
Command Center Handbook
MONITOREO PROACTIVO DE TI
Protegiendo en valor del negocio a través de la Excelencia Operativa

Manual del Centro de Control

Monitoreo Proactivo de TI

Protegiendo el valor del negocio a
través de la excelencia operativa.

Abdul A. Jaludi

Traducción: Daniel Barcena Villalba

Patrocinado por:

Consorcio One Net, S. de R.L. de C.V.
www.onet.com.mx

abby@tag-mc.net

www.tag-mc.net

Los escenarios representados en el prólogo y el epílogo son ficticios. Los nombres, personajes, negocios, sucesos y situaciones son producto de la imaginación del autor o usados de manera ficticia. Cualquier relación o semejanza con personas reales vivas o muertas es pura coincidencia.

Este libro está dedicado al personal que desempeña funciones día a día dentro de un centro de control. En ocasiones puede parecer un trabajo ingrato pero sin su trabajo y dedicación, los negocios “como los conocemos” no serían posibles.

Tabla de Contenido

Prólogo

Un huracán categoría 5 golpea la ciudad de Galveston, Texas, el sábado por la mañana y se desplaza lentamente hacia el noroeste en dirección a Abilene. Vientos de 350 km/hr barren el estado mientras que la tormenta continúa moviéndose hacia el noroeste. Dos días después, en la tarde del lunes, un segundo huracán – categoría 4 – golpea Corpus Christi, Texas, y continúa hacia New Mexico.

Para el martes en la tarde la mitad de Texas se encuentra sin electricidad y las tormentas siguen creando problemas en gran parte del estado. Para cuando la segunda tormenta deja el Estado y sigue su camino hacia New Mexico, se han perdido cientos de vidas, los daños materiales se cuentan en miles de millones y 75% de Texas no tiene energía eléctrica.

Antes de la llegada de las tormentas, Online Brands, una tienda al por menor por internet que tiene su sede

en Texas movió sus operaciones a sus sedes alternas localizadas en California y Georgia. Los pedidos en línea siguen sin que haya ninguna pérdida. El director de la compañía, John Montgomery, recibe una información de última hora de la Directora de Informática, Amanda Blakely, diciendo que el centro de datos de Texas ha sufrido daños mayores por el paso del huracán. Aunque se encuentran tristes por la destrucción y los daños causados por la tormenta, también se sienten aliviados por el hecho de que el centro de operaciones moviera toda la carga de trabajo a sus centros de datos localizados en otros Estados. El centro de datos golpeado por el huracán permanecerá cerrado para permitir al personal que labora en él, enfocarse en las necesidades que puedan tener sus familias. Los clientes dentro del área afectada tienen prioridad en pedidos y en inventarios. No se han reportado impactos negativos en clientes que se encuentran fuera del área afectada.

La sede del grupo de seguros mundial (World Insurance Group) también se encuentra en Texas pero su situación es muy diferente. Sus generadores se quedaron sin combustible y las gasolineras (estaciones de servicio) han sido cerradas por los cortes de energía por lo cual su centro de datos ha sido cerrado. La compañía no es capaz de realizar ningún trabajo relacionado con seguros. El procesamiento de nuevas solicitudes, solicitudes de pago, y la venta de pólizas, así como facturaciones, cobros y otras funciones de la compañía se encuentran paralizadas. El Director Ejecutivo Frank Mayer no ha podido localizar al Director de Informática Hank Anderson debido a las fallas en la comunicación en Texas.

El miércoles por la mañana, Mayer organiza un equipo y van en carro al centro de control de la compañía. Es un pueblo fantasma. No hay electricidad y el edificio tiene daños visibles. El equipo se dirige a la casa de Anderson y lo encuentran a él y a su

familia tratando de recuperar lo poco que queda de lo que solía ser su casa.

Las noticias que Anderson le da a Mayer y a su equipo no son buenas. Algunos miembros del personal del centro de control sufrieron heridas y muchos de ellos enfrentan también el hecho de que sus casas sufrieron graves daños por el paso del huracán y no están recibiendo ayuda para recuperar sus pertenencias. Tres de cada 60 miembros del personal están en condiciones de brindar ayuda y se encuentran en espera de instrucciones.

Están en espera de que la compañía de recuperación de desastres les diga cuándo habrá disponibilidad de sistemas y espacio. Desafortunadamente, tienen que esperar a que la atención a los clientes de prioridad alta termine antes de que ellos puedan empezar su proceso de atención, lo cual no sucederá hasta que la energía sea reestablecida en los sitios de los clientes y los clientes

prioritarios empiecen a abandonar las instalaciones.

Anderson se pone en contacto con FEMA y otras agencias de gobierno. Su empresa (World Insurance Group) tiene que enfrentar violentas demandas de clientes que no pueden llenar una solicitud ni cobrar el dinero de su seguro, el cual necesitan desesperadamente; así que las agencias de gobierno deciden ayudarlo.

Después de evaluar la situación, formulan un plan para que WIG vuelva a tener operaciones en unas instalaciones en New York en un plazo de 1 o 2 semanas.

El miércoles por la mañana, el Director de Global Financial Holdings, Víctor G. Capistrano, recibe una llamada perturbadora de su jefe de división. Clientes muy importantes en Nueva York y en Washington, D.C., así como en Londres, París, Hong Kong, Singapur, Suiza, Brasil y otros lugares, están amenazando con llevar sus

negocios a otro lado si el servicio no es restablecido pronto. Ellos han tratado de ponerse en contacto con Andrew Cunningham, el jefe de tecnología, pero no han tenido suerte.

Cunningham está de vacaciones en una expedición en África. Él ha estado fuera de contacto con sus compañeros de trabajo y no tiene idea de lo que está pasando. Global Financial tiene dos centros de datos en Texas pero ninguno de ellos ha sufrido daños por los huracanes. Sin embargo, tuvieron cortes de energía así que se cambiaron a suplemento de energía de sus generadores manteniendo todos sus sistemas funcionando correctamente. Desafortunadamente, los encargados de proveer y mantener sus líneas de comunicación fallaron y como resultado ninguno de sus centros de datos puede comunicarse con nadie fuera de sus instalaciones. El centro de control de la compañía se encuentra igualmente sin energía y sin poder comunicarse con el mundo exterior.

El jueves por la mañana, se anuncia en las noticias que las comunicaciones seguirán sin funcionar por, al menos, dos semanas.

Mike Silverman, quien está en el lugar de Cunningham y que no tiene idea del impacto a nivel global que tiene esta pérdida de comunicaciones, decide esperar a que se reestablezca el servicio eléctrico y de comunicaciones; con la pérdida del centro de control y sus herramientas de monitoreo, Silverman y sus equipos de tecnología ignoran que los clientes no pueden acceder a las computadoras que, por su parte, funcionan perfectamente dentro de los centros de datos.

Tres días después de la tormenta, el jueves por la tarde, Silverman recibe en su casa la visita de Capistrano quién se pone furioso cuando se entera de que los equipos en el centro de datos no tienen idea del corte de energía. Capistrano le ordena a Silverman que

reestablezca el servicio lo antes posible o será despedido.

No pudiendo contactar a nadie por teléfono, Silverman va en carro a la casa de todos sus supervisores y miembros clave del personal para tener una junta de emergencia con ellos. Aparentemente nadie tiene idea del corte de energía ni del alcance global de sus efectos. Silverman pospone el hacer una investigación sobre lo ocurrido y el señalar culpables hasta que el servicio sea reestablecido. El equipo se entera de que la caída del sistema de comunicación ha aislado los dos centros de datos, los cuales bajo circunstancias normales se darían soporte uno al otro. Después de hacer lluvia de ideas durante gran parte del día, el equipo empieza a formular un plan.

La compañía tiene un centro de datos fuera de servicio en Vermont el cual iba a ser vendido. Este espacio había sido un centro de datos primario hasta

que todo el equipo fue consolidado en las instalaciones de Texas. Usando un teléfono vía satélite, llaman a este centro. Todas las líneas de comunicación, los alimentadores y generadores de energía están aún en condiciones de operación.

El plan es reactivar el servicio desde el centro original trasladando físicamente todos los sistemas críticos. Trabajando con una empresa especializada en traslado de equipo computacional sensible, se trasladará todo el equipo de vuelta a la locación en Vermont, se reconfigurará y se pondrá en operación. Asumiendo que todos los técnicos que serán necesarios para realizar el proceso de reconfiguración estarán disponibles, se estima que el servicio sea reestablecido en un periodo de 7 a 10 días. La mayoría de los integrantes del equipo es pesimista en cuanto a la fecha límite debido al grado de daños en Texas y a la capacidad para conseguir los expertos necesarios o la

empresa de traslado del equipo en un estado de emergencia.

Con este plan, Silverman llama a Capistrano la tarde del viernes y lo pone al corriente en cuanto al estado del sistema y en cuanto al plan para reestablecer el servicio. Capistrano aprueba que se lleve a cabo el plan aunque sabe que es demasiado tarde. Al tiempo de finalizar esta llamada, se prepara para la siguiente que será para notificar a las agencias de gobierno correspondientes acerca del inminente fracaso de su firma; sabe que una vez que el servicio sea reestablecido habrá una deserción masiva hacia sus competidores seguida de una también masiva serie de demandas legales.

Los escenarios ficticios presentados arriba describen situaciones que surgen cuando dos huracanes de categoría 4 y 5 tocan tierra. Sin embargo, cuando una empresa pierde la habilidad de desarrollar su trabajo, sin importar cuales sean las circunstancias, siempre hay repercusiones graves. En las secuelas de la súper tormenta Sandy, las fallas catastróficas de todo el sistema no parecían tan poco probables como se pensaba en otros tiempos. ¿Qué debieron haber hecho diferente estas compañías?, ¿cómo podrían haber estado mejor preparadas?, ¿qué planes de contingencia deberían estar listos aún antes de que las tormentas se formen?

Estas preguntas pueden ser mejor contestadas, verificadas e implementadas por un centro de control configurado y supervisado apropiadamente.

Introducción

El Centro de Operaciones

(Centro de Control)

Casi todas las empresas privadas, así como casi todas las agencias de gobierno a nivel municipal, estatal y federal que quieren reducir gastos están volteando hacia la tecnología. Dentro de la tecnología de la información, los centros de datos son áreas en donde se pueden obtener grandes ahorros al consolidar locaciones y funciones (deberes). Migrar hacia locaciones centralizadas es uno de las mejores maneras de reducir gastos sin tener que hacer grandes recortes de personal (fuerza de trabajo).

Para los centros de datos, la consolidación implica ahorros en pagos por las instalaciones, pago de servicios, telecomunicaciones (conexiones de alta velocidad) y el que puede ser uno de los costos más grandes: pago de licencia de

softwares. Cuando las computadoras de varios centros de datos se trasladan a un solo sitio se puede conseguir una dramática reducción de costos en software que otorga licencias por locación.

Antes de consolidar centros de datos y cuartos para equipos, es mejor consolidar centros de control. Esto permite un manejo centralizado del hardware, tarea que hace mucho más efectivo el manejo de un centro de datos grande.

Con la tecnología de antaño, los centros de control y los centros de datos necesitaban tener cierta proximidad, debían localizarse en el mismo edificio o estar separados por no más de unos cuantos cientos de metros en una localidad cercana. Eso era un requerimiento básico debido a las consolas de sistemas usadas para monitorear y controlar sistemas computacionales los cuales requerían una conexión directa a las

computadoras centrales dentro del centro de datos.

Los avances en la tecnología permitieron que las consolas de sistemas pudieran ser conectadas de manera remota y de manera segura a través de líneas de comunicación por medio de la red o de redes dedicadas. Estos avances eliminaron la necesidad de tener un centro de control para cada centro de datos. Con la libertad de llevar los centros de control (donde el personal maneja y monitorea computadoras) a una locación remota lejos de los centros de datos (donde se albergan los equipos computacionales y de soporte) vino la habilidad para manejar y monitorear múltiples centros de datos desde una locación remota.

Un centro de control es más que un lugar lleno de gente y de paredes compuesto de monitores de video. Un centro de control asegura que su negocio sea capaz de proveer servicios críticos a sus clientes de día y de

noche, los 365 días del año, si es que eso es lo que el negocio demanda.

Los clientes que puedan tener acceso y desarrollar lo que necesiten, cuando lo necesiten dentro de los horarios de atención, serán clientes satisfechos sin ninguna necesidad de llevar sus negocios a otro lado.

Los clientes que enfrenten interrupciones constantes o, peor aún, aquellos que pierdan la confianza en tu capacidad para proveer servicios consistentes y de alta calidad, llevarán sus negocios con tus competidores. Recuperar el compromiso con clientes que han perdido la confianza en ti, es una tarea mucho más costosa que mantener contentos a los que tienes ahora. Es muy probable que los clientes insatisfechos comenten sus malas experiencias contigo a través de las redes sociales haciendo más difícil el reclutamiento de nuevos clientes. Los comentarios positivos en las redes sociales, aquellos comentarios que hagan tus clientes en sus cuentas en

las redes sociales, reducen ostensiblemente los costos para hacer que los nuevos clientes se comprometan con tu empresa.

El costo de un eficiente centro de control es minúsculo comparado con la cantidad de negocios que se perderán debido a interrupciones en el sistema. Sin embargo, un centro de control bien manejado y eficiente puede provocar que los altos ejecutivos de la empresa consideren recortes en el presupuesto debido a la percepción incorrecta de falta de trabajo o actividades relacionadas con el trabajo en sus oficinas, esta situación puede ser engañosa. La razón por la cual las interrupciones en el sistema son bajas es debido a que el centro de control está logrando su objetivo de la mejor forma posible: previniendo que ocurran interrupciones. Quítale recursos a tu centro de control, que es la razón por la cual tus aplicaciones están siempre disponibles, y, probablemente, empezarás a perder clientes por

aumento en las interrupciones en el servicio. Esa relación de causa y efecto no siempre se nota porque el director del centro de control raramente anuncia los recortes de recursos y puede no estar consciente de las correspondientes pérdidas de clientes.

Contrario a la creencia popular, el objetivo principal de los centros de control no es corregir errores cuando estos ocurren sino evitar que ocurran. Piensa en lo que pasa cuando hay un incendio en un edificio; puede que tú extingas el fuego y salves el edificio pero, el daño ya está hecho. Más que actuar como el departamento de bomberos, el centro de control debe operar como el inspector de incendios, la alarma de humo y los regadores de agua, buscando condiciones que signifiquen un riesgo de incendio y corrigiendo dichas condiciones y, si empieza un incendio, detectándolo antes de que se extienda y de que alguien pueda salir herido.

El objetivo principal del centro de control es asegurar que el cliente siempre sea capaz de llevar a cabo lo que el servicio promete, asegurarse de que ellos puedan desarrollar las actividades que le generan ganancias a la corporación. Recuperar un sistema computacional (servidor, computadora central, etc.) después de que ha fallado, es demasiado tarde. Cuando esto pasa el cliente ya ha tenido un impacto y el centro de control está en modo reactivo (de reacción), corriendo para arreglar el sistema antes de que los clientes se cansen y se vayan a otro lado.

El centro de comando exitoso es siempre proactivo, monitorea y resuelve situaciones en el menor tiempo posible para evitar cortes en el sistema. El ambiente es tranquilo y sereno en todo momento. Los problemas potenciales son detectados y corregidos antes de que puedan hacer caer tus sistemas.

Capítulo Uno

¿Qué es un centro de comando y control de operaciones?

El centro de control es el sustento de una organización. Es como el sistema nervioso de un cuerpo: monitoreo constante y envío de señales al cerebro cuando algo ocurre para que el cerebro mande las órdenes necesarias a otras partes del cuerpo para que este funcione como debe ser. El centro de control permite que una organización funcione de la manera en que ha sido diseñada, llevando a cabo operaciones día a día a pesar de lo que ocurra alrededor de ella; el centro de control trabaja de manera que nadie nota que está ahí, pero todos saben quién está a cargo cuando hay algún problema.

El centro de control monitorea el ambiente y está listo para actuar de manera rápida y decisiva en contra de una amenaza o amenaza potencial a ese ambiente. Todo aquel, dentro o fuera del centro de control, que en

algún punto necesite interactuar con él, debe saber la labor y responsabilidades del centro de control o ser capaz de acceder a esa información de manera fácil y rápida.

Cada labor y función realizada por el personal del centro de control debe tener un manual de procedimientos bien documentado. Dichos procedimientos deben estar detallados a un nivel en que un colaborador recién contratado los pueda seguir con cierta facilidad después de un periodo inicial de entrenamiento.

El centro de control es un lugar donde se guarda el orden, especialmente cuando el mundo exterior se cae a pedazos. Lo anterior se lleva a cabo monitoreando el ambiente y respondiendo a eventos, desde los relativamente inofensivos hasta crisis graves, aplicando procesos predeterminados al pie de la letra. Todo lo que pasa dentro de un centro de control debe caer dentro de sus

labores y responsabilidades y debe estar ligado a un procedimiento bien definido.

Un centro de control provee liderazgo y dirección para asegurar que se mantenga el orden y el servicio. Nunca debe ser visto como un mero centro de información o de ayuda. No es un lugar donde los operadores de un conmutador sólo ayudan a mantener la comunicación entre los miembros de una organización. Ni tampoco es el basurero en donde caen las actividades y proyectos que nadie más quiere hacer o las cuales otros departamentos no pueden realizar por falta de personal. Los miembros del personal del centro de control no son capturistas de información y no deben dedicarse a llenar listas de registros diarios ni a actualizar la información de contacto de una persona.

Hay muchos tipos de centros de control.

Ellos incluyen:

Supervisión del centro de datos: monitorea la supervisión central y el control de operaciones de los sistemas computacionales que son el sustento de la mayoría de las empresas, normalmente albergados en centros de datos y grandes cuartos de computadoras.

Supervisión de las aplicaciones de negocio: asegura que las aplicaciones que son críticas para los clientes y para el negocio se encuentren siempre disponibles y trabajando conforme a diseño.

Supervisión civil: monitorea la supervisión central y el control de las funciones operacionales de civiles. El personal de esos centros monitorea el ambiente metropolitano para garantizar la seguridad de la gente y la correcta operación de servicios de gobierno críticos, ajustando los servicios a los requerimientos y asegurando el movimiento constante apropiado.

Supervisión de emergencias (crisis): Dirige a la gente, los recursos y la información; y controla situaciones para evitar crisis/emergencias y minimiza/evita impactos en caso de ocurra un incidente.

Tipos de salas de comandos y de control y sus responsabilidades

- Centro de Control (CC)
  Centro de datos y de sistema computacional

- Centros de operación de redes (NOC)
  Equipos de redes y actividad de red

- Centros de operación táctica (TOC)
  Operaciones militares
  Policía e inteligencia

- Centros de operaciones de seguridad (SOC)

  Agencias de seguridad

  Agencias gubernamentales

  Supervisión de tráfico

  CCTV

- Centros de operaciones de emergencia (EOC)

  Servicios de emergencia

- Centros de operaciones combinadas (COS)
  Control de tráfico aéreo
  Aceite y gasolina
  Cuartos de control
  Transmisiones

- Audio visual (AV)
  Simulación y entrenamiento
  Medicina

- Centro de control de comunicación social

Dentro de cada tipo de centro de control de operaciones existen varias funciones comunes. Estas incluyen monitoreo (el cual incluye supervisión de eventos), supervisión de incidentes, coordinación e implementación de cambios aplicables, y recuperación después de un desastre (también conocido como continuidad de negocio).

Objetivos

El objetivo global de un centro de control es proteger la integridad de su dominio a través de monitoreo proactivo.

Esto significa que el personal del centro de control se encuentre muy ocupado asegurando que nada fuera de los previsto suceda, que todos los sistemas estén operando correctamente y que los clientes y el personal hagan lo que tengan que hacer sin contratiempos.

Algunos días parecerá que el personal no está haciendo absolutamente nada; esos son días perfectos. Todos están haciendo, de hecho, mucho más de lo que aparentan. Ellos están observando, preparados para entrar en acción, que alguna alerta aparezca en sus monitores.

Otros días el personal estará extremadamente ocupado, interactuando con otros miembros del personal y equipos de soporte por medio de sus audífonos al tiempo de escribir en sus teclados. Cuando todos están ocupados, están reaccionando a una alerta, corriendo diagnósticos iniciales, y reparando la causa de la alerta o notificando a soporte y trabajando con ellos para resolver el problema. También están documentando todo lo que transpire.

Ambos escenarios serían considerados exitosos si el ambiente trabajara sin fallas, donde todo trabajara como debe ser; en otras palabras, donde

clientes y colaboradores trabajaran sin dificultades.

El siguiente objetivo es reducir la duración de cualquier efecto que afecte negativamente a los clientes.

Habrá momentos en los que una interrupción no podrá ser evitada y el objetivo principal del centro de control sea fisurado. Hay es en donde el siguiente objetivo entra juego: reducir la duración del impacto. Cuando el personal del centro de control se da cuenta de la interrupción en el sistema, el equipo de supervisión de incidentes toma el control para coordinar los esfuerzos de recuperación del servicio.

Es en estos casos en los que un centro de control con personal debidamente entrenado y con procesos efectivos de supervisión de incidentes, realmente brilla. Observar cómo se va desplegando el proceso es como ver poesía en movimiento. El ambiente permanece en calma; nadie se altera mientras el equipo de supervisión de

incidentes desarrolla sus funciones de emergencia. Se establecen conferencias telefónicas para coordinar y cooperar con agencias externas y representantes para ayudar a restaurar el servicio. Se genera un ticket de incidente de problema (incident trouble ticket) (si es que no ha sido ya generado automáticamente), se actualiza el ticket, y se mandan notificaciones alertando a los correspondientes equipos de soporte, supervisores de clientes, y el supervisor en jefe del incidente, todo en cuestión de minutos.

El siguiente paso es asegurarse de que todo lo que tiene que ser monitoreado está siendo monitoreado.

En cualquier ambiente siempre hay cambio. Es vital para el centro de control saber cuándo ha sido añadido algo nuevo o cuando algo en el ambiente ha sido alterado temporal o permanentemente o cuando algo ha

sido borrado. Cualquier cosa nueva debe ser monitoreada desde el primer día y cualquier cosa que se quite debe ser también removida del monitoreo para que el personal de soporte, el cual es muy bien pagado para atender emergencias, no pierda grandes cantidades de tiempo persiguiendo fantasmas.

El último objetivo es asegurar un eficiente uso de los recursos.

Un centro de control lleno de gente muy ocupada no es una situación ideal. A través del uso de procesos de optimización, automatización y estándares, los requerimientos de recursos humanos en el centro de control (la cantidad de gente necesaria para operar completamente) debe ser bajo; no tan bajo como para poner en riesgo el ambiente pero si sólo el necesario para resolver cualquier situación.

Los requerimientos de personal deben tomar en cuenta días festivos, vacaciones, enfermedades,

emergencias y aún crisis (huracanes, tormentas de nieve y otras situaciones en las cuales las localidades puedan declarar estados de emergencia). Un centro de control apropiadamente manejado y supervisado debe ser capaz de soportar cualquier situación con un número especificado de colaboradores, incluyendo el monitoreo de sitios y empresas adicionales.

En un centro de control eficiente, la carga de trabajo se puede duplicar o triplicar sin que se afecte el servicio ni que haya necesidad de más colaboradores ni más recursos. Básicamente, si el ambiente crece en un 100%, el centro de control será capaz de mantener el nivel de servicio sin incrementar el personal ni el equipo y sin trabajar horas extra.

Como se logran los objetivos.

No es suficiente poner los objetivos: el desempeño debe ser medido en base a esos objetivos si es que te van a servir de algo a ti y a tus clientes.

Para que un centro de control alcance sus objetivos consistentemente, estos deben estar totalmente documentados y ser medibles.
Esto significa establecer y reforzar estándares para todo lo que suceda dentro del centro de control.

1. **Establecer estándares.**
   Todos deben seguir una lista detallada de instrucciones cuando se haga un cambio de aplicación y cuando se agregue un nuevo proceso, aplicación o negocio.
2. **Refuerzo de estándares.**
   Cualquier carga de trabajo adicional, ya sea que se mueva a otra locación o sea una nueva adquisición debe migrar a los estándares, políticas, procedimientos y prácticas actuales y vigentes. Cualquier desviación o excepción debe ser otorgada sólo por un periodo corto y con su correspondiente fecha de

cumplimiento. Las excepciones otorgadas sin una fecha de cumplimiento se convierten en un blanco en movimiento y dan por resultado subsecuentes pérdidas de estándares y procedimientos comunes.

3. **Métricas precisas y automatizadas.**
   Juntar y distribuir las métricas adecuadas para cada objetivo provee dirección en la efectividad del centro de control. Las métricas de tendencias le permiten a la supervisión estimar y ajustar recursos y requerimientos adecuados a la carga de trabajo.
4. **Una clara línea/cadena de comandos.**
   Aquí es donde se asignan responsabilidades. Alguien, no con un nivel bajo, ni un comité ni un grupo de co-supervisores sino un supervisor o director específico debe ser

responsable y rendir cuentas en caso de que algo falle; ya sea una pieza de un equipo, un proceso, una aplicación o una función. Lo mismo aplica si alguien tiene que escalar una dificultad. Una clara línea de comandos debe ser documentada para que si alguien no está satisfecho con el procedimiento corriente o con la forma en que se manejan las cosas pueda ir a algún lugar para buscar una resolución. Lo anterior también aplica para asignar correctamente incidentes que han sido corregidos pero que requieren de una resolución permanente para evitar reincidencia/recurrencia.

Para asegurar la consistencia en la consecución de objetivos, todos o la mayoría de estos elementos deben existir:

Alerta automatizada

Implementar manualmente el monitoreo a una nueva computadora, aplicación o aparato, suprimir alertas para actividades programadas o finalizar el monitoreo cuando o un sistema o aplicación es puesto fuera de servicio requiere mucho trabajo, consume mucho tiempo y es propenso a errores. Automatizar estas funciones asegura que las alertas se generen cuando sea necesario y se desactiven cuando ya no se necesiten. La automatización también asegura que estas tareas se realizan en tiempo, sin retrasos.

Calendarización automatizada

Los días en que se usaban hojas de rastreo para procesar la carga de trabajo diaria son cosa del pasado. Existen muchas herramientas fáciles de usar que se pagan por si solas

simplemente por la cantidad de errores humanos que se eliminan.

Recuperación de fallos automatizada

Una de las razones por las que se tienen retrasos en el procesamiento de lotes o en problemas que involucran datos es el error humano, más comúnmente en los esfuerzos de recuperación de fallos de lotes. Ya sea por la ausencia o incorrecciones en las instrucciones de reiniciado o por un error siguiendo las instrucciones correctas, pueden ocurrir errores adicionales, una base de datos se puede corromper, los mismos datos pueden ser procesados varias veces o algunos datos puede no ser procesados en absoluto. Evitar que ocurra la falla es la mejor opción aunque no siempre es posible. La siguiente mejor opción, siempre que sea posible, es automatizar el proceso de recuperación.

Soporte y supervisión de procedimientos de escalación/escalamiento

Cuando existe un problema le damos a la persona que lo va a arreglar, tiempo suficiente para encontrar y corregir la falla. Sin darnos cuenta 5 minutos se convierten en una hora. Los procedimientos de escalamiento que especifican requerimientos en cuanto al tiempo de cada tipo de problemas basados en la gravedad y el impacto del mismo, eliminan estas situaciones.

Supervisión de problemas independiente

Tener un equipo de supervisión de problemas localizado fuera del centro de control y que reporta a una supervisión diferente elimina cualquier tipo de conflicto de intereses en la captura y documentación de problemas. Provee un nivel adicional de vigilancia de manera que las acciones requeridas para identificar y corregir las causas de un problema se pueden desarrollar y la recurrencia es eliminada.

Estándares para hardware, software y seguridad (un proceso consistente para cada función)

Implementar estos estándares trae muchos beneficios. Aunque los costos puedan ser lo que determine su implementación, los estándares promueven la eficiencia y reducen errores haciendo posible que se automaticen muchas funciones que, de otra manera, tienen que ser hechas manualmente. La falta de estándares dificulta la implementación de procedimientos ejecutables.

Base de datos para supervisión de configuración y cambio (CCMDB).

Saber que aparatos y aplicaciones se verán afectadas por un cambio dado es una información invaluable. Un CCMDB ayuda a garantizar que todos los que sean afectados por un cambio se enteren del mismo. Esta información también es de mucho valor cuando ocurre una falla debido a un cambio. Tener un CCMDB puede

ser la diferencia entre tener un corte de 2 horas y uno de 10 minutos.

Base de datos de errores conocidos

Cuando ocurre un problema, lo que normalmente toma más tiempo es determinar cuál es la causa. Documentar cada falla y las correspondientes acciones de recuperación en una base de datos de errores conocidos reduce de manera substancial el tiempo de recuperación de fallas subsecuentes y de fallas similares que ocurran en otro lugar.

Supervisión de fallos

Cuando empecé a trabajar en operaciones, mucho antes de los centros de control, la eficiencia y la automatización, se usaban hojas de registro para darle seguimiento a los procesos nocturnos. Siempre a la misma hora, los viernes en la noche, el mismo lote de trabajo semanal (una serie de programas de desarrollaban una función de reconciliación) fallaba.

Se les notificaba a los de soporte de tecnología y 10 minutos después el lote estaba de regreso en el sistema. Después de que esto ocurrió por tercera vez, fui a ver al personal de soporte cuya responsabilidad era corregir este error. Me daba curiosidad saber porque su trabajo fallaba por tercera semana consecutiva. Roger me explicó que durante casi un año el lote había estado procesando más datos y necesitaba más espacio de almacenamiento. Roger y el resto de su personal incrementaban la capacidad de almacenamiento que el proceso del lote requería y después, simplemente, reiniciaban el trabajo. Eso me confundió aún más. ¿Por qué no, simplemente, hacer la corrección permanente? "Seguridad laboral" – dijo Roger. Poco tiempo después de esa conversación, el trabajo fue corregido de manera permanente. Roger y el resto de su equipo de soporte técnico conservaron sus trabajos pero, en vez de arreglar las

mismas fallas una y otra vez, ellos pudieron dedicar más tiempo a identificar y corregir otras molestias y 'cuellos de botella'.

Las causas de los fallos deben ser identificadas y corregidas para evitar que el mismo fallo se repita.

Reporte de métricas estandarizadas (incluye objetivos diarios, semanales y mensuales y faltas).

A menos de que todo dentro de un centro de control sea rastreado, medido y reportado, el conseguir objetivos será pura cuestión de suerte. Las métricas apropiadas habrían identificado el proceso del lote que estuvo fallando cada semana durante un año. Los reportes de tendencias semanales y mensuales nos ayudan a identificar áreas con problemas potenciales, anormalidades y recursos – humanos y maquinas- antes de que se vuelvan un problema.

Reporte automatizado de excepciones diarias

Es en este reporte en donde se identifican y corrigen problemas antes de que se vuelvan problemas más grandes.

Reporte automatizado mensual

Esta es tu oportunidad de brillar, de demostrar lo bien que trabaja el centro de control.

Generación automatizada de reporte de problemas

Hacer tickets de problemas (trouble tickets) manualmente, se lleva mucho tiempo y es susceptible de errores: puede ser que no se creen tickets por cada incidente ocurrido o que sean asignados a un departamento incorrecto, extendiendo, así, el tiempo de resolución de problema. Los fallos que no son rastreados y corregidos con el ticket de problema

debidamente documentado son más probables de reaparecer.

Revisiones de desempeño continuo

No hay que decir más acerca de esto. El progreso y el cambio nunca se detienen; asimismo, nunca deben detenerse los esfuerzos por encontrar oportunidades para mejorar.

Resultados de un centro de control manejado inadecuadamente:

Caída del negocio como resultado de falta de monitoreo y de no atención a alertas.

> *Si un servidor de producción nuevo que todavía no ha sido monitoreado se sale del espacio de almacenamiento (storage space), tus clientes lo sabrán antes que tú. Si las consolas de monitoreo están inundadas con falsas alertas, es muy probable que una alerta*

de emergencia real no sea atendida y que esto lleve a una falla del sistema y, una vez más, tus clientes se enterarán de la falla antes que tú.

Personal adicional será requerido para poder atender el alto número de alertas no-accionables.

La supervisión manual de eventos y alarmas consume mucho tiempo y puede producir un alto número de alertas en las consolas de monitoreo. Esto dará la impresión errónea de que se necesita más personal para atender la carga de trabajo.

Pérdida del negocio debido a que los clientes se cansan de la intermitencia en la disponibilidad del sistema.

Pérdida del negocio cuando los clientes frustrados se van a buscar el servicio a otro lado.

Moral baja y alto movimiento de personal debido cargas de trabajo pesadas.

Incremento de los costos operacionales cuando las diferentes áreas del negocio crean sus propios centros de monitoreo.

Multas normativas (regulatory fines) por no cumplir con los requerimientos de entrega del servicio (disponibilidad del sistema, actualización de cuentas, etc.)

Tomar estos pasos puede parecer mucho trabajo o hasta una amenaza en la seguridad en el trabajo. De hecho, lo opuesto es verdad. Cuesta mucho más trabajo corregir fallos que prevenirlos. Implementar la automatización y procesos eficientes puede o no amenazar la seguridad del trabajo pero fallar en la obtención de objetivos continuamente y tener

clientes insatisfechos definitivamente llevará a pérdidas de trabajos, empezando de arriba abajo.

Capítulo Dos

Composición del centro de control

Para que un centro de control sea lo más efectivo posible, las funciones, la estructura organizacional, la disposición y la localización física deben ser apropiadamente definidas, planeadas e implementadas. Esto garantiza que estén alineadas entre sí y que ayuden a alcanzar los objetivos previstos.

Funciones

Se le debe dar una atención especial a las funciones que se desarrollan dentro del centro de control. Agregar funciones que no ayuden a la consecución de los objetivos planteados, incrementará costos y complejidad. Dejar afuera funciones de emergencia le puede ahorrar dinero al centro de control pero le puede costar mucho más a la

compañía en cuanto a pérdida de clientes y, eventualmente, en ingresos.

Las funciones determinan el tipo de trabajo que se llevará a cabo en el centro de control y la vigilancia gerencial directa es vital durante una emergencia. Toda función en el centro de control que se desvíe de los objetivos preestablecidos le quitará recursos necesarios a dichos objetivos. De igual manera, las funciones que tengan un impacto directo en la consecución de los objetivos preestablecidos pero que se alberguen fuera del centro de control, donde la vigilancia gerencial directa no es posible, dificultará la consecución de dichos objetivos.

Desafortunadamente, la gran importancia de albergar las funciones correspondientes dentro del centro de control no son visibles hasta después de haber tenido una emergencia grave. Si eso pasa cuando tú estés a cargo, seguramente cuando

encuentres un nuevo trabajo le darás más importancia a la localización de las funciones.

A continuación se encuentran las funciones que se recomienda albergar en la infraestructura del centro de control:

Funciones primarias del centro de control

- Monitoreo
- Operación de consolas
- Supervisión de incidentes
- Soporte técnico

Funciones secundarias

- Vigilancia de seguridad física
- Control de cambio de emergencia fuera de horario de trabajo
- Soporte de organizaciones secundarias

- Iniciación de proceso y supervisión de mejora de procesos
- Recuperación de negocio (desastre) y coordinación

Función Uno: Monitoreo

Las alertas de monitoreo son la función más importante del centro de control. No importa que alerta son, de donde vienen o como se generen o funcionen. De hecho, todo esto importa muchísimo al departamento cargado con alertas de supervisión, usualmente el equipo de supervisión de eventos que se aborda más adelante en este libro. Lo que es más importante para el personal de monitoreo y para el negocio al que le dan soporte es que tratamiento se le da a las alertas cuando son recibidas en el centro de control.

Una locación que no lleva a cabo monitoreo pero que sí desempeña acciones

correctivas únicamente cuando el usuario llama con un problema, es un centro de atención de llamadas (call center) o un servicio de asistencia técnica (help-desk). No es un centro de control.

Una alerta es una simple notificación de que ha ocurrido un incidente. Un incidente es algo que pasa fuera de lo común que puede ocasionar una interrupción en el servicio a los clientes. Usualmente, una alarma es una advertencia de que si un incidente, algo fuera de lo ordinario, no se revisa, puede provocar un fallo de una aplicación o de alguna pieza de hardware (computadora, servidor, red o aparato de almacenamiento) o puede afectar la integridad de tus datos o de tu sistema.

En un ambiente correctamente monitoreado, nada fuera de lo común o fuera de ciertos umbrales debe activar una alerta. El tipo de evento y que tan importante o urgente es,

determina el tipo de alerta, a donde es enviada y si algo debe suceder automáticamente.

El centro de control debe tener un equipo cuya función principal sea monitorear. En un entorno de misión crítica, la peor reacción es reducir el tamaño del personal de monitoreo debido a que no haya habido problemas.

> **No hay problemas debido a que el equipo de monitoreo ha estado realizando su trabajo.** Esto quiere decir que han estado evitando que los problemas ocurran. Si el equipo de monitoreo está constantemente ocupado entonces tú tienes un problema serio. Esto quiere decir que las alertas no están configuradas correctamente o que tus aplicaciones y sistemas computacionales son muy inestables; en cualquiera de los

dos casos, tus clientes no van a estar muy felices.

El monitoreo no solo es responsabilidad del equipo que está viendo las pantallas sino de todos, más allá de sus funciones. Asegurarse de que todos sepan que esta es una responsabilidad compartida, garantiza que el objetivo principal del centro de control – un entorno de operación seguro y normal – esté en la mente de todos. Lo que pasa después de que una alerta es detectada por el personal del centro de control depende de quién desempeñe las otras funciones críticas/de emergencia mencionadas arriba.

Los tipos más comunes de monitoreo son:

- Infraestructura
- Aplicación
- Monitoreo a aplicaciones de la empresa
- Lote

Monitoreo de Infraestructura

La infraestructura de una empresa consiste de los componentes del núcleo y las aplicaciones que soportan su operación diaria y que son usadas en todas sus divisiones. Para que la mayoría de los negocios funcionen eficientemente, diferentes divisiones comparten los mismos componentes, tales como centros de datos, equipos de comunicación y computadoras centrales. También pueden tener las mismas aplicaciones, como mail, firewall, seguridad y soporte del servidor.

Alteraciones dentro de la infraestructura de la organización pueden afectar tanto a colaboradores como a clientes. Una de las funciones más importantes del centro de control es monitorear la infraestructura. Al monitorearla como un todo, el centro de control puede determinar si una situación es global en su naturaleza e involucrar a los equipos de soporte apropiados. Por ejemplo, cuando hay interrupciones que no son solucionadas rápidamente el centro de control notifica a la dirección general de las divisiones afectadas. Eso le permite a la empresa notificarle a los clientes del problema antes de que estos empiecen a llamar. Es mejor informarles que dejarlos en la obscuridad o aún peor dejarlos que ellos mismos diagnostiquen sus equipos. Los clientes que caen en la cuenta de que frecuentemente tienen que estar revisando sus equipos cuando entran a tus aplicaciones y que se dan cuenta de que de repente ya funcionan 'mágicamente',

eventualmente se cansan y se van con la competencia.

Monitoreo de aplicaciones y aplicaciones de negocio

Estos tipos de monitoreo son similares pero tiene unas cuantas diferencias importantes.

Monitoreo de aplicaciones es una vista de la aplicación desde un nivel alto, es usualmente desarrollado por el equipo global del centro de control. Examinan el hardware, la red, programas, mensajes de error y otras cuestiones que requiere la aplicación para funcionar correctamente.

Monitoreo de aplicaciones de negocio (BAM) observa cómo trabaja la aplicación desde adentro. Examina detalles: ¿las transacciones se mueven correctamente? ¿Los clientes pueden navegar por la aplicación? ¿Es aceptable el tiempo de repuesta? En

organizaciones muy grandes, BAM es desarrollado por un equipo a parte y es comúnmente llamado centro de control de negocio.

Monitoreo de lote

La mayoría de las empresas lleva a cabo funciones de limpieza reconciliando actividades de negocio durante la noche. Un equipo de calendarización, usualmente localizado fuera del centro de control pero reportando a la misma cadena de supervisión desarrolla la función administrativa de calendarización durante horas laborables. Durante horas fuera de oficina, cuando se requiere que algún programa se ejecute durante la noche, el centro de control debe monitorear los procesamientos de lote.

El monitoreo de lote notifica al equipo de soporte si hay alguna falla. También notifica al correspondiente supervisor si el lote está retrasado y no se completará dentro de los tiempos preestablecidos, lo cual

desembocaría preguntas de los clientes sobre el porqué una orden no fue procesada o porqué su cuenta no está actualizada.

El aseguramiento de que las fallas producidas durante la noche sean resueltas a tiempo para que los procesos también puedan terminar dentro de los tiempos adecuados es una función que es desarrollada de mejor manera por un centro de control. Llevar a cabo esas funciones fuera del centro de control usualmente tiene como resultado que se repiten fallas, retrasos frecuentes y procesos fuera de tiempo. Fallos de lote recurrentes y retrasos constantes hacen que tus clientes lleven sus negocios a compañías más confiables.

Mientras que el monitoreo de los lotes se hace usualmente en el centro de control, la corrección de fallos en los lotes se hace por el equipo de soporte técnico. El soporte técnico de lotes, corregir lo que funciona mal durante el procesamiento de lotes, es una

función que se puede hacer dentro o fuera del centro de control. Un factor determinante puede ser el tamaño del equipo de soporte técnico. Si es lo suficientemente pequeño y el centro de control tiene espacio, una vigilancia gerencial directa sobre esta función es preferible.

Definiciones del monitoreo

E2E (End to End) Nivel de negocio

- Vista de la salud del segmento de negocio independientemente de las plataformas subyacentes.
- Este tipo de monitoreo incluye todos los aspectos del segmento de negocio, desde el nivel del hardware hasta los puntos de entrada presentados al cliente.
- Las alertas detectadas por este tipo de monitoreo son de severidad 1 o severidad 2, donde se detecta el impacto o

inminente impacto sobre el cliente o el negocio.

Nivel de aplicación

- Vista de la salud de las aplicaciones grandes de negocio, incluyendo todas las plataformas y conexiones de red que las soportan.
- Este tipo de monitoreo detecta alertas al nivel de las aplicaciones, desde el nivel del hardware hasta los puntos de entrada y las pantallas iniciales que son presentadas al cliente.
- Las alertas detectadas por este tipo de monitoreo son de severidad 1 o severidad 2, donde se detecta el impacto o inminente impacto sobre el cliente o el negocio.

Nivel de plataforma

- Vista de las plataformas que soportan los diferentes negocios
- Este tipo de monitoreo detecta alertas de hardware o sistema de software, incluye los recursos del sistema (memoria, utilización de CPU) y los componentes (Dasd, conexiones de red e interfaces, unidad de cinta), almacenamiento y software de sistema (sistema operativo, tareas individuales, etc.)
- Las alertas detectadas por este tipo de monitoreo son de severidad 1, severidad 2, severidad 3 y severidad 4, incluye violaciones al umbral en donde no existe impacto pero este es inminente si no se corrige.

Nivel de infraestructura

- Vista de los sistemas, componentes y aplicaciones que dan soporte a los diferentes centros de datos y de negocios.
- Este tipo de monitoreo detecta alertas de hardware o sistema de software, incluye los recursos del sistema y de red (memoria, utilización de CPU) y los componentes (almacenamiento, conexiones de red e interfaces, unidad de medios) y software de sistema (sistema operativo, base de datos, tareas individuales, etc.)
- Las alertas detectadas por este tipo de monitoreo son de severidad 1, severidad 2, severidad 3 y severidad 4, incluye violaciones al umbral en donde no existe impacto pero este es inminente si no se corrige.

- Ejemplos de monitoreo de infraestructura: cortafuegos (firewalls), enrutadores (routers), switches, BigIP, 3DNS, servidores Tivoli, SAN, bases de datos.

Función Dos: Operación de Consolas

Los manuales de operación de consolas que usan hojas de registro y seguimiento son cosa del pasado. Con la gran variedad de herramientas automatizadas que hay en el mercado, o las que pueden ser desarrolladas fácilmente en casa, no es necesario meter comandos en la consola del sistema ni a través de una aplicación que provee acceso remoto a un operador de la consola, excepto en emergencias. Para operaciones diarias, la automatización debe correr todas las funciones relacionadas con la

consola. Si tú estas a cargo de un centro de control en donde todavía se usan hojas de registro, sería bueno que fueras actualizando tu currículo.

Dentro de un centro de control, normalmente, el mismo equipo realiza las dos acciones, monitoreo y las funciones de la consola de operaciones. En los viejos tiempos, los operadores tenían mucho trabajo desde el momento que llegaban hasta que se terminaba su turno, escribiendo comandos en la consola del sistema en respuesta a alertas y mensajes.

Es un modelo insostenible porque requiere personal adicional siempre que la carga de trabajo aumenta. Esa práctica incrementa el número y la duración de los cortes porque los operadores que están ocupados escribiendo comandos son más propensos a no poner atención a alertas de emergencia. Duplicar la carga de

trabajo significa duplicar también el número de colaboradores y, con operadores metiendo comandos habrá retrasos en la respuesta a alertas de emergencia. Esto dará como resultado cortes en los cuales la condición que causa la alerta no sea resuelta a tiempo.

> **El objetivo para la operación de consolas, ya sea dentro de un centro de control o no, debe ser CERO intervenciones manuales.**

Esto significa que nadie debe tocar la consola del sistema excepto en raras ocasiones tales como invocar y confirmar acciones de recuperación de desastres. Hoy en día, con la gama de herramientas automatizadas que tenemos a la mano, la intervención manual ya no es necesaria ni justificada y debe ser eliminada de los centros de control.

Cosas que se deben automatizar o eliminar

Hay muchos procesos manuales que pueden y deben ser automatizados. Entre ellos están:

Acciones de comienzo o cierre de operaciones

Estas deben ser desarrolladas por la aplicación de calendarización o la automatización del sistema. Muchos retrasos en el comienzo de operaciones son debido a cortes de la comunicación. Un e-mail o una llamada de los administradores de la aplicación – ya sea para informar operaciones para empezar procesos nocturnos o para poner disponible la aplicación al comienzo del día – se extrañará, especialmente si el destinatario no está disponible. El corte en las comunicaciones será descubierto eventualmente pero no antes de que el negocio reciba un impacto, por ejemplo en transacciones que hayan sido

procesadas o clientes tratando de acceder a una aplicación que no está disponible.

Mensajes que esperan una respuesta

Eliminar estos mensajes reduce la probabilidad de no recibir mensajes importantes. Muchas aplicaciones de software de sistema producen su propio mensaje de advertencia para proteger al usuario. Algunos te advierten que no empieces cierta aplicación hasta que no esté disponible alguna otra. Algunas otras piden un aparato nuevo después de varios errores de escritura o lectura. Antes de que las herramientas de automatización estuvieran disponibles una práctica común entre desarrolladores de aplicaciones de negocio como manera de implementar dispositivos de seguridad, era mandar un mensaje pidiendo a un operador que respondiera “Y” en el momento preciso, así como cuando los archivos

han sido cerrados o abiertos, o un archivo necesitado ha sido recibido.

Recuperación de tarea iniciada/fallo en línea

Establecer la recuperación de fallas automatizadas asegura que las interrupciones y sus consecuencias sean reducidas al mínimo. Cuando un sistema o una aplicación de negocio fallan, la respuesta normal es intentar reiniciar lo más rápido que se pueda para reducir el impacto lo más posible. En la mayoría de los casos, esto es suficiente para restaurar el servicio, seguido de un análisis de causas de raíz para encontrar y corregir las causas del fallo. En algunas ocasiones debido a rutinas internas de limpieza de la aplicación, dos reinicios son requeridos. Cuando lo anterior se hace manualmente, puede tomar desde algunos minutos hasta varias horas, dependiendo de cuando se detectan las fallas. Se pueden tener retrasos adicionales si el operador no conoce el comando de inicio correcto o manda

un comando incorrecto, por ejemplo el de comienzo de operaciones en vez del de recuperación de inicio, causando peligro en la integridad de la información lo cual toma horas y un número mayor de miembros del personal de soporte para corregirlo.

Una vez que las funciones de la consola son automatizadas, los analistas tienen más tiempo para desarrollar funciones más críticas, tales como monitorear las pantallas de alertas, resolver incidentes abiertos o buscar oportunidades para mejorar los procesos.

Función Tres: Supervisión de incidentes

Supervisión de incidentes es uno de los términos dados al proceso de resolver problemas inmediatamente después de que se presentan, para evitar o reducir el impacto causado por el incidente. Es el proceso de coordinar la recuperación de un fallo

en donde el impacto al negocio está en proceso o es inminente si no se resuelve rápidamente. Incluye asegurar la creación de un ticket de problema, lanzar todas las acciones que son parte de los esfuerzos de recuperación, involucrar a los equipos correspondientes y notificar a la gerencia en los intervalos preestablecidos. Todas estas acciones se deben hacer de forma expedita, dando prioridad a los tiempos.

Cuando el equipo de monitoreo recibe una alerta de una anomalía que afecta la operación correcta de una función o una aplicación, esta es entregada al equipo de supervisión de incidentes. Este tipo de problemas es calificado como incidentes.

Un incidente es algo que ocurre y que afecta la normalidad, por ejemplo, una falla en el suministro de luz en un centro de datos, una computadora o aplicación que se descompone, o una falla en el hardware que afecte la

operación correcta de cualquier cosa que usen tus usuarios. Si el incidente afecta a cierto número de empleados internos, clientes externos o la operación correcta de una función clave o si tiene un impacto financiero importante, entonces, el incidente se convierte en un incidente de severidad alta. El incidente de severidad alta se vuelve una crisis o emergencia si las funciones afectadas suponen un riesgo a la integridad de la empresa; en otras palabras, si estás en riesgo de perder credibilidad de tus clientes o de salir en los periódicos con una nota negativa. (En una situación de emergencia el director corporativo y el director de informática son notificados para asegurar que estén al tanto de la situación dado el caso que empiecen a haber llamadas de clientes a nivel dirección o de la prensa).

La recomendación es ejecutar la supervisión de incidentes desde dentro del centro de control.

Para entender por qué, es necesario entender cuál es el objetivo de la supervisión de incidentes y cuán importante es para los objetivos del centro de control.

> *Si el objetivo principal del centro de control es eliminar o reducir los impactos en la empresa a la cual le da servicio, entonces, la supervisión del centro de control tiene que asegurarse de que el equipo de supervisión de incidentes esté trabajando diligentemente para resolver cualquier incidente importante. Lo anterior es mucho más fácil de hacer cuando este equipo está dentro del centro de control y le reporta a la misma supervisión.*

Llevar la supervisión de un incidente cuando el equipo que está atendiendo el proceso de resolución del incidente no te reporta directamente es muy complicado.

1. El equipo de supervisión de incidentes no sólo debe estar en la misma locación sino que debe reportar directamente al director del centro de control.
2. El director del centro de control es el principal responsable de que se cumplan los objetivos y de que los problemas se resueltos en buen tiempo.
3. Cuando ocurren demasiados incidentes o toma más tiempo su resolución, normalmente, es el director del centro de control el responsable.

Si tú vas a ser el responsable, ¿no te gustaría tener el mando sobre todo el proceso de resolución?, ¿te sientes a gusto tomando la

responsabilidad sobre algo que está fuera de tu control?

Las actividades y responsabilidades más grandes del equipo de supervisión de incidentes incluyen los siguientes:

- Supervisar todos los incidentes de severidad 1 y severidad 2 hasta su resolución.
- Notificar a la dirección y a soporte técnico de los incidentes.
- Crear y actualizar tickets de problemas.
- Abrir y dirigir puentes de conferencia.
- Involucrar a todos los equipos de emergencia y soporte cuando sean necesarios.
- Resolver los tickets de problemas.

Función Cuatro: Soporte Técnico

Siempre será mejor para el negocio y para el centro de control, resolver los problemas lo más rápido posible. Para que eso sea posible, el centro de control que monitorea al personal debe ser capaz de diagnosticar adecuadamente cada alerta para poder tomar las acciones correctivas correctas o para notificar a la ayuda técnica apropiada.

Algunos tipos de fallos pueden ser identificados y corregidos por analistas principales dentro del centro de control sin ayuda de soporte adicional. Esto es particularmente cierto con errores del proceso de lote, como aquellos fallos causados por leer/escribir o errores de espacios. Se ahorra tiempo valioso al desarrollar la función desde el centro de control pero tiene un costo: se harán errores ocasionales que llevaran a un serio incidente visible para el cliente. Con los controles correctos el riesgo puede ser mitigado pero esa es una decisión

que el director del centro de control tendrá que tomar: ¿Debe el personal del centro de control desarrollar soporte técnico de nivel 1?

Para desarrollar soporte de nivel 1, hay dos líneas de pensamiento.

Una es que el diagnóstico inicial y la resolución debe ser desarrollada dentro del centro de control. En otras palabras, el personal del centro de control debe llevar a cabo funciones de soporte de nivel 1: identificar cual es la causa de la alerta o incidente y, tratar de resolverlo. Si se requiere de más conocimientos, contactarán al correspondiente equipo de soporte técnico de nivel 2 (sistema o aplicación).

La segunda línea de pensamiento es que el personal dentro del centro de control haga el diagnóstico inicial y contacte al correspondiente equipo de soporte de nivel 1 o nivel 2 para arreglar el asunto.

Cada línea de pensamiento tiene sus pros y contras, así que, depende del director de operaciones y de la cantidad de soporte que venga desde arriba. El hacer diagnósticos iniciales que determinen la causa del problema, ahorra tiempo al involucrar al equipo de soporte correcto. Esto debe hacerse independientemente de la línea de pensamiento que se escoja. Involucrar al equipo de soporte incorrecto retrasará la resolución del incidente, incrementando la probabilidad de que se convierta en un incidente que afecte a tus clientes.

Tratar de arreglar el problema y cerrar la alerta son cosas totalmente diferentes. Tener a alguien dentro del centro de control que arregle la falla, básicamente usando soporte técnico de nivel 1, tiene sus beneficios pero también conlleva algunos riesgos.

Aquí mostramos los pros y contras para cada línea de pensamiento.

Soporte técnico del centro de control que sólo hace diagnóstico inicial

Pros:

Reduce el riesgo de cometer un error

La persona que tiene la aplicación donde ocurre una falla tendrá más conocimiento del trabajo interno y pasos para recuperar la aplicación y será menos proclive a cometer un error cuando esté reparando la causa de la falla.

Reduce los eventos repetitivos

El responsable tratará de hacer una reparación permanente para evitar situaciones similares en el futuro y para evitar que el evento suceda en otro lado. Evitar que el evento se repita garantiza que la persona no será molestada mientras duerme o cuando se encuentre en actividades sociales personales.

Contras:

Más tiempo para resolver el problema

Existen retrasos en la resolución del problema y la restauración del servicio o del procesamiento de lote cuando el personal investiga a quién le corresponde el evento, contacta a dicha persona y espera a que la persona se ponga online para investigar y corregir el problema.

Perdida de habilidades técnicas

El personal del centro de control empezará a perder sus habilidades técnicas y no aprenderán nuevas habilidades.

Soporte técnico del centro de control que hace diagnóstico inicial y da soporte técnico de nivel 1 (arregla el incidente)

Pros:

Reduce el tiempo de resolución

No hay necesidad de localizar el soporte y esperar a que ellos se conecten para investigar el incidente.

Mejora las habilidades técnicas

Las habilidades del personal mejora y pueden brindar más apoyo.

Cons:

Aumenta el riesgo de errores

Se incrementa la probabilidad de cometer un error crítico que afecte a los clientes, especialmente en cuestiones que no estén documentadas apropiadamente.

Aumenta la repetición de errores

No existe la motivación dentro del personal que tiene que corregir errores que se repiten

por el miedo equivoco de que habrá reducción en el número de personal técnico requerido.

Continúan los errores realizados por los desarrolladores y por los usuarios.

Ya que las correcciones son realizadas por personal del centro de control, los equipos que manejan la aplicación pueden no estar al tanto de las fallas y ser más propensos a seguir repitiendo el mismo error.

Otra consideración que ayuda a determinar en donde se desarrollan las funciones de soporte técnico es el tamaño del equipo de soporte técnico. Una tienda que cuenta con un equipo grande de soporte técnico de nivel 1 puede carecer del espacio necesario para darle cabida a todos dentro del centro de control; y, más aún, esta tienda puede tener algo más de que preocuparse: ¿Por qué hay tantos fallos como para justificar un equipo de soporte técnico grande?

Funciones secundarias

Las funciones secundarias pueden llevarse a cabo dentro o fuera del centro de control, dependiendo de la locación del centro de control y de sus requerimientos presupuestales. Esas funciones incluyen la supervisión del acceso al centro de datos, coordinación y recuperación de negocio o de desastre e iniciación y supervisión de proyecto para mejorar los procesos.

Supervisión del acceso a centro de datos

La mayoría de los centros de control son sitios 24/7 por lo que, en ocasiones, es económico para su personal proveer un servicio de chequeo/detección para todos los que quieran acceder al centro de datos. Es benéfico para el centro de control monitorear y controlar, especialmente en horas fuera de oficina, quién entra y quién sale del centro de datos ya que también es responsable de monitorear el equipo en este lugar. En

la mayoría de los casos, la gente que necesita acceder al centro de datos en horas fuera de oficina son personal de soporte quienes han sido llamados por el mismo centro de control.

Recuperación y coordinación de negocio (desastre)

En la mayoría de los casos, especialmente en los relacionados con problemas en el centro de datos y en la computadora central, el centro de control maneja la coordinación de la recuperación de desastres. La recuperación de negocio o los directores del centro de datos toman la decisión de iniciar los pasos para la recuperación de desastre pero el personal del centro de control es quién ejecuta los pasos iniciales de la recuperación, hace las notificaciones requeridas e involucra al personal de soporte que se requiera.

Iniciación y supervisión de proyecto para mejoras en el proceso

La función de iniciación de proyecto ayuda a garantizar que el centro de control no tenga que hacer trabajos repentinos que nadie estaba esperando. El poner a miembros del equipo en proyectos clave asegura que se tengan en consideración todas las necesidades y requerimientos del centro de control.

El proceso de mejora ayuda a que el centro de control tenga mejora continua y haga recomendaciones a equipos de aplicaciones que tengan problemas para cumplir con sus plazos/fechas límite. El equipo entrega recomendaciones a los comités de estándares basadas en lecciones aprendidas y en análisis detallados de monitoreo y supervisión de incidentes.

- *Es preferible que esta función se desarrolle dentro del centro de control pero es igualmente*

bueno desarrollarla afuera pero en cierta proximidad. El equipo que desarrolle esta función deberá visitar el centro de control para aprender en donde se generan los problemas y que partes requieren más atención.

El músculo operacional y organizacional del liderazgo del centro de control determina en donde se desarrollan algunas de estas funciones. Algunas funciones por su naturaleza pertenecen al centro de control sin duda, tal es el caso del monitoreo. La localización de otras funciones depende de los objetivos del centro de control. En donde se hagan esas funciones depende, a final de cuentas, de la influencia que tenga el líder de departamento con los altos mandos.

Cuando han sido determinadas las funciones dentro del centro de control, ahora puedes empezar a construir la estructura organizacional.

Esta, incluirá a la gente que hace el trabajo diario, supervisores, gerentes y todo aquel que se requiera para que el centro opere adecuadamente.

Una vez que la estructura organizacional está determinada, el siguiente paso es hacer el diseño del centro de control.

Capítulo Tres

Estructura Organizacional

Después de que se han determinado las funciones del centro de control, el siguiente paso es definir sus labores y responsabilidades. Tomadas en su conjunto, los roles y responsabilidades deben ser una combinación de lo siguiente, dependiendo del tipo de centro de control.

Roles y responsabilidades

Supervisión del centro de control

Estos son los roles y responsabilidades para cada supervisor dentro del centro de control.

- **Obtener objetivos preestablecidos**
  Una vez que se han decidido los objetivos para el centro de control, es responsabilidad de cada supervisor asegurar la obtención de los objetivos

generales así como aquellos relacionados con sus funciones específicas.

- **Monitorear, supervisar y controlar el entorno.**

  Monitorear y reaccionar a alertas desarrollando acciones de recuperación de sistema y de su hardware asociado, software de sistema y de aplicación, y calendarización de lote dentro del dominio del centro de control.

  Es responsabilidad del supervisor garantizar que las alertas se atiendan en los tiempos adecuados. El supervisor acepta la culpa por cada interrupción en el servicio debida a omisión o mala atención de alertas o a retrasos excesivos para avisar a los equipos de soporte. El supervisor también es responsable de darle seguimiento a la corrección de deficiencias en el monitoreo de

un sistema o una aplicación que sufran una interrupción que pudiera haber sido evitada si el centro de control hubiese recibido una alerta. Una interrupción prevenible que se da en una aplicación o sistema computacional que no es monitoreado debe ocurrir sólo una vez.

- Garantizar que todos los acuerdos de nivel de servicio (SLAs) o indicadores de calidad (QIs) se cumplan para proveer un servicio consistente a la comunidad de usuarios.

Esta es básicamente una manera de medir que tan bien el centro de control cumple con las obligaciones que tiene con sus usuarios.

Por ejemplo, si la supervisión del centro de control está de acuerdo en que se tenga un sistema para poner precios y hacer inventario en una tienda, que se actualice y

esté disponible a las 8 am cada mañana, entonces, cada vez que el sistema no se actualice ni esté listo a las 8 am contará como perder un proceso clave. (Es irrelevante si la tienda no abre hasta las 9 am y si los sistemas están actualizados y listos antes de esa hora; todavía contará como un proceso perdido toda vez que a las 8 am no se cumpla con SLA).

Un error que cometen los gerentes del centro de control es contar un proceso perdido sólo cuando alguien llama para quejarse. Ese es un camino muy peligroso para tomar ya que las métricas se vuelven discrecionales y subjetivas más que basadas en eventos y mediciones objetivas.

- Trabajar con servicios empresariales para garantizar que los SLAs y los QIs estén estructurados correctamente para proveer ventanas de recuperación máxima sin poner

en riesgo el servicio a la comunidad de usuarios.

Normalmente, un requerimiento cuando se firma un acuerdo SLA o QI es que cada proceso tenga una ventana de recuperación suficiente para que, aún con fallas durante el proceso, la fechas límite puedan ser alcanzadas. Habrá ocasiones en las que un cambio en la aplicación de negocio o en el sistema afecte negativamente un proceso eliminando por completo la ventana de recuperación, provocando que se sobrepasen las fechas límite frecuentemente. Los gerentes deben estar conscientes de esta situación para poder tomar acciones correctivas ya sea negociando nuevas fechas límite o corrigiendo la condición que eliminó la ventana de recuperación.

- Proveer una escalatoria en tiempo real, capacidad de recuperación y restauración por cualquier falla en el servicio; notificar a los equipos de soporte apropiados; y coordinar la recuperación como sea necesario.

  El gerente está encargado de garantizar que los procedimientos de supervisión de incidentes se lleven a cabo en tiempo. En situaciones en las cuales el equipo de supervisión de incidentes está alojado fuera del centro de control, el gerente es, aun así, responsable de que el equipo se ponga en acción tan rápido como sea posible en cada incidente y que las acciones que se lleven a cabo sean las adecuadas. Esta es una de las razones por las cuales es conveniente que el equipo de supervisión de incidentes se

encuentre dentro del centro de control.

- Coordinar y ejecutar el apagado y prendido del sistema cuando sea requerido por cambios aprobados (siguiendo los estándares de procedimiento de control de cambios).

  Hay muchos tipos de cambios en los cuales el equipo operacional dentro del centro de control será requerido para implementar, asistir o coordinar actividades entre los equipos. Los gerentes son los responsables de garantizar que esos cambios sean revisados para su aprobación o rechazo dentro de los tiempos correctos y coordinar las acciones adecuadas para cubrir todos los requerimientos necesarios para llevar a cabo un cambio.

- Escalar problemas mayores y notificar a la dirección – si están en operaciones o el negocio afectado – asegurando que la gente correcta sepa del incidente a tiempo.

- Revisar constantemente procesos existentes e investigar nuevos procesos buscando posibles mejoras de automatización, diseñar e instalar mejoras a proyectos especiales cuando sea necesario. En un entorno de centro de control, la automatización es obligada, especialmente cuando un porcentaje de las interrupciones en el servicio al cliente se debe a errores humanos. Es necesario que los gerentes sean los principales causantes de la automatización y asegurarse de que todos estén conscientes de que automatizar una tarea no

elimina trabajadores sino que les permite a estos trabajadores enfocarse en sus actividades principales. Un gerente que no cree y no promueve la automatización, no tiene nada que hacer dentro de un centro de control.

- Cumplir con las reglas de auditorías, seguridad y regulaciones; garantizar que los procedimientos de un centro de control establecido estén debidamente documentados, actualizados y llevados a cabo.

- Garantizar que los procedimientos de recuperación de desastre estén en su lugar y hayan sido probados para asegurar que cumplen con los requerimientos y que proveen soporte y coordinación a los servicios para empresas o

pruebas para recuperación de desastre en centros de datos o eventos reales. Lo anterior incluye planeación y pruebas de recuperación de desastre para equipo de centro de datos.

- Proveer soporte técnico, consultoría, recomendaciones para mejora de proceso y asistencia de implementación para equipos de aplicación en proyectos mayores y cambios.

  Como el punto focal, el centro de control está en una posición para observar y reunir las mejores prácticas de proyectos y cambios desarrollados por los diferentes grupos con los que interactúa. Asimismo, identificar las prácticas que tienen un efecto negativo en aplicación o en SLA y difundir esa información a todos los grupos les permite a los

gerentes mantener sus ventanas de recuperación lo más grandes que se pueda ayudando a mantener o exceder los objetivos de nivel de servicio.

- Proveer reportes diarios de estatus de la supervisión y métricas, revisándolas diariamente para identificar tendencias y problemas potenciales. Aquí es en donde los problemas potenciales son identificados y atendidos antes de que tengan un impacto negativo en el centro de control o en el negocio mismo. A menos de que los gerentes sepan que pasa diariamente y las tendencias actuales, no podrán resolver problemas sino que estarán ocupados teniendo que explicar porque ciertos problemas no fueron identificados ni atendidos.

- Desarrollar los deberes de recursos humanos como sea necesario para garantizar que se encuentren trabajando la cantidad de personas que se requiera y proveer el necesario entrenamiento inicial y de refresco.

Monitoreo y personal operacional

- Monitorear las pantallas de alertas y resolver todas las situaciones que no impactan a los clientes (usualmente clasificadas como severidad 3 o más alta). Notificar en tiempo a los equipos de soporte correspondientes.

  Estas son sus actividades principales y, cualquier cosa que interfiera con ello debe ser reportada inmediatamente a la supervisión. Cualquier requerimiento de ignorar

alertas debe ser rechazado y notificado a la gerencia.

- Involucra al equipo de supervisión de incidentes en todos los problemas que impactan a los clientes (usualmente clasificados como severidad 1 y 2).
- Se asegura de que se genere un ticket de problema para casa situación y que se actualice si es necesario.
- Garantiza la correcta operación de plataformas y sistemas, aplicaciones operadas en plataformas supervisadas y plataformas de soporte de infraestructura y aplicaciones.
  Esto va de la mano con el monitoreo. Cualquier plataforma, sistema o aplicación supervisada por el equipo debe tener el nivel apropiado de monitoreo para que las alertas sean mandadas

a las pantallas de monitoreo adecuadamente.

- Dar soporte como sea necesario a los equipos de incidentes, cambios y problemas.
- Monitorear procesamiento de lotes.
- Cumplir con las responsabilidades de vigilancia y operación para cumplir con los SLAs.
- Notificar a la gerencia de cualquier potencial ruptura en los SLAs.
- Llevar a cabo funciones de recuperación de desastre.
- Escalar a la supervisión, cualquier evento o equipo que interfiera con la capacidad de llevar a cabo sus deberes.

Supervisión de incidentes

Roles y responsabilidades de los miembros del equipo de supervisión de incidentes:

- Supervisar todos los incidentes de severidad 1y 2 hasta su conclusión.
- Clasificar y categorizar adecuadamente todos los incidentes.
- Actualizar y revisar la base de datos de errores conocidos.
- Notificar a la gerencia y a soporte técnico cuando se necesite.
- Crear (si aún no se hace de manera automatizada o no lo ha hecho la unidad que reporta el incidente) y actualizar tickets de problema de los incidentes.
- Abrir y dirigir puente de conferencias para la resolución de incidentes.
- Involucrar a todos los equipos de soporte y emergencias cuando se requiera.

- Resolver los tickets de problemas.
- Producir reportes de supervisión diarios, semanales y mensuales.
- Medir resultados contra objetivos de negocio y hacer recomendaciones para mejoras.

  Asegura los objetivos a nivel de servicio por medio de resolución de incidentes, notificación a soporte y escalaciones de supervisión.
- Revisar y actualizar regularmente los procesos y procedimientos de la supervisión de incidentes.
- Garantizar que a lo largo de toda la organización esté implementado un proceso de supervisión de incidentes consistente.

Soporte técnico

Roles y responsabilidades de los miembros del equipo de soporte técnico del centro de control:

- Garantizar que los SLAs del procesamiento de lote se cumplan.
- Revisar, analizar y corregir fallos en el procesamiento de lote y otras situaciones que sean necesarias para asegurar que el procesamiento se complete bajo los estándares establecidos.
- Notificar al soporte de aplicación cuando se requiera recuperación de reinicio de lote.
- Garantizar la existencia de un ticket de problema bien documentado por cada fallo que exista (el ticket de problema debe ser creado y asignado al equipo correspondiente por automatización).

- Garantizar la existencia de un registro de cambios de emergencia para cambios en el lote que afecten como la información confidencial es creada, cambiada, guardada y leída.
- Iniciar y dar soporte a proyectos de automatización para eliminar configuraciones manuales e intervenciones, asegurando calendarización automática de producción y de procesamiento de lote por requerimiento.
- Dar soporte e implementar requerimientos de control de cambios de emergencia para la recuperación de fallos en lotes.
- Hacer reportes de supervisión diarios, semanales y mensuales.
- Hacer valoraciones de mejora de proceso continuamente y dar recomendaciones a equipos de aplicación.

- Analizar procesos del centro de control para buscar mejoras.
- Implementar mejoras de procesos usando procedimientos de supervisión de cambios estándar.
- Revisar y actualizar regularmente los procesos y procedimientos del soporte técnico.
- Garantizar que a lo largo de todo el centro de control esté implementado un proceso de supervisión de incidentes consistente.

Capítulo Cuatro

Diseño del centro de control

Hay muchas consideraciones que hacer en el diseño y construcción de un centro de control. El presupuesto es una de las más importantes. Si te vas muy arriba una desagradable sorpresa puede descarrilar tu proyecto: acabarás haciendo pequeñas actualizaciones a tu espacio existente. Si te vas muy abajo puede que no tengas los recursos necesarios para conseguir tus objetivos. Hay un punto medio, y la dificultad reside en encontrar el balance entre 'necesito tener', 'debo tener', 'me gustaría tener' y 'wow'.

En caso de que pienses diferente, hay un valor en algunos 'wow': es una gran herramienta de mercadotecnia (marketing) y es usualmente respaldada por fuertes resultados de previsión de incidentes. El chiste es no exagerar. El propósito del factor 'wow'

es mostrar a tus clientes hasta dónde quieres llegar para salvaguardar sus negocios y clientes, no para impresionar a tu personal o a tus gerentes. Una video conferencia de primer nivel con hologramas en 3D de la persona en el otro lado de la conferencia, no impresionará a tus clientes. Una video-pared en verde a cada lado de sus empresas, lo hará.

Si tu equipo de supervisión de eventos puede acomodar todas las alertas en una sola pantalla de monitoreo, entonces no habrá necesidad para una video-pared. Si tú puedes ver todas las pantallas de monitoreo sin tener que mover tus ojos de una a otra, entonces no hay necesidad de una video-pared. La idea es tener muchos ojos sobre la pantalla de monitoreo todo el tiempo. A menos de que tu centro de control monitoreo sólo unas cuantas empresas y aplicaciones, hacer esto es muy difícil sin una video-pared.

La video-pared le da la posibilidad a unas cuantas personas de monitorear un entorno grande. De una sola mirada la video-pared le puede dar a la gerencia y a cualquier otra persona que entre en el centro de control, la sensación de alivio de un negocio protegido.

Otra consideración importante es el tamaño del entorno a monitorear: la cantidad de centros de datos, sistemas computacionales, sucursales, aplicaciones de negocio, etc. Estos números, en conjunto con la estructura organizacional, nos proporcionarán el tamaño del personal necesario y de la video-pared que, a su vez, determinará el mínimo espacio requerido para el centro de control.

Otra consideración más es el respaldo activo/caliente; esto significa dividir la carga de trabajo entre dos o más centros de control, de manera tal que, al fallar uno de ellos, la carga de trabajo pueda ser llevada por el otro u

otros centros de control; otro caso, podría ser recuperar el centro de control caído en una locación alternativa pero dentro de parámetros específicos de tiempo y sin impactos en el entorno controlado. Los principales factores para decidir que opción implementar son presupuesto y el impacto de pérdidas de tiempo al ejecutar las funciones de un centro de control. Si el centro de control tiene que estar activo todo el tiempo sin importar nada, entonces la mejor opción es dividir la carga de trabajo entre múltiples locaciones que se den respaldo entre ellas.

Durante la etapa de diseño, se debe tomar en cuenta lo siguiente: la planta del edificio, la locación física y otras consideraciones de diseño.

La planta del edificio nos hace decidir si construir, comprar, rentar o usar un espacio existente para el centro de control. Las razones principales para la planta son las funciones que se desarrollarán, número de asientos

requeridos, expectativas de crecimiento (orgánico o mediante adquisición), y requerimientos de recuperación de desastre. Desde luego, el presupuesto manda, excepto, claro, cuando ya has comprobado el valor de tener un centro de control apropiadamente construido y supervisado.

La locación física del centro de control debe ser diferente del ocupado por el equipo y el entorno bajo su control dado que un evento que deshabilite las funciones del centro de datos no deshabilite también las del centro de control. La locación debe tener accesibilidad durante una crisis, es decir, el personal debe poder entrar y salir durante una emergencia. También debe tener alojamiento disponible en algún lugar cercano.

Otras consideraciones para la locación incluyen la habilidad del centro de control para operar durante una crisis donde hay interrupción de la electricidad y las comunicaciones, así

como su habilidad para lanzar procedimientos de recuperación de desastre del centro de control o del centro de datos cuando sea requerido.

En esta etapa es mejor involucrar a una firma de integración de audio/video y a un arquitecto que tenga experiencia en diseño de centros de control.

Seguridad

Debido a la naturaleza crítica de las funciones realizadas, la naturaleza sensible de la información y al nivel de autoridad de las consolas de sistemas activos, un centro de control es usualmente un área altamente restringida. En algunos casos el acceso deberá ser controlado por un portal donde cada persona tendrá que mostrar una autorización antes de que se le permita la entrada. En locaciones donde se necesite un portal de entrada seguro, se debe prevenir que se formen filas por lo que debe haber

accesos múltiples para personas que usen tarjetas de acceso. Debe haber cámaras que registren quién entra y quién sale.

Consideraciones ambientales y de confort

El centro de control debe ser diseñado para operar tan eficientemente como sea posible al mismo tiempo que proporcionar un ambiente confortable al personal que necesita estar alerta por periodos largos. Instalar una video-pared ayuda a reducir el espacio y el personal requerido pero debe ser diseñado a manera que no cause estrés en los colaboradores que la usen. El ambiente también debe limitar el ruido para que dos personas sentadas una al lado de la otra puedan estar viendo la video-pared pero teniendo conversaciones telefónicas independientes.

Consideraciones de diseño

Hay muchas consideraciones de diseño para un centro de control, incluyendo que sea geográficamente amigable y con un equipo de trabajo grande pueda trabajar en un entorno pequeño y abierto de manera confortable y sin afectar el trabajo del otro. Los requerimientos de espacio deben ser determinados, así como la localización, los planos de diseño, el tamaño y el número de pantallas para la video-pared. Además, existen consideraciones en relación a los colaboradores (la duración de sus turnos, la luz, el flujo del aire, los sonidos y el confort.

El centro de control debe ser auto-alimentado con un suplemento de electricidad continuo; una combinación de baterías y generadores para que el equipo de cómputo sensible y crítico nunca se quede sin energía.

Todo dentro del centro de control de estar respaldado (backup), en sitio y

fuera de sitio, para las aplicaciones y los centros de datos. Debe tener equipo y conexiones de red de respaldo y comunicación de voz de respaldo.

También es una buena idea incluir un cuarto de guerra, una locación en donde la gerencia se pueda reunir durante una emergencia sin afectar la labor de los equipos de manejo de crisis e incidentes y las llamadas en conferencia.

Capítulo Cinco

Interacciones del centro de control

El monitoreo y el incidente, el cambio y el manejo de problema, están fuertemente entrelazados y deben trabajar de manera conjunta para garantizar que los incidentes sean evitados o corregidos lo más rápido posible y que no se vuelvan a presentar.

Proceso de monitoreo

El monitoreo debe ser proactivo y no reactivo; su propósito es sonar una alerta cuando algo tiene el potencial de fallar, no para notificar cuando algo ya ha fallado. Alerta a la gente correcta cuando una falla puede ocurrir si no es tomada una acción para corregir una situación que acabe de ocurrir.

Una advertencia de alerta temprana y el monitoreo pueden hacerse de varias maneras y con diferentes herramientas. Una manera es colocando umbrales para que la alerta

sea activada cuando un evento alcance un valor específico. Por ejemplo, se generará una alerta si el disco duro (hard drive) de un servidor con 500 MB de espacio llega a 75 MB libres, en otras palabras, si el 85% del espacio disponible ha sido ocupado. La primera alerta será enviada al centro de control (y, con suerte, al personal de soporte) cuando el espacio disponible en el disco alcance el 15%. Cuando se presente la primera alerta, se debe mandar a alguien a investigar y corregir la situación. Si el incidente no es corregido, se activará una segunda alerta cuando el espacio llegue a 10%, y una tercera cuando llegue a 5%. Si la condición no es corregida, cuando el espacio disponible llegue a cero, el servidor se caerá y tus clientes no podrán realizar las funciones que te generan ingresos. Si tu dejas que eso suceda con frecuencia, tus clientes se llevaran sus negocios a otro lado.

A algunos miembros del equipo de soporte querrán saber cuándo el

espacio disponible alcance, digamos 15%, pero no actuarán hasta que llegue a 10%; le dirán a la persona del centro de control que les hace una llamada que ignore la alerta y que llame de nuevo cuando el espacio disponible llegue a 10%. Esto es un error y siempre que a alguien se le pida que ignore una alerta debe decir que no. Situaciones como la anterior pueden ser encontradas cuando se le manda la alerta del 15% sólo al personal de soporte y las alertas subsecuentes al centro de control. Ignorar alertas en la pantalla de monitoreo de un centro de control, por la razón que sea, es una receta para el desastre; en poco tiempo, las pantallas de monitoreo estarán repletas de alertas no accionables incrementando la probabilidad de que una alerta real no sea observada y que ocurra un corte del servicio.

El espacio disponible en un disco duro es un ejemplo pero el equipo de monitoreo recibirá cientos de alertas diferentes. Todo lo que pueda afectar

la integridad de lo que es responsabilidad del centro de control debe tener una manera de mandar una notificación en caso de que exista una falla potencial antes de que la situación sea crítica.

Otra manera de generar advertencias de alerta temprana es mediante rutinas de reporte de errores internos de las aplicaciones, escogiendo mensajes críticos y desplegándolos en las pantallas de monitoreo. Este tipo de alerta es implementado con la ayuda del equipo de desarrollo de aplicación.

Proceso de manejo de incidentes

Un equipo de supervisión de incidentes con un proceso definido y ejecutado adecuadamente ayuda a garantizar que los problemas sean bien documentados, transmitidos a donde se requiera y resueltos lo más pronto posible. Una de las funciones más importantes del equipo de supervisión de incidentes es documentar cada acción tomada

durante el proceso de supervisión de incidentes. A quién se llamó, quién respondió, quién hizo qué y lo que pasó durante el proceso, todo debe estar documentado en el ticket de problema que es creado para cada evento específico.

Nunca combines los procesos de supervisión de incidentes con los de supervisión de problemas con el mismo equipo. Es un conflicto de intereses muy grande y una ¡receta para el desastre! De hecho, la función de supervisión de problema no debe caer dentro del centro de control sino que debe ser un equipo autónomo que reporte a la alta dirección para evitar cualquier conflicto de intereses entre ellos y los equipos con los que interactúa.

Además de supervisar el proceso de resolución del incidente, el equipo de supervisión de incidente también hace monitoreo, usualmente a un nivel alto, lo que les permite correlacionar impactos de tipo global con un evento

específico o un problema, ayudando así a evitar situaciones globales o a reducir la duración de los cortes.

Proceso de supervisión de cambios

Los centros de control, por su naturaleza, están estrechamente relacionados con el proceso de supervisión de cambios; esto es así por 2 razones: Primera, el equipo de control de cambios opera sólo durante horas de oficina así que la supervisión del centro de control asume algunas de las funciones de vigilancia durante una emergencia para poder resolver incidentes en proceso que puedan afectar a los usuarios. Segunda, muchos de los cambios se realizan en sistemas que ellos mismos supervisan lo cual implica que están directamente interesados en el éxito o fracaso de esos cambios. En algunos casos se requiere la intervención de personal del centro de control para implementar ciertos cambios.

Es en el mejor interés del centro de control tener una relación saludable

con los equipos de supervisión de cambios. Hay muchas instancias en las cuales el personal de supervisión de cambios ve una alerta y detiene un cambio que sería perjudicial para el sistema. Otro beneficio de una buena relación es que los equipos de supervisión de cambios pueden ayudar a implementar y cumplir con estándares determinados por el centro de control a través de iniciativas de mejora de proceso.

Proceso de supervisión de problemas

Un proceso de supervisión de problemas bien manejado ayuda a garantizar que los problemas tengan una solución permanente y que se lleven a cabo las acciones necesarias para que no ocurra en el futuro o para resolver el problema más rápido si hay una recurrencia.

Como parte del proceso de supervisión de problema, es posible que algunas tareas sean asignadas al equipo de supervisión de eventos para implementar monitoreo o para

corregir problemas que podrían haber sido corregidos si hubiera habido un monitoreo.

Las herramientas y procedimientos también deben estar listos para que todos los problemas y acciones correctivas sean documentados y estén disponibles para que el equipo de supervisión de incidentes los puedan utilizar para reducir la duración de una interrupción por error conocido.

Una buena práctica es usar las recomendaciones de ITIL como base para construir cada uno de estos procesos.

ITIL (IT Infraestructure Library; Biblioteca de Infraestructura de IT) es un entramado de las 'mejores prácticas' para los cinco procesos principales usados por la tecnología de la información para identificar, planear, entregar y dar soporte a los servicios de IT. Los cinco procesos principales son: estrategia de servicio, diseño de servicio, transición de

servicio, operación de servicio y mejora continua de servicio. Más información puede ser encontrada en el sitio de ITIL: http://www.itilofficialsite.com

Que hacer y qué no hacer

Que sí hacer.

- Ten procedimientos bien documentados del rol del centro de control en monitoreo, supervisión de cambio, recuperación de desastre, escalamiento, supervisión de incidente, supervisión de seguridad, supervisión de evento y supervisión de problema. Estos procedimientos deben ser seguidos por todos los colaboradores. No debe haber excepciones a menos de que alguien esté trabajando directamente en alguno de los procedimientos.

- Ten instrucciones bien documentadas para los diferentes niveles de severidad. Estos determinarán como debe ser tratada cada interrupción, los tipos y frecuencia de las notificaciones y los puntos de escalamiento. Las definiciones ambiguas pueden traer como resultado notificaciones y escalamientos insuficientes que lleven a retrasos más prolongados en la resolución de un problema mayor. Se deben hacer revisiones frecuentes para asegurar que las instrucciones son correctas.

- Centraliza todo tu monitoreo. Todos los sistemas y aplicaciones que son críticas para la operación de la empresa y sus divisiones a las que se les da soporte, deben ser monitoreadas en el centro

de control. Esto le permite al centro de control determinar rápidamente si un problema es global en su naturaleza y acelerar el proceso de recuperación. Saber que alertas son las que generan la situación cuando se tiene un problema mayor ayuda a identificar los equipos de soporte adecuados que deben ocuparse del problema y reduce la longitud del mismo.

- Estandariza tus herramientas de monitoreo y crea perfiles de 'mejores prácticas' para que ciertas funciones sean completamente automatizadas, tal como adicionar monitoreo a un servidor nuevo.

- Actúa en cada alerta. Cada alerta recibida por el centro de control debe ser atendida. Si

un miembro del personal de soporte dice que se ignore una alerta por la razón que sea, la respuesta debe ser que no. La alerta debe ser documentada con su correspondiente ticket de problema. esa debe ser una 'alerta de una sola vez'. El equipo de soporte debe corregir el sistema de alertas para que las alertas sean disparadas únicamente cuando haya una situación procesable.

- No permitas que un equipo de manera aislada use productos independientes si hay una herramienta de monitoreo estándar para una plataforma dada.
- No permitas revisiones manuales de una función de una aplicación. Confiar en que alguien realice una revisión manual de la funcionalidad de una aplicación genera retrasos y tiene el potencial para

alargar las interrupciones. Los operadores deben ser alertados automáticamente cuando ocurra una excepción que pueda impactar en la funcionalidad de la aplicación.

- No permitas que los equipos de soporte realicen sus propios monitoreos exclusivos. Es posible que algunos equipos quieran hacer sus propios monitoreos: eso no es aceptable. Está bien si quieren ver lo que el centro de control ve; no está bien dejar que ellos realicen monitoreo en vez del centro de control. Los departamentos y equipos que realizan sus propio monitoreo tienden a 'esconder su ropa sucia'. También tienden a hacer reparaciones temporales. Como resultado, tendrás más interrupciones, más tiempo de interrupción y mayor porcentaje de

interrupciones recurrentes. Debido a que no hay vigilancia, la gerencia no tiene idea de la cantidad de interrupciones; los clientes se van con otros proveedores y el director de la empresa se queda preguntándose porqué.

Cuando el centro de control realiza el monitoreo, tiene dos propósitos:

Primero, el centro de control tiene la capacidad para determinar si un problema en un área está afectando otras áreas. Si una línea de comunicación se cae y varios negocios se ponen en rojo, el personal del centro de control sabrá a que equipo de soporte llamar primero. Un equipo monitoreando su propia área podría no darse cuenta de la falla en las comunicaciones y perderá tiempo valioso diagnosticando el problema.

El segundo propósito es transparencia. Los equipos que están siendo observados por otros tienden a funcionar mejor. Cuando algo va mal, realmente buscan una solución permanente para que el problema no vuelva a aparecer.

- No ignores las alertas. Ignorar alertas es una manera segura de tener problemas. En algún momento aparecerá un error y alguien va a ignorar la alerta incorrecta. Evita el problema por completo asegurándote de que las alertas no procesables ni siquiera aparezcan en la pantalla.

- No permitas que las pantallas de monitoreo se llenen de alertas. Cuando esto pasa es muy fácil no ver una alerta crítica. Las alertas deben ser atendidas y corregidas lo antes

posible. No es aceptable que las alertas 'hagan cola' hasta que sea el horario normal de trabajo del equipo de soporte. Si esta condición es aceptable fuera de horas de trabajo entonces la alerta sólo debería ser generada cuando no es aceptable, esto es, cuando hay alguien que pueda resolver el problema. Las alertas que no son atendidas dentro de un tiempo específico deben ser escaladas al siguiente nivel de supervisión.

Capítulo Seis

Automatización

Un centro de control que es capaz de monitorear y controlar los sistemas de información primarios de una organización y de los centros de datos asociados y sus aplicaciones, se encuentra en una posición ideal para dar un valor extra a sus clientes.

Estar en el centro de estas actividades significa que el centro de control tiene la habilidad de influir e impactar en casi todo. Los problemas globales son revisados por el centro de control, retrasos en las aplicaciones e interrupciones, retrasos en procedimientos nocturnos, problemas relacionados con cambios y otros muchos problemas de naturaleza global. De esta manera, cuando el centro de control realiza supervisión de incidentes, mira de reojo el trabajo interno de toda empresa,

aplicación y equipos con los que interactúa.

Desde esta perspectiva, el personal del centro de control tiene el deber de buscar oportunidades para eliminar o reducir prácticas inútiles e iniciar mejora de procesos.

Cuando se buscan oportunidades para mejorar el servicio no debería haber limitaciones; cualquier cosa que caiga bajo la lupa del centro de control, cae bajo la responsabilidad de mejorar del centro de control.

Una de las mejores maneras de mejorar el servicio es a través de la automatización. Por medio de esta, se reducen o eliminan retrasos y problemas causados por la interacción humana. Si tu no estás seguro de cuán útil puede ser la automatización en tu entorno, revisa tus registros de interrupciones: ¿cuántas veces ha habido retrasos en aplicaciones

debido a que un mensaje importante ha pasado inadvertido por horas?, ¿Cuántos incidentes, como doble posteo de órdenes o transacciones, fueron causados por errores en el procedimiento o errores de vigilancia de soporte técnico? La mayoría de estos incidentes pueden ser eliminados o minimizados con el uso de la automatización.

La automatización es aplicable a cualquier tarea realizada por un humano que no requiera pensamiento y análisis. Cualquier proceso repetitivo que siga un patrón específico puede ser automatizado. Es responsabilidad del centro de control con sus clientes, señalar los beneficios de la automatización cada vez que encuentre un proceso manual ineficiente o en donde ocurren errores con frecuencia, independientemente de quién realice dicho proceso.

Hay muchas herramientas para automatizar lo que sea; si una herramienta existente no puede realizar la automatización que necesitas, es muy simple desarrollarla por ti mismo. En estos tiempos no hay excusas para seguir haciendo tareas repetitivas manualmente.

La automatización le permite al personal del centro de control hacer monitoreo en vez de realizar tareas manuales, esto le permite operar mejor con menos gente.

Asimismo, la automatización permite que el centro de control acepte carga de trabajo adicional sin tener que aumentar el personal, el espacio ni el equipo.

Una estrategia de automatización debe incluir lo siguiente:

- Alerta automática y escalamiento.
- Supervisión de sistemas y operaciones de consola

automatizados (es decir, cero intervención manual).

- Trabajo de lote automatizado: calendarización/configuración/ recuperación.
- Ticket de problema y generación de reporte automatizados.
- Servicio de asistencia automatizado: auto servicio.
- Reporte de excepción diaria automatizado.

Alerta automatizada y escalamiento

El propósito de la alerta automatizada y el escalamiento es que todos los sistemas de producción estén monitoreados, que sólo las alertas de producción lleguen a las pantallas de monitoreo del centro de control y para asegurar que las alertas sean resueltas oportunamente.

Aquí hay algunos ejemplos donde la automatización puede ser aplicada efectivamente.

1. Una de las tareas más comunes del personal del centro de control es identificar las alertas y avisar al personal de soporte adecuado. Cualquier retraso en estas acciones puede resultar en un impacto en el cliente o en un impacto más largo. También existe la tecnología para notificar de manera automática a la persona indicada vía celular, teléfono fijo o e-mail o, seguir la cadena de personas a cargo, hasta que alguien sea localizado. El sistema de alerta también notifica a los supervisores del equipo de soporte y al centro de control si los de soporte no responden.

Las llamadas de alerta automáticas a la persona de soporte que recibe las llamadas por el método que él o ella prefiera, por celular o teléfono fijo, pueden ahorrar tiempo valioso y reducir la probabilidad de contactar a la persona incorrecta. Complementado con el

escalamiento automatizado a la persona de respaldo de soporte y luego al gerente de departamento significan la diferencia entre evitar una interrupción o reducir la extensión de una existente.

Un error común que se debe evitar, una vez que el equipo de soporte sabe de una alerta, es esperar indefinidamente a que se investigue la causa de la alerta. Algunos miembros del personal de soporte pierden la noción del tiempo cuando están tratando de corregir una situación complicada, con los minutos convirtiéndose en horas sin muestras de progreso; para evitar que esto suceda, la persona de soporte trabajando en el problema debe reportar el estatus de la situación a cada determinado intervalo, digamos, cada 30 minutos. Después de un número x de intervalos,

dependiendo de la severidad de la alerta, la notificación debe llegar al gerente de soporte.

Automatizar el requerimiento de actualización de estatus y el escalamiento a la gerencia, evitarán que el personal de soporte y del centro de control pierdan la noción del tiempo.

Una vez que estas funciones son automatizadas, se debe observar una considerable reducción en las métricas de duración de las interrupciones.

2. Los días en los que el operador revisaba manualmente una lista de registros para validar que todo estuviera funcionando correctamente, son cosa del pasado. Ahora existe la tecnología para validar automáticamente que una aplicación está trabajando bien, que todos los prerrequisitos y componentes están

disponibles y pueden detectar problemas potenciales y notificarlos al centro de control y al equipo de soporte adecuado por medio de una alerta detallando el problema encontrado.

¿Alguna vez te has sentido frustrado cuando la luz de checar el motor se prende cuando tú sabes muy bien que es un sensor específico el que manda esta señal? Una lista de registro automatizada funciona igual que los numerosos sensores en tu carro, checando constantemente cada componente. Una diferencia importante es que la automatización en vez de decirte que revises la aplicación, te dirá específicamente que sensor detectó el problema y en qué condiciones se encontró.

4. Como parte de una solución automatizada, sincronizar las

alertas con los sistemas de supervisión de cambios e inventario, evitará que se disparen alertas no procesables causadas durante la implementación de un cambio aprobado y puede ayudar a garantizar que todos los sistemas de producción tenga una alerta apropiada.

Todos los departamentos de IT deben requerir que todos los sistemas de producción sean monitoreados. Si tu entorno no tiene ese requerimiento, entonces, tal vez, sea necesaria una revisión de tus estándares de IT como punto de partida. Integrar tu aplicación de monitoreo con tu sistema de inventario hace posible que cada sistema de producción nuevo genere alertas desde el primer día, sin necesidad de que alguien requiera

monitoreo o la implementación de monitoreo nuevo. Lo opuesto sucede con sistemas retirados del servicio: el monitoreo es deshabilitado automáticamente, eliminando la necesidad de un requerimiento formal o que alguien lo deshabilite manualmente.

Supervisión de sistemas automatizados y las operaciones de consola

El propósito de la Supervisión de sistemas automatizados y las operaciones de consola es asegurar que haya cero procesos manuales para todas las tareas cotidianas, permitiendo al personal del centro de control concentrarse en sus funciones principales: prevenir y resolver situaciones dentro del entorno monitoreado.

La automatización del sistema y las operaciones de consola cubren el sistema operativo y productos relacionados. Supresión de mensajes y contestación automática, pseudo-comandos (versiones cortas de comandos largos y complejos para un resultado especifico), inicio y apagado del sistema, operaciones de cinta y recuperación de fallo de aplicación son los focos principales de esta área. Un operador de consola nunca de debe de tener que desarrollar sus actividades cotidianas en una computadora central, de medio rango o un sistema de cómputo del servidor. Toda interacción debe ser debida a una alerta que necesita ser investigada. Todo lo demás debe ser desarrollado por automatización o debe ser eliminado. Cosas como mensajes de estatus de un proceso de lote nocturno, el cual despliega mensajes con información en la consola, puede ser eliminado o mandado únicamente al registro de salida y quitado de la consola. Los

mensajes que vienen del proceso de lote y que piden que se dé 'Yes' si el archivo recibido ha sido recibido, también pueden eliminarse. Hoy en día muchas aplicaciones para programación de lotes pueden realizar esas tareas fácilmente. La automatización del sistema puede rellenar esas pocas instancias que no son cubiertas por la aplicación de programación.

Las operaciones de consola automatizada proveen los mayores beneficios al personal operacional dentro del centro de control. Este tipo de automatización incluye, pero no es limitado a, lo siguiente:

Supresión de mensajes y contestación automática

Los mensajes que van al operador y a las consolas de sistema tienen múltiples efectos adversos. Primero, utilizan energía del procesamiento de sistema que podría servir mejor para las

transacciones de los clientes; segundo, tienden a inundar las pantallas de monitoreo aumentando la probabilidad de que no se detecten alertas críticas. El mejor método es eliminar mensajes innecesarios desde la fuente, recuperando así, energía para el proceso de cómputo y el almacenamiento usados para crear, mostrar y guardar dichos mensajes. Si esto no es posible, entonces, la supresión de mensajes automatizada puede servir para evitar que se muestren los mensajes para que no distraigan la atención del personal de monitoreo y ellos puedan centrarse en los mensajes importantes creados durante los problemas.

Puede haber ciertos mensajes de sistema y aplicaciones que no puedan ser eliminados. Algunos de ellos requieren una respuesta, como cuando una

unidad de cinta recibe un error de lectura o cuando se crean ciertas condiciones. Los mensajes que requieren la respuesta de un operador tienen el potencial de causar retrasos largos si no son vistos y contestados en un período de tiempo corto. Permitir que esos mensajes existan son una invitación a tener problemas y la mayoría pueden ser eliminados con el uso de una programación correcta, cambios en aplicaciones o, como último recurso, a través de la automatización del sistema.

Este tipo de limpieza y automatización:

1. Reduce el número de mensajes enviados al operador de la consola; al reducir el tráfico de mensajes

en las consolas, se incrementa la probabilidad de ver las alertas críticas ya que estas no se hallan escondidas entre cientos de mensajes.

2. Responde automáticamente los mensajes, reduciendo el número de respuestas que genera el operador.

Pseudo comandos, inicio y apagado de sistema

Los pseudo comandos son creados para permitir que procedimientos complejos se ejecuten con un solo comando; por ejemplo, sin automatización puede tomar hasta 50 comandos apagar todas las tareas y aplicaciones

activas en un sistema central; usando pseudo comandos, un operador central oprime un solo botón que desencadena todos los pasos necesarios para el apagado y en una fracción del tiempo. Lo mismo aplica para el inicio del sistema, especialmente después de una caída del sistema, un operador puede iniciar el sistema con un solo comando o el inicio puede estar totalmente automatizado después de una falla de sistema reduciendo considerablemente la duración de la interrupción.

Muchos errores de procedimiento del operador ocurren al tratar de reiniciar un sistema que ha fallado de una computadora central; esto sucede en un entorno con inicio manual, cuando el operador activa el inicio normal de comienzo de día en vez del inicio en modo de

recuperación, indicado después de una falla. La automatización puede detectar una falla en el sistema y activar el comando de inicio adecuado, eliminando por completo ese error de procedimiento que, además, es visible para el cliente en la mayoría de los casos.

Operaciones de cinta

Los centros de datos que utilizan unidades de cinta manuales o automatizadas, ocasionalmente, encuentran errores de lectura o escritura. Cuando esto sucede, el proceso de lote que se está corriendo falla o le indica al operador que seleccione otra unidad a la cual cambiarse; la automatización puede responder a ese cambio de unidad, determinando si existen unidades compatibles disponibles y cambiando la unidad. Una vez que el cambio se completa, la automatización

pondrá fuera de línea la unidad con errores para que sea diagnosticada y generará un ticket de problema.

Muchos retrasos en los procesos de lote nocturnos son causados por requerimientos de cambio generados por un error de lectura o escritura que no son respondidos oportunamente.
Automatizando la función reducimos tiempo de recuperación y eliminamos posibles retrasos futuros ya que se saca de operación la unidad dañada evitando así que otro proceso la utilice, lo cual pasa usualmente cuando estas acciones se realizan manualmente. La creación automática de tickets de problema permite un seguimiento preciso de unidades con fallos a través de métricas diarias, semanales y mensuales.

Recuperación de falla de la aplicación

De vez en cuando y por razones variadas, las aplicaciones se caen, de manera similar a lo que le pasa a una PC. Cuando esto ocurre, el cliente no puede seguir usando la aplicación. Tú empiezas a perder dinero, tus clientes no están contentos y tu servicio de asistencia se llena de llamadas. En estas situaciones la automatización puede estar pre-programada para realizar acciones de recuperación que consigan que la aplicación funcione otra vez y que tus clientes sigan haciendo lo que necesiten. El proceso de recuperación puede ser programado con diagnóstico incluido y pasos para restauración y un número específico de re-intentos. Por ejemplo, si la automatización intenta un reinicio y la

aplicación se cae de nuevo, la automatización puede estar programada para detenerse o para tratar de reiniciar la aplicación por segunda vez usando una opción de inicio diferente.

La recuperación automatizada usualmente recupera la aplicación mientras que los usuarios están tratando de re-entrar al sistema o aún antes de que sean afectados.

Programación de trabajo de lote automatizada y recuperación de fallo automatizada

El propósito de los cambios programados y la recuperación de fallos automatizados es ayudar a los equipos de desarrollo reduciendo tiempos y permitiendo cambios de último momento aún en aplicaciones con cientos de

módulos, así como la reducción de errores.

- La programación automatizada de tareas usando la documentación provista por el proveedor de desarrollo introducida en el proceso de cambio, elimina errores de clave (keying) y reduce considerablemente la cantidad de recursos requeridos para implementar cambios programables; de hecho, la gran mayoría de cambios programables puede ser implementada automáticamente, sin que nadie tenga que intervenir.

Automatizar la función de programación reduce el número de errores clave relacionados con el cambio durante el procesamiento de lote nocturno. Su velocidad mejorada y facilidad también permiten la implementación de entrega de aplicaciones que llegan después de

tiempo pero que son críticas para el negocio o para cumplir con los requerimientos regulatorios.

- La automatización del reinicio y recuperación de fallo de lote puede ser usada en muchos procesos de lote para fallos que no requieren acciones complicadas de recuperación, tales como errores de espacio o lectura/escritura. Esto elimina la probabilidad de error humano y los retrasos mientras el soporte técnico encuentra y corrige las situaciones para reestablecer el proceso de lote.

Generación automatizada de ticket de problema (incidente) y de reporte

Con todas las herramientas disponibles, no hay ninguna razón que justifique a nadie dentro del centro de control que cree un ticket de problema manualmente para una notificación de alerta. Llano y simple: si el sistema puede generar una alerta y mandarla a las pantallas de

monitoreo del centro de control, no hay razón por la cual no pueda generar también un ticket de problema para el evento.

Automatizar la generación de tickets de problema también permite la implementación de estándares para que métricas con valor y reportes puedan ser generados automáticamente, lo cual contribuye a los procesos de supervisión de problemas y de incidentes.

Tener un ticket de problema asegura que todas las alertas sean seguidas como parte de un proceso de supervisión de problemas e incidentes. Los reportes de tendencias ayudan a identificar áreas con problemas recurrentes, ofreciendo la oportunidad de evitar su ocurrencia. Otros beneficios de la automatización de la generación de tickets de problema incluyen:

- La oportunidad de implementar

notificación y escalamiento automatizado.

- Las alertas pueden ser desactivadas desde la pantalla de monitoreo una vez que el ticket de problema ha sido resuelto.
- Reducción de los recursos requeridos para monitorear y reaccionar a las alertas.

Advertencia para cuando se implementen tickets automatizados: filtros y lógica tienen que ser implementados para evitar la generación de una cantidad excesiva de tickets por alertas duplicadas o fallas del sistema. La creación de un número excesivo de alertas le quita propósito al proceso, distorsionan las métricas y los reportes de tendencias, esconden los problemas reales y, eventualmente, son ignoradas por los equipos de soporte quienes sienten

que persiguen fantasmas y no tienen los recursos para supervisar tal cantidad de tickets.

Servicio de asistencia automatizado: auto-servicio

El objetivo de proporcionar una herramienta de auto-servicio al cliente es dejar al centro de control fuera de la parte de asistencia al cliente y enfocada a la prevención de incidentes por medio del monitoreo proactivo.

Como resultado de su función y del acceso que tiene, el personal del centro de control puede tener llamadas del tipo de servicio de asistencia; algunas de esas llamadas tienen que ir al centro de control como parte de las funciones del operador de consola, por ejemplo, reiniciar una impresora. Los requerimientos pueden parecer inofensivos, especialmente cuando

son poco frecuentes. El problema se da cuando el centro de control toma carga de trabajo adicional, con el tiempo, las llamadas se incrementan al punto de que el personal del centro de control puede perder alertas críticas por estar ocupados en esas llamadas.

Convertir las llamadas y los mails a un proceso de auto servicio reduce los requerimientos de personal y es fácil de hacer. A menos de que tu compañía esté nadando en dinero, la administración de IT esté enfocada en hacer un imperio masivo o molestias del tipo de servicio de atención sean infrecuentes, no hay ninguna razón para que el personal del centro de control se dedique a esas actividades. Casi todas las llamadas, e-mails, faxes y requisiciones dirigidas al centro de control, soporte técnico o programación para tareas repetitivas comunes, pueden ser convertidas a un proceso de auto servicio.

Los requerimientos que se pueden convertir a un proceso de auto servicio incluyen:

- Activar una tarea agendada bajo requerimiento. En vez de llamar al centro de control para empezar el proceso de cierre de operaciones, las divisiones del negocio puede empezar el cierre por si solas, eliminando la necesidad de mandar un e-mail o hacer una llamada y posibles retrasos en el proceso de lote.

- Sistema de consulta o estatus del trabajo de lote
  En una tienda, el centro de control y el personal de programación dedican varias horas cada mañana a contestar llamadas de usuarios, desarrolladores y otros que preguntan por el estatus de un trabajo de lote en particular; cuatro horas diarias son

recuperadas al descargar los datos de programación en la base de datos donde los usuarios pueden consultar la información de lotes ellos mismos.

- Requerimiento para acceder a producción
  Muchos lugares hacen este tipo de acceso a producción manualmente para el equipo de soporte técnico y desarrolladores que quieran diagnosticar incidentes activos. Cuando la función es automatizada, usualmente, el requerimiento se hace en la parte delantera y, entonces, se entrega a un empleado y se procesa manualmente. Aunque racionalizar la entrada del requerimiento, ayuda, no es suficiente en términos de tiempos, errores, excepciones de auditoria o requerimientos

de personal. Para implementar esta característica adecuadamente, las dos partes del proceso, al principio y al final, deben ser automatizadas, quitando la interacción humana por completo y, así, todos los requerimientos y problemas asociados a ella.

Una validación en tiempo real de esos requerimientos puede ser desarrollada y registrada automáticamente por la aplicación, validando al mismo tiempo el requerimiento y a la persona haciendo el requerimiento. Algunos de los criterios que pueden ser validados son:

- Un registro/número de cambio aprobado
- Un ticket de problema válido que debe cumplir con criterios de validación específicos.

- Restricciones a un sistema en específico, por ejemplo,
  desarrollo; así como a dispositivos específicos.
- Restricciones al ID de usuario y trabajos de lote de desarrollo.

Otras restricciones que no ocurren con tanta frecuencia pero que distraen al personal de sus labores principales son:

- Actualizar el proceso de lote con entrada de usuario

- Recreación de reporte

- Reinicio de dispositivo (terminales, impresoras, etc.)

- Cancelar un trabajo de lote de desarrollo

- Cancelar o reiniciar ID de usuario

- Empezar o parar una tarea de desarrollo

Cuando implementes una herramienta de auto servicio, asegúrate de que el proceso de fondo esté automatizado. Hay algunas herramientas que sólo automatizan el proceso frontal dejando algunas acciones manuales. La mayoría de los errores, retrasos y necesidad de recursos se dan en la parte del cumplimiento de los procesos de fondo. Para implementar una solución adecuada de auto servicio deben ser automatizados los dos procesos: el frontal de requerimiento y el de fondo de cumplimiento.

Monitoreo Proactivo

Reporte de recepción diaria automatizada

El reporte de excepción te ayuda a estar informado avisándote cuando algo deja de funcionar, en vez de que

te enteres después por otros medios o, peor aún, por medio de tus clientes.

Las cosas cambian con el tiempo y lo que está trabajando ahora puede no estar trabajando bien en 6 meses o hasta días después de que fue implementado.

Una locación pensada que todo estaba trabajando muy bien hasta que un servidor que alojaba una aplicación de negocio crítica falló después de quedarse sin espacio en el disco duro primario; la aplicación de monitoreo había sido configurada para mandar una alerta al centro de control cuando el espacio fuera menor de tres umbrales específicos; una revisión de los registros mostró que no se mandó ninguna alerta a las pantallas de monitoreo. Las pruebas a la aplicación del monitoreo nos revelaron que no estaban generando alertas. Investigaciones posteriores mostraron que la aplicación de monitoreo había dejado de funcionar varios meses antes después de que se habían hecho

cambios en las políticas de seguridad del servidor.

Ese incidente provocó una revisión completa del entorno de monitoreo el cual reveló que el monitoreo no estaba funcionando el 25% del entorno. Naturalmente, el monitoreo fue inmediatamente arreglado en cada uno de estos dispositivos.

Para evitar una recurrencia, fue creado un reporte de excepción diaria que mandaba una notificación al dueño del dispositivo, al supervisor de la aplicación, y al equipo de supervisión del evento para cualquier dispositivo de producción el de las alertas no estuvieran siendo enviadas a las pantallas del monitoreo del centro de control. Este reporte detallaba la razón específica del problema y los posibles cursos de acción para corregir. También fue creado y enviado a los supervisores de cada equipo un resumen semanal de reportes de excepción.

Los reportes de excepción diaria son una buena manera de informar de un problema a las partes responsables. Los reportes con el resumen semanal garantizan que la gerencia esté al tanto de los problemas para poder atender los dispositivos cuando el monitoreo no ha sido arreglado.

Cuando la automatización empieza a ser implementada, se vuelve más fácil la generación de métricas y reportes, permitiendo reportes de uso y excepción diarios más precisos así como reportes de resumen de tendencias.

Automatizar las funciones de tu centro de control tiene muchos beneficios, los más importantes son:

Para la empresa que se está soportando:

- Reducir el número de interrupciones del servicio
- Reducir la duración de las interrupciones del servicio

- Notificación oportuna de emergencias
- Mejora del nivel de servicio al cliente

Para los equipos de soporte técnico y desarrollo:

- Reducir el número de llamados
- Mejorar los tiempos de requerimiento y la precisión, especialmente con el centro de control tiene mucho trabajo y no puede recibir llamadas de los usuarios.
- Reducir los tiempos requeridos para desarrollo y prueba
- Reducir los tiempos de impresión y de otros dispositivos

Para el centro de control:

- Mejorar el alcance de objetivos
- Reducir o eliminar las interrupciones que se pueden evitar con un monitoreo proactivo mejorado.

- Reducir la duración de las interrupciones que son inevitables, tales como falla del hardware o interrupciones en la comunicación.
- La carga de trabajo adicional y los sistemas adicionales pueden ser incorporados sin la necesidad de personal adicional.
- Alivio de la carga de trabajo constante.
- Mejorar el manejo de la lista de contactos.
- Mejorar la documentación de alertas.
- Reducir el número de alertas no procesable.
- Reducir las llamadas al centro de control permitiendo el monitoreo proactivo del entorno.
- Reducir los requerimientos de fax y e-mail al centro de control.

Capítulo Siete

Mejora del proceso

(También conocido como reingeniería u optimización de proceso)

Mejora de proceso, reingeniería de proceso y optimización son términos que requiere al acto de reducir los recursos requeridos para desarrollar una función o tarea. Es el acto de hacer que las cosas funcionen mejor, más rápido, a menor costo y con menos defectos.

Si tú quitas un paso irrelevante de un sistema de procesamiento de órdenes,

ahorras 30 minutos por orden, y eso es una mejora de proceso. Por otro lado, si tu eliminas el proceso de ordenes completamente haciendo que las ordenes se generen automáticamente al hacer el requerimiento del proceso, eliminas días o hasta semanas en tu proceso de adquisiciones. De esta manera tú optimizas el sistema completo de adquisición.

Aunque las pequeñas mejoras de proceso individuales son buenas y deben hacerse cuando sea posible, una optimización completa debe ser el objetivo ideal. Toma por ejemplo un sistema de Recursos Humanos que necesita 8 horas para generar la nómina de todos los empleados de la compañía A. ¿Qué pasa si uno de los desarrolladores del sistema encuentra una mejora de proceso que reduce el tiempo a 7 horas? Bajo circunstancias normales ese ahorro de 1 hora sería una mejora importante, pero ¿Qué tal si el sistema de nómina es capaz de completar la tarea en 4 horas? Un

esfuerzo de optimización de proceso miraría al sistema completo de RH y no solo un paso dentro del proceso de pago de nómina para encontrar una manera más eficiente que puede funcionar todo el sistema. Una mejora aquí y allá está bien si tú estás bien aunque el sistema se tarde 7 horas y no estás preocupado por los gastos. Recuerda, optimizando el proceso y reduciendo el tiempo de 8 horas a 4 horas también reducen a la mitad los recursos usados permitiendo que otros procesos usen esos recursos y posiblemente también funcionen más rápido.

Las mejoras de proceso se enfocan en un proceso individual para ver cómo puede ser mejorado están bien si no tienes problemas económicos y no estás preocupado por los gastos y el crecimiento. Esa noción ya no encaja con el actual ambiente corporativo de crecimiento mientras que limitas o reduces gastos. Aunque las pequeñas mejoras aisladas pueden ayudar a ciertos procesos y pueden resultar en

alguna reducción de gastos, no van tan lejos como podrían o deberían.

La parte más difícil y crucial de un esfuerzo de optimización es determinar el alcance del proceso bajo revisión. Si revisas un subconjunto del proceso completo puedes terminar con solo algunas mejoras de proceso; si abarcas demasiado en tu revisión, puedes terminar con pasos que no se acoplan como conjunto y con un esfuerzo fallido. Por ejemplo, para documentar el flujo del proceso para hacer un huevo para desayunar, ¿Dónde empiezas? ¿Empiezas con romper el huevo? ¿De dónde vino el huevo? ¿Empiezas por tomar el huevo del refrigerador? ¿Cómo llegó al refrigerador? ¿Empiezas en la tienda? ¿Qué tal salir de la casa para ir a la tienda? ¿Cuál es el mejor punto de inicio para el flujo del proceso?

Obviamente esta no es una pregunta fácil y es la razón por la cual hay muchas pequeñas mejoras de proceso individuales pero muy pocas

optimizaciones de funciones o de procesos completos. Esto es lo que distingue a las grandes compañías que tienen ganancias más grandes que sus competidores.

El objetivo debe ser optimización integral de proceso la cual abarca el flujo de trabajo de principio a fin. Para conseguir una optimización integral de proceso deber haber muchas pequeñas mejoras de proceso o un esfuerzo mayor de reingeniería. Algunos sistemas estarán diseñados óptimamente y sólo se encontrarán unas cuantas oportunidades de mejoras de proceso; otros sistemas requerirán reingeniería completa que puede que no suceder debido a consideraciones de presupuesto.

El primer paso en el proceso es desarrollar un diagrama de flujo del flujo de trabajo completo. La parte más importante de este paso es determinar exactamente el primer paso. No considerar algunos de los pasos y escoger el punto de partida

erróneo para que esto sea una simple mejora en vez de una optimización de proceso global.

Lo siguiente es determinar el último paso en el proceso; si escoges el paso incorrecto; el proceso no quedará tan simplificado como tú hubieras querido. Ponemos el ejemplo del huevo para el desayuno ¿Cuándo está terminado? ¿Cuándo el plato está enfrente de ti? ¿Qué hay del jugo o el pan tostado? ¿Qué pasa con la servilleta, la sal, el cuchillo y el tenedor? Si tu fueras el cocinero ¿Cuál sería tu último paso?: Poner el huevo en el plato, llamar para que lo recojan o cuándo se llevan el plato?

Este ejemplo resalta la importancia de encontrar el punto de inicio correcto:

> *El equipo de supervisión de eventos en una tienda estaba recibiendo muchas quejas por la lenta implementación del nuevo monitoreo. Los equipos de desarrollo de aplicación de soporte técnico estaban*

frustrados por no tener el monitoreo instalado en los nuevos servidores y en las aplicaciones a tiempo. En algunas ocasiones el lanzamiento del producto se detuvo varias semanas hasta que el monitoreo fue habilitado; en otras fueron colocadas en producción sin monitoreo y se habilitó la generación de alertas, dejando al negocio vulnerable a interrupciones que, de otra manera, podrían haber sido evitadas.

Los miembros del personal de la supervisión de eventos también estaban frustrados debido a que la gerencia se rehusó a contratar personal adicional para manejar de mejor manera la carga de trabajo. Antes que acceder a contratar más colaboradores la gerencia preguntó al equipo responsable del trabajo en la

herramienta de monitoreo como el equipo de ingeniería, que vieran si se podían hacer mejoras para reducir el tiempo de implementación del nuevo monitoreo.

El equipo de ingeniería revisó cuidadosamente el proceso desarrollado por el equipo de supervisión de evento para requerir nuevo monitoreo y fue capaz de simplificarlo, reduciendo el tiempo para habilitar nuevo monitoreo de 1 hora a 15 minutos. Con frecuencia, mensualmente debido a documentación obsoleta, un administrador del servidor instala la versión incorrecta de la herramienta del monitoreo. Cuando eso pasa, habilitar el monitoreo para ese servidor en particular y su aplicación tomará días.

Una vez que las mejoras para el proceso de requerimiento del

nuevo monitoreo fueron implementadas, el trabajo atrasado para el nuevo monitoreo bajó de 2 semanas a 1 semana.

Dos meses después la carga de trabajo se incrementó como resultado de una actualización del hardware. Pocas semanas después de esta actualización el trabajo atrasado para el nuevo monitoreo era de 3 semanas.

Un mes después, los negocios se quejaron con la gerencia de IT por el pobre desempeño del centro de control después de que la supervisión del problema notara que varias interrupciones que impactaron a una gran cantidad de clientes podrían haber sido evitadas si el monitoreo hubiera estado habilitado.

Se llamó a un equipo de mejora de proceso el cual realizó

completamente al equipo de supervisión de evento y al proceso que se llevaba a cabo. El equipo identificó como inicio del proceso el punto cuando un nuevo servidor empieza a ser configurado con el sistema operativo y software requerido, y el final cuando el servidor se clasifica como producción en el sistema de clasificación de inventario.

La solución que fue desarrollada e implementada automatizó completamente todo el proceso. Se crearon perfiles de mejor practica de monitoreo. La herramienta de monitoreo fue incluida en el sistema de inventarios e incluida en el estándar para instalar cada tipo de servidor; esto significa que el monitoreo sería instalado automáticamente inmediatamente después de

que el sistema operativo fuera instalado.

En el curso de la noche el trabajo atrasado desapareció. Con el 75% de la carga de trabajo eliminada, el equipo de supervisión de evento pudo reducir su personal 25% y utilizar otro 25% en proyectos de mejora de proceso. Los miembros del equipo de aplicación y soporte tuvieron más tiempo para enfocarse en sus funciones principales porque ya no tuvieron que hacer requerimiento para el nuevo monitoreo, instalar software para nuevo monitoreo o deshabilitar versiones incorrectas.

Como puedes ver, pequeñas mejoras producirán algunos beneficios pero no harán una gran diferencia.

Puedes leer más detalles en relación al ejemplo

mencionado arriba en el caso de estudio No. 1 dentro del capítulo 10.

La mejor manera de empezar es encontrar un factor común a todas las partes individuales que estás tratando de optimizar. Para algunos, podría ser el proceso de cambio; para otros puede ser el proceso de aprobación, el sistema de inventario o compras. Cada esfuerzo de optimización necesita considerar lo anterior cuidadosamente porque el factor común es donde la mayoría de las mejoras y cambios se originarán y donde serán más efectivas. El factor común determinará qué modificaciones son necesarias en otros puntos.

Si no hay un factor común entonces tienes que examinar si las diferentes interacciones están realmente interconectadas dentro del flujo de proceso o si hay un paso que no debería ser parte del proceso. Si al final de la revisión se determina que todas las interacciones son necesarias

entonces tú llegas al primer punto de decisión: ¿Alguna de las interacciones debe ser alterada para convertirla en el factor común y convertir todas las demás en sub puntos o, se necesita desarrollar un factor común?

Si ya hay múltiples interacciones, cada una representando a una herramienta diferente, en el flujo de proceso y ninguna de ellas se puede eliminar, lo último que quieres hacer es introducir otra herramienta que necesite desarrollo, soporte y mantenimiento. Si una o más herramientas pueden ser eliminadas entonces el ahorro conseguido con la optimización justificará la introducción de la nueva herramienta.

Un factor muy importante a recordar dentro de cualquier proyecto de optimización es el enfoque y KISS (Keep It Simple, Stupid); no lo hagas más difícil de lo que es. Evitar formar comités o grupos grandes como parte de la fase de planeación e investigación; estos crean un efecto de

burocracia que tiene un gran impacto en el éxito del proyecto. El proyecto necesita ser dirigido por una persona o un grupo pequeño (tres o cuatro miembros) con la autoridad de determinar la dirección a seguir. Por supuesto que ellos necesitarán la ayuda de un gran número de personas y asistencia de las diferentes funciones que se están analizando pero el líder del proyecto debe tener el apoyo de la alta dirección llevar a cabo decisiones que puedan molestar a algunas personas.

Cuando escribas los preliminares de tu propuesta asegúrate de incluir los beneficios de cada recomendación de optimización que estás haciendo. ¿Qué objeto tendría todo tu trabajo si las optimizaciones no son implementadas? Para que tus recomendaciones de optimización trabajen, tienen que ser implementadas. Hay varias características que aumentarán tu probabilidad de éxito; si no las tienes deberías aprender a desarrollarlas: Ser

persuasivo, no aceptar un no como respuesta y saber cómo escalar.

Tu propuesta debe responder estas 6 preguntas:

1. **¿Quién es afectado?**
2. **¿Cuál es el cambio?**
3. **¿Cuándo debe ser hecho el cambio?**
4. **¿Dónde debe ser hecho el cambio?**
5. **¿Por qué debe ser hecho el cambio?**
6. **¿Cómo debe ser hecho el cambio?**

Durante el proceso, el equipo de proyecto se encontrará con procesos individuales o dueños de herramientas que no quieren ceder su poder, se pondrán en contra de cualquier intento de invasión de subdominio; estas son personas que necesitan estar en control o fabricantes de armas que ven esto como una amenaza a su poder. El número de excusas que pondrán para evitar cualquier automatización exterior o

influencia sobre sus dominios será inacabable; por ejemplo, dirán cosas tales como:

1. No puedes garantizar la integridad de la información.
2. Esto no cumple con nuestros estándares.
3. Es una violación de a la auditoria.
4. Nuestro sistema será susceptible a la perdida de información o corrupción.
5. El desempeño se volverá insoportable.
6. Tiene que ser hecho manualmente, de otra manera a la gente se le olvidará que hacer si la automatización falla.
7. Mi gerencia no me permitirá hacer esto.
8. No tenemos ni los recursos ni el tiempo para hacer esto.

Aquí es donde entra el efecto del padrino. Para poder complementar estas optimizaciones necesitarás apoyo a nivel directivo. Este apoyo debe ser tan importante como para vencer las objeciones como las que hemos mencionado.

También te encontrarás con gerentes que tendrán razones legítimas por las cuales no puedan ayudarte, la más grande de ellas será la falta de recursos. Aquí tienes varias opciones para atacar este problema:

1. Ofrece a tu equipo y a ti mismo para completar el trabajo requerido.
   Documenta claramente qué cambios es necesario hacer, paso por paso, en un documento tipo diagrama de flujo. En donde sea posible asigna tareas a los miembros de tu equipo o a un equipo externo que haya sido programado para apoyar tu proyecto de optimización.

2. Ofrece a tu equipo y a ti mismo para realizar actividades cotidianas.

   Si el trabajo requerido es demasiado técnico o especializado y debe ser hecho por un miembro de ese equipo de supervisión, ofrécete a realizar actividades de tipo genérico. Puede ser que no puedas librar los recursos al 100% pero es posible que si puedas intercambiar varias horas de tu tiempo aquí y allá para su tiempo haciendo algunas actividades no técnicas.

3. Ofrece ayuda temporal para realizar los cambios requeridos o para descargar trabajo cotidiano para liberar en recursos. Ya que el proyecto de optimización tendrá muchos

ahorros significativos a largo plazo (ahorro en costos, satisfacción del cliente o reducción de errores), la gerencia, en la mayoría de los casos, no se podrá contratar uno o dos empleados eventuales por tiempo limitado. El dinero invertido será más que compensado por las mejoras que se obtendrán con esta optimización.

En algunos casos la buena voluntad generada con las sugerencias mencionadas puede ser suficiente para que el gerente reasigne la carga de trabajo de su personal para aceptar tus propuestas de ayuda.

Si una de las razones mencionadas influye en el gerente, ahora habrá que acercarse a su gestión para ver si las prioridades de trabajo y su equipo pueden ser ajustadas o cambiadas; habrá situaciones en donde no se pueda aplicar nada de

lo mencionado arriba debido a la naturaleza del trabajo o a que la gerencia no es capaz de periodizar la carga de trabajo, esto es, que hay mucho trabajo y no suficiente personal o tiempo. Estos serán departamentos que están saturados; su carga de trabajo aumenta consistentemente pero el tamaño de su personal no cambia.

Ve las cosas de la manera más simple; no trates de complicar un proceso que debe ser simple; no aceptes un no por respuesta; recuerda el enfoque KISS. Algunas veces es mejor se ignorante del aspecto técnico o de limitaciones sobre lo que estás viendo. Cuando escuchas algo como “Eso no puede hacerse”, pregunta por qué no. Si ese producto en particular no puede hacerse, ¿Hay alguna razón por la cual el producto no pueda cambiarse? Si sí hay, tal vez deba ser desarrollada una interface que pueda completar el mismo

objetivo. Si hay un vendedor externo o un producto

En algunos casos la buena voluntad generada con las sugerencias mencionadas puede ser suficiente para que el gerente reasigne la carga de trabajo de su personal para aceptar tus propuestas de ayuda.

Si una de las razones mencionadas influye en el gerente, ahora habrá que acercarse a su gestión para ver si las prioridades de trabajo y su equipo pueden ser ajustadas o cambiadas; habrá situaciones en donde no se pueda aplicar nada de lo mencionado arriba debido a la naturaleza del trabajo o a que la gerencia no es capaz de periodizar la carga de trabajo, esto es, que hay mucho trabajo y no suficiente personal o tiempo. Estos serán departamentos que están saturados; su carga de trabajo

aumenta consistentemente pero el tamaño de su personal no cambia.

Ve las cosas de la manera más simple; no trates de complicar un proceso que debe ser simple; no aceptes un no por respuesta; recuerda el enfoque KISS. Algunas veces es mejor se ignorante del aspecto técnico o de limitaciones sobre lo que estás viendo. Cuando escuchas algo como “Eso no puede hacerse”, pregunta por qué no. Si ese producto en particular no puede hacerse, ¿Hay alguna razón por la cual el producto no pueda cambiarse? Si sí hay, tal vez deba ser desarrollada una interface que pueda completar el mismo objetivo. Si hay un vendedor externo o un producto off-the-shelf, contacta a la compañía que desarrolló el producto. La idea de las compañías desarrollarán las mejoras que tú necesites por una tarifa establecida. Si el requerimiento tiene el potencial de beneficiar a otros clientes tú

debes negociar un buen descuento a cambio de dejar que el vendedor incorpore las mejoras en sus productos para sus futuras ventas.

Recomendaciones de mejora

Temas centrales

Identificar todas las tareas manuales

Realizar el registro de sistema para las entradas del operador.

- A menos de que sea para activar recuperación de negocio, nadie debe ingresar comandos en las consolas de sistemas; cualquiera que lo haga parecerá en el registro del sistema.

Rastrear todas las llamadas entrantes.

- Las únicas llamadas que entren al centro de control pueden ser para reportar un problema actual o potencial. En una llamada del tipo de servicio de asistencia, (como reiniciar una impresora o una contraseña de usuario, debe hacerse al centro de control).

Revisar los registros a auditorias programación y aplicación para todas las aplicaciones manuales.

- Pedir al personal que documente todas las actividades manuales solo dará resultados parciales; algunos pueden estar demasiado ocupados como para documentar todo y otros pueden hacer cosas

en piloto automático, sin darle mucha importancia a algunas actividades o pensando que no vale la pena mencionarlas. También habrá otros haciendo "favores y favores" (cosas que no deberían hacer) que no documentarán.

Identificar fallas de lote por tipos

Utilizar auto reinicio para todos los errores de tipo lectura/escritura y fallas de sistema para todos los trabajos que pueden ser reiniciados desde el comienzo sin ninguna acción de intervención.

- Algunas aplicaciones de programación automatizadas tienen la capacitada de reiniciar automáticamente un proceso de lote fallido basándose en el tipo de

falla. Los reinicios automatizados, con su correspondiente ticket de problema, reducen los retrasos de procesamiento y evitan la probabilidad de error del soporte técnico.

Adoptar y reforzar los estándares JCL para la utilización de espacio y otras mejores prácticas apuntan a reducir los tiempos de procesamiento y las fallas.

- Los estándares también ayudan a reducir errores durante la implementación de cambio y los tiempos de aseguramiento de la calidad por que las herramientas pueden ser utilizadas para efectuar verificaciones automáticas.

Asegurar que todos los conjuntos de datos estén manejados por un paquete de gestión del espacio, tal como SMS.

Usando clasificaciones de información global para cada tipo de gestión de espacios elimina la necesidad de una gestión de espacio específica; por ejemplo, usando clases de datos (pequeño, grande, etc.) reduce la cantidad de fallas relacionadas al espacio.

Instalar la generación de tickets de problemas y acciones de recuperación automatizada donde sea posible.

Las fallas en el lote de producción y tareas iniciadas son candidatas ideales para la recuperación automatizada porque, usualmente, sólo requieren un reinicio directo sin ninguna modificación. Para tareas iniciadas, la automatización puede ser programada para intentar un número específico de reinicios o para usar diferentes parámetros antes de mandar una alerta a las pantallas de monitoreo del centro de control.

Las fallas del lote debidas a errores de hardware ocurren de vez en cuando.

La automatización puede desactivar un dispositivo si encuentra algún error o tomar pasos preventivos para corregir la situación aún antes de que ocurra una falla.

Además de llevar a cabo acciones de recuperación, la automatización puede documentar totalmente el error y las acciones subsecuentes que se hayan tomado en el sistema de tickets de problema.

Identificar todas las interrupciones en el proceso de lote.

Utilizar la aplicación de automatización y programación para eliminar interrupciones el proceso de lote que son dependientes de las acciones de un operador, tales como inicio/cierre de tareas o apertura/cierre de archivos. La eliminación de estas interrupciones reduce el tiempo requerido para completar procesamientos nocturnos y evita la posibilidad de que a alguien se le olvide realizar una acción requerida.

Implementar procesos de autoservicio para permitir a los usuarios realizar activaciones

Para cosas como procesamientos de cierre de actividad o cálculo de totales, permitir que los usuarios activen automáticamente la continuación del proceso en vez de que llamen o manden e-mail al centro de control para que haga esa función.

Por ejemplo algunas áreas requieren de un departamento de validación para comparar los totales generados por lote contra los totales esperados por los clientes para asegurar que todos los archivos requeridos hayan sido recibidos y procesados adecuadamente; cuando están satisfechos unos resultados, usualmente, se hace una llamada al centro de control para que este procesamiento de lote se reanude. En vez de este proceso de dos pasos, provee al departamento de validación un método en el cual la aprobación automáticamente reanude el proceso

de lote, eliminando la necesidad de la llamada y el riesgo de retraso.

Convertir la lista de verificación en una pantalla de monitoreo de actualización automática en tiempo real

Casi todas las acciones que hace una persona en un sistema de cómputo para validar algo pueden ser automatizadas. Muchas de las herramientas tienen la capacidad de cambiar el color de la barra de estado a verde si todo está trabajando adecuadamente, cambiar el color a rojo si se encuentra una excepción, crear un ticket de problema si es necesario y mandar una alerta a las pantallas de monitoreo.

Implementar un portal de autoservicio avanzado en la web

Si tu centro de control se ha vuelto un servicio de asistencia, un portal de autoservicio por internet puede ayudar a que vuelva a ser un centro de

monitoreo y prevención de incidentes. Hay muchas herramientas que pueden automatizar la mayoría de esas funciones o puedes conseguir una herramienta personalizada que cubra tus necesidades específicas.

Algunos de los procesos son candidatos ideales para el autoservicio son las llamadas, e-mails, faxes y requerimientos al hechos al centro de control, soporte técnico y equipos de programación para tareas repetitivas comunes.

Aquí hay algunos ejemplos de este tipo de requerimientos:

- Validación y aprobación de ID funcional (emergencia)
- Sistema UAT y aplicación de encendido o apagado
- Iniciación de trabajo programado bajo requerimiento
- Estatus de sistema de consumo

- Estatus de trabajo de lote de consumo
- Actualización de proceso de lote con entrada de usuario
- Recreación de reporte de lote
- Reinicio de dispositivos (terminales, impresoras, etc.)
- Cancelación de un trabajo de lote de desarrollo
- Cancelación de IDs de usuario
- Iniciar o detener una tarea de desarrollo

Vigilancia de alto nivel del proceso a seguir con oportunidades de mejora

- Identificar áreas problemáticas
- Determinar objetivos
- Priorizar
- Procesos existentes de mapeo
- Mapear nuevos procesos

- Determinar cómo implementar y medir los nuevos proceso
- Implementar mejoras

Puede ser una buena idea involucrar ayuda externa cuando se haga automatización y mejora de proceso por primera vez. Hay muchos consultores y firmas de consultoría, grandes y chicos, que pueden ayudarte a empezar a desarrollar un proceso que dé seguimiento a la iniciativa.

Capítulo Ocho

Métricas (Estadísticas) (KPI)

Medir lo que haces es casi tan importante como hacerlo. Métricas, la colección de estadísticas clave (fundamentales) o indicadores clave de desempeño (rendimiento) (KPI), Las métricas son como se juzga el desempeño. De la misma manera en que se mide el desempeño de un colaborador por su alcance de objetivos, un centro de control mide su desempeño con métricas específicas. Las métricas adecuadas que permiten determinar qué tan efectivo es tu centro de control comparar el rendimiento entre centros de control de una manera significativa.

Las métricas también son necesarias para medir la efectividad de las mejoras de proceso de un centro de control. El uso de métricas adecuadas es crucial para mostrar el valor del derivado de un centro de control supervisado de manera efectiva. Vamos a ver un caso de estudio en el uso de las métricas.

> *Una empresa que busca reducir gastos contrató consultores para medir su eficiencia. Los expertos en eficiencia vinieron y empezaron por repartir hojas de registro a cada colaborador para que ellos escribieran todo lo que hacían cotidianamente. Los trabajadores que tuvieron tiempo, llenaron las hojas completamente, asegurándose de poner todo lo que hacían durante el día; los colaboradores en departamentos en los que repartieron las hojas al final tuvieron muy poco tiempo para*

llenarlas y dejaron muchos huecos.

Al final de la revisión de eficiencia, se concluyó que estos últimos departamentos tenían muchos colaboradores y que era necesario hacer recorte de personal. A los departamentos que tenían exceso de personal les dijeron que eran muy eficientes y no necesitaban hacer recorte.

Dos centros de control fueron revisados como parte de ese ejercicio:

El primero supervisaba 6 computadoras centrales alojando algunas aplicaciones que eran requeridas solo durante horas de oficina,

empleaba 60 trabajadores de tiempo completo. Los consultores para la revisión de la eficiencia determinaron que no había necesidad de recortes.

El segundo centro de control supervisaba 50 computadoras centrales alojando cientos de aplicaciones con operaciones que eran requeridas casi 24/7. La mayoría de las aplicaciones no estaban disponibles únicamente por 4 horas los domingos por la mañana; notó los cambios de sistema requeridos fueron hechos y varios de los que se requerían con disponibilidad 24/7 tuvieron que ser movidos a sistemas de respaldo para implementar cualquier cambio requerido. Este centro de control tenía 40 trabajadores de tiempo completo. La compañía de revisión de eficiencia determinó que tenía

exceso de personal y necesitaba un recorte del 30%.

Aquí es donde aprendemos el valor de las métricas y como pueden ser manipuladas para cubrir una necesidad específica. El primer centro de control arrojó métricas que mostraron cuánto trabajaban; el segundo centro de control arrojó métricas que mostraban productividad del sistema. La primera desarrollaba una gran cantidad de trabajo así que medir la productividad hubiera sido muy benéfico para él. El segundo midió productividad para mostrar todas las mejoras de proceso que se habían hecho y lo eficientes que eran. Para gente externa, incluyendo los expertos en eficiencia, el primer centro de control era más productivo merecía mejor valoración.

Los departamentos con múltiples sitios, la mejor práctica es estandarizar las métricas y los reportes a través de la mesa directiva para garantizar que estás comparando manzanas con

manzanas y naranjas con naranjas. El equipo que desarrolla la función no debe ser el mismo que determine qué medir y qué métricas usar. Esto se le debe asignar a un equipo a parte así como distribuir la información y asegurarse de que las métricas son aplicadas de manera uniforme a cada equipo dentro de los centros de control que desarrollan la misma función.

Aquí tenemos un ejemplo de lo que hay que medir y reportar para un centro de control de infraestructura:

Número de clientes servidos por sistema supervisado

El número total de clientes servidos por los sistemas bajo tu supervisión es una muy buena métrica. Este número también es muy bueno como tendencia. Toma en cuenta que los números en sí mismos no dan un panorama completo. Ocho millones de usuarios en una solo computadora

central es mucho más impresionante que ocho mil; sin embargo, esto no sería verdad si los 8 millones fueran clientes individuales a los 8 mil fueran clientes corporativos (cada uno manejando miles de clientes en tu sistema).

Transacciones ejecutadas y tipos

Este número va de la mano con el número de clientes y refleja la actividad realizada por dichos clientes. Esta métrica probablemente mostrará mucho más transacciones ejecutadas en la computadora central con los clientes corporativos.

Notificaciones y escalamientos

Estos número son difíciles de agrupar si las notificaciones y escalamientos se llevan a cabo manualmente; si están automatizados, entonces, el número de notificaciones debe ser casi el mismo que el número de alertas. Un número alto de escalamientos debe preocupar a la gerencia: el número de escalamientos representa las veces

que las alertas no fueron respondidas y tuvieron que ser escalas al siguiente nivel, así como las veces en las que se tuvo que hacer escalamiento debido a que un miembro del equipo de soporte extendió el tiempo establecido para resolver un incidente.

Alertas

Este número representa la cantidad total de alertas que aparecieron en las pantallas de monitoreo del centro de control. En un centro de control apropiadamente configurado, cada una de esas alertas generó trabajo para el personal de monitoreo así como para los equipos de soporte. Un número muy alto es un buen indicador de problemas con la aplicación de monitoreo o en algún lugar del proceso de monitoreo. Un número alto usualmente significa que se están enviando muchas alertas falsas o no ejecutables a las pantallas de monitoreo provocando que muchas sean ignoradas. Estas pueden ser validadas de manera simple, viendo si

están vacías o llenas de páginas de alerta.

Sistemas con supervisión y soporte, incluyendo locaciones y tipos

Sin tomar en cuenta el número de clientes, todos los sistemas supervisados representan trabajo para el centro de control.

Incidentes

La información sobre incidentes es muy importante para todos, especialmente IT y gestión de negocios. La información de incidentes debe incluir la cantidad de incidentes por cada nivel de severidad, sí estuvieron relacionados con cambio, recurrentes o prevenibles, los negocios afectados y el departamento responsable del incidente.

Interrupciones que impactan al cliente

Estos totales son incluidos usualmente en las métricas más altas de severidad; la causa, el arreglo, número de

clientes afectados, pérdidas financieras, duración y otra información relevante para cada interrupción debe estar detallada en este reporte.

Cambios realizados

Esta es la cantidad de cambios que afectas sistemas y aplicaciones supervisadas por el centro de control. Se debe incluir la cuenta de cambios en los cuales el centro de control estuvo involucrado. La segunda cantidad representa trabajo del personal del centro de control. Se debe tener extremo cuidado al decidir el tipo de métricas a realizar. Es bueno capturar el número de cambios así como el propósito funcional de los cambios. Por ejemplo, un cambio en la aplicación para agregar una función nueva, seguido de cuatro cambios para hacer correcciones, deberían contar como cinco cambios cuando, en realidad, son 1 cambio y cuatro acciones correctivas.

Estadísticas para cualquier automatización

Estas estadísticas representan la efectividad del centro de control en mejora de proceso y es una buena manera de auto evaluación.

Estadísticas de llamadas

Los centros de control no deben recibir una gran cantidad de llamadas porque no son centros de atención de llamadas y en general deberían tener más llamadas salientes que entrantes. Si hay muchas llamadas entrantes es porque la gente los ve como un servicio de atención o de asistencia; esto debe ser algo que preocupe a la gerencia.

Estadísticas de tickets de problemas (totales, por automatización, creados manualmente, abiertos, resueltos, etc.)

Estas cantidades serán los tickets abiertos manualmente por el personal

del centro de control, a su nombre o con su asignación. Son una buena métrica para revisar cotidianamente para los responsables de turno.

Estadísticas de proceso de lote

Estas estadísticas deben incluir el número total de trabajos de lote ejecutados, la cantidad de fallos, la cantidad de fallos repetidos, la cantidad de los que se pasaron el tiempo límite y cualquier otra información relevante.

Desempeño a nivel de servicio

Aquí es donde un centro de control manejado adecuadamente brillará. Los números representan que tan bien has llegado a tus objetivos.

Para garantizar la precisión, las métricas deben ser reunidas automáticamente y los reportes deben ser generados también de forma automática (esto aplica para métricas diarias, semanales y mensuales).

Una buena práctica es tener un equipo interno de reportes que tenga el entrenamiento, experiencia y autoridad necesarias para crear y mantener un programa de métricas efectivo cargado con búsqueda de datos, análisis y reporte; este equipo será responsable, únicamente, de reportar la información más no de decir lo que pueda representar la información. La responsabilidad sobre la información seguirá siendo de los equipos individuales a los cuales aplica esa información. Recuerda: castigar o premiar a los mensajeros por el contenido de la información, asegura que solo se presenten resultados positivos sin considerar las condiciones reales.

Distribución de la información

Toda la información de las métricas del centro de control debe ser distribuida a los clientes a los que se les da soporte y estar disponible para todos. No debe haber métricas escondidas que puedan poner al

centro de control en un enfoque negativo. El objetivo de entregar métricas es el de mostrar la realidad para que los directivos sepan exactamente qué está pasando con las empresas, sea bueno o malo.

Es por esta razón que los centros de control no deben ser vistos como la causa del problema o ser acusados del pobre desempeño de un sistema o departamento bajo supervisión, por la simple razón de que son los que están reportando las malas noticias.

El centro de control es el mensajero y, para garantizar que la información siempre sea precisa y concisa, no maten al mensajero.

Para ayudar a garantizar un reporte y un comportamiento neutral, es una buena práctica que el centro de control le reporte a una línea de comando que no sea directamente responsable del entorno que se esté monitoreando.

Precauciones

El centro de control no debe ser el encargado de reducir el número de incidentes, excepto aquellos que pueden ser evitados gracias a un monitoreo proactivo. Para que cada incidente e interrupción sean reportados de manera precisa y oportuna, lo mejor es que la tarea del centro de control sea resolver incidentes e interrupciones cuando estas ocurren. Los equipos de supervisión de problemas y las divisiones individuales deben ser los responsables de proveer soluciones permanentes a las interrupciones al mismo tiempo de tratar de reducirlas.

Si es posible, el personal del centro de control debe hacer recomendaciones a los dueños de las empresas para reducir o evitar interrupciones pero nunca deben ser tomados como responsables de las cantidades de incidentes. Cuando al centro de control se le hace responsable, la cantidad de incidentes de severidad alta empieza a disminuir mientras que

el número de incidentes de severidad baja empieza a aumentar o, ambos empiezan a disminuir; las quejas de los clientes, por otro lado, empiezan a aumentar. Esta es una de las razones por las cuales hacer métricas adecuadas es crucial y de que no haya conflicto de interese al reportar la información.

Naturalmente, el centro de control debe responsabilizarse por interrupciones que ocurran por haber ignorado una alerta, pero aún en esas instancias, el centro de control no debe ser hecho responsable por la interrupción en si misma sino por la deficiencia en el monitoreo. Por ejemplo, si un servidor falla porque el disco duro primario se queda sin espacio, el centro de control sería responsable si se generara una alerta y fuera ignorada; pero, el dueño del servidor sería responsable porque el disco se quedó sin espacio y de las acciones necesarias para prevenir que volviera a suceder.

La cantidad de incidentes e interrupciones no son un buen indicador del desempeño de un centro de control. Por ejemplo, un centro de control con un volumen alto de incidentes puede ser el reflejo de un desempeño extraordinario ya que más usuarios llaman pidiendo servicios de supervisión de incidentes y, un centro de control con volumen bajo de incidentes puede ser el reflejo de un mal servicio cuando los usuarios luchan con un problema, se rinden y buscan una solución en otro sitio.

Un centro de control considerado bueno, en una empresa que tiene una cantidad muy alta de quejas del cliente o baja satisfacción del cliente, es una señal inequívoca de que las métricas no son adecuadas, los equipos incorrectos están siendo premiados o castigados o existe un conflicto de interesen en la línea de comando del centro de control.

Capítulo Nueve

Supervisión de alertas

La gestión de alerta es el proceso de convertir eventos que pueden causar un problema en acciones de recuperación automatizadas o alertas que son enviadas a los equipos correspondientes. Las alertas críticas para una aplicación de producción irán al centro de control y las alertas para un sistema de evaluación irán directamente a los equipos de soporte.

Los centros de control usualmente no hacen monitoreo a sistemas y aplicaciones sin producción o sin

respaldo. Estos tipos de sistemas requieren interacción constante la cual desviaría al personal del centro de control de eventos relacionados con la producción.

Instrucciones para los equipos de supervisión de alertas

Enviar únicamente alertas procesables a los monitores del centro de control.

Una alerta procesable es aquella que requiere de acción inmediata para atender una anormalidad que puede llevar a una falla de un sistema, dispositivo, o aplicación.

> *Los víveres de una organización nos pidieron que revisáramos un centro de control después de que habían ocurrido muchas fallas de sistema que podrían haber sido prevenidas*

en un periodo de tiempo corto. Se encontró que las pantalla de monitoreo del centro de control tenían cientos de alertas, con sólo 25 visibles y el resto con 30 o más páginas interiores.

No nos sorprendió que los dueños del negocio estuvieran furiosos. Enterradas entre esas 30 o más páginas de alertas informativas, de sistema de evaluación, de entorno a QA, relacionadas con cambios, decomisadas y otros tipos de alertas no procesables, se encontraron, ocasionalmente, alertas que advertían de una condición crítica seguidas un poco después de alertas

constatando que el sistema había fallado. El centro de control se enteró de estas fallas de sistema cuando los clientes empezaron a quejarse.

Identificar el problema fue la parte fácil, arreglarlo fue otra cosa; se requirieron semanas de análisis, cambios en procesos y e iniciativas de automatización seguidas de la implementación de nuevos controles de estándares para evitar que los problemas se presentaran nuevamente.

Las alertas informativas tienen el potencial para inundar las pantallas de monitoreo, causando que alertas de producción reales pasen

inadvertidas por la pantalla principal. Las alertas informativas, no críticas y no de producción deben ser enviadas a los equipos de soporte en vez de al centro de control de producción.

Generar automáticamente un ticket de problema por cada alerta enviada a los monitores del centro de control.

Implementar umbrales e inteligencia para eventos multi relacionados o alertas duplicadas para evitar la duplicación de tickets de problema o sobrecarga del sistema de tickets de problema.

Crear una pantalla de monitoreo en una locación central para que el centro de control vea todos los tickets de problema creados como resultado de las alertas.

En ocasiones, el personal de monitoreo recibe el estado de las alertas y actualizaciones de resoluciones de los tickets de problema. Poner una pantalla con los últimos tickets de problema elimina la necesidad de hacer una búsqueda cada vez que se necesitan actualizaciones de estado.

La pantalla de monitoreo debe incluir la descripción de la alerta, estado, sistema y número de ticket de problema, grupo asignado, fecha y hora. Las alertas se deben actualizar automáticamente para garantizar que el estado más actualizado esté disponible o esté siempre disponible.

Por ejemplo, cuando una situación está resuelta, la alerta debe ser quitada de la vista del centro de control automáticamente y debe ser puesta en la lista de "resueltas". Cuando un ticket de problema es resuelto o

cerrado, la alerta correspondiente debe ser actualizada en consecuencia.

- Esto también aplica a eventos que son auto corregibles (reinicio de proceso o de servidor) y para eventos que son corregidos con intervención manual; por ejemplo, si un proceso falla y es reiniciado automáticamente, el proceso ya no estará detenido y la alerta no debe permanecer en un monitor. Un ticket de problema debe ser generado y asignado a grupo donde se generó la alerta para identificar y corregir la causa de la falla y rastrear adecuadamente el evento.

Estos requerimientos facilitan que el personal de monitoreo determine que alertas requieren acciones posteriores o escalamiento; también reducen la carga de trabajo de los equipos de soporte y del centro de control.

Implementar alertas inteligentes para que los monitores no se sobrecarguen por un solo evento o múltiples casos del mismo evento y para detectar problemas potenciales a gran escala.

- Una falla en el servidor debe generar solo una o dos alertas críticas que abarquen la falla inicial y todos los componentes afectados.
- Desplegar una alerta por alertas duplicadas con un contador dinámico (cuando sea

posible) que muestre la cantidad de casos por la falla.

- Desarrollar reglas de negocio para analizar eventos mediante patrones que puedan indicar un problema mayor que esté por ocurrir.

Cierto tipo de fallas, tal como una falla de sistema, puede resultar en la generación de cientos de alertas; en estas situaciones, solo una o unas alertas requieren acción, el resto pueden ser cerradas o quitadas de la pantalla por que el evento que disparó la alerta será resuelto automáticamente una vez que el sistema sea puesto en servicio. Una pantalla de monitoreo inundada en esta situación escondería otros problemas que hayan

podido ocurrir como resultado de la falla de sistema. Eliminando de la pantalla las alertas no procesables, elimina la necesidad del personal de monitoreo del centro de control de determinar cuáles alertas requieren acción o cuales pueden ser ignoradas.

Implementar procedimiento o reglas de negocio para establecer umbrales para evitar alertas falsas.

- Se deben proveer los medios necesarios para el reporte y remedio de las alertas falsas para evitar su recurrencia.

Si algo es muy difícil de corregir, es muy probable que sea ignorado o que sea puesto en lista de espera. Facilita la corrección de

umbrales inapropiados para los equipos de sistemas y aplicaciones y tendrás un índice más alto de alertas no procesables eliminadas.

Evitar que se generen alertas como resultado de un cambio aprobado o una actividad operacional semanal, lo cual ocurre normalmente durante el tiempo de mantenimiento (Greenzone) definido de una aplicación.

- Los requerimientos de cambios aprobados normales y de emergencia deben ser tomados en cuenta para evitar alarmas falsas.

Algunos cambios programados requieren que se apague el sistema o quedar fuera de línea mientras se implementa el cambio; si las alertas se generan mientras esto ocurre, son ignoradas.

El sistema de alertas debería estar ligado al sistema de cambios para detectar de manera automática interrupciones debidas a cambios normales y de emergencia y suprimir las alertas generadas por dichas interrupciones.

El monitoreo y las alertas deben continuar aún durante los tiempos de mantenimiento (Greenzone) cuando no se están implementando cambios.

> *Algunos cambios implementados en la aplicación A pueden causar, inadvertidamente, una falla en la aplicación B. darse cuenta de esto en el momento en el que sucede, le permite al centro de control la oportunidad de corregirlo antes de que termine la 'zona verde', que será cuando los clientes trataran de usar la aplicación.*

Sistema de archivo para alertas que incluye secuencia temporal de

eventos, las decisiones que fueron tomadas y por quién y el resultado / impacto de la mitigación / resolución.

- Reduce el tiempo para resolver cualquier alerta recurrente en algún momento en el futuro.

Además de las alertas que aparecen en las pantallas de monitoreo, otros métodos para llamar la atención del centro de control sobre incidentes, son:

- Llamadas recibidas de centro de atención o servicio de asistencia (centros de servicio al cliente.
- Otros centros de control
- Otras regiones
- Soporte de sistema
- Desarrollo de aplicaciones
- Soporte técnico

- Del personal del centro de control cuando no pueden llevar a cabo una función.

Estrategias de reducción de alertas

Algo que pasa con frecuencia con la supervisión de monitoreo y de eventos
es que con el tiempo las cosas se empiezan a deteriorar. Inicialmente, se
asignan muchos recursos para implementar una estrategia de monitoreo
llegando a un punto en que los eventos son detectados antes de que ocurra una interrupción; tiempo después, todos empiezan a hacer otras cosas y después de cierto tiempo hay demasiadas alertas y muchas interrupciones.

Cuando se implementa una estrategia de monitoreo, es muy importante implementar y reforzar estándares y reglas estrictos, sin desviaciones ni excepciones. Cuando se hacen excepciones en los estándares, estas tienden a volverse permanentes y son seguidas por más requerimientos de excepciones. Después de algún tiempo, hay más excepciones a las alertas que aquellas que siguen los estándares, haciendo que la supervisión de eventos y los equipos de monitoreo sean inefectivos.

- Elimina automáticamente o suprime las alertas durante el tiempo de mantenimiento semanal (Greenzone) para actividades de operación, como respaldos y cambios aprobados.
- Permite que los administradores de sistema y el personal de soporte puedan definir y modificar tiempos de mantenimiento recurrentes

usando un portal de auto servicio.

- Instala un proceso de auto servicio puntual (una sola vez) para suprimir y reestablecer alertas automáticamente para cambios de emergencia aprobados de último minuto.
- Permite que sea posible crear un tiempo de mantenimiento (Greenzone) temporal dentro de un requerimiento de ticket de cambio, el cuál será entonces alimentado dentro de la aplicación de alertas.

Esta mejora elimina la necesidad de que el personal de supervisión de evento busque, valide y acepte o rechace que el historial de cambios que requieren alertas sea suprimido fuera de horas de mantenimiento estándar y entonces,

procesar el requerimiento manualmente.

Cuando se hacen manualmente, cerca del 25% de los recursos de la supervisión de eventos son usados en esa función. Cuando se hacen automáticamente, todos los sedimentos manuales relacionados a ese tipo de cambios no se tienen que hacer. Adicionalmente, con un equipo menos requerido para revisar y aprobar los historiales, el tiempo de aprobación de cambios puede ser reducido.

El seguimiento de contabilidad y auditoría que asocia el historial de cambios con la

función de supresión de mensajes con el propósito de hacer auditoría se hace posible.

- Crear un entorno en fase de alerta

Para nuevos sistemas y cambios, se deben generar alertas y estas deben mostrarse en una pantalla de monitoreo para ser revisadas por los equipos de soporte antes de moverse a producción. Alertas de prueba y no críticas deben ser eliminadas de las consolas de producción.

El personal del centro de control nunca debe de ignorar una alerta o aceptar cuando hacerlo cuando se lo pidan. Cada alerta debe tener su ticket

de problema correspondiente y sus acciones de seguimiento para identificar y corregir la causa inicial del evento que disparó la alerta. La intención es resolver permanentemente el evento para que no ocurran otra vez.

Tickets automáticos

El propósito principal de los tickets automáticos es garantizar su rigurosidad y precisión, no para reducir recursos aunque este es un efecto colateral. Los tickets automáticos aseguran la creación de un ticket de problema para cada alerta; es asignado al equipo correspondiente y resuelto de manera oportuna. Documentar el proceso de resolución permite que la información se guarde en la base de datos de errores conocidos reduciendo el tiempo de resolución si el evento se presenta otra vez.

Varios puntos a recordar cuando se implemente el ticket automático, incluyen:

- Generar automáticamente un ticket de problema para cada alerta.

La automatización no puede distinguir ente una alerta real y una que puede ser ignorada así que creará un ticket sin importar las condiciones. El personal del centro de control tiende a simpatizar con algunos equipos de soporte y pueden no crear algunos tickets para ciertas alertas que les piden que ignoren reduciendo la oportunidad de

corregir dichas alertas.

- Garantiza que los filtros estén en su lugar para evitar que se generen un número excesivo de tickets debido a alertas duplicadas o a una ocurrencia única.

En nada afecta que el sistema de tickets sea más inútil que la generación de demasiados tickets; cuando los equipos de soporte no pueden mantener el paso, simplemente ignoran todos los tickets, forzando al equipo que maneja el sistema de tickets

a hacer cierres masivos cotidianamente.

- Borrar las alertas automáticament e de la consola de monitoreo una vez que el ticket de problema correspondiente sea resuelto.

Ordinariamente, el personal de monitoreo hace el contacto inicial con soporte y después hace varios intentos para tener actualizaciones de estado. Esta opción le ahorra tiempo al personal de monitoreo de centro de control eliminando la

necesidad de pedir una actualización de estado a algún miembro de soporte al cual se le olvidó llamar para avisar que el problema había sido resuelto.

Llamadas automáticas y herramienta de escalamiento

La mayoría de la supervisión de incidentes se dan por no poder contactar al soporte; ya sea que haya un retraso en hacer la llamada inicial, que se llame a la persona incorrecta o se le otorga mucho tiempo a la llamada inicial a la persona de soporte antes de llamar a la siguiente persona. Automatizar las funciones elimina todas estas condiciones reduciendo el tipo de resolución de problema.

Una VRU (unidad de respuesta) para llamadas y escalamiento

1. **Contacta automáticamente a la persona que se le quiere llamar a su casa o a su celular, dada una alerta.**
2. **Permite a los grupos de negocio y a los equipos de soporte mantener y actualizar sus contactos y su información de escalamiento en una locación central.**
3. **Llama automáticamente al siguiente contacto cuando sea necesario.**
4. **Escala hasta el gerente de ese grupo y finalmente al centro de control si una alerta no es atendida**

Autoservicio

La implementación de una acción de autoservicio para supervisión de eventos reduce la carga de trabajo de

este equipo, reduce errores y aumenta la posibilidad de eliminar alertas no procesables al instalar los umbrales apropiados y la programación de interrupciones.

Aquí hay algunos de los servicios que pueden ser descargados en la herramienta:

- Requerimientos para acciones comunes que se repiten.
    - Ajustar umbrales
    - Crear o modificar la lista de alertas pendientes
    - Crear o modificar una lista de escalamiento de alertas
    - Personalizar el monitoreo para una aplicación o dispositivo particular.
    - Implementar un horario de mantenimiento temporal para cambios de emergencia.
    - Consulta de estado del monitoreo para una aplicación o dispositivo particular.
    - Ver los errores de monitoreo

- Ver el historial de información para alertas
- Requerir acceso a las pantallas de monitoreo
- Requerir tableros de monitoreo de alto nivel

Beneficios

Una buena estrategia de supervisión de eventos entregará muchos beneficios directos e indirectos para todos los equipos en IT.

- Mejorar el nivel de servicio hacia los clientes.
- Mejorar el proceso de supervisión de cambios.
- Mejorar las actividades de cambio semanal.
- Mejorar las actividades recurrentes semanales.

- Mejorar la supervisión de la lista de contactos
- Mejorar la documentación de alertas
- Reducir la duración de las interrupciones de negocio
- Reducir la cantidad de las interrupciones de negocio
- Reducir la cantidad de alertas no procesables
- Reducir la cantidad de llamadas al equipo de supervisión de eventos.

- Reducir los tiempos requeridos para desarrollo y validación

Capítulo Diez

Casos de estudio

Los seis casos siguientes describen problemas reales en varios centros de control alrededor del mundo. En la mayoría de los casos las soluciones identificadas e implementadas se basaron en conceptos clave de los capítulos anteriores.

Caso de estudio #1

Centro de control con infraestructura de pobre desempeño

La gerencia responsable de los centros de datos y sus correspondientes centros de control a lo largo de áreas de servicio en tres continentes, incluyendo Europa, Oriente Medio y África solicitaron ayuda después de que sus líderes de división de negocios se quejaran de un mal servicio y de clientes insatisfechos. El centro de control obtuvo métricas que mostraron que estaban cumpliendo con su obligación de crear tickets de problema y de notificar a soporte dentro de un lapso de 15 minutos después de cada alerta; sin embargo, las interrupciones en el servicio eran cada vez más frecuentes. Los directivos de la división de negocios recibían un número creciente de quejas de clientes que no podían entrar en las aplicaciones de la empresa o que podían entrar pero el

servicio era tan lento que rápidamente abandonaban la aplicación. Los directivos de la empresa no estaban contentos con IT por varias razones:

1. **Estaban enterándose de los problemas directamente por los clientes y no por Operaciones.**
2. **Los servidores se caían, provocando que las aplicaciones corriendo en ellos no estuvieran disponibles. La gerencia estaba aún más molesta al enterarse de que las alertas se estaban generando y se estaban enviando al centro de control pero que no se estaba**

tomando ninguna acción ni medida para corregir la causa de las alertas lo cual llevaba a fallas del sistema.

3. **Varias alertas críticas generadas por la aplicación habían sido mandadas al centro de control indicando que algo no estaba funcionando bien pero los desarrolladores no les habían prestado atención hasta mucho tiempo después, hasta que los clientes habían comenzado a quejarse.**

   Un acuerdo de servicio había sido implementado como una solución rápida después de una queja anterior hecha por la división de negocio acerca del mal servicio. En ese momento se detectó que no se estaban haciendo notificaciones de una cantidad grande de alertas. En vez de realizar una inspección

detallada de la situación, se hizo un acuerdo entre las dos partes de que se crearía un ticket de problema y también una notificación dentro de los siguientes 15 minutos siguiendo las instrucciones de contacto provistas por los equipos de soporte.

Inicialmente, hubo una mejora notable en el servicio pero con el tiempo, el número de alertas se incrementó. Este incremento provocó que el personal del centro de control no tuviera tiempo de verificar que las notificaciones estuvieran siendo respondidas ni de que las alertas estuvieran siendo atendidas.

La dirección de IT quiso saber porque había desconexiones entre el personal del centro de control, quienes parecían estar cumpliendo con sus acuerdos de nivel de servicio, y los

negocios, los cuales estaban perdiendo ingresos como resultado de la gran cantidad de interrupciones y mal servicio al cliente.

Con amenazas de contratar por fuera de la división de negocio, los centros de datos y las operaciones del centro de control, la gerencia del centro de datos necesitaba un análisis detallado del problema y una solución permanente tan pronto como fuera posible.

Análisis

Dado que el centro de control clamaba haber cumplido con sus objetivos, el primer paso era ver al objetivo en si mismo y determinar si estaba alineado con los objetivos del negocio.

El objetivo del centro de control era asegurar generar un ticket de problema y enviar una notificación a soporte dentro de los siguientes 15 minutos después de recibir una alerta.

El primer problema era el objetivo:

1. No era un objetivo válido sino un acuerdo a nivel de servicio; el centro de control no había establecido objetivos y solo tenía uno implícito: garantizar que el acuerdo a nivel de servicio, el relacionado a los tickets de problema y a las notificaciones, se cumpliera.
2. El acuerdo no estaba alineado con los objetivos del negocio. De hecho, el centro de control no tenía objetivos que involucraran a los clientes a los que se les daba el servicio.
3. La única obligación del centro de control era generar los tickets de problema y enviar la notificación, punto. Nunca les importó si la notificación no era recibida

o era ignorada o iba dirigida a la persona, e-mail o teléfono incorrecto; la resolución de la alerta era igual de irrelevante para ellos; su única obligación era generar el ticket de problema y notificar en un máximo de 15 minutos sin importar si alguien recibía la notificación en el tiempo adecuado.

La siguiente parte del análisis era platicar con todas las partes involucradas para escuchar lo que ellas habían percibido como situaciones de presión: supervisión de alertas (eventos), supervisión de incidentes, equipos de soporte y el personal de monitoreo del centro de control.

Preocupaciones del personal de supervisión de alertas (eventos):

- carga excesiva de trabajo; el equipo de supervisión de alertas había estado lleno con requerimientos para nuevo monitoreo, modificaciones a umbrales, eliminación de monitoreo y muchos otros requerimientos relacionados con alertas hechos por los equipos de soporte y del personal del centro de control.

- Personal insuficiente; el personal no habia podido llevar el paso con los incrementos en el entorno monitoreado.

- Herramientas obsoletas; el personal procesaba el trabajo usando hojas de Excel y con un proceso de requisición

sumamente engorroso que la mayoría de los equipos había cambiado por un proceso de auto servicio automatizado.

Además de los cambios en la configuración del monitoreo, varios miembros del equipo se dedicaban a revisar y aprobar/rechazar cambios en el historial de control para aplicaciones que requerían cambios en el monitoreo. La carga de trabajo se incrementó substancialmente al crecer el número de sistemas monitoreados que requerían haber aumentado el personal cada año, simplemente para mantener el trabajo pendiente bajo un nivel de dos semanas.

Preocupaciones del personal de supervisión de incidentes:

Una vez notificados de una interrupción, el equipo de supervisión de incidentes hacía lo que era necesario para restaurar el servicio. Las quejas aquí eran:

- La mayoría de las llamadas venían del servicio de asistencia después de que los clientes comenzaban a quejarse, en vez de venir antes del centro de control.
- Retrasos para avisar al correspondiente miembro del personal de soporte debido a información de contacto incorrecta o inexistente (en ocasiones esta situación retrasaba la resolución del incidente por horas).
- Había una respuesta muy lenta del centro de control cuando buscaba soporte operacional.

Preocupaciones del personal de soporte:

Los equipos de aplicación y de sistema, ambos, recibían las mismas quejas:

- Los equipos de soporte eran inundados con e-mails relacionados a alertas y tickets de problema del centro de control. Inicialmente, el personal de soporte investigaba cada una de las alertas pero, con el tiempo, empezaron a quedarse a trabajar toda la noche resolviendo alertas que le pertenecían a alguien más, eran para servidores de desarrollo y aplicaciones, o, algunas alertas eran ignoradas debido a una configuración incorrecta. Al no tener manera de distinguir las alertas que sí eran válidas y para poder dormir un poco, los equipos de soporte empezaron a ignorar todos los tickets de problema relacionados con alertas y todas las notificaciones por e-mail, respondiendo únicamente al ser llamados directamente.

- Los requerimientos hechos a la supervisión de alertas para modificaciones en las alertas tomaban semanas en completarse o nunca se completaban.

- La habilitación o eliminación de monitoreo era un proceso largo y arduo; donde ya existía el monitoreo era mejor 'dejarlo así' e instruir al personal de monitoreo a ignorar esas alertas.

- Los requerimientos de cambios se retrasaban con frecuencia debido a aprobaciones pendientes de parte del equipo de supervisión de alertas. Se requerían grandes cantidades de llamadas, e-mails y

escalamientos de parte de los creadores de los cambios para que les fuera aprobado el historial de cambios antes de la ventana de corte.

- los procedimientos de control de cambios requerían que el equipo de supervisión de alertas revisara y aprobara cada requerimiento de cambio donde un sistema o una aplicación fuera a ser modificada para que se pudieran hacer las modificaciones

pertinentes en las alertas.

Preocupaciones de los equipos de monitoreo:

- Una gran cantidad de alertas. Casi siete alertas por cada equipo monitoreado, un total de 55,000 alertas por mes, estaban llegando a las pantallas de monitoreo del centro de control; en cualquier momento habían, por lo menos, 15 páginas de alertas en las pantallas de monitoreo, haciendo imposible para el personal de monitoreo hacer algo más que abrir un ticket de problema y mandar la notificación inicial.

- Información de contacto incorrecta o inexistente hacía difícil cumplir con el requerimiento de los 15 minutos.
- Las alertas constante suponían que el personal de monitoreo se encontraba ocupado desde el momento en que empezaba su turno hasta que terminaba el mismo; el ambiente era como el de una línea de ensamblado de una fábrica: todos repitiendo los mismos pasos una y otra vez.
- Cerca del 90% de los tickets de problema eran cerrados por el personal de soporte con la instrucción para el personal de monitoreo de ignorar la alerta.

- Cientos de alertas inundaban las consolas, haciendo más probable que alertas válidas pasaran inadvertidas.

Problemas identificados

El principal problema identificado fue la cantidad de alertas (55,000 por mes) que llegaban a las pantallas de monitoreo del centro de control. Con las 15 páginas de alertas en las pantallas de monitoreo, era imposible determinar cuáles eran por tonterías y cuáles si requerían acciones para prevenir una interrupción o para restaurar un servicio. Todo lo que se vaya después de la primera página queda escondido y muy probablemente provocará una larga interrupción; las pantallas de monitoreo deberían permanecer vacías o casi vacías todo el tiempo. Las más de 55 mil alertas significaban serios problemas para las alertas y el monitoreo.

1. Una mirada a la supervisión de alertas y eventos reveló lo siguiente:

   - Una cantidad excesiva de alertas no procesables (falsas) debido a:

   - Umbrales inadecuados

   - Cambios programados

   - Servidores dados de baja

   - Sistema de evaluación y desarrollo

   - Evaluaciones de pre-producción

   - Las alertas durante la evaluación de desarrollo se marcaron como producción y aparecían en las pantallas del centro de control.
   - El monitoreo y la generación de alertas no habias sido implementados en muchos sistemas de producción nuevos, se encontraban en la lista de

pendientes de la supervisión de alertas.

2. No automatización. Todos los pedidos para añadir, eliminar o modificar la configuración del monitoreo y las alertas se hacían manualmente y se terminaban en dos semanas. Simples ajustes a los umbrales eran considerados lo menos importante y se hacían en más de dos semanas o eran de plano ignorados.

3. No existen vínculos entre las aplicaciones de supervisión de alertas, los recursos y los cambios.

4. No hay estándares de monitoreo ni de alertas; tampoco hay mejores prácticas.

5. El monitoreo no servía en 25% de los servidores, como resultado, no se generaban alertas cuando hubieron

condiciones adversas en esos servidores o aplicaciones.

Solución

La mayor parte de la carga de trabajo del equipo de supervisión de alerta se dividía entre revisar el historial de la supervisión de cambios y añadir o eliminar monitoreo conforme a cambios en el servidor.

La mayoría de las alertas que llegaban a las pantallas de monitoreo eran no procesables, generadas por cambios programados, clasificación de administración de recursos inadecuada o alertas de sistema de desarrollo.

Se empezaron varias acciones:

1. Se crearon perfiles estándar de monitoreo de mejores prácticas para todos los sistemas nuevos; para sistemas existentes con perfiles múltiples, se creó una opción común a todos.

a. Con los perfiles estándar, el monitoreo pudo ser automatizado para los sistemas nuevos o para servidores agregados a aplicaciones existentes.

2. Se creó automatización para integrar los sistemas de supervisión de recursos con el sistema de supervisión de alertas.

   a. habilitó automáticamente el monitoreo en nuevos sistemas de producción.

   b. habilitó o eliminó automáticamente monitoreo de servidores agregados o eliminados de aplicaciones existentes.

   c. evitó que las alertas de sistemas de no producción o puestos

fuera de servicio llegaran al centro de control.

3. Se creó automatización para integrar el sistema de supervisión de cambios con el sistema de supervisión de alertas.

    a. evitó que las alertas generadas por cambios programados llegaran a las pantallas de monitoreo de producción durante el tiempo de inicio y finalización de los cambios.

    b. los registros de cambios, que requerían una alerta para ser suprimidos, ya no requirieron la aprobación ni ninguna otra acción por parte del equipo de supervisión de alertas,

eliminando, así, una parte importante de su carga de trabajo semanal.

4. Se implementó una nueva política de requerimiento de respuesta del equipo de soporte indicado por cada alerta de producción enviada a las pantallas de monitoreo del centro de control.

a. a los equipos de monitoreo ya no se les permitió ignorar alertas.

i. respuestas como ‘avíseme cuando llegue a 90%’, ya no fueron aceptadas; en todos los casos se tuvieron que realizar acciones para corregir la causa de la alerta o tuvieron que ser

modificados los umbrales de alerta para que alertaran en las condiciones apropiadas.

b. algunas de las alertas eran generadas por personas implementando cambios sin un registro de cambio aprobado.

i. esta política ayudó a reforzar los controles de supervisión de cambios resaltando cambios no autorizados.

5. Se automatizó el ticket de problema

a. los tickets de problema se crearon automáticamente para cada alerta de producción mandada a las pantallas de

monitoreo del centro de control.

6. Se automatizó la notificación de alerta y la gestión de escalamiento a los equipos de soporte correspondientes.

    a. se hacía una notificación inmediata por medio de una Unidad de Respuesta de Voz (Voice Response Unit) al miembro de soporte encargado de recibir llamadas, con una llamada automática a la siguiente persona o al gerente del equipo en caso de que el primero no respondiera. Una notificación final era enviada al centro de control en caso de que no hubiera respuesta de los equipos de soporte.

7. Se integró la información de contacto de soporte y gestión

de escalamiento con los recursos y el sistema de supervisión de RH para garantizar que la información siempre fuera precisa y estuviera actualizada.

8. Se crearon reglas separadas para alertas de producción y de no producción.

    a. las alertas de producción iban directamente a las pantallas de monitoreo del centro de control con su correspondiente ticket de problema y notificación a soporte, requiriendo respuesta inmediata de los equipos de soporte.

    b. las alertas de no producción iban directamente a los equipos de soporte; las reglas de procesamiento de

alertas pudieron ser configuradas por los equipos de soporte para que cada individuo eligiera la manera en que deberías ser notificado.

9. Se crearon pantallas AC (QA) para evitar que las alertas de pre-producción inundaran las pantallas de producción y para dar oportunidad de eliminar las alertas ambiguas e incoherentes.

    a. aquí fue en donde el monitoreo y las alertas fueron evaluados, modificados y ajustados antes de que un sistema o una aplicación fueran puestos en producción.

10. Se implementaron juntas en cambio de turnos en el centro de control con la participación de supervisores del turno que empezaba y del que terminaba

así como el director del centro de control para abordar situaciones que estuviesen pasando y que no parecieran importantes en el momento pero que pudieran convertirse en problemas si no fueran atendidas en los tiempos correctos.

Seguimiento

Mientras se implementaban las mejoras señaladas arriba:

- La cantidad y duración de las interrupciones empezó a bajar dramáticamente.
- Las interrupciones de servicio prevenibles fueron virtualmente eliminadas y la duración de las que sucedieron disminuyó dramáticamente.
- Casi de la noche a la mañana, los requerimientos de nuevo monitoreo bajaron de varios

cientos por semana, con un retraso de quince días, a una docena. Las alertas y el monitoreo se volvieron un proceso automatizado una vez que un sistema era clasificado como producción en el sistema de supervisión de recursos.

- Para requerir un monitoreo nuevo, la persona tenía que llenar una forma difícil de entender en Excel; esas formas eran muy confusas y era necesario que la persona tratara de adivinar la configuración de umbrales adecuada. La creación de perfiles estándar de mejores prácticas permitió que se implementara la automatización, la cual alivió la carga de trabajo de los equipos de soporte y del equipo de supervisión de alertas.

- Al final del primer año, la cantidad de alertas no

procesables virtualmente desapareció de las pantallas de monitoreo del centro de control.

- Después de un periodo de tres años, la cantidad de sistemas monitoreados se incrementó en 600% y el tamaño de los equipos de alertas y monitoreo disminuyó 25%.
- El equipo de supervisión de alertas tuvo los recursos suficientes para crear cursos de entrenamiento detallados para los equipos de soporte y para expandir su oferta a monitoreo de negocio y de base de datos, ayudando a reducir aún más otros problemas que pudieras afectar a sus clientes.

Caso de estudio #2

Fusionar los centros de control bajo limitaciones de tiempo, recursos y compatibilidad.

Una adquisición trajo a bordo un cuarto de computadores subcontratado, pequeño y compuesto de servidores UNIX y el correspondiente centro de control; poco después de la adquisición, daba la impresión de que la recientemente adquirida compañía tenía serios problemas de servicio, mayormente por cuestiones relacionadas con IT.

Análisis

Las revisiones iniciales del sitio dejaron ver serios problemas de procedimiento, tales como la falta de controles de cambio, seguridad y operación.

Los equipos de operación y desarrollo tenían acceso completo, irrestringido y

no monitoreado a los sistemas de producción y estaban implementando cambios a gran escala durante horas de oficina.

Ninguno de los sistemas tenía instalado hardware, software ni ningún sistema de monitoreo; no se detectaban fallas en los equipos dentro del cuarto de cómputo hasta que los clientes llamaban para quejarse.

En vez de tratar de ir arreglando las cosas gradualmente, la decisión había sido no renovar el contrato con el outsourcing y traer todas las cosas de regreso a casa en donde se podrían utilizar estándares, procedimientos y controles existentes. Desafortunadamente, para cuando esa decisión fue tomada, el contrato de outsourcing estaba a punto de expirar, dejando solo tres meses para completar la mudanza.

Problemas identificados

1. La mudanza se debe llevar a cabo en tres meses.

2. Los controles de cambios y de seguridad deben ser implementados lo antes posible.

3. Nadie del personal de la compañía de outsourcing quizo unirse a la nueva compañía, lo cual significaba que se debía contratar y capacitar nuevo personal dentro de ese periodo de tres meses.

4. Ninguna automatización, ni siquiera una aplicación para programar, fue instalada en los sistemas del centro de datos; los operadores de computadoras lo hacían todo manualmente usando procedimientos escritos, hojas de rastreo e e-mails para desarrollar sus labores cotidianas.

5. Los sistemas en el centro de datos adquirido eran no-estandarizados, lo cual significaba que ninguna de las automatizaciones existentes en el centro de control era compatible ni podía ser usada.

Solución

Un gerente del centro de control fue enviado al recién adquirido centro de operaciones a entrenar y estar a cargo de la supervisión del sitio. Este

gerente empezó el proceso de verificación de los procedimientos operacionales, actualizando o creando aquellos que eran obsoletos o inexistentes.

- Se estaban haciendo duplicados de todos los documentos de procedimiento y referencia durante el proceso de verificación y eran mandados al centro de control.

Se aceleró el proceso de contratación de 10 administradores de sistemas senior con experiencia en programación para sustituir a los que estaban operando de la compañía que se retiraba.

Aprender los procesos manuales de los sistemas y desarrollarlos cotidianamente le daría al nuevo personal una ventaja de inicio hacia el

desarrollo de las mejoras requeridas y hacia la automatización.

- Los miembros del personal de operaciones temporales fueron llegando mes tras mes para ayudar con actividades operacionales, permitiendo a los administradores con experiencia, enfocarse en las mejoras de servicio y la automatización.

El acceso de seguridad a producción fue revocado para el personal de operación y desarrollo. Los miembros del personal de soporte técnico fueron provistos con acceso para situaciones de emergencia, para ser usado

únicamente durante el curso de la restauración del servicio a los usuarios.

El espacio existente del centro de control, reservado para crecimiento futuro, se utilizó para albergar al nuevo personal.

Aunque no existían herramientas para supervisión de cambios en la nueva adquisición, se le dio capacitación por parte del personal de supervisión de cambios a los equipos de desarrollo de adquisiciones para la promulgación a corto plazo de un manual de proceso de supervisión de cambios para que las reglas y controles existentes pudieran ser implementados.

- A largo plazo, esos sistemas serían incorporados a las herramientas estándar de

supervisión de cambios para reducir los requerimientos de recursos y para proveer reportes y auditoria automatizados.

Durante los primeros dos meses, miembros del personal del centro de operaciones fuente volaban hacia el centro de control para capacitar a las nuevas contrataciones. Alternando semanas, miembros del personal del centro de control volaban hacia el centro de operaciones fuente para capacitación práctica.

Durante el segundo mes, el personal del centro de control empezó a desarrollar funciones cotidianas con operadores del centro fuente en stand-by. El administrador senior en turno documentaba cualquier situación en la que alguien salía del

stand-by en el sitio fuente para asegurarse de que solo pasara una vez. Para el inicio del tercer mes ya no hubo situaciones en las que alguien tuviera que salir de stand-by.

Para la mitad del tercer mes, se les dio completo control operacional.

- La documentación y la información de contacto había sido actualizada para dirigir a todos al centro de control.

Al final del tercer mes, el contrato de subcontratación (outsourcing) expiró.

- Todas las conexiones a red fueron desconectadas.
- El acceso de seguridad para los trabajadores por subcontratación fueron revocados.

Seguimiento

En un año, los sistemas estaban totalmente automatizados, permitiendo a los operadores del centro de control hacerse cargo de las funciones de operación cotidianas mientras que los administradores de sistemas recién contratados eran instruidos hacia posiciones de sistema avanzadas.

Caso de estudio #3

Fusión de dos centros de control bajo una escasez de recursos

Debido a reducciones en el presupuesto, se tomó la decisión de unir dos centros de control que se hallaban a 600 millas de distancias y que servían a diferentes tipos de clientes y usaban diferentes sistemas de cómputo; el primer centro de control, que era en donde se estaba reubicando todo, tenía 32 miembros del personal quienes manejaban 30 computadoras centrales IBM y alrededor de mil servidores, todos ellos completamente automatizados; el segundo centro de control, el que se estaba cerrando, manejaba 8 computadoras centrales y 500 servidores y 100 computadoras centrales más viejas y de mediana capacidad, con solo 60 miembros del personal. Cualquier colaborador que aceptara el cambio del segundo centro de control al primero, tendría el trabajo asegurado.

Cuando se traslada un centro de control a una locación lejana, siempre habrá colaboradores que prefieran no mudarse. Cuando se tomó la decisión

de la unión, la economía aún experimentaba un crecimiento tremendo y no era difícil encontrar trabajos bien pagados para trabajadores experimentados; en consecuencia, de los 60 trabajadores del centro de control que se cerró, solo 4 decidieron mudarse a la nueva locación.

Análisis

El personal del primer centro de control confiaba en la automatización y aplicaciones de monitoreo para desarrollar sus rutinas cotidianas; en vez de confiar en notas, memoria y hojas de registro, confiaban en alertas de excepción automatizadas y aplicaciones de monitoreo.

El personal del segundo centro de control utilizaba notas, memoria, hojas de registro y procedimientos escritos detallados para desarrollar sus labores cotidianas en las computadoras centrales IBM,

servidores y sistemas de cómputo de mediana capacidad. Las computadoras centrales y los servidores utilizaban el mismo software de sistema que los usados por el primer centro de control; esto quiere decir que la automatización y las aplicaciones de monitoreo usadas en el primer centro de control eran compatibles con los sistemas manejados manualmente por el segundo. Esto daba oportunidad de instalar y utilizar la automatización, las aplicaciones de monitoreo y las reglas permitiendo que el personal del primer centro de control pudiera manejar los sistemas con un mínimo de entrenamiento y personal.

El problema iba a ser las computadoras de mediana capacidad. El personal del primer centro de control no tenía experiencia con este tipo de sistemas.

Problemas identificados

1. Solo cuatro miembros del personal estaban dispuestos a

relocarse en el segundo centro de control.

2. Había falta de experiencia en computadoras de mediana capacidad en el personal del primer centro de control.

3. No había automatización ni monitoreo en ninguno de los sistemas de cómputo manejados por el personal del segundo centro de control.

Solución

El traslado se dividió en dos fases, una para los operadores de mediana capacidad y la otra para la computadora central y los operadores de servidor.

Mediana capacidad

Un tercer centro de control, localizado entre los dos primeros, fue incluido en la mezcla. Tenía 15 miembros y

supervisaba varias computadoras de mediana capacidad. Los 8 miembros del personal que se hacían cargo de las computadoras de mediana capacidad aceptaron mudarse al tercer centro de control.

1. Se configuraron e instalaron puestos de trabajo con las aplicaciones requeridas para que el personal manejara las computadoras de mediana capacidad.
2. Se estableció y valoró conectividad para sistemas de mediana capacidad.

Todos los miembros del personal fueron llevados al tercer centro de control en un día no laborable para asegurar que pudieran desarrollar sus funciones cotidianas sin problemas. Una vez que los 8 colaboradores

constataron que todo funcionaba correctamente, se estableció una fecha para que se hicieran las transferencias telefónicas.

Cuando llegó la fecha, los operadores de computadoras de mediana capacidad del segundo centro de control se reportaron a trabajar en el tercer centro de control; todas las llamadas telefónicas fueron automáticamente direccionadas al tercer centro de control.

Computadora central y servidor

Aplicaciones para automatización de manejo de mensajes, supresión y flujo de trabajo fueron instaladas en las computadoras centrales y en los servidores que eran supervisados por el centro de control más cercano.

Las aplicaciones de monitoreo y reglas asociadas fueron instaladas en los servidores y las computadoras centrales. Las alertas generadas fueron entonces incorporadas dentro

de las pantallas de monitoreo utilizadas por el primer centro de control.

Una vez que las herramientas estandarizadas utilizadas por el primer centro de control estuvieron completamente funcionales en los sistemas supervisados por el segundo centro de control, se estableció una fecha a 4 meses para completar la mudanza de todas las funciones.

- Ese período de tiempo alcanzaba para capacitación, identificación y documentación de huecos en los procesos y la terminación del proceso de RH.

La información de contactos del centro de control que se estaba cerrando se incluyó dentro de las aplicaciones que usaba el primer centro de control.

Los controles de seguridad estándar en sitio del primer centro de control fueron implementados en los sistemas supervisados por el centro de control que se estaba cerrando. Al personal del primer centro de control, se le otorgó acceso de seguridad a las computadoras centrales y a los servidores.

- Se llevó a cabo un análisis para determinar huecos o fallas en accesos requeridos para desarrollar acciones cotidianas y funciones de emergencia.
- Se llevó a cabo un segundo análisis para garantizar que todos los accesos de seguridad otorgados cumplieron con los estándares y controles de seguridad vigentes.

Dos miembros del personal por cada turno del centro de control que se estaba cerrando fueron enviados al otro sitio para capacitar a los miembros del personal del mismo turno.

- Con herramientas estándar, procesos, monitoreo y documentación en línea, el personal del primer centro de control fue capaz de supervisar los sistemas casi inmediatamente.

Los cuatro colaboradores del segundo centro de control que aceptaron mudarse de centro, fueron transferidos a diferentes turnos dentro del centro de control establecido, asegurándose de que

existiera un colaborador del segundo centro de control en todos los turnos.

Durante dos semanas, todas las funciones operacionales de las computadoras centrales y de los servidores fueron desarrolladas por miembros del primer centro de control con personal del segundo en stand by.

Como no se presentaron problemas durante la prueba piloto, la mudanza se llevó a cabo dentro de los tiempos preestablecidos.

- Todas las llamadas a los operadores de las computadoras centrales y de los servidores eran transferidas automáticamente al primer centro de control.

- Todas las funciones se volvieron responsabilidad del primer centro de control.
- Se expandieron reportes de métricas diarias, semanales y mensuales para incluir información de los sistemas recién incorporados a supervisión, provistos por el monitoreo y las aplicaciones de automatización.
- El acceso de seguridad fue revocado al resto del personal del segundo centro de control.

Seguimiento

Durante los siguientes meses, la cantidad de incidentes que afectaban

a los usuarios empezó a declinar en los sistemas que se habían trasladado al primer centro de control. Con el reporte de métricas en su sitio, los miembros del personal pudieron empezar proyectos de mejora de proceso en estos sistemas, ayudando a reducir retrasos que habían ocurrido con frecuencia durante los procedimientos de lote nocturnos.

Caso de estudio #4

Fusionar cuatro grandes centros de control en dos sitios

Como resultado de la demanda de espacio del centro de datos y para cumplir con las nuevas regulaciones

del gobierno en cuanto a la locación de sitios primarios y de respaldo, se tomó la decisión de consolidar cuatro centros de control.

Esos cuatro centros de control fueron el resultado de varias fusiones finalizadas a nivel de negocio pero no totalmente a nivel tecnológico.

Cada centro de control desarrollaba funciones para diferentes centros de datos; dos de ellos también desarrollaban funciones de recuperación de desastre el uno al otro pero estaban separados 15 kms. solamente y no cumplían con los requerimientos federales referentes a la proximidad de un sitio de respaldo.

Estos centros de control consistían de:

1. El centro de control 1 tenía 40 colaboradores que supervisaban 38 computadoras centrales grandes IBM y 2,000

servidores dando servicio a 4 centros de datos a lo largo de U.S.

2. El centro de control 2 tenía 64 colaboradores supervisando 20 computadoras centrales grandes IBM dando servicio a dos centros de datos. Se localizaba en un centro de datos y necesitaba cambiar de lugar para tener espacio para equipo de cómputo.

3. El centro de control 3 tenía 36 colaboradores supervisando 8,000 servidores dando servicio a dos centros de datos. Se localizaba en un centro de datos y necesitaba cambiar de lugar para tener espacio para equipo de cómputo.

4. El centro de control 4 tenía 72 colaboradores supervisando 16 computadoras centrales grandes IBM y aproximadamente 1,000 servidores dando servicio en dos centros de datos.

Los centros de control debían ser fusionados sin provocar interrupciones en el servicio, manteniendo la capacidad de respaldo y cumpliendo las regulaciones federales en cuanto a la distancia entre sitios.

Análisis

Los centros de control 1, 2 y 3 fueron situados dentro de un radio de 15 kms.

Dos de ellos en estados diferentes pero con accesos de transporte público y estacionamiento disponible.

Los centros de control 2 y 3, que se hacían respaldo mutuo, tenían que ser puestos en otro lugar con urgencia pues estaban ocupando espacio dentro de los centros de datos que era necesario para otras cosas; el espacio de los centros de datos es muy caro y muy difícil de encontrar, a diferencia de los centros de control que pueden usar casi cualquier espacio asegurado. Los avances en la tecnología de las computadoras centrales eliminaron la necesidad de tener centros operacionales cercanos. La mejor estrategia era duplicar los requerimientos del sitio en las otras locaciones y después mover a todo el personal. Cualquier mejora, automatización o capacitación sería puesta en marcha después del cambio.

Los dos sitios también tenían equipo de cómputo especializado con operaciones personalizadas. La

mayoría de los equipos y aplicaciones podían ser duplicadas, excepto por dos piezas de hardware, una primaria y una de respaldo, las cuales significarían un gasto muy grande al ser duplicadas; se decidió mover las originales en vez de hacer el gasto al duplicarlas.

Problemas identificados

1. El sitio 1 no tenía espacio suficiente para acomodar al personal que llega ni a su carga de trabajo.

2. El sitio 4 no tenía suficiente espacio de video pared para acomodar las pantallas de monitoreo adicionales requeridas.

3. Debido a requerimientos de tiempo y cuestiones políticas, ningún cambio en los sistemas o en el

personal se haría durante las fusiones.

Solución

La estrategia fue mudar a todo el personal y a las funciones primarias de los sitios 2 y 3 al sitio 1 y sus funciones de respaldo al sitio 4, el cual estaba a la mitad del camino.

Una compañía de arquitectura con experiencia en centros de control y una compañía de integración de centros de control, fueron contratadas para ayudar con la expansión de los sitios 1 y 4.

El centro de control 1 fue expandido aproximadamente al 150%. Un espacio adyacente que habia sido usado para guardar cintas de respaldo (las cuales fueron enviadas a otras instalaciones) proveyó espacio suficiente para agregar dos video-paredes adicionales con sus correspondientes estaciones de operación. El sitio fue dispuesto en forma de ovalo, con estaciones de operación y video paredes en los lados

largos y en uno corto, las oficinas de supervisión con la capacidad de ver los tres sitios se situó en el centro y el portal de entrada de seguridad único en el cuarto lado.

El centro de control 4 tenía suficientes estaciones de operación pero insuficiente espacio para las video paredes. Con la ayuda de una compañía de integración, la video pared existente, la cual usaba proyectores obsoletos, fue desmantelada y reemplazada con cubos de video de diseño y tecnología de punta. La nueva video pared era cuatro veces más grande, ofreciendo espacio suficiente para la fusión y para futuras necesidades. La pared fue renovada por partes de manera que las pantallas de monitoreo estuvieran siempre en funcionamiento.

Cuando la construcción estuvo terminada, se instaló el equipo de cómputo requerido usando las mismas especificaciones de los centros de control 2 y 3, con redundancia añadida

para red, energía y fallas en computadoras en cada estación.

Los sitios 2 y 3 usaban sistemas de telefonía VoIP, así que duplicar esos sistemas fue bastante simple y directo. Cuando los sistemas de telefonía estuvieron listos, cualquier llamada entrante en esos centros, aparecía también en el sitio 1.

El respaldo para el sistema que no pudo ser duplicado y que se construyó de manera personalizada, se movió al sitio 1. La compañía que construyó el sistema fue traída para configurarlo para la nueva locación.

Cuando todo el equipo estuvo configurado al 100%, se fueron trayendo por etapas a los miembros del personal para hacer pruebas piloto. Cada miembro del personal tuvo que ir al sitio 1 para verificar que pudiera tener acceso a las instalaciones y al centro de control y, acceder a los sistemas de cómputo y a toda aplicación requerida. Debido a la gran cantidad de miembros del

personal y a varios problemas que fueron identificados y corregidos, la prueba piloto se llevó cerca de un mes en completarse, lo cual estuvo dentro de los tiempos proyectados.

Varios miembros del personal de los sitios 2 y 3 que fueron reubicados voluntariamente, volaron al sitio 4 para completar sus pruebas piloto.

Cuando el equipo fue verificado totalmente y todos los problemas fueron corregidos, los operadores del sitio 2 empezaron a reportarse al trabajo en el sitio 1. Las transferencias se llevaron a cabo en un periodo de dos semanas, de manera que siempre hubo alguien disponible en el sitio 2 en caso de que hubiera habido algún problema que requiriera apoyo.

No hubo ningún problema y todo el cambio se llevó a cabo sin que un solo cliente se diera cuenta de que el centro de control completo había sido reubicado.

A continuación, el respaldo del sistema personalizado se hizo primario y fue manejado por personal del sitio 2 en la nueva locación. El primario anterior fue, entonces, llevado al sitio 4 y configurado para ser el nuevo respaldo.

Los miembros del personal que accedieron a reubicarse fueron transferidos al sitio 4; una vez en su lugar, la carga de trabajo del sitio 3 fue transferida al sitio 4. Después de un periodo de dos semanas, con todo el trabajo siendo realizado en los sitios 1 y 4, todo el personal que permanecía aún en el sitio 3 fue pasado al sitio 1.

Se conservaron los sitios 2 y 3 tal como estaban durante dos semanas después de que todo el personal y todas las funciones habían sido trasladados, para prevenir algún problema serio en las nuevas locaciones. Después de ese periodo, los sitios 2 y 3 fueron desmantelados y el espacio fue usado para centros de datos.

Seguimiento

Se hicieron pruebas de recuperación de desastre para garantizar que cada sitio fuera totalmente capaz de soportar y desarrollar toda la carga de trabajo.

Después de que finalizaron todos los movientos, se llevó a cabo una reorganización completa que puso todas las funciones de los centros de control bajo la responsabilidad de un solo gerente, limpiando el camino para mejoras de proceso en cada sección para poder saltar hacia la creación de herramientas de mejores prácticas y estándares que serían implementados frente al consejo directivo.

Caso de estudio #5

Centro de control de negocio

El director de una empresa muy rentable, requirió ayuda debido a un

número creciente de quejas de clientes muy importantes en relación con un mal servicio, retraso en transacciones o sistemas que no estaban disponibles. El director se sentía frustrado ante la falta de progreso de su centro de control de negocio para implementar el monitoreo que detectaría y corregiría los problemas antes de que los clientes fueran afectados o que evitaría que los problemas ocurrieran. El objetivo era reducir los problemas y garantizar que la directiva supiera de problemas graves, antes de que los clientes se enteraran.

Objetivo

1. Trabajar con la supervisión del centro de control de negocio para mejorar el monitoreo proactivo.
2. Reducir la cantidad y duración de todos los problemas que impacten al cliente.

3. Garantizar que la directiva esté al tanto de los impactos al negocio al ocurrir estos, antes de que los clientes se den cuenta de que hay un problema.

    a. La supervisión quiere poder llamar a los clientes para avisarles de que hay un problema que está siendo atendido, en vez de que los clientes lo tomen por sorpresa en relación a algo que ya esté ocurriendo.

Análisis

Una revisión de las interrupciones críticas en el negocio en un periodo de tres años, encontró lo siguiente:

1. La cantidad y duración de las interrupciones estaba creciendo porcentajes de doble dígito cada año.

2. Cerca del 50% de las interrupciones se daban por cambios programados realizados por la división de IT, con un porcentaje grande atribuible a los equipos de desarrollo.

3. Quince por ciento de las interrupciones eran problemas recurrentes que no eran corregidos hasta después de 2 o 3 recurrencias.

    a. Muchos problemas que afectaban a los

clientes no eran documentados, aun cuando los clientes se hubieran quejado y una notificación de resolución del problema (post mortem) hubiese sido mandada.

4. Una gran cantidad de interrupciones causadas por cambios y mejoras realizadas por IT o las que fueron por problemas recurrentes, no fueron clasificadas apropiadamente; la causa era anotada en el campo de texto de los tickets de problema pero los campos para marcar la causa como relacionada con

cambios o recurrente, no fueron marcados.

a. Esto quiere decir que las métricas producidas por el centro de control eran imprecisas y no confiables.

Una revisión en el centro de control de negocio encontró lo siguiente:

1. No había monitoreo proactivo.

a. La gerencia del centro de control había dejado de hacer todo monitoreo proactivo, enfocándose, en cambio, en funciones de reacción y de soporte, y en métricas.

2. Había rastreo selectivo y reporte de impacto de negocio, también selectivo.

    a. Una gran cantidad de problemas no era rastreada en el sistema de supervisión de problema.

        i. Sin historial de supervisión de problemas, no habría manera de determinar si los problemas eran resueltos adecuadamente. Sin un registro de cómo se

arreglaba el problema, cualquier ocurrencia futura requería de un análisis detallado para resolver la situación, alargando la duración de la introducción.

b. No había automatización: todo dentro del centro de control, incluyendo las métricas producidas, se realizaba manualmente.

c. No había equipo de supervisión de problema

i. La función de reportar de la supervisión de problema era realizada por el personal del centro de control, pero el análisis para determinar la causa e implementar acciones correctivas para evitar recurrencias similares no era realizada por nadie.

d. No había métricas imparciales estandarizadas.

i. Las métricas producidas

mostraban que IT estaba haciendo las cosas bien y fallaban en mostrar los problemas sin resolver.

3. Había una falta de cooperación de los equipos de desarrollo y del de atención a usuarios.

    a. Durante las conferencias telefónicas todos prometían completa cooperación pero nadie la llevaba a cabo.

Todas las situaciones eran síntomas de un problema subyacente; a menos de que se resolviera, atender los problemas de forma individual sería

como poner un curita en alguien que sangrará por huesos rotos.

El problema subyacente era un conflicto de intereses entre el centro de control y a los equipos sobre los cuales se haría la vigilancia y los reportes. Aunque los objetivos establecidos del centro de control estaban alineados con los objetivos de negocio, las acciones del personal estaban orientadas a hacer ver bien a IT, esto incluía desarrollo y atención a usuarios.

Cuando el centro de control de negocio fue desarrollado, le reportaba a la división de negocios, con el tiempo y después de varias reorganizaciones, el centro de control fue trasladado y empezó a reportar al equipo de desarrollo. El objetivo no escrito se había convertido en hacer ver bien a los equipos de desarrollo. El monitoreo proactivo, que había sido efectivo previamente, se descuidó para reducir la atención en las causas principales de los problemas que

afectaban a los usuarios: cambios hechos por los equipos de desarrollo.

Recomendación

Un centro de control nunca debe ser puesto en una posición donde pueda haber conflicto de intereses. El gerente responsable de supervisar todas las actividades del centro de control de negocio debe reportar ya sea a las divisiones de negocio a las cuales monitorea o a una tercera parte independiente.

Cuando el conflicto de intereses y, por consecuencia, todos los obstáculos para la transparencia, es eliminado, se puede progresar la automatización de todas la funciones manuales, quitando las funciones relacionadas con desarrollo y las funciones secundarias, implementando monitoreo proactivo y creando un equipo independiente de supervisión de problema.

- Un equipo independiente de supervisión de

problema también servirá para garantizar la transparencia y la comunicación de los eventos cuando estos ocurren.

- El monitoreo proactivo, la automatización y la supervisión de problema adecuada:
    - Ayudarán a identificar las causas de las fallas
    - Reducirán la duración de las interrupciones
    - Reducirán la cantidad de situaciones recurrentes
    - Presentarán a la directiva una visión de los problemas confiable y sus

verdaderas causas

Caso de estudio #6

Clientes atrasados

Al pasar el tiempo y como resultado de un crecimiento y las adquisiciones, el número de clientes aumentó. Este es un problema que a la mayoría de las empresas les encantaría tener. Al crecer el número de cuentas, los sistemas centrales fueron actualizados para poder seguir el ritmo de la demanda. Desafortunadamente, aunque hay mucho hardware que se puede agregar, en algún momento, especialmente con códigos de programación antiguos, incrementar la velocidad de procesamiento, el tamaño del disco, y el tamaño de la memoria ya no tendrá ningún efecto en cuanto tiempo toma una aplicación en completarse. Para aprovechar los nuevos avances tecnológicos tales como multiprocesadores y otras mejoras complejas, muchos de los

programas viejos necesitan ser completamente reescritos, usualmente a un costo muy alto y a expensas del desarrollo de otras mejoras críticas que las divisiones de negocio requieren para poder seguir creciendo.

Este punto fue alcanzado por las aplicaciones que producen estados de cuenta diarios semanales y mensuales de los clientes; los estados de cuenta semanales y mensuales atrasados se volvieron la norma; los estados de cuenta diarios se completaban a tiempo el 75% de las veces si no había problemas durante el procesamiento del otro. En las noches, que era cuando se encontraban problemas, los estados de cuenta diarios se retrasaban 100% de las veces.

Los equipos de desarrollo de aplicación enfrentaban una gran presión de la directiva para que atendieran el problema de entrega tardía de estado de cuenta. Después de 6 meses de modificar el código

existente y de hacer otras mejoras de desempeño, alcanzaron solo mejoras mínimas, reduciendo los retrasos levemente pero sin poder dejar de incurrir en el retraso.

Después de las mejoras, en los casos donde todo el procesamiento era perfecto y sin problema, los estados de cuenta semanales de los clientes eran enviados cerca de un día tarde; en los casos donde había problemas en el procesamiento, los estados de cuenta semanales se retrasaban 2 o 3 días y los mensuales cerca de 1 semana.

El gerente de los equipos de desarrollo estaba frustrado y no podía asignar personal para reescribir toda la aplicación de estados de cuenta en ningún momento del futuro cercano así que, le pidieron ayuda al equipo de mejora de proceso del centro de control.

Objetivo

Entregar los estados de cuenta de los clientes a tiempo.

Análisis

La aplicación de estados de cuenta consistía de salidas diarias, semanales y mensuales, cada una de las cuales era disparada cuando la salida previa se completaba. Un proceso similar a la teoría de restricciones fue utilizada para vigilar el flujo del proceso completo de estados de cuenta para determinar cuellos de botella.

Un análisis encontró que cuando los estados de cuenta diarios estaban en tiempo, los estados de cuenta semanales se realizaban durante el fin de semana cuando el procesamiento de cómputo estaba en su nivel más bajo; si había retrasos, el proceso semanal seguiría en los días de la semana (entre semana) pero ahora en el tiempo en que la utilización estaba en sus niveles más altos, provocando que el proceso de estados de cuenta y otro procesos que se llevaban al mismo tiempo tomaran mucho más

tiempo en completarse, causando retrasos también en otras aplicaciones

Lo mismo ocurría con el procesamiento mensual, teniendo un efecto aún más adverso en otros procesos.

Los flujogramas revelaron que la mayoría de los procesamientos de estado de cuenta tenían un solo flujo, esto es, que hasta que terminara totalmente el proceso que se estaba ejecutando, no empezaba el siguiente. Había muy pocas aplicaciones de estados de cuenta que pudieran ejecutar más de un proceso simultáneamente. En una revisión de la duración de los procesos se encontró que estas variaban mucho.

Teóricamente, el procesamiento de estados de cuenta debería tomar el mismo tiempo en cada proceso de un número determinado de cuentas; algunas variaciones fueron provocadas

por cuellos de botella del proceso pero, la gran mayoría de los procesos más largos eran provocados por limitaciones en el subsistema de entradas y salidas. Esta era la parte de la computadora central que leía y escribía información. Las aplicaciones de estados de cuenta procesan una tremenda cantidad de información y cualquier cuello de botella al leer o escribir dicha información tendrá un efecto adverso en todo el proceso. En muchos casos esos cuellos de botella duplican o triplican la duración, provocando retrasos en la entrega de estados de cuenta.

Se encontró que se estaban usando dos archivos muy grandes para la mayoría de los procesos diarios, semanales y mensuales de estados de cuenta. Los archivos de nombres y direcciones eran los que más se utilizaban seguidos por los archivos de historial. Casi todos los procedimientos de lote de estados de cuenta que duraban mucho, a causa de los cuellos de botella de

entrada/salida, utilizaban uno o ambos archivos mencionados.

Otro cuello de botella era causado por los archivos en sí mismos; dado que estos archivos eran muy grandes, se les guardaba en cintas de cartucho físicas, lo cual implicaba que podían ser usadas en una sola aplicación cada vez.

El tercer cuello de botella era el job del lote principal (el grupo de programas de aplicación que procesan la información), el cual creaba los estados de cuenta diarios. La duración del job de lote variaba de 1 a 4 horas. Además, todo en el flujograma del procesamiento de estados de cuenta estaba detenido hasta que el job de lote terminara. Observado más de cerca, se encontró que el job de lote estaba compuesto de muchos pasos, cada uno creando estados de cuenta para una categoría de negocio específica.

El cuarto cuello de botella eran errores de lectura y escritura en la cinta.

Debido al tamaño y al uso continuo de los archivos, de vez en cuando se daban errores de lectura o escritura que detenían todo el proceso de estados de cuenta hasta que se creaba una nueva serie de archivos.

Solución

Las computadoras centrales tienen la capacidad de usar almacenamiento virtual, similar a la memoria flash, para información a la cual se accede continuamente; este tipo de almacenamiento es caro y se reserva, usualmente, a archivos pequeños. Esta solución no fue considerada previamente para estos archivos pues funciona solo con archivos guardados en disco, no funciona para archivos guardados en cinta o cartucho. Con los precios de almacenamiento mucho más bajos de lo que solían ser, se adquirió almacenamiento adicional para esos archivos.

El primer cambio fue crear los archivos en disco en vez de en cinta; fue un cambio simple y tuvo un efecto

inmediato en el procesamiento, 15% de mejoría. No mucho tiempo después, los archivos fueron agregados a la aplicación de supervisión de almacenamiento virtual, la cual cargó en su memoria, las partes de los archivos a las que se tenía acceso con mayor frecuencia. Este cambio es transparente a las aplicaciones de estados de cuenta: los archivos y el trabajo de procesamiento seguían iguales pero el efecto del cambio se veía en que ya no había cuellos de botella de entrada/salida. Esto generó un 10% de mejoría, adicional, pero aún más importante fue que la duración de los procesos se volvió más consistente.

Con estos cambios, fue posible modificar el flujograma de los procesos de estados de cuenta. Los procedimientos de lote que tenían que ser corridos uno a la vez porque los archivos utilizados estaban en cartuchos, pudieron ser leídos simultáneamente. 5 jobs de lote que requerían 5 horas para terminar,

pudieron hacerse en 45 minutos después de los cambios.

El siguiente cambio fue dividir el job de lote que generaba los estados de cuenta diarios, en Jobs separados y más pequeños; con los archivos almacenados virtualmente, los Jobs más pequeños podían ejecutarse simultáneamente, permitiendo que se completaran en 20 minutos.

Los retrasos debidos a errores de lectura o escritura en la cinta, fueron virtualmente eliminados; si existía algún error al crear los respaldos de los archivos en cinta o cartucho, el proceso de respaldo se reiniciaba sin ningún impacto en el proceso de lote de estados de cuenta que se estaba procesando.

Después de la implementación de los cambios, los procesamientos de estados de cuenta diarios, semanales y mensuales empezaron a terminar antes de los tiempos preestablecidos.

Seguimiento

Consecuencias no intencionales: como resultado de los cambios en el lote de estados de cuenta, otros procesos de lote que se retrasaban con frecuencia debido al procesamiento continuo y a los requerimientos de entrada/salida de los Jobs de estados de cuenta, empezaron a completarse antes de lo usual.

Cierre

Existen dos momentos en los cuales un centro de control realmente brilla: cuando se implementa por primera vez y en una crisis mayor.

Cuando un centro de control es implementado por primera vez con las funciones apropiadas, herramientas, estándares, controles y estructura de supervisión, los directivos verán los frutos de aquellos cambios en los reportes de tendencias. Verán reducción en las quejas de los clientes y en los gastos, con su correspondiente aumento en los ingresos. Los gerentes de IT verán disponibilidad de sistema mejorada,

indicadores de calidad y una fuerza de trabajo más productiva.

Un centro de control realmente brilla durante una crisis porque es entonces que se vuelve visible a los altos dirigentes, a menos de que la crisis haya sido creada por el mismo personal del centro de control. Observar a un centro de control, eficiente y debidamente implementado, desarrollar manejo de crisis, es poesía en movimiento: las notificaciones y escalamiento suceden como un mecanismo de relojería; todo lo que pasa es totalmente documentado; no se deja ninguna piedra sin voltear hasta que la crisis es resuelta y, aún entonces, la atención se vuelve hacia la prevención.

Desafortunadamente, esos momentos son pocos y muy de vez en cuando; con el tiempo la gente tiende a olvidarlos y a seguir adelante, solo para ser reemplazados por nuevos dirigentes que no están familiarizados

con los centros de control y sus beneficios e historia.

Los problemas en los centros de control usualmente ocurren cuando una nueva gerencia, no familiarizada con la automatización y sin idea del entorno previo, viene y empieza a hacer cambios. Los miembros del personal que monitorean las pantallas son vistos como fuerza de trabajo para otras labores. Las ramificaciones de cualquier cambio no son aparentes sino hasta después de algún tiempo y, lo más importante, los primeros en darse cuenta son los mismos líderes de negocio cuando empiezan a aumentar las quejas de los clientes.

En muchas ocasiones los centros de control se condenan por su propio éxito. Esto pasa mayormente cuando la gerencia falla al promover los logros alcanzados o las interrupciones evitadas por el centro de control, pues, lo que sucede entonces, es que otros departamentos toman el crédito

por los resultados de las mejoras hechas por el centro de control y este último, lentamente empieza a cambiar de ser proactivo a ser reactivo.

Los centros de control también tienen problemas cuando se hacen comparaciones del tipo manzanas y naranjas, entre un entorno manual y uno automatizado. La comparación suele hacerse en cuanto a la cantidad de trabajo desarrollado en vez de ser en cuanto a lo productivo que es el trabajo o el tamaño del entorno. A primera vista, un centro de control con 5 miembros del personal monitoreando pantallas de alerta va a parecer menos productivo que un equipo con 10 miembros súper ocupados metiendo instrucciones en sus teclados y llenando formatos. El hecho de que 30 computadoras centrales estén siendo monitoreadas y operadas en el centro de control con cinco miembros del personal por turno contra 4 computadoras centrales con 10 miembros, se vuelve irrelevante.

Muchos problemas pueden ser mitigados con las métricas correctas, que deben incluir la cantidad de interrupciones y eventos importantes que hayan sido evitados y, la promoción de logros en mejora de procesos. Estas dos características deben ser consideradas tan importantes como cualquier otra acción dentro del centro de control.

Además de las mejoras en el servicio, un centro de control implementado correctamente puede reducir los costos de IT, mejorar el índice de éxito en recolocación y consolidación de centros de datos, y reducir el tiempo para absorber nuevas adquisiciones. La consolidación del centro de control reduce riesgos y tiempos muertos al eliminar confusiones en cuanto a quién llamar para supervisión de incidentes y permitiendo que los estándares y mejores prácticas pasen sin interrupciones hacia nuevos sistemas.

Un poco más de tiempo invertido en la etapa de planeación puede ayudar a asegurar que tu centro de control sea un recurso valioso para la compañía. Un centro de control sin las funciones apropiadas nunca será tan efectivo como uno que si las tenga, sin importar cuánto monitoreo se lleve a cabo.

Mostrar lo exitoso que es el centro de control, generando y distribuyendo las métricas correctas, ganará el respaldo y apoyo de la directiva y de los líderes de IT. La promoción de las mejoras hechas y de las interrupciones evitadas por el centro de control ayudará a asegurar que al paso del tiempo y con la venida de nuevos directivos, el centro de control permanezca como el motor principal para estándares, mejores prácticas, automatización y, lo más importante, monitoreo proactivo.

Epilogo

Global Financial Holdings ha estado en las noticias todos los días desde el

miércoles en la mañana, con reporteros y clientes preguntando si el banco se ha vuelto insolvente. A excepción de la mayoría de la gente en Texas, casi todo el país ve estas noticias, incluyendo al Secretario del Tesoro, Ben Heyward.

Heyward no llegó tan lejos en su carrera política, esperando a ver como pasan las cosas; cuando leyó por vez primera acerca de los problemas con las computadoras de Global Financial, sospechó que las cosas podrían estar peor de lo que parecían. Sus sospechas son confirmadas el miércoles en la tarde cuando el presidente de la compañía, Victor G. Capistrano, un amigo desde el colegio, le llama para ponerlo al tanto de los problemas del banco y para pedirle un favor.

Los dos saben que los reguladores estarán respirando en el cuello de Capistrano la mañana siguiente si los sistemas no están disponibles aún. Capistrano le pide a Heyward que

haga un poco de ‘interferencia’ que le dé tiempo a Global de corregir la situación.

Terminando la llamada, Heyward le llama a Sharon Lazinby, presidenta de FDIC, cuyo trabajo, llegadas esas instancias, será decidir la suerte de Global.

Heyward and Lazinby tienen entonces una conversación privada con sus más cercanos consultores para decidir el curso de acción en caso de que Global no pueda restaurar su servicio.

La decisión es acercarse a la cabeza de TAG Bank Holdings, Steven Van Olsen, y pedirle que se haga cargo de Global Financial. TAG, la sociedad financiera mixta más grande, es conocida por tener la división de IT más eficiente en el sector.

A la siguiente mañana, Lazinby y Heyward hacen una visita privada a Olsen y Paul Hamilton, presidente de TAG, y les explican los problemas del centro de datos de Global Financial y

les ofrecen varios días para que puedan formular un plan y tomar una decisión.

Olsen platica con Hamilton, el arquitecto detrás de la estrategia de tecnología de TAG, quién hace una pregunta: ¿Cuál es el estado de los sistemas de cómputo y cintas de respaldo de Global Financial?

Heyward no puede contactar a Capistrano así que instruye a FEMMA para que mande personal a cada centro de datos para obtener un reporte de estado; en 2 horas se entera de que todo el equipo en cada centro de datos está operando normalmente usando un generador de energía y todos los respaldos de información han sido completados y están listos para ser enviados al depósito externo.

Cuando Olsen y Hamilton reciben la información, tienen una junta privada. Dos horas después, Olsen acepta hacerse cargo: TAG tomará control de Global Financial una vez que se

apruebe su decisión. Los clientes tendrán acceso a sus cuentas tres días después de la absorción.

Los huracanes deshabilitaron uno de los centros de control de TAG y uno de sus centros de datos. Al paso de los años, TAG ha consolidados equipo en tres grandes centros de datos a lo largo del país y personal dentro de tres centros de control localizados estratégicamente lejos de los centros de datos y cerca de áreas metropolitanas.

Los miembros del personal de los dos centros de control restantes desarrollan su trabajo sin ningún impacto y empiezan inmediatamente sus procedimientos de recuperación para rehabilitar las aplicaciones afectadas por la paralización del centro de datos. Después de dos horas, todas las aplicaciones han sido recuperadas y todo opera sin interrupciones usando los dos centros de datos restantes. La mayoría de los clientes no notan que hay una

interrupción. A los miembros del personal del centro de control de Dallas y del centro de datos de Houston se les da el resto de la semana libre para que puedan estar con sus familias y disponibles como voluntarios.

Siete días después de que Global Financial tuvo el problema, Mike Silverman, el jefe de tecnología temporal de la compañía, le llama a Capistrano para informarle que la compañía encargada de la movilización del equipo de cómputo está teniendo problemas para movilizar el personal suficiente para hacer el trabajo. El movimiento requiere por lo menos 6 personas y hasta el momento la compañía de mudanzas solo ha podido traer a dos. El resto de los equipos en Texas están ocupados trabajando con Fema y la compañía de electricidad para reestablecer la energía y las comunicaciones pero, tienen dos miembros disponibles en la costa oeste y tres más en Florida.

Capistrano autoriza el gasto adicional para la compañía de mudanzas y termina la llamada sabiendo que pronto se quedará sin trabajo. No hay más tiempo, ha retrasado la llamada a Anderson y a los federales, esperando que las cosas mejoraran durante el fin de semana pero, éstas últimas noticias refuerzan su idea de que todo está terminado para Global Financial. Las llamadas deben ser hechas ahora.

Capistrano llama primero a Hayward, su corazón desfallece cuando Hayward le dice que tienen un plan para recuperar las cuentas de los clientes entregando su banco a TAG Bank Holdings y que las LAZINBY tiene una conferencia de prensa lista. La llamada termina rápidamente y Capistrano se siente de alguna manera aliviado. Ahora puede tomar esa vacaciones que su esposa le ha estado pidiendo los últimos 4 años.

En cuestión de minutos se hace la conferencia de prensa y se da la aprobación a Olsen.

Trabajando conjuntamente con FEMA, el Departamento del Tesoro, la oficina del gobernador y funcionarios locales, vehículos blindados son enviados a cada centro de datos para recoger y transportar todas las cintas de respaldo a los centros de datos de TAG. Son enviados carros para transportar al personal técnico de Global a los centros de control de TAG. El plan para mover el equipo de Global es cancelado.

Son instalados platos satelitales de alta velocidad en los techos de cada centro de datos de Global y estos son conectados a su red. Cualquier tipo de información que no quiera ser recuperada usando las cintas de respaldo será tomada en tiempo real usando los enlaces satelitales.

Tres días después, los sistemas de cómputo principales de Global son restablecidos usando equipo en los centros de datos de TAG. Las pruebas confirman que los cajeros automáticos (ATM) están trabajando que los

clientes pueden acceder a sus aplicaciones. El trabajo continuará en el curso de los siguientes días para corregir problemas que puedan ocurrir, pero en su mayor parte Global Financial Holdings está de regreso ahora con el nuevo nombre de TAG Globla Financial.

Acerca del autor

Abdul Jaludi tiene 28 años de experiencia con centros de control en la industria de servicios financieros. Ha patrocinado y defendido la eficiencia operacional y de monitoreo como un elemento crucial para cubrir las necesidades y expectativas de los clientes de manera exitosa y consistente. Facilitar estabilidad 24/7 y disponibilidad dentro del ambiente de negocios de intensa presión competitiva y estrictas regulaciones ha sido un ensayo siempre cambiante a lo largo de su trayectoria; sin embargo es dentro de ese entorno de retos y

grandes riesgos que Jaludi se ha convertido en un líder exitoso.

Sus contribuciones incluyen ayudar a establecer una de las computadoras centrales más eficientes en el entorno bancario en el mundo y dirigir muchas innovaciones que se han convertido en el stand-by global dentro de su antigua organización. Sus logros incluyen innovación y optimización de departamentos, funciones, procesos y herramientas. Transformó operaciones de plataforma manual basada en papel a procesos completamente automatizados mucho antes de que las herramientas de automatización existieran o siquiera se pensara que fueran prácticas o posibles. Jaludi ha desarrollado numerosas auditorías en centros de control para identificar y corregir las razones de la insatisfacción de los clientes. Su trabajo incluyó una revisión completa del monitoreo, del procesamiento de lote nocturno, de la notificación de alerta de incidentes, de la supervisión de incidentes y

problemas y de los reportes de servicio al cliente.

También ha completado muchas consolidaciones de centros de control, usualmente, sub-productos de funciones y adquisiciones, llevados a cabo para mejorar el servicio al cliente, reducir los tiempos muertos y mejorar la entrega a tiempo de estados de cuenta y de procesamiento de lote nocturno, a tiempo de reducir los gastos.

La experiencia de primera mano de Jaludi lo ha facultado para entender completamente la manera en que la mejora de proceso, la gestión de cambio y la cultura corporativa son factores críticos que determinan como una organización puede aprender y reaccionar de manera eficiente a los cambios constantes en el entorno de negocios. Las lecciones aprendidas durante 28 años son el génesis de este libro, el cual se enfoca en el concepto de mejora de proceso, como implementar cambios e innovación y

el papel del liderazgo en hacer estos elementos cruciales de éxito una parte integral de la cultura corporativa.

AGRADECEMOS QUE TE HAYAS DADO LA OPORTUNIDAD DE LEER ESTE CONTENIDO.

SI DESEAS SABERS MÁS DE ESTE TEMA Y/O CASOS DE EXITO DE SU APLICACIÓN EN MEXICO,

COMUNICATE CON NOSOTROS

www.onet.com.mx

info@onet.com.mx

 @ONET

 ONET