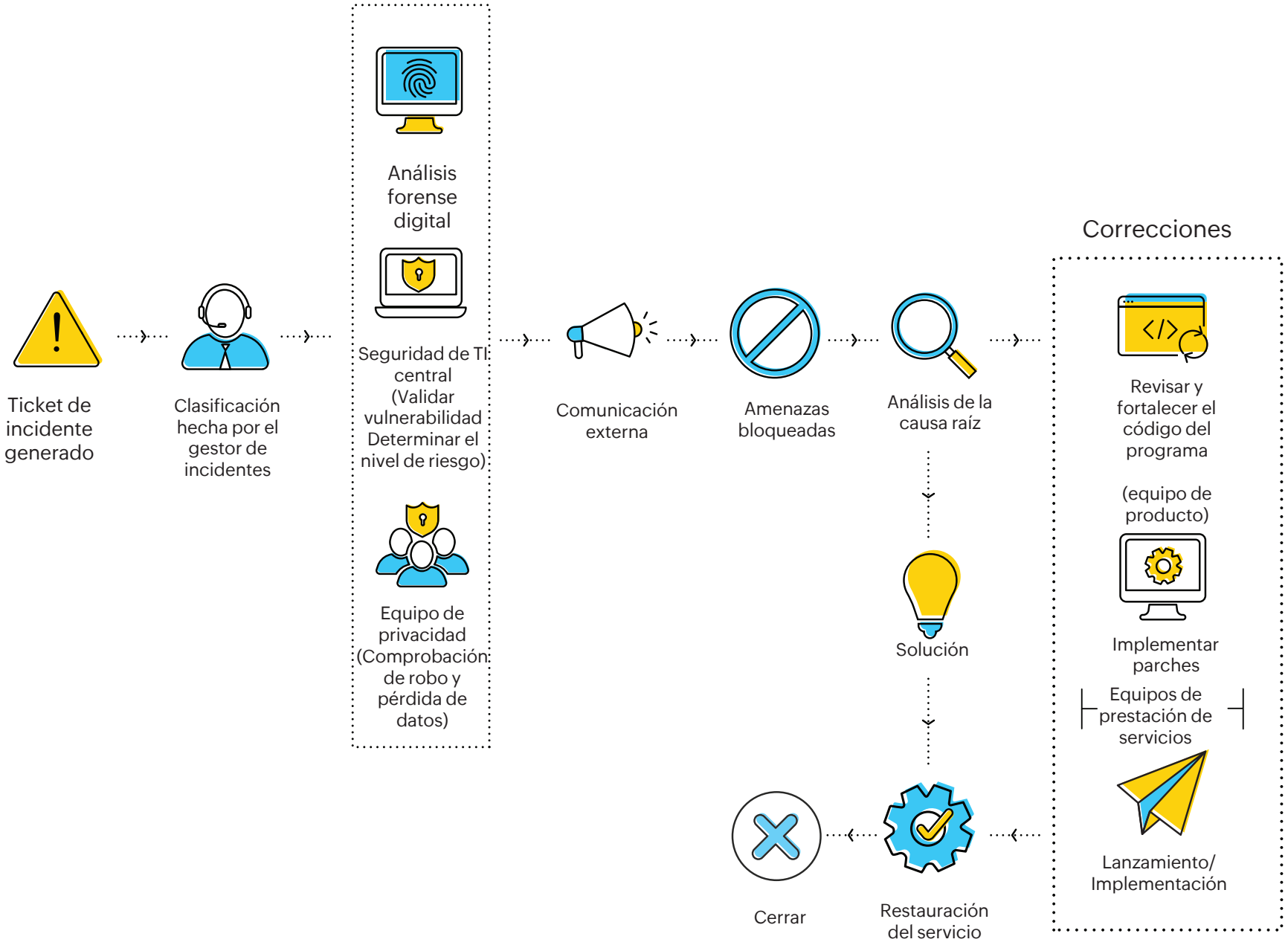
(Fallos críticos/Incidentes de seguridad)

La seguridad es la base de nuestra organización. Nuestro equipo de seguridad de TI protege la confidencialidad, integridad y disponibilidad de nuestros sistemas y datos, protegiendo nuestra organización contra malware, APT, ransomware, phishing, ingeniería social, ataques internos y otras amenazas a la seguridad. Tenemos un grupo de hackers de sombrero blanco llamado equipo rojo que intenta continuamente burlar nuestros controles de seguridad. Los coordinadores de seguridad participan en el ciclo de vida del desarrollo del producto, garantizando que la seguridad se incorpore a cada producto que desarrollamos.

En previsión de que algún día podamos ser objeto de un ataque cibernético, queremos estar preparados. El proceso CyberSec es un proceso maduro de detección, contención, coordinación y recuperación de vulnerabilidades que hace a nuestra empresa resistente frente a las amenazas informáticas. Puede ayudarnos a recuperarnos de las brechas de seguridad minimizando el tiempo de exposición y el impacto de las amenazas en los datos, las aplicaciones y nuestra infraestructura de TI.

La siguiente figura muestra nuestro flujo de procesos de CyberSec.




Ticket de incidente generado
Clasificación hecha por el gestor de incidentes
Análisis forense digital
Seguridad de TI central (Validar vulnerabilidad Determinar el nivel de riesgo)
Equipo de privacidad (Comprobación de robo y pérdida de datos)
Comunicación externa
Amenazas bloqueadas
Análisis de la causa raíz
Solución
Restauración del servicio
Cerrar
Correcciones
Revisar y fortalecer el código del programa
(equipo de producto)
Implementar parches
Equipos de prestación de servicios
Lanzamiento/ Implementación

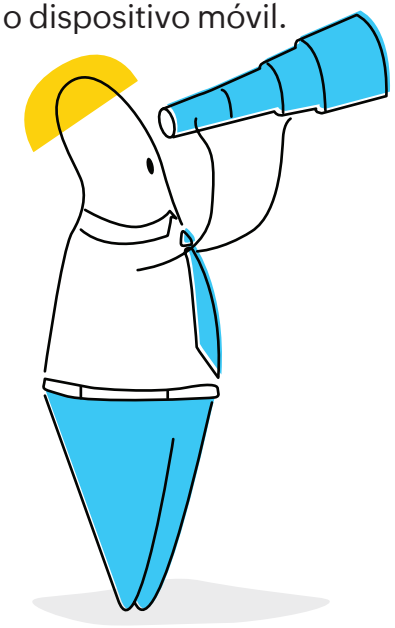
Equipos, roles y responsabilidades

Equipo	Roles	Responsabilidades
Gestión de incidentes	Respuesta a incidentes y coordinadores de incidentes	Gestiona el incidente de ciberseguridad desde su detección hasta su resolución
Equipo central de seguridad de TI	Seguridad de TI	Monitorea y analiza continuamente los procedimientos de seguridad de nuestros productos
Equipo de respuesta a incidentes de seguridad (SIRT)	El SIRT incluye al equipo de gestión de incidentes (gestor de incidentes, coordinadores de incidentes) y al equipo central de TI	El SIRT evalúa el impacto, garantiza el SLA, se coordina con los equipos de privacidad, legal y de producto y con la alta dirección durante las situaciones de crisis
Alta dirección	Responsables de la toma de decisiones	Recibe información del gestor de incidentes, evalúa el impacto en la empresa y toma decisiones empresariales clave; por ejemplo, decidir si debe desconectar la conexión a Internet de un sistema comprometido. En caso afirmativo, ¿cuándo es el momento adecuado? También decide cuándo ponerse en contacto con las autoridades
Equipo jurídico	Departamento jurídico/ asesores jurídicos	Evalúa el impacto contractual y judicial de un incidente. Garantiza que las actividades de respuesta a incidentes cumplan las normas legales y reglamentarias junto con los límites de la política de la organización. Orienta a la empresa sobre los pasos para presentar una denuncia
Equipo de privacidad	Consultores y asesores	Analiza el impacto de los incidentes de seguridad en la privacidad de las personas afectadas comparando el incidente con los requisitos de la legislación aplicable en materia de privacidad de datos; proporciona orientación sobre cómo gestionar la notificación de incidentes y el CAPA
Equipo de productos (cada equipo de producto tiene un coordinador de seguridad)	Ingenieros de producto	Corrigen vulnerabilidades y publican actualizaciones de productos
Equipo rojo	Hackers de sombrero blanco	Intentan penetrar en nuestras aplicaciones, eludir los protocolos de seguridad y exponer posibles vulnerabilidades de ciberseguridad para garantizar la seguridad de nuestros productos

El proceso

Detectar

Nuestros empleados tienen el mayor potencial para ayudar a la organización a detectar e identificar incidentes de ciberseguridad. Desempeñan un rol importante en la detección de amenazas para la seguridad. Todos los miembros de nuestra organización conocen las formas de alertar a nuestro equipo de seguridad cuando detectan algo anormal en su equipo o dispositivo móvil.



También tenemos un programa Bug Bounty para animar y recompensar a los empleados que detecten e informen de una vulnerabilidad de seguridad a Zoho. Nuestros empleados pueden notificar un incidente de seguridad a través de:

El portal de autoservicio

Un número de teléfono gratuito

La aplicación Bug Bounty

Redes sociales

Correo electrónico

Comunicación interna:

Consulte Big Bang. Página 21

Evaluar

Cuando suena una alarma de seguridad, es crucial evaluar primero lo ocurrido, reunir los detalles, realizar un análisis del impacto en el negocio (BIA) y tomar las medidas adecuadas. El SIRT, que incluye al gestor del incidente y al equipo central de seguridad de TI, comienza la clasificación para recopilar y analizar la información antes de actuar.

El gestor del incidente convoca una reunión en la que participan el equipo central de seguridad de TI y el equipo de privacidad, junto con el responsable de la protección de datos (DPO), y abre un canal Cliq para las conversaciones de seguimiento y las actualizaciones. El equipo central de TI recopila toda la información disponible y lleva a cabo una investigación forense para examinar la magnitud y profundidad del ataque; el equipo de privacidad identifica cualquier violación de la privacidad de los datos.

El SIRT formula las siguientes preguntas para evaluar el incidente y sus repercusiones.

Gestor de incidentes	Equipo central de TI	Equipo de privacidad
• ¿Quién identificó y notificó el incidente? • ¿Cuándo se identificó y notificó el incidente? • ¿Dónde se descubrió o localizó el incidente? • ¿Qué impacto tiene el incidente en las operaciones de la empresa? • ¿Ha habido pérdida de datos y está en juego la privacidad? • ¿Cuál es el alcance del incidente con la red y las aplicaciones?	• ¿Es un ataque a la seguridad? • ¿Tuvo éxito el ataque? • ¿Cuál es la puntuación de la IP de origen? • ¿Cuál es la puntuación de la IP de destino? • ¿Cuál es la puntuación de la fuente contra amenazas? • ¿Cuál es la puntuación de la vulnerabilidad? • ¿Qué activos se vieron comprometidos? • ¿Cuáles son las vulnerabilidades asociadas? • ¿Cómo debe responder la organización a este ataque? • ¿Qué podría ocurrir si no se contiene el incidente? • ¿Es necesario preservar la evidencia? • ¿Qué fuentes de evidencia debe adquirir la organización? • ¿Dónde se almacenarán las evidencias? • ¿Cuánto tiempo deben conservarse las evidencias?	• ¿Se ha visto comprometida la cuenta de usuario implicada? • ¿Estaba cifrado el equipo de datos del dispositivo? • ¿La cuenta comprometida tenía acceso a información sensible? • ¿Qué actividades realizó el atacante? • ¿Cuál es la densidad de ataque? • ¿Cuál es el número de personas potencialmente afectadas? • ¿Este evento estaba asociado a algún otro evento o artefacto? • ¿Cuál es el nivel de riesgo para las personas y la empresa? • ¿Qué tipos de controles existen para mitigar los riesgos?

Contener

Un incidente de seguridad es análogo a un incendio forestal, y hay que contenerlo lo antes posible. El SIRT pone en cuarentena las redes infectadas o comprometidas y los dispositivos afectados por virus

u otros programas maliciosos, e instala parches de seguridad para resolver problemas de malware o vulnerabilidades de la red.

Cuando el incidente se identifica como el resultado de una vulnerabilidad de software, el SIRT desactiva la función utilizada en el exploit, escribe una regla de firewall personalizada que bloquea solicitudes específicas dirigidas a la vulnerabilidad, o incluso desinstala temporalmente el software como acciones preventivas. La dirección IP atacante también se bloquea para evitar nuevos intentos.

Mientras tanto, el gestor del incidente reúne los detalles necesarios y abre las comunicaciones externas.

Comunicación externa

La comunicación externa es un paso clave en la respuesta a incidentes de ciberseguridad. El gestor de incidentes trabaja con la alta dirección para controlar el flujo de comunicación y garantizar que se facilite la información adecuada en el momento oportuno.

Por ejemplo, es probable que un intento de hackeo interno no justifique la comunicación con los medios de comunicación o las autoridades. Por el contrario, si el incidente implica la exposición o el robo de registros sensibles de clientes, entonces podría ser obligatorio informar a los medios de comunicación y a las autoridades a la luz del GDPR y otras regulaciones de privacidad del consumidor.

¿Quién?	¿Qué?
Clientes	Los detalles del incidente incluyen: la fecha y hora del suceso, una descripción del problema indicando si se han perdido o robado datos de algún cliente, las medidas que se están tomando para mitigar los riesgos y el tiempo estimado para la recuperación.
Medios de comunicación	A veces, no se puede evitar la atención de los medios de comunicación y el portavoz de nuestra empresa emite una declaración sobre el incidente y sus repercusiones para mostrar nuestro compromiso y capacidad para gestionar el incidente.
Policía	En los casos de intención delictiva, el SIRT, el equipo jurídico y la alta dirección colaboran para informar del incidente a las autoridades policiales.

Delegar

Una vez concluida la investigación y tomadas las medidas necesarias para contener el ataque, el incidente pasa al estado de delegación. El SIRT delega la responsabilidad de la resolución a los ingenieros del producto para que revisen y fortalezcan el código del programa, garantizando la resolución de la vulnerabilidad.

Resolver

La erradicación y la recuperación se logran como un paso singular. La fase de erradicación incluye una corrección más permanente para los sistemas infectados. Si la amenaza ha entrado en un sistema y ha proliferado en otros, el objetivo del SIRT es eliminar la amenaza y borrar toda traza del ataque de nuestros dispositivos y de la red mediante software antivirus, sustitución de hardware o reconstrucción de la red. Nuestro objetivo es que los sistemas vuelvan a "funcionar como siempre". Aquí está la lista de control de erradicación de nuestro SIRT:

- ¿Se han reforzado todos los sistemas infectados con nuevos parches?
- ¿Hay que reconfigurar los sistemas y aplicaciones?
- ¿Se han parcheado todos los posibles puntos de entrada del ataque?
- ¿Se han cubierto todos los procesos para erradicar la(s) amenaza(s)?
- ¿Se necesitan medidas de defensa adicionales para erradicar la(s) amenaza(s)? ¿Se han erradicado todas las actividades maliciosas de los sistemas afectados?

En el caso de una vulnerabilidad de software, el incidente se delega en el equipo de ingeniería de ese producto específico. Los ingenieros de producto corrigen las vulnerabilidades y publican la actualización del software.

Revisión

Después de que el equipo de producto aplique una resolución, suele ser verificada y revisada por el jefe de ingeniería, el SIRT y el equipo de privacidad. Una vez aprobado por los equipos SIRT y de privacidad, el incidente pasa a la fase de cierre. Este paso garantiza que no se ha pasado nada por alto y que el incidente se ha corregido y evitado que se repita. Aunque resulte tentador saltarse este paso, se recomienda encarecidamente revisar la corrección aplicada.

Cerrar

Todos los incidentes de ciberseguridad, como cualquier otro incidente, deben cerrarse adecuadamente. El gestor de incidentes cierra el incidente. Como medida posterior al incidente, el gestor del incidente envía una comunicación a todas las partes afectadas, a los medios de comunicación y a las autoridades confirmando que la amenaza ha sido contenida.

Esta es nuestra lista de control para cerrar tickets:

- ¿Se ha resuelto el incidente a satisfacción de los grupos de resolución?
- ¿Se encarga el personal de resolución de las tareas de limpieza?
- ¿Se han cerrado y notificado todas las tareas relacionadas?
- ¿Ha notificado el gestor del incidente a todas las partes?
- Y lo que es más importante, ¿se ha notificado la resolución a los clientes?
- ¿Han acordado todas las partes interesadas el cierre de seguridad?
- ¿Se ha registrado e iniciado el RCA?
- ¿El gestor del incidente ha iniciado el RCA?
- ¿Se ha notificado el cierre a la mesa de servicio?

La fase final del ciclo de vida de la respuesta a incidentes de seguridad implica RCA y bucles de retroalimentación. El gestor de incidentes inicia el RCA, ya que es crucial aprender de cada incidente para la mejora continua del servicio.

Las mejores prácticas en caso de incidentes de seguridad

Disponga de un proceso de respuesta a incidentes bien definido:

Disponga de un proceso procesable para identificar, abordar y gestionar las consecuencias de una violación de la seguridad o un ataque cibernético de forma que se limiten los daños y se reduzcan el tiempo y los costos de recuperación. Asegúrese de que el plan de respuesta a incidentes se ajuste a las políticas de la empresa.

Defina claramente los equipos, los roles y las responsabilidades:

Identifique los equipos que son responsables en gran medida de cada fase o paso (por ejemplo, contención, erradicación y recuperación) en el proceso de respuesta al incidente. Identifique a las personas clave de los respectivos departamentos y equipos, quién les servirá de apoyo y cómo localizarles de día o de noche. Como mejor práctica, creamos un gráfico RACI que nos ayuda a identificar a las personas que son responsables, las que son aprobadoras, a las que hay que consultar o a las que hay que informar (RACI) de las actividades definidas antes y después de un incidente.

Haga un balance de sus datos:

Es importante evaluar los datos de su organización para saber qué necesita más protección durante una violación de la seguridad de los datos.

Disponga de un plan de comunicación:

Disponer de líneas de comunicación definidas para implicar a las partes interesadas y gestionar la comunicación entre el equipo de respuesta a incidentes de seguridad y otros grupos es crucial para el éxito de la recuperación de incidentes. Un plan de comunicación garantiza que todo el mundo siga los protocolos durante una emergencia a la hora de ponerse en contacto con las partes interesadas, los socios, los proveedores de servicios, los medios de comunicación, las autoridades y los clientes.

Recopile pruebas contra el atacante:

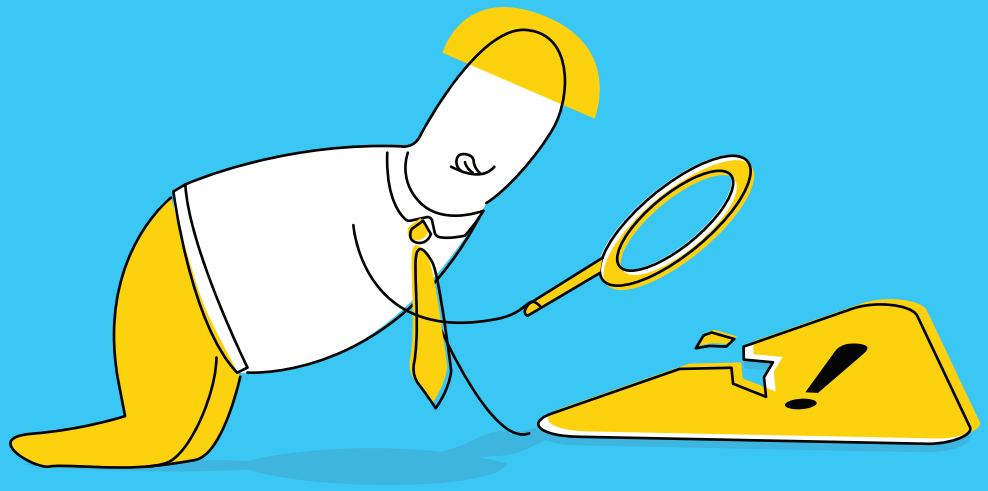
Tomar medidas correctivas durante una crisis, como retirar sistemas de la red o limpiar sistemas, puede alertar a un atacante o destruir evidencias vitales. La organización tiene mucho que perder ante un tribunal si las evidencias se destruyen o son insuficientes. Recopile las pruebas de una manera correcta desde el punto de vista forense para que puedan presentarse de forma creíble ante un tribunal.

Mantenga la calma durante una crisis:

Hacer frente a incidentes de seguridad puede ser bastante estresante. Es necesario mantener la calma cuando se produce un ataque y seguir el plan de respuesta a incidentes.

Realice un análisis de la causa raíz:

Un análisis posterior al incidente en el que participen el equipo de respuesta a incidentes y otros grupos de resolución puede ayudar a comprender el origen del problema y evitar que se repita.



ANÁLISIS DE LA CAUSA RAÍZ (RCA)

¿Qué es el RCA?

El análisis de la causa raíz (RCA) es un enfoque sistemático que profundiza en la identificación de la causa raíz de un incidente formulando repetidamente preguntas del tipo "¿por qué?" hasta que no se pueden dar más respuestas diagnósticas. Suele consistir en un análisis o un debate poco después de que se haya producido un incidente. Un recurso adicional, el documento de estado del incidente, sirve como registro escrito de lo ocurrido antes y durante el incidente, y da respuesta a las preguntas necesarias para realizar un análisis de la causa raíz.

El documento de estado del incidente, también conocido como informe del incidente, es el mejor lugar para empezar con el análisis de la causa raíz. Sin embargo, es fundamental profundizar más allá de lo que indica el formulario. En Zoho, creamos un registro de problemas desde el ticket del incidente para realizar un RCA completo a través de nuestra herramienta ITSM.

¿Por qué realizar el RCA?

En Zoho, nunca dejamos que una buena crisis se desperdicie. Vemos un evento desafortunado como una oportunidad para aprender de nuestros errores, identificar dónde fallaron los procesos o sistemas y estar mejor preparados para gestionar incidentes similares en el futuro.

Principios de RCA

- El RCA se lleva a cabo para determinar los factores que provocaron el incidente y adoptar medidas correctivas en lugar de limitarse a tratar los síntomas.
- Un RCA exitoso se realiza sistemáticamente con conclusiones respaldadas por evidencias reales.
- Lo más frecuente es que haya más de una causa raíz de un incidente.
- "Si no estás cometiendo errores, no estás haciendo nada". En Zoho, creemos en aprender de nuestros errores. Contar con un proceso de RCA "libre de culpa" permite a nuestros empleados y equipos dar los detalles exactos de su actuación, como las medidas que tomaron y las suposiciones que hicieron al gestionar el incidente.

Proceso de RCA

La Acción Preventiva y Correctiva (CAPA) es nuestro enfoque estructurado para investigar, identificar la causa raíz, tomar medidas correctivas y evitar que se repitan.

Ticket de incidente generado

Investigar (Recopilar información sobre el historial de fallos)

RCA (Identificar la causa raíz, los cinco porqués)

CAPA (Identificar las acciones correctivas y preventivas)

Revisión (Revisar la efectividad del CAPA)

Cerrar

Estas son las acciones que realiza el gestor de incidentes durante el RCA:

Crear: Crea un registro de problema a partir del ticket de incidente para realizar el RCA.

Investigar: La información del documento de estado del incidente sirve de base para realizar el RCA. El gestor de incidentes identifica los departamentos y los procesos asociados a CAPA, y lleva a cabo una investigación exhaustiva. A lo largo del proceso de RCA, aprendemos lecciones y descubrimos oportunidades de mejora. Formulamos las siguientes preguntas para llegar a una conclusión.

Etapa	Preguntas	Caso de uso
Resumen del incidente	• ¿Cuándo se detectó el incidente por primera vez? (fecha y hora del incidente) • ¿Dónde se produjo el incidente? (Ubicación del incidente, red, servidor, producto y otros) • ¿Qué tipo de incidente? (falla/problema notificado) • ¿Cuál es el verdadero problema y qué está pasando? (observaciones de los equipos involucrados) • Partes afectadas (partes interesadas, clientes o ambos)	**Declaración de la causa raíz:** Los servidores de Zoho Accounts estaban activos pero no podían servir ninguna solicitud, lo que provocaba que Zoho CRM y Zoho Mail tuvieran problemas de accesibilidad. **Resumen del incidente:** Este incidente de disponibilidad se activó el 22-Ene-2019 a las 15:31 IST y finalizó el 22-Ene-2019 a las 15:52 IST. El incidente fue detectado por Site24x7 y afectó a los servicios Zoho CRM y Zoho Mail. El evento se mitigó adoptando las siguientes medidas: **Corrección temporal (inmediata):** La entrada de servicio causante del problema se eliminó inmediatamente en los 15 minutos siguientes a la interrupción. Los servidores de Zoho Accounts funcionaron y se pudo acceder a los servicios en 20 minutos. **Corrección permanente (actualización de la compilación el día siguiente):** Cuando se añade un nuevo servicio, borramos la caché, lo que borra la caché del JVM y la vuelve a llenar. Como paso alternativo, ahora estamos repoblando el servicio recién añadido en la caché del JVM para que, incluso si la repoblación falla en el futuro, se utilice la lista de servicios más antigua.
Impacto	• ¿Cuánto duró el impacto y cómo se mitigó? • ¿Qué vieron los clientes? • ¿Cuántas personas se han visto afectadas? (por ejemplo: clientes de una suite o producto) • ¿Cuántos tickets de asistencia se han generado?	El tiempo de inactividad duró 21 minutos, y los clientes de Zoho CRM y Zoho Mail no pudieron acceder a los servicios. Tras el incidente, se generaron 20 tickets de asistencia por teléfono, correo electrónico y chat.

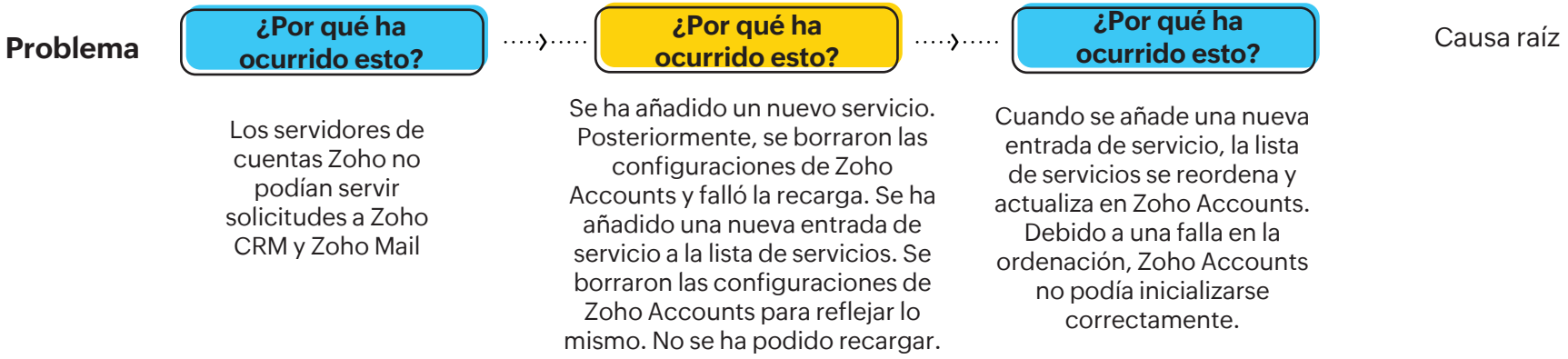
Etapa	Preguntas	Caso de uso
Respuesta	• ¿Quién respondió y cuándo? • ¿Cuál fue el tiempo de respuesta?	El incidente fue detectado por los clientes, y los coordinadores de incidentes de los equipos de Zoho CRM y Zoho Mail respondieron al incidente informando al gestor de incidentes e involucrando a los jefes de los equipos de producto y otras partes interesadas. Se respondió al incidente en los 15 minutos siguientes a su aparición y se proporcionó una corrección temporal.
Recuperación	• ¿Cómo se restableció el servicio? • ¿Qué sorpresas tuvieron que manejar los grupos de resolución? • ¿Qué circunstancias no se habían previsto? • ¿Hubo alguna solución alternativa útil que surgiera durante la crisis?	**Corrección temporal (inmediata):** La entrada de servicio causante del problema se eliminó en los 15 minutos siguientes a la interrupción. Los servidores de Zoho Accounts funcionaron y se pudo acceder a los servicios en 20 minutos. **Corrección permanente (actualización de la compilación el día siguiente):** Cada vez que se añada un nuevo servicio en Zoho Accounts, se borrará la lista en la que están almacenados todos los servicios. Al rellenar la lista ahora vacía, intentamos ordenar los servicios obtenidos de la base de datos. Dado que esta lista ya no es necesaria, la hemos eliminado completamente de nuestra base de código.
Línea de tiempo	• Una línea de tiempo detallada del incidente, en orden cronológico, con indicación de la zona horaria.	22-Ene-2019 15:27 IST: Se ha añadido una nueva entrada de servicio a las cuentas. 22-Ene-2019 15:30 IST: Se borraron las configuraciones de Zoho Accounts para reflejar la nueva entrada. Posteriormente, los servidores de Zoho Accounts no pudieron recargarse. 22-Ene-2019 15:31 IST: Los servidores de Zoho Accounts estaban caídos y los servicios inaccesibles. 22-Ene-2019: 15:51 IST: Se ha ejecutado una corrección temporal en 20 minutos. 22-Ene-2019 15:52 IST: Zoho Accounts se estabilizó y los servicios volvieron a ser accesibles.

Etapa	Preguntas	Caso de uso
Lecciones aprendidas	• ¿Qué se podría hacer para evitar que se repitan este tipo de incidentes? • Si tuviéramos que volver a hacerlo, ¿qué haríamos de forma diferente?	La clasificación de los servicios formaba parte de la antigua UI. Como el listado ya no era necesario, lo hemos eliminado del código base. También identificamos y eliminamos funciones similares en las que se emplea el mismo algoritmo de clasificación para que este tiempo de interrupción no se produzca en el futuro

RCA

El gestor de incidentes determina la causa raíz de los incidentes mediante la técnica de los "5 porqués", que consiste en plantear repetidamente la pregunta "¿por qué?" hasta identificar la causa raíz. No se trata de culpar a nadie, sino de averiguar por qué se produjo el incidente.

Análisis de los 5 porqués



Nota: a veces basta con hacer tres preguntas del tipo "¿por qué?" para llegar a la causa raíz; a veces, requiere más. Se tarda un tiempo en dominar el arte del interrogatorio, pero cuando se hacen las preguntas adecuadas, la causa raíz puede identificarse rápidamente. En este caso, la causa raíz se identificó con solo tres preguntas.

CAPA

En pocas palabras, las acciones correctivas se basan en un evento adverso ocurrido en el pasado. Las acciones preventivas se basan en frustrar un evento adverso en el futuro. Las Acciones Preventivas y Correctivas (CAPA) son parte integrante de nuestro proceso de mejora continua.

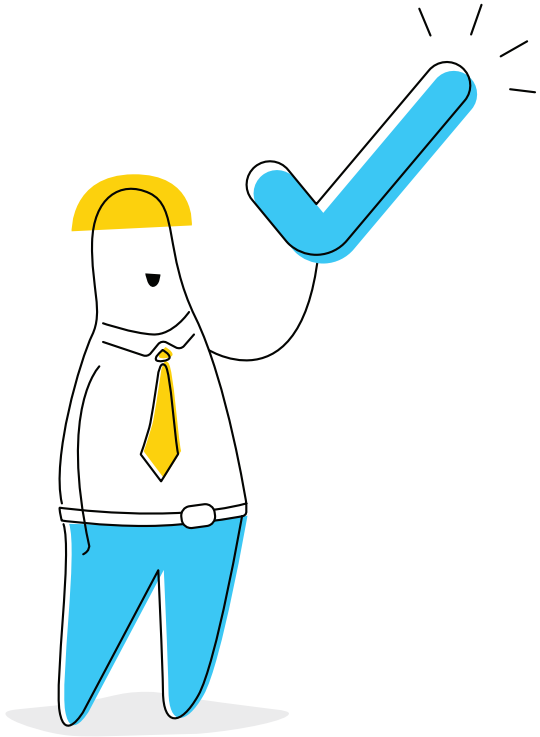
El éxito de RCA requiere una gestión cuidadosa del plan de acción. Así pues, la siguiente etapa del proceso de RCA consiste en establecer una propuesta de plan de acción que defina la lista de acciones correctivas y acciones preventivas. El plan de acción debe definir el plazo en el que se completarán las acciones y quién se encargará de cada tarea.

Aquí está nuestra lista de control para garantizar un plan de acción sistémico:

- ✓ ¿Hay medidas correctivas enumeradas que no estén respaldadas por el análisis?
- ✓ ¿Son las medidas correctivas claras y adecuadas a la causa?
- ✓ ¿Se enumeran las medidas correctivas por orden de prioridad?
- ✓ Si interviene un tercero, ¿se entregarán las medidas en el plazo previsto?
- ✓ ¿Es probable que las medidas correctivas tengan consecuencias imprevistas?
- ✓ ¿Las medidas correctivas están bajo el control de la dirección?
- ✓ ¿Es probable que las medidas correctivas eviten que se repitan?
- ✓ ¿El departamento/propietario de la acción ha aceptado realizar la acción correctiva?
- ✓ ¿Tiene cada acción correctiva un propietario y una fecha de vencimiento claros?

El proceso de acciones preventivas consiste en incorporar salvaguardias y cambios en los procesos para evitar incumplimientos. Como medida proactiva, nosotros:

- Analizamos los procesos y servicios en busca de tendencias negativas que puedan agravar un incidente.
- Realizamos análisis de riesgos para descubrir peligros latentes.
- Llevamos a cabo programas de formación para mejorar las capacidades de nuestros empleados y estar mejor preparados durante un incidente.
- Introducimos planes de recuperación de desastres, seguridad y contingencia para situaciones de crisis impredecibles.
- Establecemos un mantenimiento preventivo para garantizar que nuestros servicios estén siempre seguros, disponibles y rindan al máximo.
- Realizamos auditorías para ayudar a agilizar los procesos y prestar un servicio de calidad.



Revisión

Por último, el RCA se envía a la dirección para que apruebe los cambios y evite que se repitan los problemas. El gestor de incidentes establece un seguimiento exhaustivo con los grupos de resolución para garantizar que las medidas correctivas sean efectivas y que se haya evitado su repetición.

Todos los equipos de TI pueden utilizar la siguiente lista de control para evaluar la calidad general de un plan de respuesta a incidentes.

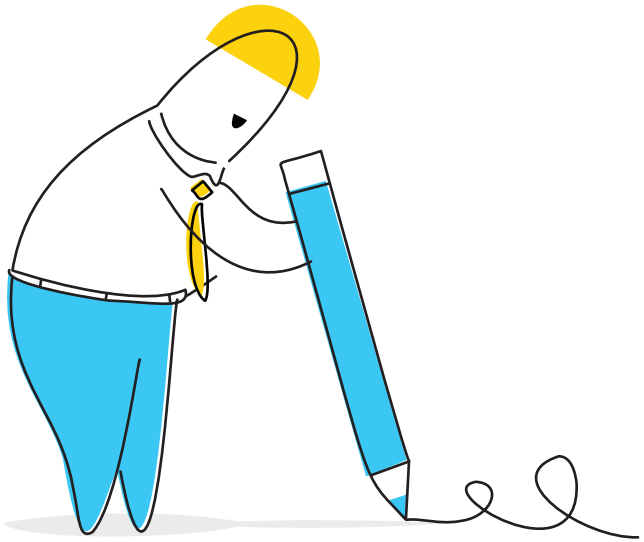
- ¿El plan de respuesta a incidentes ayudó a resolver el incidente o la organización recurrió a actividades "fuera del plan"?
- ¿Existe un documento de síntesis claro para comprender rápidamente el incidente?
- ¿Se basa en hechos todo el análisis del incidente?
- ¿Era la arquitectura de TI lo suficientemente sólida como para limitar el impacto entre sistemas internos?
- ¿Hasta qué punto los equipos asociados, por ejemplo RRHH, jurídico, producto, etc., han participado en la evaluación y la comunicación?
- ¿Fueron adecuadas la política y las prácticas de protección de datos para identificar y priorizar los datos críticos?
- ¿Cuál ha sido la efectividad del plan de comunicación?
- ¿Hemos preguntado "por qué" suficientes veces para determinar la causa raíz?
- ¿Existe un vínculo claro entre los hechos, las causas y las medidas correctivas?
- ¿Se identificó en el análisis si el incidente se había producido con anterioridad?
- ¿Se identificó antes al personal de resolución para este tipo de incidentes, o se recurrió a ellos más tarde en función de sus conocimientos?
- ¿Se evaluaron y gestionaron los riesgos para la organización?
- ¿Ha pasado el RCA por el mecanismo de aprobación?

Reuniones de RCA

Llevamos a cabo reuniones de RCA para llegar al fondo del asunto, tomar las medidas correctivas necesarias para solucionar el problema de forma permanente y emprender acciones preventivas. La directriz más importante de nuestras reuniones de RCA es aprender y mejorar continuamente, no culpar ni desahogarse..

Aquí hay algunos consejos para garantizar una reunión efectiva de RCA:

- Programe una fecha y hora convenientes para todos los participantes en la reunión, teniendo en cuenta a los miembros del equipo que trabajan por turnos y a otros equipos distribuidos.
- Elabore y siga un orden del día de reuniones que no supere las dos horas.
- Reserve una sala de conferencias/reuniones con asientos suficientes para todos los grupos de resolución, las partes interesadas y la alta dirección.
- Programe e invite a los participantes (nosotros utilizamos Zoho Calendar) uno o dos días antes de la reunión de RCA, haciendo hincapié en la importancia de la reunión e incluyendo el orden del día de la misma.
- Lleve un registro escrito de la duración de la reunión.



Conclusión

Los procesos de gestión de incidentes están pensados para proteger a las organizaciones frente a eventos adversos. Esto es especialmente cierto para organizaciones como Zoho Corporation, que dependen en gran medida de Internet y las redes informáticas, y manejan una gran cantidad de datos personales.

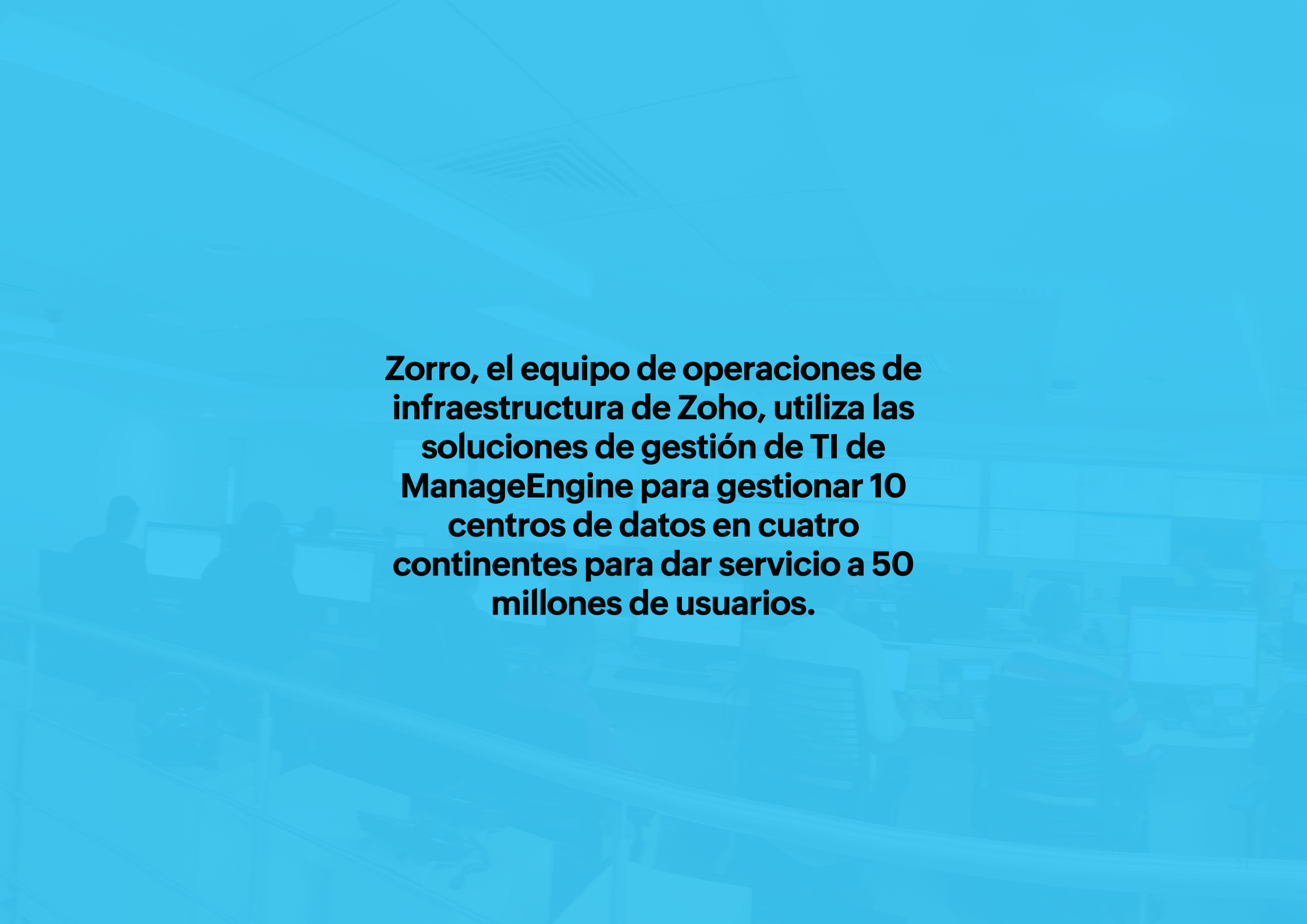
Una política efectiva de respuesta a incidentes se centra en cuatro aspectos clave: gestión de riesgos, auditorías periódicas, medidas preventivas y, lo más importante, capacitación de los empleados. En Zoho, contamos con el personal, los procesos y las herramientas adecuadas para adelantarnos a futuros ataques cibernéticos.

Ahora que ha visto cómo Zoho gestiona los incidentes, esperamos que su organización pueda diseñar y llevar a cabo una estrategia similar teniendo en cuenta las operaciones de su negocio, el equipo de trabajo y la cultura de la empresa.

Devika Subbaiah
Gestor de incidentes, Zorro

Meghna Reddy
Autor

Nikhilesh Raaja
Diseño de libros



Zorro, el equipo de operaciones de infraestructura de Zoho, utiliza las soluciones de gestión de TI de ManageEngine para gestionar 10 centros de datos en cuatro continentes para dar servicio a 50 millones de usuarios.

Acerca de ServiceDesk Plus

ServiceDesk Plus es un software de mesa de ayuda preparado para ITIL con funciones integradas de gestión de activos y proyectos. Con una funcionalidad ITSM avanzada y funciones fáciles de usar, ServiceDesk Plus ayuda a los equipos de asistencia de TI a ofrecer un servicio de primera clase a los usuarios finales con costos y complejidad reducidos. Se presenta en tres versiones y está disponible en 29 idiomas diferentes. Más de 100.000 organizaciones de 185 países confían en ServiceDesk Plus para optimizar el rendimiento de la mesa de servicio de TI y lograr una alta satisfacción del usuario final.

Para obtener más información sobre ServiceDesk Plus, por favor visite manageengine.com/latam/service-desk/

ManageEngine

ServiceDesk Plus

www.manageengine.com/latam/service-desk/