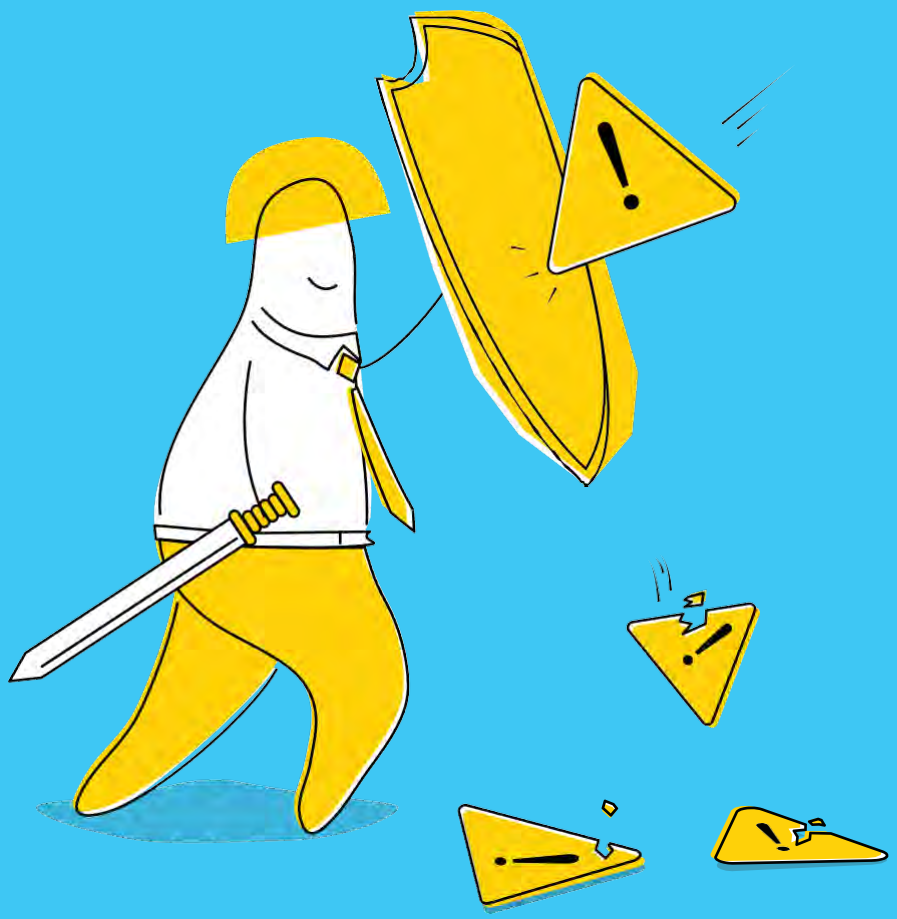
ManageEngine



MANUAL DE GERENCIAMENTO DE INCIDENTES

COMO GERENCIAR O ESPECTRO DE INCIDENTES DE TI

Conteúdo

“Ufa! Essa foi por pouco.
Tomara que isso nunca aconteça de novo!”

Introdução

Na última década, combatemos milhares de incidentes.

Como pioneiros, experimentamos incidentes de baixo impacto que normalmente precisavam de técnicos, mas ainda exigiam uma estrutura de gerenciamento de incidentes (IM) bem estabelecida. Para a maioria deles, confiávamos na solução de problemas pelas pessoas. No entanto, à medida que nossa infraestrutura de TI cresce, enfrentamos incidentes mais complexos e de alto impacto, forçando-nos a aprimorar nosso processo de gestão.

Percebemos logo que não há um processo único para gerenciar todos os diferentes tipos de incidentes enfrentados por nossa organização. Portanto, tomamos as estruturas que foram mais eficazes e adicionamos, combinamos ou omitimos etapas para lidar com cada tipo de acordo com seu impacto e em nossas operações de negócios. Isso garante que cada resposta seja bem adaptada aos desafios apresentados.

O resultado? Nosso processo gora se estende além das estruturas estabelecidas do setor. Nossas estruturas são classificadas com base na gravidade e no impacto que os diferentes tipos de incidentes têm nas operações de negócios.

Estrutura de IM		Impacto	Cenários
Desktop sprint	• Interromper/corrigir incidentes que afetam cada usuário	• Um único usuário é afetado • Nenhum serviço crítico está envolvido	• Redefinições de senha • Internet lenta
	• Incidentes de impacto baixo ou médio que afetam grupos de usuários ou departamentos	• Um único usuário VIP é afetado • Um pequeno grupo de usuários finais é afetado • Não há possibilidade de perda financeira	• O notebook do CEO não está funcionando e não consegue enviar e receber comunicações • Uma impressora não está funcionando em um andar específico
Big bang	• Alta urgência • Afeta o serviço	• Um determinado componente de serviço, aplicação ou infraestrutura essencial aos negócios está indisponível, e o tempo estimado para recuperação é desconhecido ou muito longo • Serviço não disponível. Restauração imediata do serviço é esperada	• Nossa conexão de rede de alta velocidade falha, e a comunicação interna e externa da organização é interrompida • A funcionalidade principal de uma aplicação está inativa, afetando vários clientes • Uma de nossas aplicações está indisponível Um ataque de negação de serviço distribuído (DDoS)
Pane total	• Urgência imediata • Situações críticas ou de alerta vermelho que afetam os negócios	• Afeta os resultados financeiros da empresa • Grande impacto sobre receita, reputação e casos legais	• Bugs de software e vulnerabilidades • Malware • Ameaça persistente avançada (APT) • Ransomware • Phishing e engenharia social • Ameaça interna

Quando se trata de mensagens instantâneas, não há uma solução única, pois cada organização é diferente. O que funcionará para sua organização dependerá do seu modelo de negócios, infraestrutura, operações, informações que você está protegendo, seus recursos e muito mais. Algumas técnicas só vêm com tempo e experiência. No entanto, isso não deve desencorajá-lo de começar!

Para quem serve este guia?

Este e-book foi escrito para líderes, gerentes e profissionais de TI sob uma perspectiva de gerenciamento de serviços. Vamos orientá-lo em nossos processos de IM com fluxos ilustrados, funções e práticas recomendadas. Este guia está repleto de lições que aprendemos com tentativa e erro, para que você não tenha que aprender dessa forma.

Antes de entrarmos nos detalhes, vamos tirar o básico do caminho.

O que é um incidente?

Um incidente é uma interrupção não planejada que pode causar ou reduzir a qualidade de um serviço de TI. Alguns exemplos clássicos são que a internet ficou lenta, uma aplicação empresarial ficou indisponível ou uma impressora não funciona.

A verdade é que podemos definir um incidente de muitas maneiras. O que mais importa é que cada um deles tenha uma resposta e resolução bem estruturadas e oportunas.

O que é gerenciamento de incidentes?

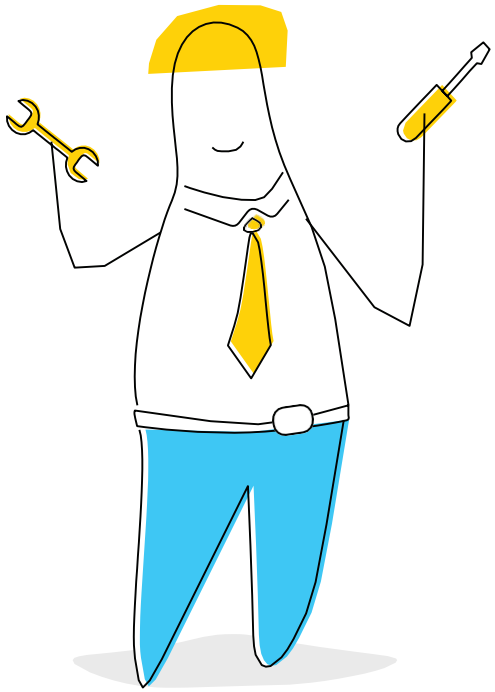
O gerenciamento de incidentes é uma maneira de restaurar as operações normais de serviço o mais rápido possível, minimizando qualquer impacto adverso nas operações de negócios ou no usuário.

Nossos valores de incidentes

Princípios do incidente	Abordagem
Seja proativo, não reativo	• Uma abordagem proativa: a manutenção preventiva é realizada regularmente para reduzir a probabilidade de falha, antes mesmo que os usuários sejam afetados. • As ferramentas de monitoramento fornecem visibilidade da integridade e do desempenho da rede e nos alertam sobre problemas antes que eles se tornem incidentes.
Seja aberto e comunique-se	• Comunicamos nossos clientes cedo e com frequência para que eles saibam que estamos cientes e trabalhando no problema. • Um grupo predefinido de partes interessadas é notificado automaticamente por meio de seus métodos de contato preferidos quando ocorre um incidente.
Alinhe as equipes, colabore com eficiência	• Distribuímos equipes de vários fusos horários trabalhando juntos durante incidentes de alto impacto, discando para um número de ponte de teleconferência e utilizando aplicações de comunicação ou produtividade para lidar com o incidente.
Retome rapidamente	• O gerenciamento de incidentes pode significar muitas coisas. No entanto, para nós, isso se traduz em gerenciamento de tempo. • Utilizamos o Site24x7, que nos permite saber assim que algo para de funcionar. Ficar à frente dos problemas é crucial para a nossa IM. Às vezes, nossos funcionários se transformam em um sistema de alerta. Eles usam nossos sistemas diariamente e provavelmente serão as primeiras pessoas a perceber quando algo não está certo. • Temos um sistema de mensagens instantâneas aberto, seguimos protocolos quando necessário e trabalhamos em equipe para resolver o problema o mais rápido possível.
Documente as lições	• Às vezes cometemos erros. Quem não comete? No entanto, garantimos que aprenderemos com esses erros, documentando as lições aprendidas.
Melhore continuamente	• Mergulhamos profundamente no que deu errado para garantir que não cometeremos o mesmo erro duas vezes. • Às vezes, realizamos incidentes simulados para ver como nossa estratégia se comporta, e continuamos a ajustá-la antes da situação real.

Nossas ferramentas de IM

Utilizamos várias ferramentas para auxiliar nossos processos



Incidentes na área de trabalho

Rastrear e gerenciar incidentes:

O ServiceDesk Plus Cloud é personalizado para se ajustar aos nossos processos de gerenciamento de incidentes.

Redefinições de senha:

O ADSelfServicePlus é uma ferramenta de autoatendimento para redefinição de senha.

Gerenciamento de senhas:

Password Manager Pro é um cofre seguro para armazenar e gerenciar informações confidenciais compartilhadas, como senhas, documentos e identidades digitais de empresas.

Gerenciamento de endpoints

O Desktop Central é uma solução integrada de gerenciamento de endpoints que ajuda a gerenciar servidores, notebooks, desktops, smartphones e tablets a partir de um local central.

Incidentes graves de disponibilidade

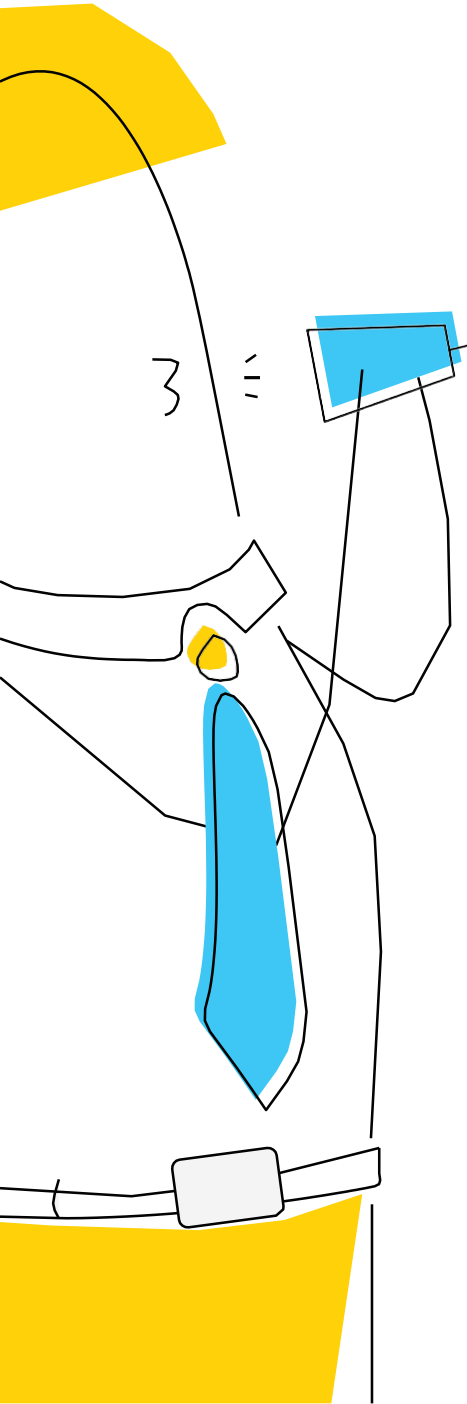
Ferramenta de alerta:

Usamos o Site24x7 para monitorar a disponibilidade de servidores e aplicações.

Incidentes de segurança

Programa Bug Bounty:

O Bug Bounty é uma ferramenta de terceiros para funcionários e indivíduos relatarem bugs, como explorações e vulnerabilidades.



Comunicação

Nota:

Também usamos sites de redes sociais, plataformas de mensagens como WhatsApp e chamadas telefônicas como formas alternativas de comunicação caso o Cliq fique inativo, pois é importante ter meios alternativos de comunicar durante um desastre.

Documentação:

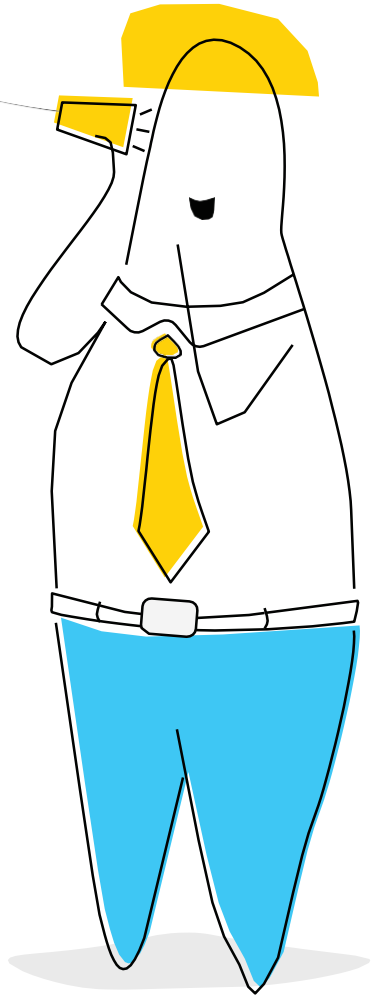
O Zoho Docs é um sistema central para armazenar todos os documentos de análise de incidentes e causas raiz (RCA).

Chat:

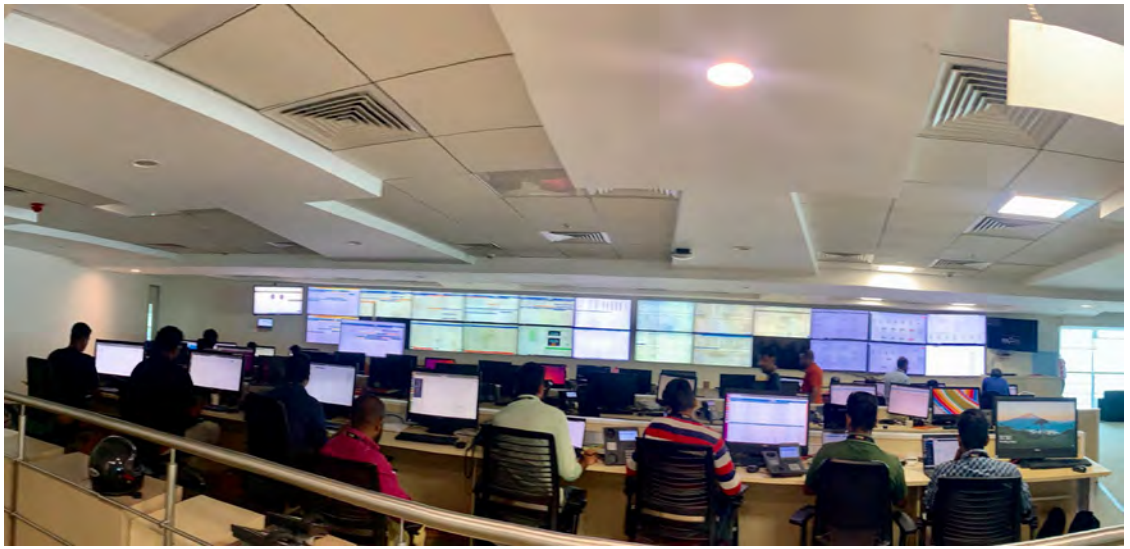
O Zoho Cliq é uma aplicação de mensagens empresariais em tempo real que ajuda nossos funcionários a se comunicarem de forma eficaz a qualquer momento, inclusive durante um incidente.

Colaborar:

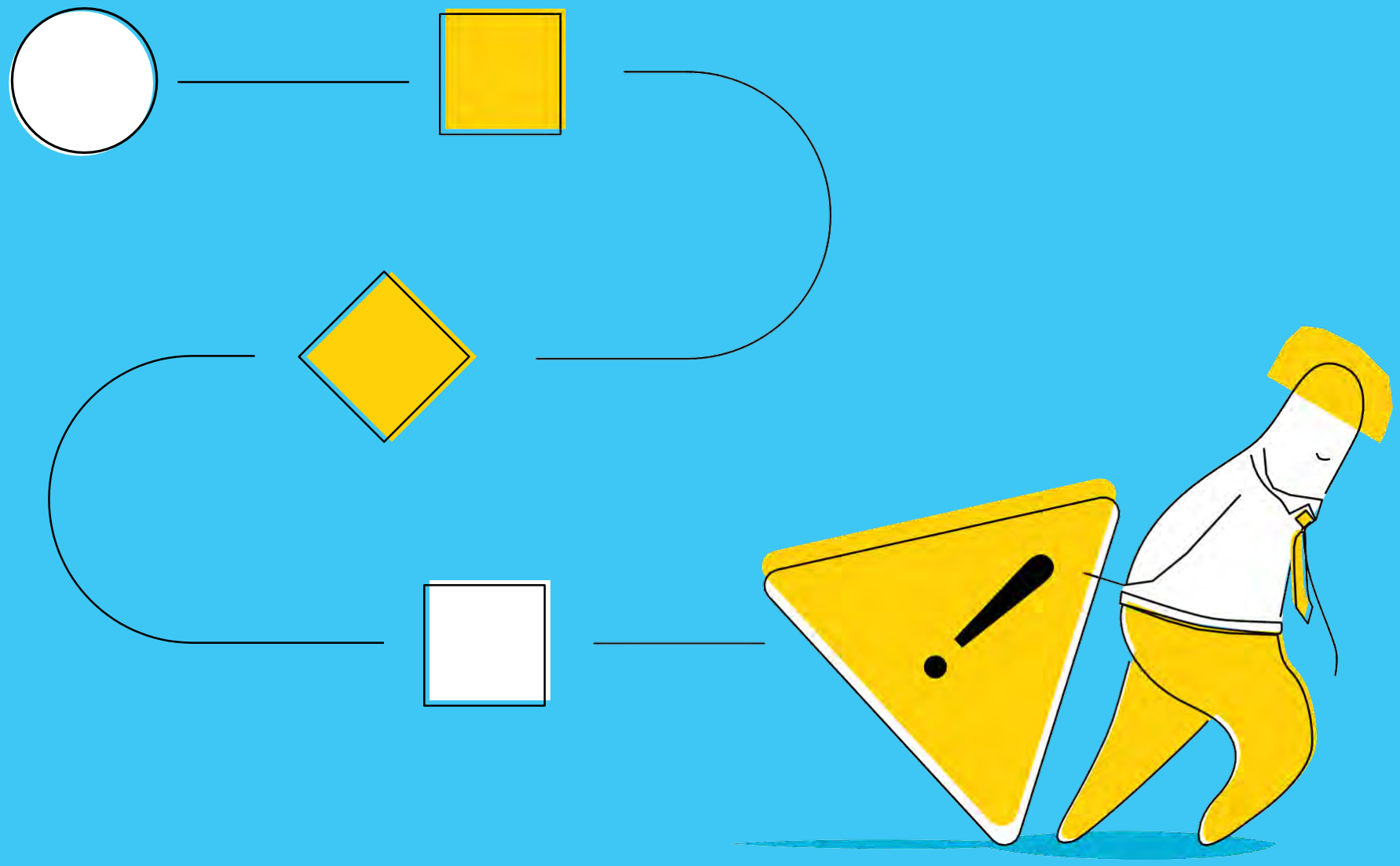
O Zoho Connect é um software de colaboração que garante que todas as equipes falem a mesma língua ao resolver incidentes. Alguns o chamam de Facebook do nosso local de trabalho.



Nosso centro de comando de gerenciamento de incidentes (IMCC)



Nosso centro de comando de gerenciamento de incidentes (IMCC) é uma grande sala segura com telas grandes, semelhantes à NASA, de dispositivos de monitoramento para fornecer métricas e visibilidade detalhadas, permitindo que nossas equipes de IM reajam rapidamente e solucionem problemas de forma eficaz durante incidentes. Esta sala hospeda três equipes principais: a equipe do centro de operações de rede (NOC), a equipe da Zoho e a equipe de administração central do sistema. Temos controle de acesso dinâmico em outros locais de trabalho para realizar atividades de monitoramento.



PROCESSO DE GERENCIAMENTO DE INCIDENTES

Desktop sprint
(interrupção/correção e incidentes de baixa importância)

Big bang
(Incidentes graves de disponibilidade)

CyberSec
(pane total ou incidentes críticos)

Desktop sprint

(Incidentes na área de trabalho)

Equipes, funções e responsabilidades

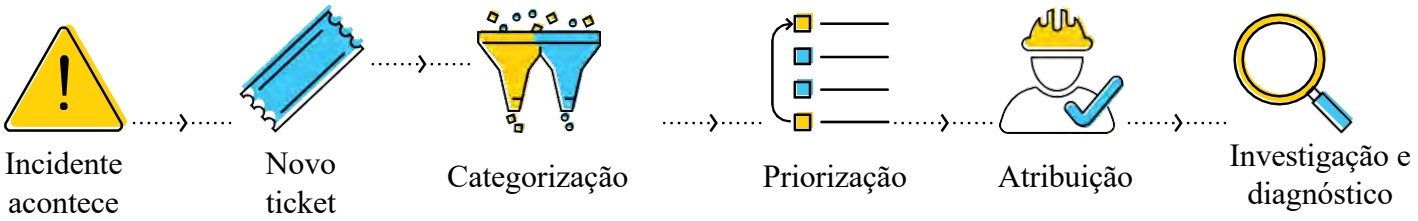
Técnicos do PitStop:

Assim como qualquer organização de TI, nossa equipe de suporte da linha de frente lida com incidentes na área de trabalho. Chamamos nosso centro de suporte de TI de PitStop.

Equipe central sysadmin:

Temos uma equipe central de administração de sistemas como parte de nosso centro de comando de gerenciamento de incidentes que supervisiona todos os incidentes recebidos em nosso prédio de 12 andares. Nós colocamos um PitStop com um técnico em todos os andares; na ausência de um técnico em um andar, a equipe central do sysadmin lida com os incidentes de desktop naquele dia específico.

Na maioria das vezes, os incidentes são encaminhados aos técnicos pelo coordenador que supervisiona todos os incidentes de desktops recebidos usando regras de negócios em nossa ferramenta de gerenciamento de serviços de TI (ITSM). Os técnicos também podem atribuir tickets automaticamente na ausência do coordenador.

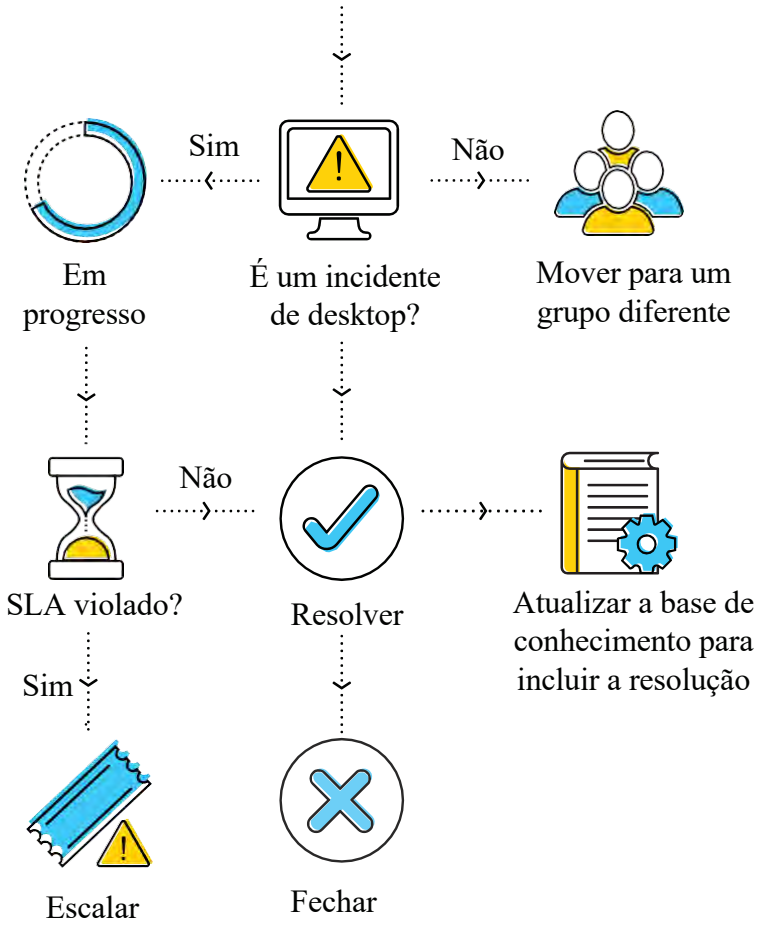


O processo

Em um dia típico, nossos técnicos do PitStop solucionam incidentes de baixo a médio impacto, como redefinições de senha, problemas de impressora e problemas de rede, e executam uma variedade de tarefas, incluindo:

- Comunicar interrupções de serviço a todos os usuários finais.
- Abrir a comunicação com os usuários finais para investigar e reunir o máximo possível de informações sobre incidentes para resolução rápida. Criar solicitações de alterações ou registros de problemas.
- Aderir aos contratos de nível de serviço (SLAs) de incidentes e encaminhá-los conforme necessário.
- Resolver e encerrar incidentes.
- Fornecer atualizações de status aos usuários finais durante todo o ciclo de vida do incidente.

Para lidar com incidentes do dia a dia, usamos um modelo de resolução de alta velocidade com o qual você provavelmente está familiarizado. É um processo simples e direto que aborda obstáculos e garante um fluxo contínuo.



Novo incidente

Um incidente normalmente começa com nossos funcionários relatando um problema por meio de um e-mail, chamada telefônica, chat ao vivo ou portal de autoatendimento em nossa ferramenta ITSM. O incidente é registrado como um ticket de incidente e preenchemos os seguintes detalhes padrão.

Título	Resumo do incidente
Descrição	Forneça detalhes para ajudar os técnicos a diagnosticarem o incidente e resolver mais rápido
Impacto	Quem foi afetado - um usuário ou toda a operação de negócios?
Urgência	Quão rápido o incidente deve ser resolvido?
Prioridade	Qual a importância do incidente baseado no impacto e na urgência?
Grupos	Qual grupo de resolução irá cuidar do incidente? Por exemplo, criamos grupos para problemas específicos como hardware, software, impressoras, etc.
Ativos	Quais os ativos e serviços que são afetados devido ao incidente? É um único ativo ou múltiplos ativos?

Após o registro, o incidente é movido para o estado aberto, que é o primeiro estado em nosso fluxo de trabalho de incidente.

Categorização

Nosso coordenador de incidentes começa com a atribuição as categorias e subcategorias corretas para fácil classificação. Sem categorização, o gerente não saberá quantos problemas de sistema operacional e aplicações tivemos ou quais ações precisam ser tomadas para reduzir esses incidentes.

Categorizamos pelos seguintes motivos.

- Para agrupar incidentes semelhantes em uma categoria comum para acelerar o ciclo de vida do incidente.
- Para rotear e atribuir incidentes automaticamente às equipes certas para resolução rápida, por exemplo, atribuir automaticamente problemas relacionados ao Linux à equipe certa.
- Para análise de problemas.
- Para gerar um relatório bem estruturado.

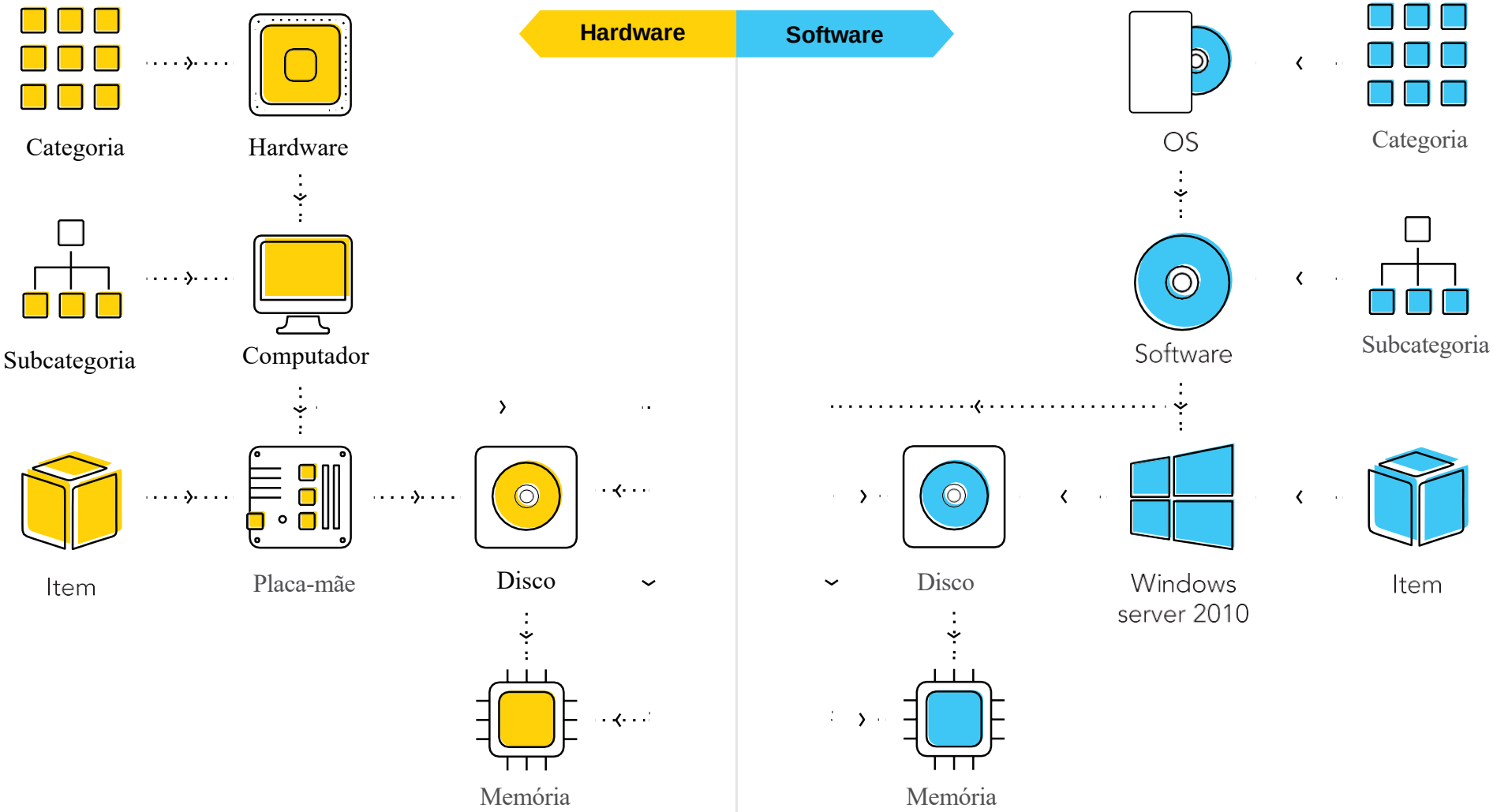
Como prática recomendada para categorização eficaz, nós nos limitamos a três níveis de categorização. Muitos níveis podem complicar o processo, e poucos níveis podem acabar com o propósito. Ela geralmente começa com a categoria principal, depois uma subcategoria e, finalmente, o item de configuração afetado.

Limitamos as principais categorias a cerca de 10-15 para mantê-las amplas, mas gerenciáveis. A cada três a seis meses, nosso coordenador de incidentes verifica os registros históricos e classifica os incidentes de acordo com as principais categorias para verificar se os incidentes se enquadram nessas categorias. O log de incidentes é analisado e a categoria é determinada, perguntando:

- Como os incidentes são distribuídos pela árvore de categorias?
- As principais categorias e subcategorias estão bem definidas?
- Os níveis de categorização estão acelerando a resolução de incidentes?
- Quantos incidentes estão caindo na categoria “Outro”?
- A geração de relatórios está comprometida devido à categorização ineficiente?

Com base nas respostas e nas necessidades de nossos negócios, o coordenador de incidentes ajusta a profundidade da árvore de categorias.

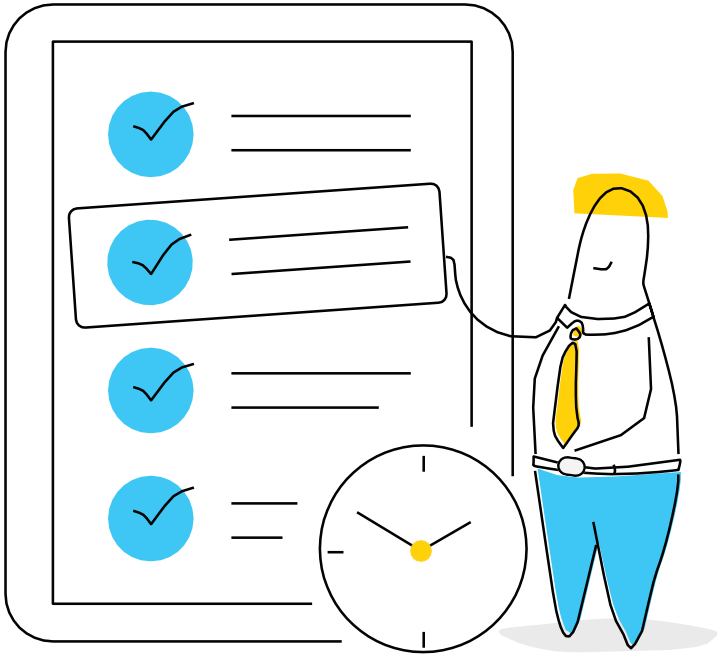
Aqui está um exemplo típico de uma árvore de categorias que usamos para lidar com problemas de hardware e software.



Priorização

Nosso coordenador de incidentes começa com a atribuição de incidentes às categorias e subcategorias corretas para fácil classificação. Sem categorização, o gerente não saberá quantos problemas de sistema operacional e aplicações tivemos ou quais ações precisam ser tomadas para reduzir esses incidentes.

Embora todos precisem ser resolvidos, alguns incidentes têm maior impacto em nossos negócios e exigem um maior senso de urgência. Determinamos a prioridade de um incidente por uma matriz de priorização(impacto x urgência) para garantir a satisfação do usuário final, o uso ideal dos recursos e o mínimo de impacto em nossas operações de negócios.



Para mapear nossa matriz de prioridade, nós nos perguntamos:

- Como a produtividade é afetada?
- Quantos usuários são afetados? É um único usuário ou um grupo? Os usuários VIP são afetados?
- Quantos sistemas ou serviços são afetados?
- Qual é a importância desses sistemas/serviços para a organização?
- Os clientes são afetados? Há um impacto significativo na receita?
- Há um grande impacto na receita/reputação do negócio?

A matriz define automaticamente a prioridade de um determinado incidente com base nas informações fornecidas (impacto e urgência) pelos usuários finais ao registrar um ticket em nossa ferramenta de ITSM. Em nossa matriz de prioridade, o impacto é listado no eixo y, e a urgência é listada no eixo x. Agrupamos impactos por usuário, grupo, departamento e empresa. Para urgência, os quatro níveis são baixo, médio, alto e crítico.

Ela fornece uma visão geral de cada incidente e garante que os principais sejam priorizados e tratados rapidamente; também garante que incidentes de baixa prioridade, como desktop, sejam tratados dentro de um período aceitável.

Aqui estão alguns casos de uso que mostram como utilizamos nossa matriz de prioridades:

Urgência	Impacto	Cenários
Interrupção/correção (Afeta indivíduos e pequenos grupos)	• Um único usuário é afetado • Nenhum serviço crítico está envolvido	• Redefinições de senha • Internet lenta
Baixa importância (Afeta um grupo/incidentes de impacto médio)	• Um único usuário VIP é afetado • Um pequeno grupo de usuários finais é afetado • Não há possibilidade de perda financeira ou perda de reputação	• O notebook do CEO não está funcionando e não consegue enviar e receber comunicações • Uma impressora não está funcionando em um andar específico
Big bang (Afeta o serviço)	• Um determinado componente de serviço, aplicação ou infraestrutura essencial aos negócios está indisponível, e o tempo estimado para recuperação é desconhecido ou muito longo • Serviço não disponível. É esperada a restauração imediata do serviço	• Nossa conexão de rede falha, e a comunicação interna e externa de nossa organização é interrompida • Uma de nossas aplicações principais está inativa, afetando vários clientes • Ataque DDoS
Situações críticas/pane total/alerta vermelho (afeta os negócios)	• Afeta os resultados financeiros da nossa empresa • Grande impacto sobre receita, reputação e assuntos jurídicos	• Bugs e vulnerabilidades de software • Malware • APT • Ransomware • Phishing e engenharia social • Ameaças internas

Atribuição e roteamento

O incidente agora é atribuído a um técnico do PitStop para investigação e diagnóstico adicionais. Fazemos isso usando regras de incidente fornecidas pela nossa aplicação ITSM. que definem a ordem de roteamento e atribuem incidentes a grupos selecionados. Digamos que uma impressora no terceiro andar esteja inativa e um incidente seja registrado. Nossa ferramenta de ITSM captura a localização do usuário no formulário e, por causa de onde ele foi originado, ele é roteado automaticamente para o técnico do PitStop no terceiro andar. Uma notificação também é enviada para o técnico logo após o incidente ser roteado, para que ele saiba que pode começar a trabalhar no problema.

Comunicação aberta

Depois que um incidente é atribuído, o técnico abre as comunicações com o usuário final afetado. Eles fazem e respondem perguntas e fornecem aos usuários finais atualizações regulares antes, durante e depois do incidente. É importante que se comuniquem bem com os usuários finais em cada etapa.

Utilizamos principalmente três métodos de comunicação:

- Uma conversa de e-mail começa logo após o técnico iniciar uma conversa com o usuário final dentro da ferramenta ITSM, garantindo que toda a comunicação esteja em um só lugar. Notificações e atualizações regulares são enviadas aos usuários finais afetados até que o incidente seja resolvido e encerrado.
- Usamos anúncios em nossa ferramenta para publicar informações relacionadas ao suporte técnico em toda a organização ou a determinados grupos de usuários finais com relação a problemas de servidor, atualizações de serviço, renovação de licença etc. É importante que os técnicos e usuários finais do PitStop em nossa empresa permaneçam cientes dos detalhes do incidente.
- Para obter uma resolução mais rápida e mais detalhes sobre o incidente, o técnico liga para os usuários finais em seus computadores ou celulares.

Encaminhamento

O incidente agora passa para o status em andamento e mostra o estágio do ciclo de vida do ticket. O técnico atualiza o status para manter o usuário final informado e cumprir os SLAs aplicáveis. Se ele não conseguir resolver o ticket, ele será encaminhado ao coordenador do incidente, que reatribui o ticket a um técnico com um conjunto de habilidades mais avançado.

Para incidentes de desktop com baixa prioridade, o SLA geralmente é definido como três a cinco dias, e os usuários finais devem receber uma resposta em quatro horas; para um incidente de média prioridade, é definido como um dia e os usuários finais devem receber uma resposta em duas horas.

Encerramento

Quando nenhum encaminhamento é necessário, o técnico pode encerrar o ticket; esta é a etapa final do ciclo de vida do incidente. Isso envolve registrar a resolução na ferramenta ITSM para referência futura antes de encerrá-la. Uma vez encerrados, os incidentes ainda estarão acessíveis aos técnicos do PitStop e ao coordenador de incidentes para que, se o usuário final ligar de volta, o técnico possa visualizar o histórico e reabrir o incidente, se necessário.

Práticas recomendadas para incidentes de desktop

- Tenha vários canais para a criação de tickets para permitir que os usuários finais levantem tickets facilmente por e-mail, chat, portal e chamada telefônica.
- Incentive os usuários finais a encontrar respostas mesmo antes de abordar um técnico para obter ajuda com o autoatendimento.
- Peça que os técnicos utilizem aplicações móveis para gerenciar seu suporte e responder a solicitações dos funcionários, mesmo quando eles estão longe de sua mesa.
- Automatize o gerenciamento de usuários integrando-se ao Active Directory da empresa.
- Classifique seus usuários finais em grupos que são baseados em seu departamento e gerenciados pelo Service desk.
- Gerencie proativamente incidentes recorrentes, como redefinições de senha, usando ferramentas de redefinição de senha automática que permitem que os administradores do sistema forneçam aos funcionários acesso a um portal de autoatendimento baseado na Web para que eles possam redefinir suas senhas com segurança.
- Automatize atividades que melhoram a eficiência e a produtividade da equipe, incluindo incidentes rotineiros de desktop, como categorização, priorização e atribuição.
- Tenha uma base de conhecimento em vigor para permitir que os técnicos pesquisem soluções existentes, para que possam resolver problemas com eficiência.
- Não mantenha seus usuários finais em uma espera sem fim. Cumpra seus SLAs.
- Mantenha os usuários finais notificados em cada estágio do ciclo de vida do incidente.
- Automatize as atividades de notificação para economizar tempo.

Big bang

(Incidentes graves de disponibilidade)

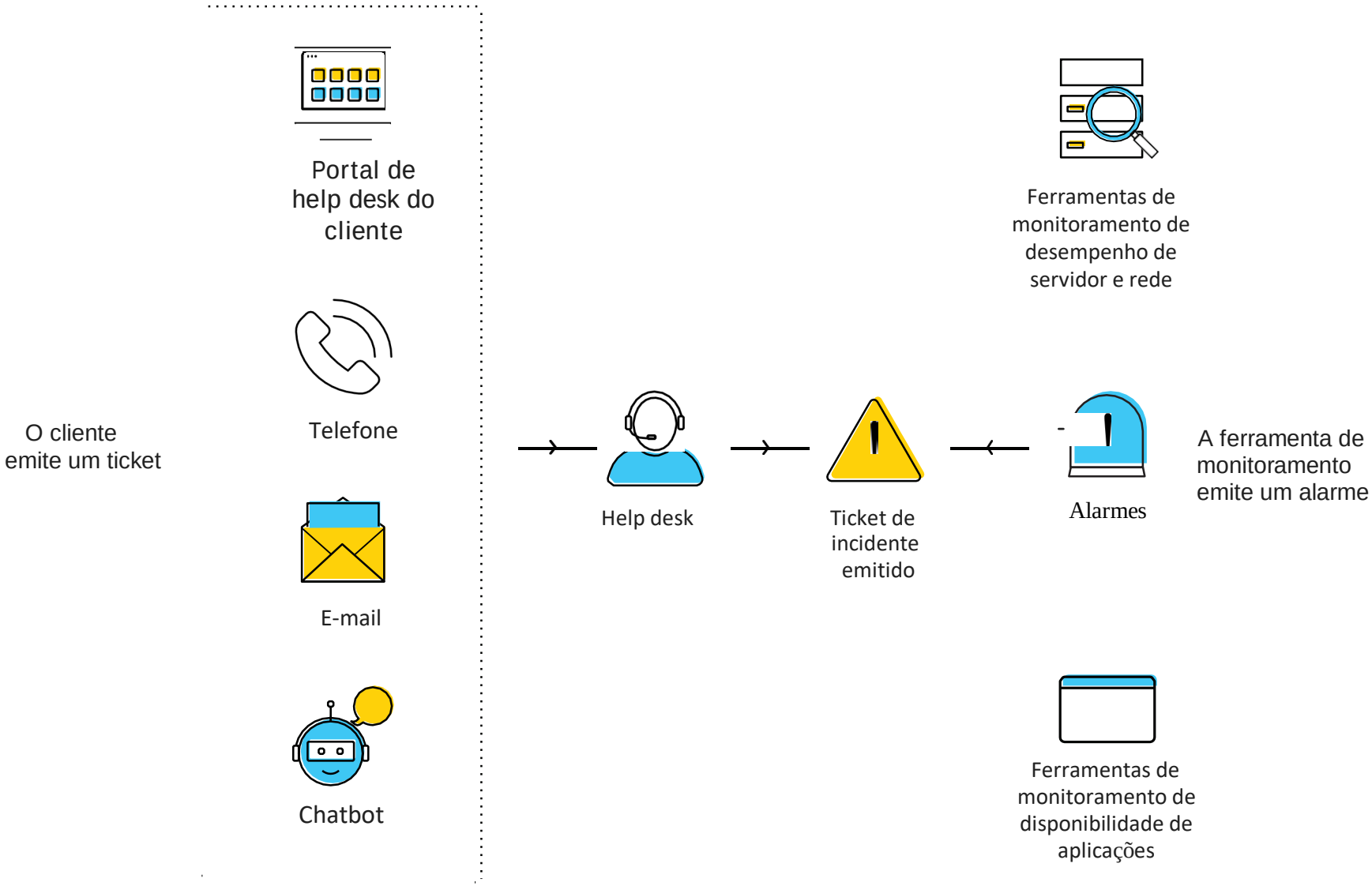
Qualquer incidente que afete muitos usuários, impeça os negócios de um ou mais serviços cruciais e exija uma resposta rápida e eficiente é considerado grave. No mundo da tecnologia em nuvem, alcançar 99,99% de disponibilidade tornou-se o padrão. Na Zoho, nosso compromisso com nossos clientes é garantir 99,99 por cento de disponibilidade.

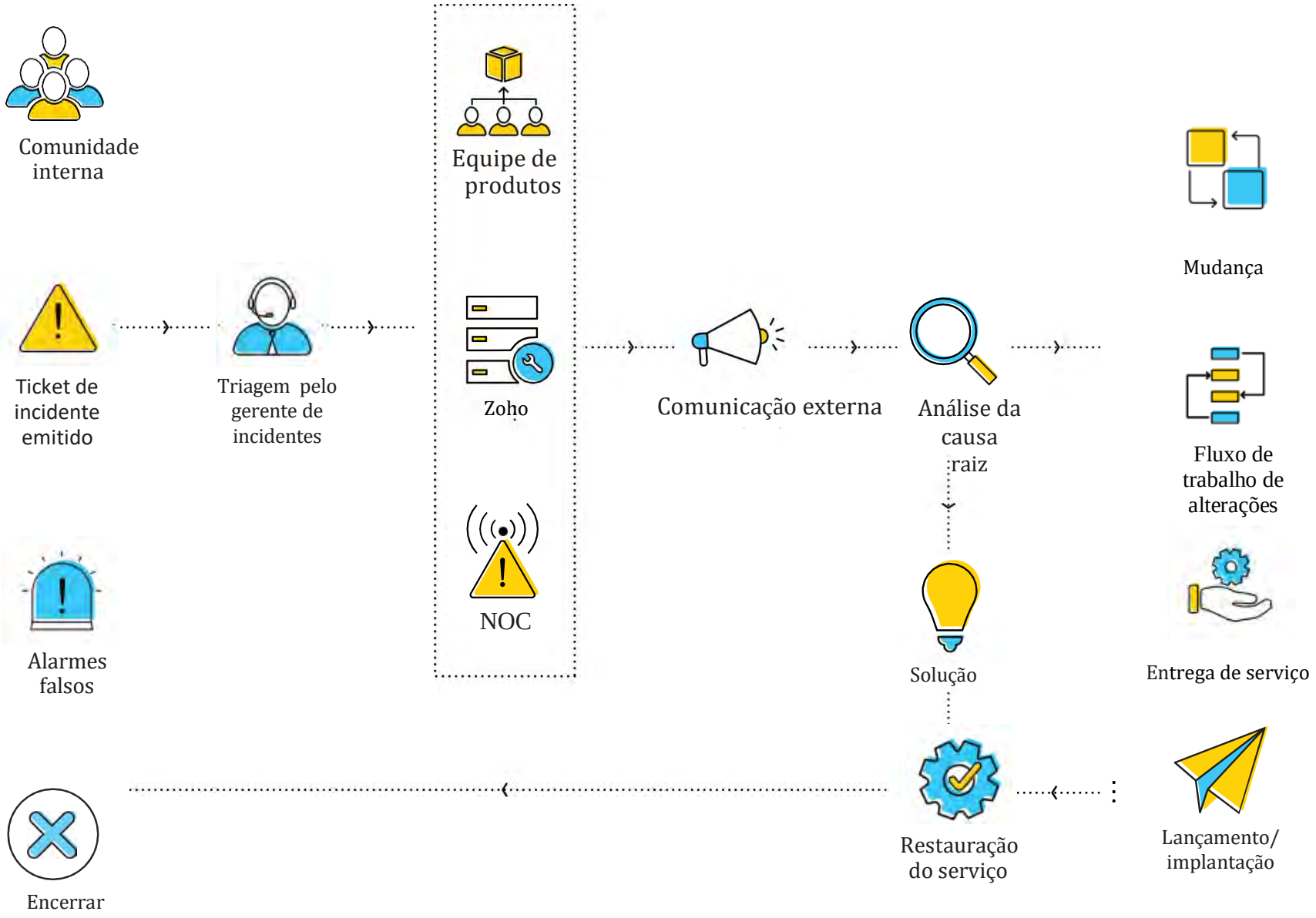
Os clientes podem verificar a disponibilidade de nossos serviços em nossa página de status. Quando um incidente grave de disponibilidade ocorre, seguimos o processo “big bang” de IM; isso inclui facilitar a colaboração, alinhar as partes interessadas, informar os clientes e, por fim, trabalhar continuamente até a resolução.

Esta seção aborda três diferentes problemas de disponibilidade:

- Problemas de rede
- Problemas de servidor físico
- Problemas de aplicações

A figura abaixo mostra o processo que seguimos durante um incidente de disponibilidade.



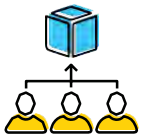

Comunidade interna
Equipe de produtos
Mudança
Ticket de incidente emitido
Triagem pelo gerente de incidentes
Zoho
Comunicação externa
Análise da causa raiz
Fluxo de trabalho de alterações
Alarmes falsos
NOC
Solução
Entrega de serviço
Encerrar
Restauração do serviço
Lançamento/ implantação

Equipes, funções e responsabilidades

Equipe de resposta a incidentes (IRT)

Gerente de incidentes:

Atuando como o capitão do navio que supervisiona o incidente, o gerente de incidentes trabalha com as equipes NOC, Zoho e de produtos, e seus respectivos coordenadores de incidentes, para resolver problemas e manter SLAs.



Engenharia e desenvolvimento (equipes de produtos):

Para um incidente relacionado a uma aplicação, a equipe de produto individual é o principal ponto de contato para o gerente de incidentes. Os engenheiros da equipe de produto são normalmente o grupo que resolve problemas durante os incidentes de responsabilidade.

Equipe de software como serviço (SAS):

Controla o inventário dos ativos do data center.

Centro de operações de rede (NOC):

Lida com incidentes de disponibilidade de rede.

Coordenador de incidentes:

Um coordenador de incidentes designado é atribuído a cada equipe de produto e é responsável por avaliar e coordenar um incidente de disponibilidade.

Servidores e manutenção:

Quando um incidente é identificado como um incidente relacionado ao servidor, a equipe ajuda, lidando com o provisionamento e manutenção dos servidores nos data centers.

Equipe de Entrega do serviço (SD):

Lida com o envio de atualizações para todas as aplicações Zoho.

Gerente de comunicações externas:

O gerente de incidentes atua como nosso gerente de comunicações externas, fornecendo aos clientes atualizações frequentes sobre interrupções.

Detectar

O **Site24x7** é uma ferramenta de monitoramento de disponibilidade que usamos para monitorar nossas aplicações em vários locais. Essa aplicação se integra perfeitamente à nossa ferramenta de ITSM, reconhece a indisponibilidade e envia alertas proativos para criar incidentes. Em caso de alarme falso, o incidente é encerrado.

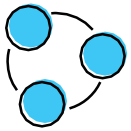
Novo incidente

Configuramos nosso principal processo de IM em nossa ferramenta usando um ciclo de vida de solicitação (RLC). Sempre que um incidente é criado, as notificações são enviadas ao gerente e aos coordenadores das equipes de produtos ZoHo, NOC e relacionadas. Essas notificações incluem o número do ticket, a descrição e a prioridade. Depois que o incidente é registrado como um ticket em nossa ferramenta de ITSM, ele está no estado aberto – o estado inicial em nosso RLC.

Comunicar-se com as partes interessadas

O gerente de incidentes, depois de obter as informações necessárias do alerta e do coordenador de incidentes, abre as comunicações com as partes interessadas internas.

Ferramenta ITSM:
A partir do ticket de incidente, um e-mail é enviado para as equipes de gerenciamento de incidentes, NOC, Zoho e de produto para iniciar a investigação inicial.



Zoho Connect:
O Connect é um software de colaboração em equipe, como uma aplicação interna semelhante ao Facebook, que conecta todos os interessados e permite discussões abertas durante um incidente. Temos um grupo chamado Incidents, que inclui mais de 1.200 membros, incluindo respondentes, principais partes interessadas e tomadores de decisão para garantir maior transparência e coordenação.

Zoho Cliq:
Um software de bate-papo de colaboração empresarial que permite ao gerente de incidentes, coordenadores, equipes de produtos e outras partes interessadas fornecer atualizações rápidas, compartilhar arquivos e pesquisar um contato ou conversa do passado. Os bate-papos em grupo nos permitem entrar em contato e adicionar mais respondedores e solucionadores, conforme necessário para trabalhar com incidentes mais rapidamente.

Documente a interrupção:
Uma chamada de conferência ou um encadeamento de discussão não é suficiente para ajudar todos a ver o que está acontecendo e o que está por vir. As partes interessadas e os clientes precisam de relatórios de progresso significativos, garantias de que o incidente pode ser corrigido e sem surpresas. O gerente de incidentes mantém um documento de estado do incidente no Zoho Writer para fornecer um lugar claro para ver como, por que e quando o incidente ocorreu, as ações tomadas ou em andamento, os dados compartilhados e uma compreensão do caminho claro para a resolução.

Este documento pode ser editado, comentado e compartilhado em toda a organização. O gerente de incidentes compartilha este documento na conversa correspondente ao incidente no Connect, e também o usa para a análise de causa-raiz (RCA). Essa também é uma ótima maneira de o gerente de incidentes registrar as principais observações e decisões que acontecem em conversas não gravadas em outros meios, como conversas de bate-papo e discussões.

Avaliar

Lidamos com muitos tipos de incidentes graves de disponibilidade, e trazemos várias equipes para realizar a correção. A resposta dada a esses incidentes depende de muitos fatores, como coordenação, comunicação e gerenciamento. Para uma resposta bem-sucedida, todos esses fatores devem funcionar juntos. Para otimizar, precisamos de uma linguagem comum para nos comunicarmos, e a ordem pela qual as equipes precisam estar envolvidas e as tarefas executadas precisam ser bem definidas.

Quando um incidente de disponibilidade vem do Site24x7, a triagem entre as equipes começa. Nosso gerente de incidentes atua como o agente de triagem, reunindo o NOC, o Zoho e as equipes de produtos. Um canal é criado no Cliq para identificar se o problema está relacionado à rede (NOC), ao servidor (Zoho) ou a um produto, para que o ticket possa ser delegado às equipes certas e resolvido.

O gerente de incidentes começa com a avaliação, fazendo algumas perguntas para comunicar as informações certas às partes interessadas e aos clientes.

- Quando a interrupção ocorreu?
- A interrupção é visível para os clientes?
- Quantos clientes foram afetados?
- Quantos tickets de suporte existem?
- Qual equipe (NOC, Zorro ou produto) lida com a correção?
- A equipe está equipada com os recursos certos naquele dia específico?
- A equipe de resolução concorda com seus protocolos e programações de comunicação?

Depois que a propriedade do incidente tiver sido identificada, e for considerada um incidente grave – ou seja, é urgente e tem um impacto na organização –, o gerente de incidentes envia a comunicação externa inicial.

Comunicar-se externamente

O gerente de incidentes agora está razoavelmente informado sobre o incidente e sobre o envolvimento da equipe, e tem que divulgar aos clientes o mais rápido possível. Ele recebe ajuda para atualizar o blog sobre a indisponibilidade da equipe de comunicações.

Durante uma interrupção, fazemos um comunicado do blog que inclui detalhes como a data e a hora da ocorrência, a natureza do incidente e as ações corretivas com atualizações frequentes. Sempre que os clientes tentam acessar o serviço durante uma interrupção, eles são redirecionados ao anúncio do blog para que possam se manter atualizados sobre os acontecimentos.

Uma publicação de comunicado também é feita na comunidade durante uma interrupção, onde fornecemos atualizações frequentes e respondemos às perguntas dos clientes. Os clientes também podem verificar a disponibilidade do serviço em nossa página de status.

Delegar

O gerente de incidentes trabalha com o coordenador no NOC, Zoho e equipes de produtos para gerenciar todas as operações de incidentes, aplicação de recursos e responsabilidades de todos os envolvidos. Depois que as respectivas equipes retornarem pelo canal do Cliq e a propriedade da equipe tiver sido identificada, um conjunto de tarefas será automaticamente acionado por meio do ciclo de vida da solicitação para a equipe que possui o incidente, conforme mostrado abaixo.

Enviar acompanhamento

O gerente de incidentes faz o ping regularmente à equipe de resolução para receber atualizações rápidas sobre o progresso que eles encaminharão ao cliente. Detalhes curtos e concisos, que incluem o início do tempo de inatividade, uma breve descrição da causa conhecida, o tempo estimado para restauração e o tempo programado para a próxima atualização de status, são frequentemente atualizados no fórum e no blog para manter os clientes informados.

Resolver e encerrar

Depois que o incidente não afeta mais os clientes, ele é considerado resolvido, e um técnico encerrará manualmente o ticket ou, depois de passar tempo suficiente, o estado mudará para encerrado automaticamente. O gerente de incidentes envia as comunicações internas e externas finais e inicia a RCA usando o documento de estado do incidente como base.

Aqui está nossa lista de verificação para resolver (e encerrar) tickets:

- ✓ O incidente foi resolvido de forma a satisfazer os proprietários do ticket?
- ✓ Os solucionadores estão cuidando das tarefas de limpeza?
- ✓ Todas as tarefas relacionadas foram encerradas e os usuários relevantes foram notificados?
- ✓ O gerente de incidentes notificou todas as partes? Os clientes foram notificados da resolução?
- ✓ Todas as partes interessadas concordaram com o encerramento do incidente grave?
- ✓ A RCA foi registrada e iniciada?
- ✓ A agenda da reunião de RCA foi enviada aos grupos de resolução?
- ✓ O suporte técnico foi notificado sobre o encerramento?

Nós verificamos isso para concluir o processo de incidente principal da forma mais limpa possível e para assegurar que não perdemos nada.

Práticas recomendadas para incidentes graves

Definir claramente um incidente grave:

Dizemos que um incidente é grave quando afeta muitos usuários, priva os negócios de um ou mais serviços cruciais e exige uma resposta além do processo de gerenciamento de incidentes de rotina. Às vezes, um incidente de desktop de alta prioridade pode ser percebido como grave. Um notebook VIP com problema durante uma conferência de usuários é um incidente de alta prioridade, mas certamente não é um incidente grave. Para evitar qualquer confusão, você deve definir um incidente grave claramente com base em fatores como urgência, impacto e gravidade.

Tenha um plano de comunicação em vigor:

O plano de comunicação deve incluir os detalhes do evento (como, quando, plano de ação, tempo estimado de correção e tempo de intervalo de atualização), as partes envolvidas e a frequência de comunicação.

Configure SLAs:

Configure SLAs separados de resposta e resolução com caminhos claros de encaminhamento. Se a equipe tiver pouco pessoal naquele dia, não hesite em obter os recursos necessários de outras equipes para trabalhar na resolução e garantir que o SLA não seja afetado.

Tenha um processo de IM exclusivo:

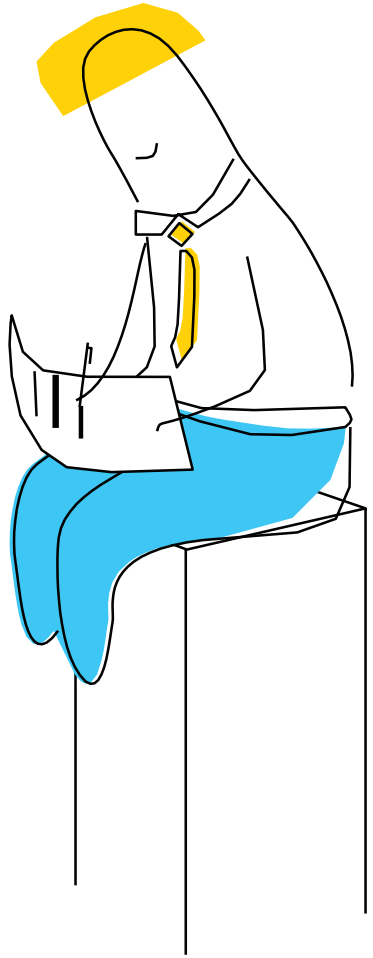
Fluxos de trabalho ou processos separados para o gerenciamento de incidentes graves ajudarão você a lidar com vários tipos de incidentes de forma eficiente, como indisponibilidade de serviços ou problemas de desempenho e falha de hardware ou software, para que você possa garantir uma resolução perfeita.

Traga os recursos e as equipes certas:

Garanta que a equipe e os recursos certos estejam trabalhando em incidentes com funções e responsabilidades claramente definidas

Documente o processo para melhoria contínua do serviço:

Como prática recomendada, nosso gerente de incidentes captura detalhes como o número de pessoas envolvidas no processo, suas funções e responsabilidades, os canais de comunicação, as ferramentas usadas para os fluxos de trabalho de correção, aprovação e encaminhamento, e o plano de ação geral usado para a resposta e a resolução no documento de estado do incidente. As partes interessadas, incluindo o gerenciamento superior, avaliam este documento para garantir a melhoria contínua do serviço.



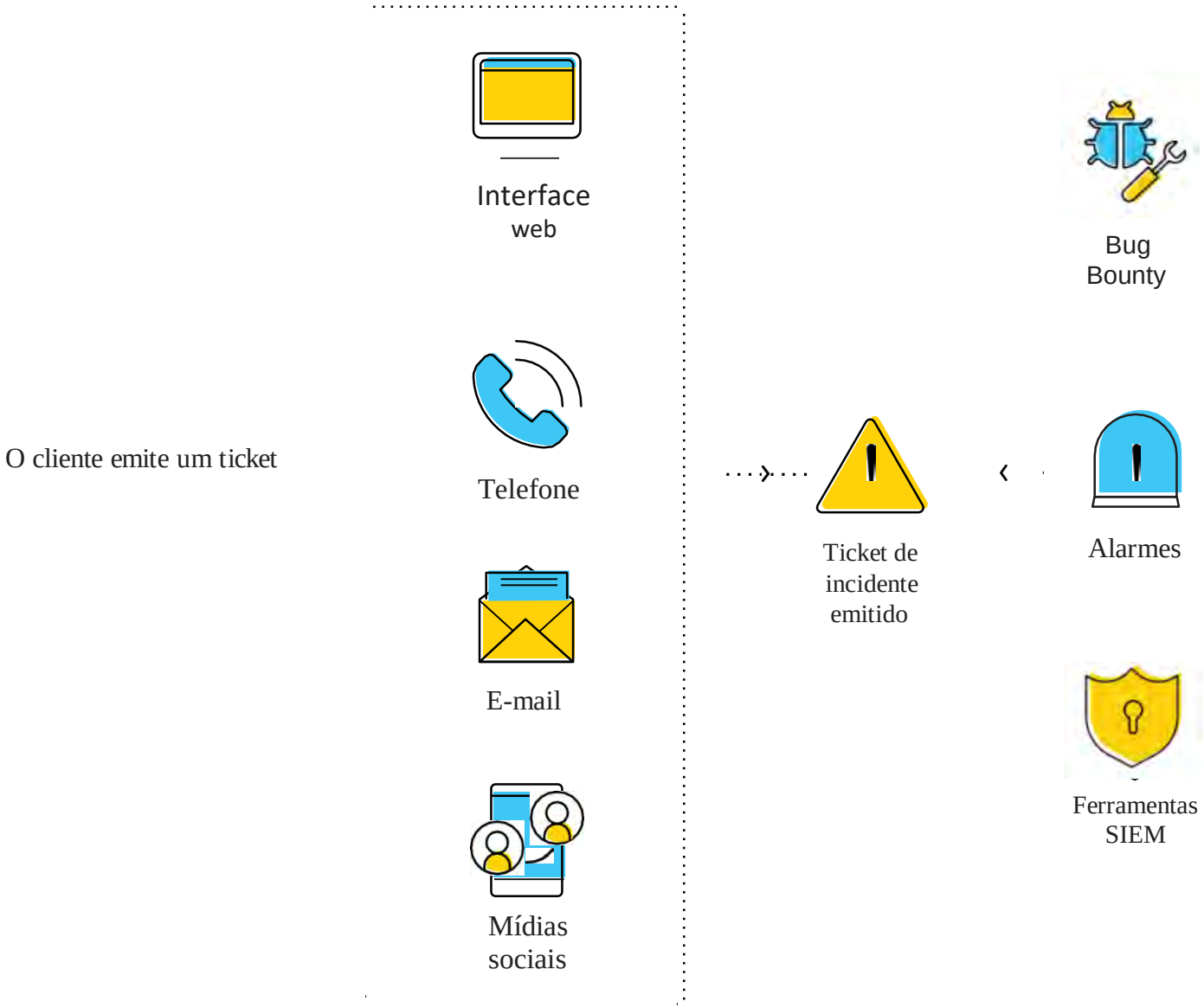
CyberSec

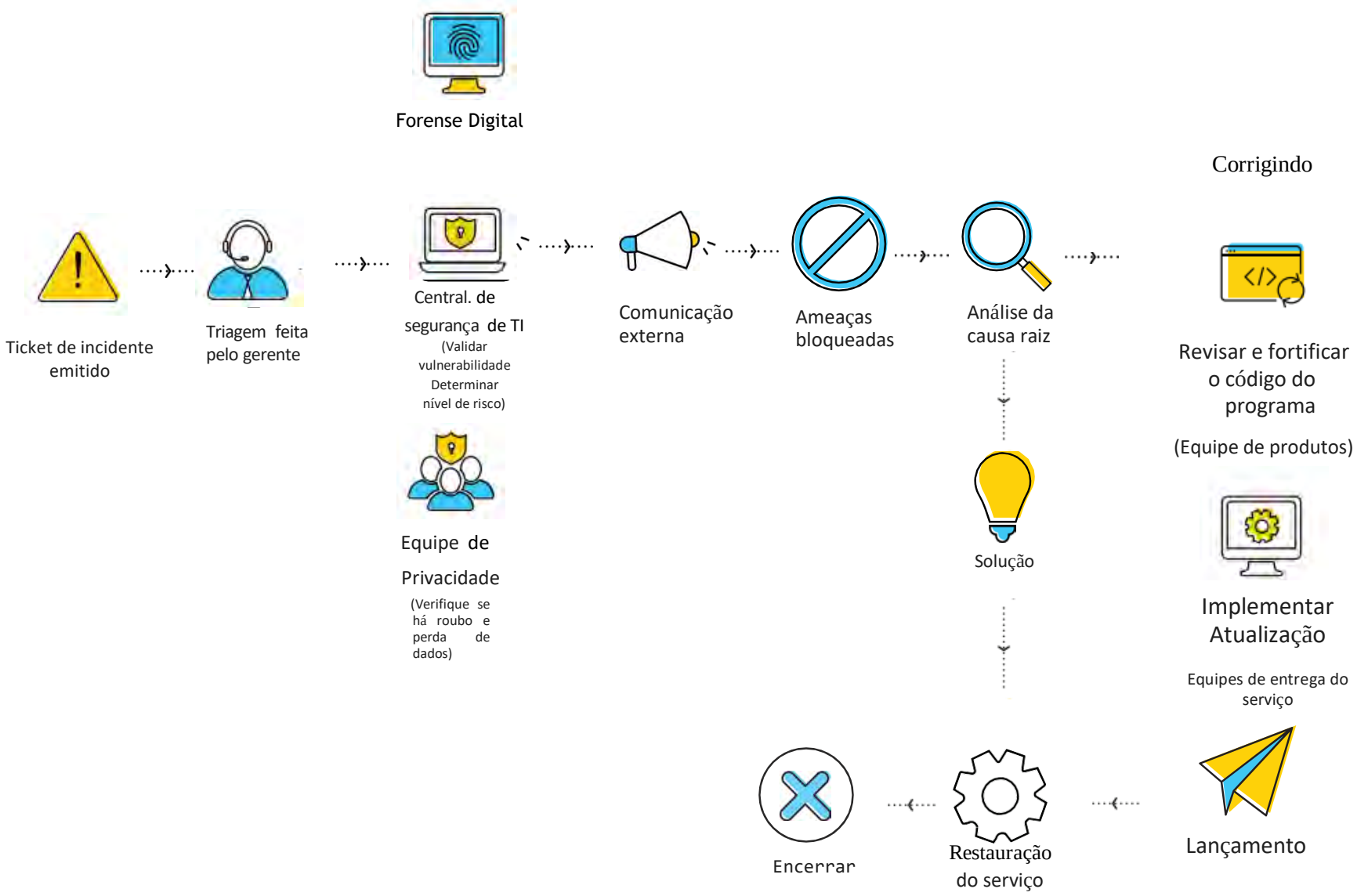
(Pane total/incidentes de segurança)

A segurança é a base em nossa organização. Nossa equipe de segurança de TI protege a confidencialidade, a integridade e a disponibilidade de nossos sistemas e dados, protegendo nossa organização contra malware, APTs, ransomware, phishing, engenharia social, ataques internos e outras ameaças. Temos um grupo de hackers white hat que está continuamente tentando burlar nossas verificações de segurança. Os coordenadores de segurança estão envolvidos no ciclo de vida de desenvolvimento do produto, garantindo que a segurança seja integrada a todos os produtos que desenvolvemos.

Antecipando que um dia poderemos ser o alvo de um ataque cibernético, queremos estar preparados. O CyberSec é um processo maduro de detecção, contenção, coordenação e recuperação de vulnerabilidades que torna nossa empresa resiliente contra ameaças cibernéticas. Ele pode nos ajudar a se recuperar de violações de segurança, minimizando o tempo de exposição e o impacto de ameaças em dados, aplicações e nossa infraestrutura de TI.

A figura abaixo é nosso fluxo de processo do CyberSec.




Forense Digital
Corrigindo
Ticket de incidente emitido
Triagem feita pelo gerente
Central. de segurança de TI
(Validar vulnerabilidade Determinar nível de risco)
Comunicação externa
Ameaças bloqueadas
Análise da causa raiz
Revisar e fortificar o código do programa
(Equipe de produtos)
Equipe de Privacidade
(Verifique se há roubo e perda de dados)
Solução
Implementar Atualização
Equipes de entrega do serviço
Encerrar
Restauração do serviço
Lançamento

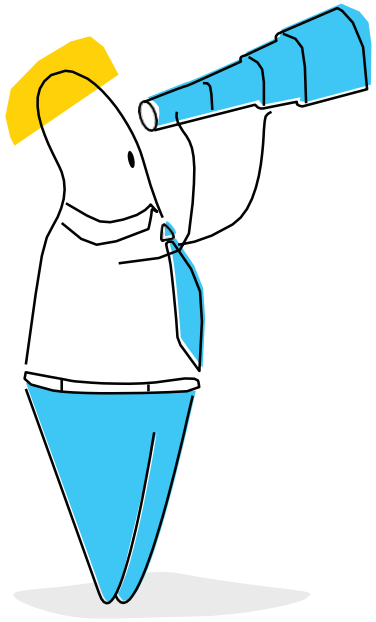
Equipes, funções e responsabilidades

Equipe	Funções	Responsabilidades
Gestão de incidentes	Resposta e coordenador de incidentes	Gerencia os incidentes de cibersegurança desde detecção até resolução
Central de segurança de TI	Segurança de TI	Monitora continuamente e analisa procedimentos de segurança dos produtos
Resposta de incidentes	Inclue a equipe de IM e central de TI	Acessa o impacto, assegura SLA e coordena com as equipes de privacidade, jurídica e de produtos em situações de crise.
Alta gestão	Tomada de decisões de negócios	Ouvir as análises do gestor de incidentes, cuidar do impacto aos negócios e gerenciar decisões chave, por exemplo: decidir se a conexão da internet deve ser desligada. Caso sim, quando seria o momento apropriado? Também decide quando entrar em contato com as autoridades.
Equipe jurídica	Departamento jurídico/ consultores	Encarregado do impacto contratual e judicial de um incidente. Assegura que as atividades de resposta ao incidente estejam de acordo com políticas da organização e regulamentações. Guia a empresa para estar em conformidade.
Privacidade	Consultores	Analisa o impacto dos incidentes de segurança na privacidade de indivíduos afetados comparando com os requerimentos de dados aplicados as leis de privacidade; fornece guia sobre como lidar com notificações de incidentes e o CAPA
Produtos	Engenheiros de produtos	Conserta vulnerabilidades e lançamentos de produtos
Equipe vermelha	Hackers white hat	Tentam invadir as aplicações, quebrar os protocolos de segurança e expor ameaças de cibersegurança em potencial para garantir a segurança de nossos produtos

O processo

Detectar

Nossos funcionários têm o maior potencial para ajudar a organização a detectar e identificar incidentes de segurança cibernética. Eles desempenham um papel significativo na detecção de ameaças à segurança. Todos os membros da nossa organização estão cientes das formas de alertar a nossa equipe de segurança quando notarem alguma anomalia no seu computador ou dispositivo móvel.



Também temos um programa Bug Bounty para incentivar e recompensar os funcionários que detectam e relatam uma vulnerabilidade de segurança para a Zoho. Nossos funcionários podem relatar um incidente de segurança por meio de:

O Portal de autoatendimento

Um número de ligação gratuita

Aplicação Bug Bounty

Mídias sociais

E-mail

Comunicar-se internamente:

Consulte o Big Bang - Página 21

Avaliar

Quando um alarme de segurança soa, é fundamental primeiro avaliar o que aconteceu, reunir os detalhes, realizar uma análise de impacto nos negócios (BIA) e tomar as medidas certas. O SIRT, que inclui o gerente de incidentes e a equipe central de segurança de TI, inicia a triagem para coletar e analisar informações antes de agir.

O gerente de incidentes convoca uma reunião que inclui a equipe central de segurança e a equipe de privacidade, juntamente com o DPO (Data Protection Officer) e abre um canal Cliq para discussões e atualizações de acompanhamento. A equipe coleta todas as informações disponíveis e realiza uma investigação forense para examinar a magnitude e a profundidade do ataque; e a equipe de privacidade identifica qualquer violação de privacidade de dados.

O SIRT faz as perguntas abaixo para avaliar o incidente e seu impacto.

Gerente de Incidentes	Equipe Central de TI	Equipe de Privacidade
• Quem identificou e reportou o incidente? • Quando o incidente foi identificado e reportado? • Onde o incidente foi descoberto e está localizado? • Qual impacto o incidente tem nas operações de negócio? • Teve perda de dados e a privacidade foi envolvida? • Qual a extensão do incidente na rede e aplicações?	• É um ataque de segurança? • O ataque foi bem sucedido? • Qual é o score da fonte IP? • Qual é o score do destino IP? • Qual o score do feed de ameaça? • Qual o score de vulnerabilidade? • Quais ativos foram comprometidos? • Quais eram as vulnerabilidades associadas? • Como o organização deve responder a esse ataque? • O que pode acontecer se o incidente não for contido? • É necessário preservar a evidência? • Quais tipos de evidência a empresa deve adquirir? • Onde a evidência será armazenada? • Por quanto tempo a evidência vai ser retida?	• A conta envolvida do usuário foi comprometida? • O equipamento de dados do dispositivo foi encriptado? • A conta comprometida tem acesso a informações sensíveis? • Quais atividades o invasor realizou? • Qual a densidade do ataque? • Qual o número dos indivíduos potencialmente efetados? • Esse evento foi associado com algum outro evento ou artefato? • Qual o nível de risco para indivíduos da empresa? • Quais os tipos de controles para mitigar os riscos?

In cases of criminal intent, the SIRT, legal team, and top management work together to report the incident to law enforcement authorities.

Conter

Um incidente de segurança é análogo a um incêndio florestal e deve ser contido o mais rapidamente possível. O SIRT coloca em quarentena as redes e os dispositivos infectados ou comprometidos afetados por vírus ou outro malware e instala atualizações de segurança para resolver problemas de malware ou vulnerabilidades de rede.

Quando o incidente é identificado como resultado de uma vulnerabilidade de software, o SIRT desativa o recurso usado na exploração, grava uma regra de firewall personalizada bloqueando solicitações específicas ou até mesmo desinstala temporariamente o software como ações preventivas. O endereço IP de ataque também é bloqueado para evitar outras tentativas.

Enquanto isso, o gerente de incidentes reúne os detalhes necessários e abre comunicações externas.

Comunicar-se externamente

Comunicar-se externamente é uma etapa fundamental na resposta a incidentes de segurança cibernética. O gerente de incidentes trabalha com a alta gerência para controlar o fluxo de comunicação a fim de garantir que as informações certas sejam fornecidas no momento oportuno.

Por exemplo, uma tentativa de invasão interna provavelmente não garantirá a comunicação com a mídia ou com as autoridades. Por outro lado, se o incidente envolver exposição ou roubo de registros confidenciais de clientes, pode ser obrigatório relatar à mídia e às autoridades de normas de privacidade do consumidor.

Quem?	O quê?
Clientes	Detalhes do incidente incluem: data e hora da ocorrência, descrição do problema constando se qualquer dados de clientes foram perdidos ou roubados, os passos tomados para mitigar os riscos e o tempo estimado de recuperação
Media	Às vezes, atenção da media não pode ser evitada e as relações públicas da empresa devem emitir um pronunciamento sobre o incidente e seu impacto para mostrar comprometimento e capacidade de gerenciar o incidente.
Polícia	Em casos de intenção criminosa, o SIRT, equipe jurídica e alto gestão trabalham juntos para reportar o incidente as autoridades.

Delegar

Depois que a investigação é concluída e as medidas necessárias são tomadas para conter o ataque, o incidente muda para o estado de delegação. O SIRT delega a responsabilidade da resolução aos engenheiros de produto para revisar e fortificar o código do programa, garantindo a resolução da vulnerabilidade.

Resolver

A erradicação e a recuperação são realizadas como uma etapa única. A fase de erradicação inclui uma solução mais permanente para sistemas infectados. Se a ameaça ganhou entrada em um sistema e se proliferou em outros sistemas, então o SIRT busca removê-la e apagar todos os vestígios do ataque de nossos dispositivos e rede por meio de software antivírus, substituição de hardware ou reconstrução de rede. Nosso objetivo é retornar os sistemas aos “negócios como de costume”. Aqui está a nossa lista de verificação de erradicação do SITRT:

- ✓ Todos os sistemas infectados foram protegidos por novas atualizações?
- ✓ Os sistemas e aplicações precisam ser reconfigurados?
- ✓ Todos os pontos de entrada possíveis do ataque foram corrigidos?
- ✓ Todos os processos para erradicar a(s) ameaça(s) foram abordados?
- ✓ Há alguma medida adicional de defesa necessária para erradicar a(s) ameaça(s)?
- ✓ Todas as atividades mal-intencionadas foram erradicadas dos sistemas afetados?

No caso de uma vulnerabilidade de software, o incidente é delegado à equipe de engenharia desse produto específico. Os engenheiros de produto corrigem as vulnerabilidades e liberam a atualização de software.

Revisar

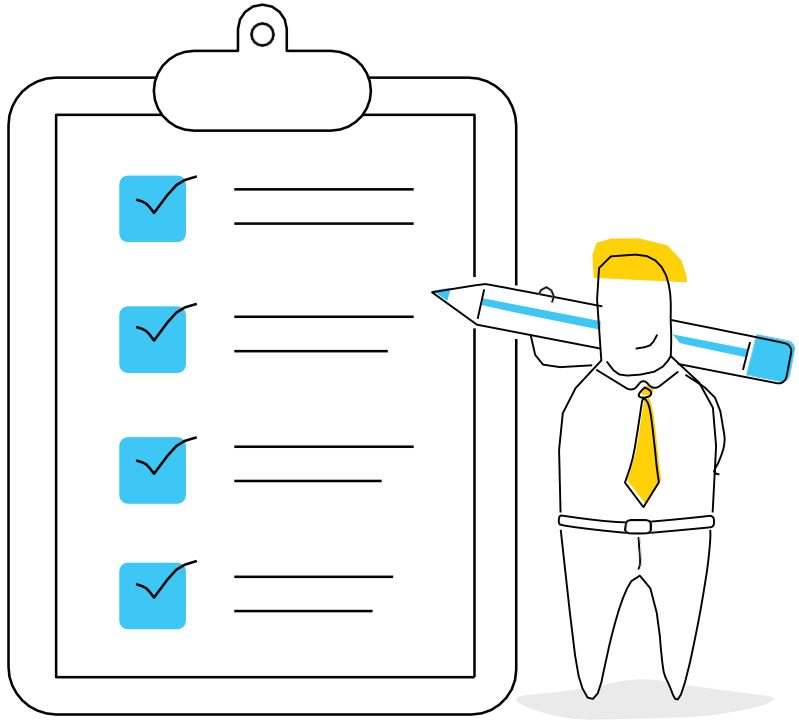
Após a implementação de uma resolução pela equipe de produtos, ela é normalmente verificada e revisada pelo chefe de engenharia, pelo SIRT e pela equipe de privacidade. Na aprovação das equipes, o incidente muda para o encerramento. Essa etapa garante que nada tenha sido perdido e que o ele tenha sido corrigido e impedido de ser recorrente. Pode ser tentador pular esta etapa; porém, garantir que haja uma revisão da correção implementada é altamente recomendável.

Encerrar

Todos os incidentes de segurança cibernética, como qualquer outro, precisam ser encerrados corretamente. Como medida pós-incidente, o gerente envia comunicação a todas as partes afetadas, à mídia e às autoridades confirmando que a ameaça foi contida.

Veja a nossa lista de verificação para encerrar tickets:

- O incidente foi resolvido de forma a satisfazer os grupos de resolução?
- Os solucionadores estão cuidando das tarefas de limpeza?
- Todas as tarefas relacionadas foram encerradas e notificadas?
- O gerente de incidentes notificou todas as partes?
- O mais importante: os clientes foram notificados da resolução?
- Todas as partes interessadas concordaram com o encerramento da segurança?
- A RCA foi registrada e iniciada?
- A RCA foi iniciada pelo gerente de incidentes?
- O suporte técnico foi notificado sobre o encerramento?



A fase final do ciclo de vida de resposta a incidentes de segurança envolve RCA e loops de feedback. O gerente de incidentes inicia a RCA, pois é fundamental aprender com cada incidente para melhoria contínua do serviço.

Práticas recomendadas para incidentes de segurança

Tenha um processo de resposta a incidentes bem definido:

Tenha um processo acionável para identificar, tratar e gerenciar as consequências de uma violação de segurança ou ataque cibernético de uma forma que limite os danos e reduza o tempo e os custos de recuperação. Certifique-se de que o plano de resposta a incidentes esteja alinhado com as políticas da empresa.

Defina claramente as equipes, as funções e as responsabilidades:

Identifique as equipes que são amplamente responsáveis por cada fase ou etapa (por exemplo, contenção, erradicação e recuperação) no processo de resposta a incidentes. Identifique as pessoas-chave dos respectivos departamentos e equipes, quem servirá como backup delas e como entrar em contato com elas dia ou noite. Como prática recomendada, criamos um gráfico RACI que nos ajuda a identificar as pessoas que são responsáveis, consultadas ou informadas (RACI) para atividades definidas antes e depois de um incidente.

Faça o inventário de seus dados:

É importante avaliar os dados de sua organização para saber o que precisa de mais proteção durante uma violação de dados.

Tenha um plano de comunicação em vigor:

Ter linhas de comunicação definidas para envolver as partes interessadas e gerenciar a comunicação entre a equipe de resposta a incidentes de segurança e outros grupos é crucial para a recuperação bem-sucedida de incidentes. Um plano de comunicação garante que todos sigam os protocolos durante uma emergência ao entrar em contato com partes interessadas, parceiros, provedores de serviços, mídia, autoridades e clientes.

Colete evidências contra o invasor:

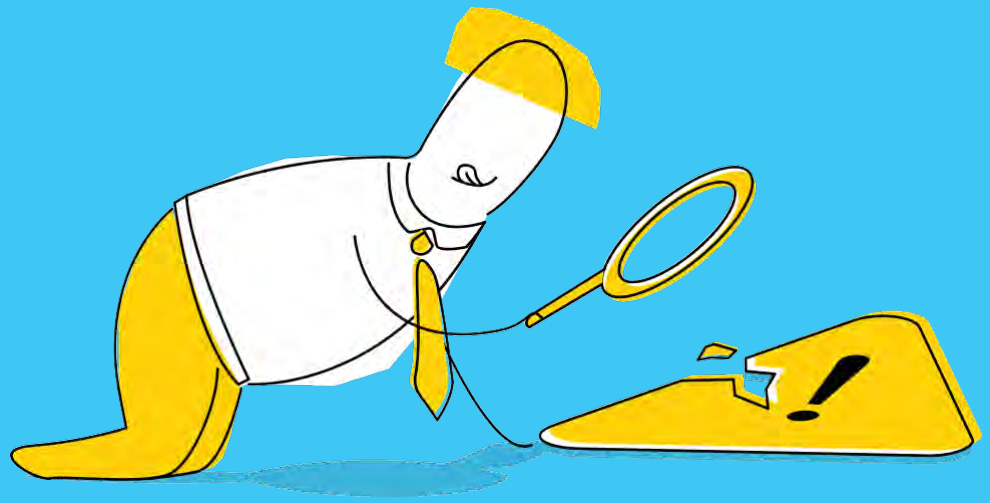
Tomar ações corretivas durante uma crise, como tirar sistemas da rede ou limpar sistemas, pode resultar em alertas para um invasor ou em destruição de evidências vitais. A organização tem muito a perder no tribunal se as provas forem destruídas ou insuficientes. Colete as evidências de maneira legal e sólida para que possam ser apresentadas com credibilidade no tribunal.

Mantenha a calma durante uma crise:

Lidar com incidentes de segurança pode ser bastante estressante. É necessário manter a calma quando um ataque ocorre e seguir o plano de resposta a incidentes.

Realize a análise da causa-raiz:

Uma análise pós-incidente envolvendo a equipe de resposta a incidentes e outros grupos de resolução pode ajudar a fornecer percepções sobre a origem do problema e evitar a recorrência.



ANÁLISE DA CAUSA RAIZ (RCA)

O que é RCA?

A Análise da causa-raiz (RCA) é uma abordagem sistemática que se aprofunda para identificar a causa-raiz de um incidente, fazendo vários "por que" até que nenhuma resposta de diagnóstico adicional possa ser fornecida. Normalmente, envolve uma análise ou uma discussão logo após a ocorrência de um incidente. Um recurso adicional, o documento de estado do incidente, serve como um registro por escrito do que aconteceu antes e durante e dá respostas às perguntas necessárias para conduzir uma análise de causa-raiz.

O documento de estado do incidente, também conhecido como relatório, é o melhor lugar para começar com a análise da causa-raiz. No entanto, é fundamental aprofundar-se mais do que apenas o que o formulário afirma. Na Zoho, criamos um registro de problema a partir do ticket para executar uma RCA completa por meio de nossa ferramenta de ITSM.

Por que realizar RCA?

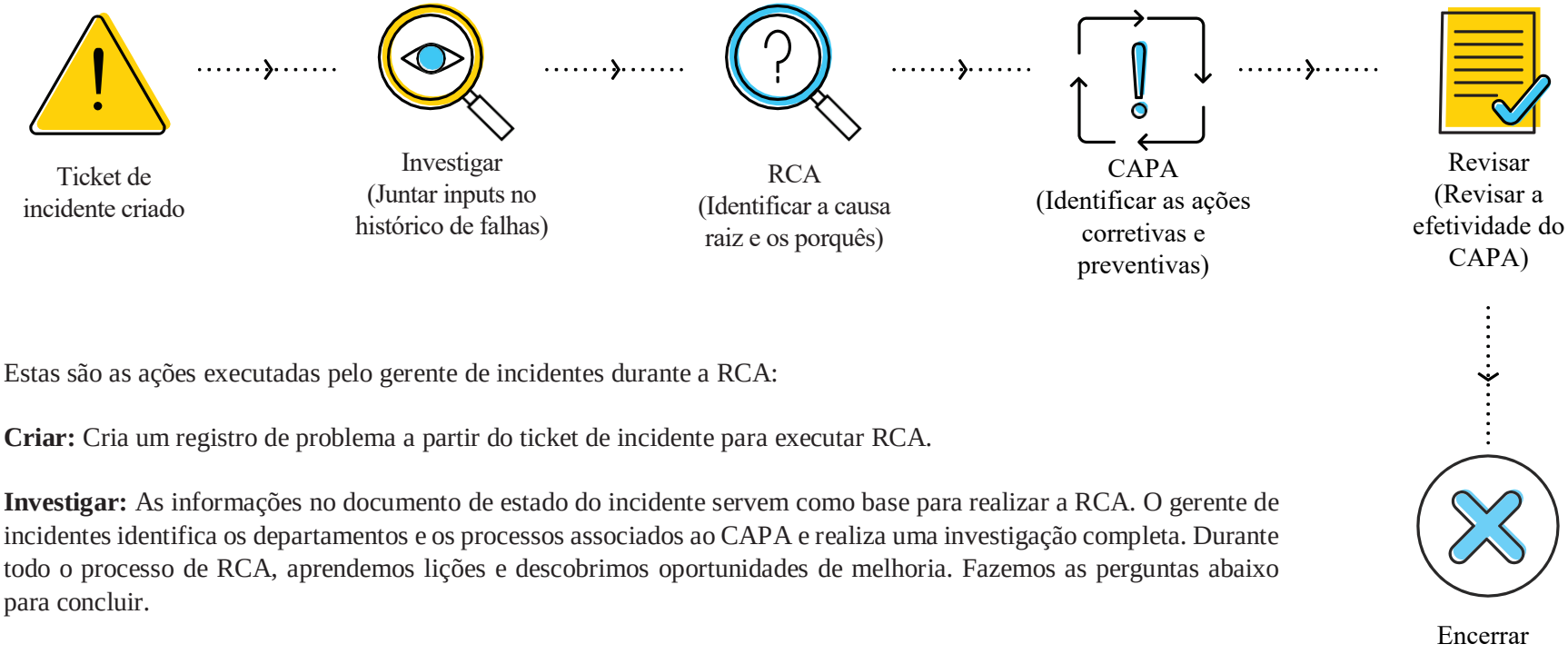
Na Zoho, nunca deixamos que uma boa crise seja desperdiçada. Vemos um evento infeliz como uma oportunidade de aprender com nossos erros, identificar onde os processos ou sistemas falharam e estar mais preparados para lidar com incidentes semelhantes no futuro.

Princípios de RCA

- A RCA é conduzida para determinar os fatores que resultaram no incidente e para tomar ações corretivas em vez de simplesmente tratar os sintomas.
- Uma RCA bem-sucedida é realizada sistematicamente com conclusões respaldadas por evidências reais.
- Na maioria das vezes, há mais do que apenas uma causa-raiz para um incidente.
- "Se não estiver cometendo erros, então não está fazendo nada." Na Zoho, acreditamos em aprender com nossos erros. Ter um processo RCA "sem culpa" permite que nossos funcionários e equipes forneçam os detalhes exatos de sua abordagem, como as ações que tomaram e as suposições que fizeram ao lidar com o incidente.

Processo RCA

Ação corretiva Ação preventiva (CAPA) é nossa abordagem estruturada para investigar, identificar a causa-raiz, tomar medidas corretivas e prevenir a recorrência da(s) causa(s) raiz.



Estas são as ações executadas pelo gerente de incidentes durante a RCA:

Criar: Cria um registro de problema a partir do ticket de incidente para executar RCA.

Investigar: As informações no documento de estado do incidente servem como base para realizar a RCA. O gerente de incidentes identifica os departamentos e os processos associados ao CAPA e realiza uma investigação completa. Durante todo o processo de RCA, aprendemos lições e descobrimos oportunidades de melhoria. Fazemos as perguntas abaixo para concluir.

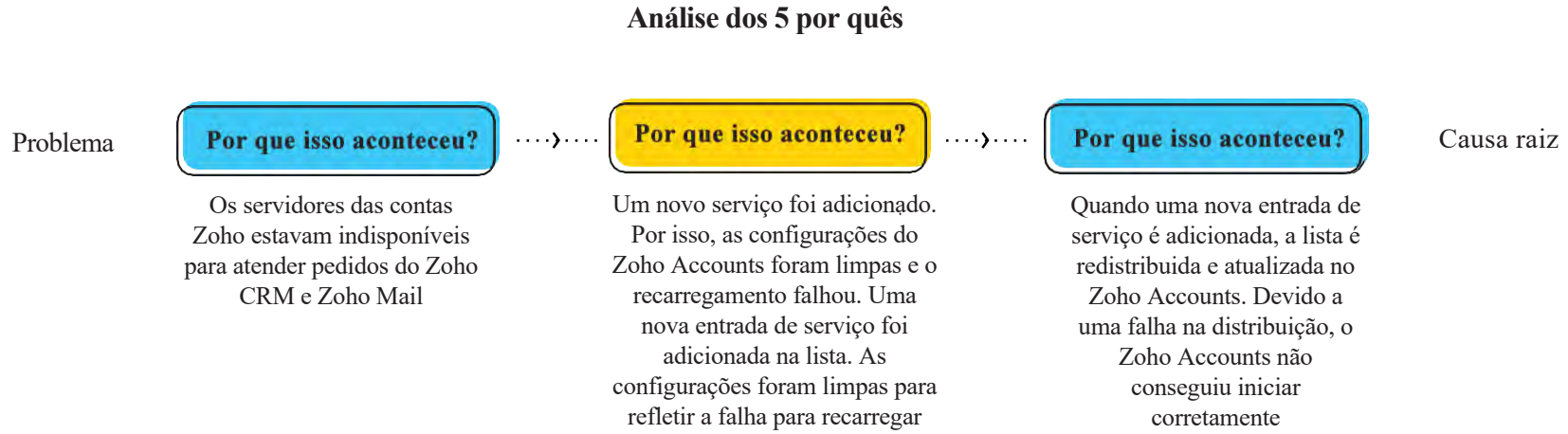
Estágio	Perguntas	Caso de uso
Resumo do incidente	• Quando o incidente foi percebido pela primeira vez? (Data e hora do incidente) • Onde o incidente ocorreu? (Localização, rede, servidor, produto e outros) • Que tipo de incidente? (falha/problema relatado) • Qual é o problema real e o que está acontecendo? (Observações das equipes envolvidas, partes afetadas, interessadas, clientes ou ambos)	• Declaração da causa-raiz: Os servidores do Zoho Accounts estavam em funcionamento, mas não puderam atender a nenhuma solicitação, resultando em problemas de acessibilidade enfrentados pelo Zoho CRM e pelo Zoho Mail. • Resumo do incidente: Este incidente de disponibilidade foi disparado em 22-Jan-2019 às 15:3l IST e terminou em 22-Jan-2019 às 15:52 IST. O incidente foi detectado pelo Site24x7 e afetou os serviços Zoho CRM e Zoho Mail. • O evento foi atenuado por meio das seguintes ações: Correção temporária (imediata): A entrada de serviço que estava causando o problema foi removida imediatamente dentro de 15 minutos após a interrupção. Os servidores do Zoho Accounts estavam em funcionamento e os serviços estavam acessíveis em 20 minutos. Correção **permanente** (**atualização da versão** no dia seguinte**):** Quando um novo serviço é adicionado, limpamos o cache, o que limpa o cache JVM e o repopula. Como uma etapa alternativa, agora estamos repopulando o serviço recém-adicionado no cache JVM para que, mesmo se a repopulação falhar no futuro, a lista de serviços mais antiga seja usada.
Impacto	• Quanto tempo o impacto durou e como ele foi mitigado? • O que os clientes viram? • Quantos foram envolvidos ou afetados? (Por exemplo: clientes de um pacote ou produto) • Quantos tickets de suporte foram emitidos?	• O tempo de inatividade durou 21 minutos, e os clientes do Zoho CRM e do Zoho Mail não puderam acessar os serviços. • 20 tickets de suporte foram emitidos após o incidente por telefone, e-mail e bate-papo.

Estágio	Perguntas	Caso de uso
Resposta	• Quem respondeu e quando? • Qual foi o tempo de resposta?	• O incidente foi detectado pelos clientes, e os coordenadores de incidentes das equipes do Zoho CRM e do Zoho Mail responderam ao incidente informando o gerente de incidentes e envolvendo os chefes das equipes de produtos e outras partes interessadas. • O incidente foi respondido dentro de 15 minutos da ocorrência, e uma correção temporária foi fornecida.
Recuperação	• Como o serviço foi restaurado? • Com que surpresas os grupos de resolução tiveram que lidar? • Quais circunstâncias não foram previstas? • Houve soluções alternativas ou soluções úteis que surgiram durante a crise?	• **Correção temporária (imediata):** A entrada de serviço que estava causando o problema foi removida dentro de 15 minutos após a interrupção. Os servidores do Zoho Accounts estavam em funcionamento e os serviços estavam acessíveis em 20 minutos. • Correção permanente (atualização da versão no dia seguinte): Sempre que um novo serviço for adicionado ao Zoho Accounts, uma lista na qual todos os serviços são armazenados será limpa. Ao preencher a lista agora vazia, tentamos classificar os serviços obtidos do banco de dados. Como esta lista não é mais necessária, nós a removemos completamente da nossa base de código.
Linha do tempo	• Um cronograma detalhado do incidente, em ordem cronológica com marca de data e hora com o fuso horário.	•Jan-2019 15:27 IST: Uma nova entrada de serviço foi adicionada às contas. •Jan-2019 15:30 IST: As configurações do Zoho Accounts foram apagadas para refletir a nova entrada. Subsequentemente, os servidores de contas Zoho não puderam ser recarregados. • 22-Jan-2019 15:31 IST: Os servidores do Zoho Accounts estavam inativos, e os serviços estavam inacessíveis. • 22-Jan-2019: 15.51 IST: Uma correção temporária foi executada em 20 minutos. • 22-Jan-2019 15:52 IST: As contas Zoho tornaram-se estáveis, e os serviços estavam acessíveis novamente.

Estágio	Perguntas	Caso de uso
Lições aprendidas	• O que poderia ser feito para prevenir esse tipo de incidente de acontecer novamente? • Se tivéssemos que fazer de novo, o que faríamos diferente?	• O uso de serviços foi parte de uma AI velha. Como a listagem não era mais necessária, removemos da base de códigos. • Também identificamos e removemos funções similares onde o mesmo algoritmo está empregado para que esse downtime não aconteça no futuro

RCA

O gerente de incidentes determina a causa-raiz dos incidentes usando a técnica de "5 por quês", que envolve fazer repetidamente a pergunta "por quê?" até que a causa-raiz seja identificada. O objetivo não é colocar culpa, mas descobrir por que um incidente ocorreu em primeiro lugar.



Nota: Às vezes, pode levar apenas três "por quês?" para chegar à causa-raiz; muitas vezes, são necessárias mais perguntas. Demora algum tempo para dominar a arte do questionamento, mas quando as perguntas certas são feitas, a causa-raiz pode ser identificada rapidamente. Nesse caso, a causa-raiz foi identificada com apenas três perguntas.

CAPA

Em resumo, as ações corretivas são baseadas em um evento adverso que aconteceu no passado. As ações preventivas são baseadas em impedir um evento adverso no futuro. Ações corretivas e Ações preventivas, normalmente chamadas de CAPA, são partes integrantes de nosso processo de melhoria contínua.

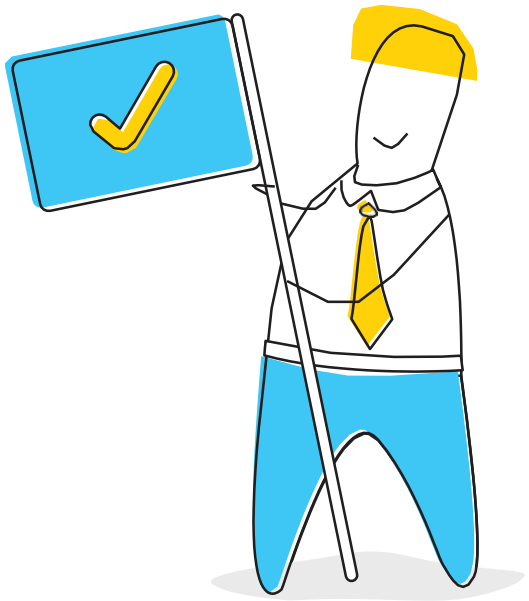
O sucesso de RCA requer um gerenciamento cuidadoso do plano de ação. Portanto, a próxima etapa do processo é estabelecer uma proposta de plano de ação que defina a lista de ações corretivas e ações preventivas. O plano de ação deve definir o período em que as ações serão concluídas e quem controlará cada tarefa.

Aqui está nossa lista de verificação para garantir um plano de ação sistêmico:

- ✓ Há ações corretivas listadas que não são suportadas pela análise?
- ✓ As ações corretivas são claras e apropriadas para a causa?
- ✓ As ações corretivas estão listadas em ordem de prioridade?
- ✓ Se um terceiro estiver envolvido, os itens de ação serão entregues dentro do prazo previsto?
- ✓ As ações corretivas provavelmente causarão consequências indesejadas?
- ✓ As ações corretivas estão sob o controle da gerência?
- ✓ É provável que as ações corretivas impeçam a recorrência?
- ✓ O departamento/proprietário da ação concordou em executar a ação corretiva?
- ✓ Cada ação corretiva tem um proprietário e uma data de vencimento claros?

O processo de ações preventivas consiste em criar proteções e processar alterações para evitar a não conformidade. Como medida proativa, nós:

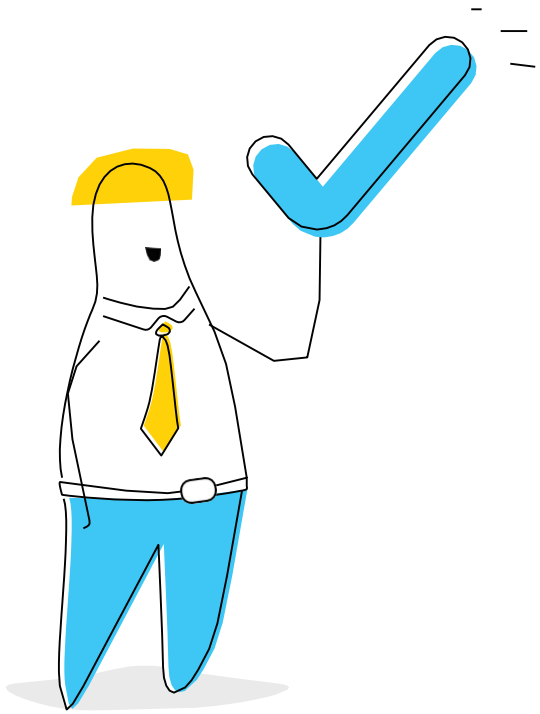
- Analisamos processos e serviços para ver se há tendências negativas que podem escalar um incidente.
- Realizamos a análise de risco para descobrir riscos latentes.
- Realizamos programas de treinamento para aprimorar as habilidades de nossos funcionários e estar mais bem preparados durante um incidente.
- Apresentamos planos de recuperação de desastres, segurança e contingência para situações de crise imprevisíveis.
- Configuramos a manutenção preventiva para garantir que nossos serviços estejam sempre seguros, disponíveis e com desempenho ideal.
- Realizamos auditorias para ajudar a simplificar os processos e fornecer serviços de qualidade.



Revisar

Por fim, a RCA vai para a gerência para aprovação e para fazer as alterações e evitar problemas repetidos. O gerente de incidentes estabelece acompanhamentos completos com grupos de resolução para garantir que as etapas corretivas sejam eficazes e que a recorrência tenha sido impedida.

A lista de verificação abaixo pode ser usada por todas as equipes de TI para avaliar a qualidade geral de um plano de resposta a incidentes.



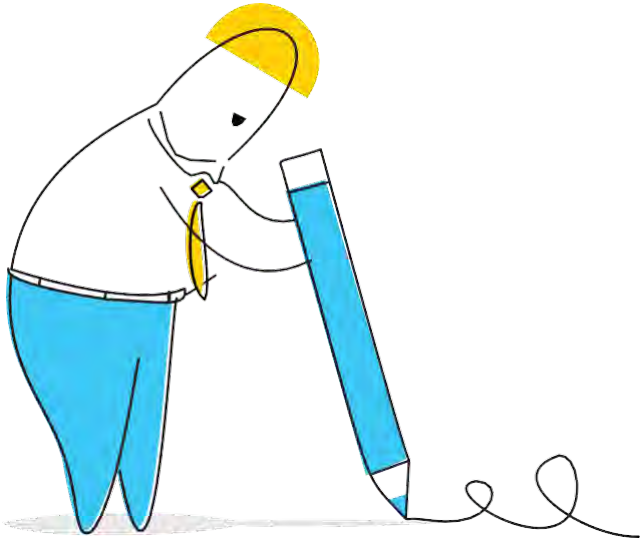
- ✓ O plano de resposta a incidentes ajudou a resolver o incidente ou a organização dependia de atividades “fora do plano”?
- ✓ Há um documento de resumo claro para entender rapidamente o incidente? Toda a análise de incidentes é baseada em fatos?
- ✓ A arquitetura de TI foi robusta o suficiente para limitar o impacto entre os sistemas internos?
- ✓ Até que ponto as equipes associadas, por exemplo, RH, jurídico, de produtos, etc., participou da avaliação e comunicação?
- ✓ A política e as práticas de proteção de dados foram adequadas para identificar e priorizar dados críticos?
- ✓ Qual foi a eficácia do plano de comunicação?
- ✓ Perguntamos “por que” o suficiente para determinar a causa-raiz? Existe um vínculo claro entre fatos, causas e ações corretivas? A análise identificou se o incidente ocorreu anteriormente?
- ✓ Os solucionadores foram identificados anteriormente para lidar com esse tipo de incidente ou retirados posteriormente com base em seu conhecimento?
- ✓ Os riscos para a organização foram avaliados e gerenciados? A RCA passou pelo mecanismo de aprovação?

Reuniões sobre RCA

Realizamos reuniões RCA para chegar ao fim do problema, tomamos as ações corretivas necessárias para corrigir o problema permanentemente e tomar ações preventivas. A diretriz mais importante para nossas reuniões de RCA é aprender e melhorar continuamente, não atribuir culpa ou desabafar.

Aqui estão algumas dicas para garantir uma reunião de RCA eficaz:

- Agende uma data e hora convenientes para todos os participantes da reunião, tendo em mente que os membros da equipe que trabalham em turnos e outras equipes distribuídas.
- Desenvolva e mantenha uma pauta de reunião que não exceda duas horas.
- Reserve uma sala de conferência/reunião com assentos suficientes para todos os grupos de resolução, partes interessadas e a alta gerência.
- Agende e convide participantes (usamos o Zoho Calendar) um a dois dias antes da reunião de RCA, enfatizando a importância da reunião e incluindo a pauta da reunião.
- Mantenha um registro por escrito da duração da reunião.



Conclusão

Os processos de gerenciamento de incidentes destinam-se a proteger as organizações contra eventos adversos. Isso é especialmente verdadeiro para organizações como a Zoho Corporation, que dependem muito da internet e das redes de computadores e lidam com uma grande quantidade de dados pessoais.

Uma política eficaz de resposta a incidentes se concentra em quatro aspectos principais: gerenciamento de riscos, auditorias regulares, medidas preventivas e, o mais importante, treinamento de funcionários. Na Zoho, temos as pessoas, os processos e as ferramentas certos em vigor para nos mantermos à frente de futuros ataques cibernéticos.

Agora que você viu como a Zoho lida com incidentes, esperamos que sua organização possa projetar e buscar uma estratégia semelhante, tendo em mente suas operações de negócios, força-tarefa e cultura da empresa.

Devika Subbaiah

Gerente de incidentes, Zoho

Meghna Reddy

Autor

Nikhilesh Raaja

Designer do livro

Zorro, a equipe de operações de infraestrutura da Zoho, usa as soluções de gerenciamento de TI da ManageEngine para gerir 10 centros de dados em quatro continentes para servir 50 milhões de usuários.

Sobre o ServiceDesk Plus

O ServiceDesk Plus é um software de help desk pronto para ITIL com recursos integrados de gerenciamento de ativos e projetos. Com funcionalidade avançada de ITSM e fácil capacidade de uso, o ServiceDesk Plus ajuda as equipes de suporte de TI a fornecer serviços de classe mundial aos usuários finais com custos e complexidade reduzidos. É fornecido em três versões e está disponível em 29 idiomas diferentes. Mais de 100.000 organizações em 185 países confiam no ServiceDesk Plus para otimizar o desempenho do service desk de TI e obter alta satisfação do usuário final.

Para saber mais sobre o ServiceDesk Plus, visite www.manageengine.com.br/service-desk

ManageEngine

ServiceDesk Plus

manageengine.com/br/service-desk/