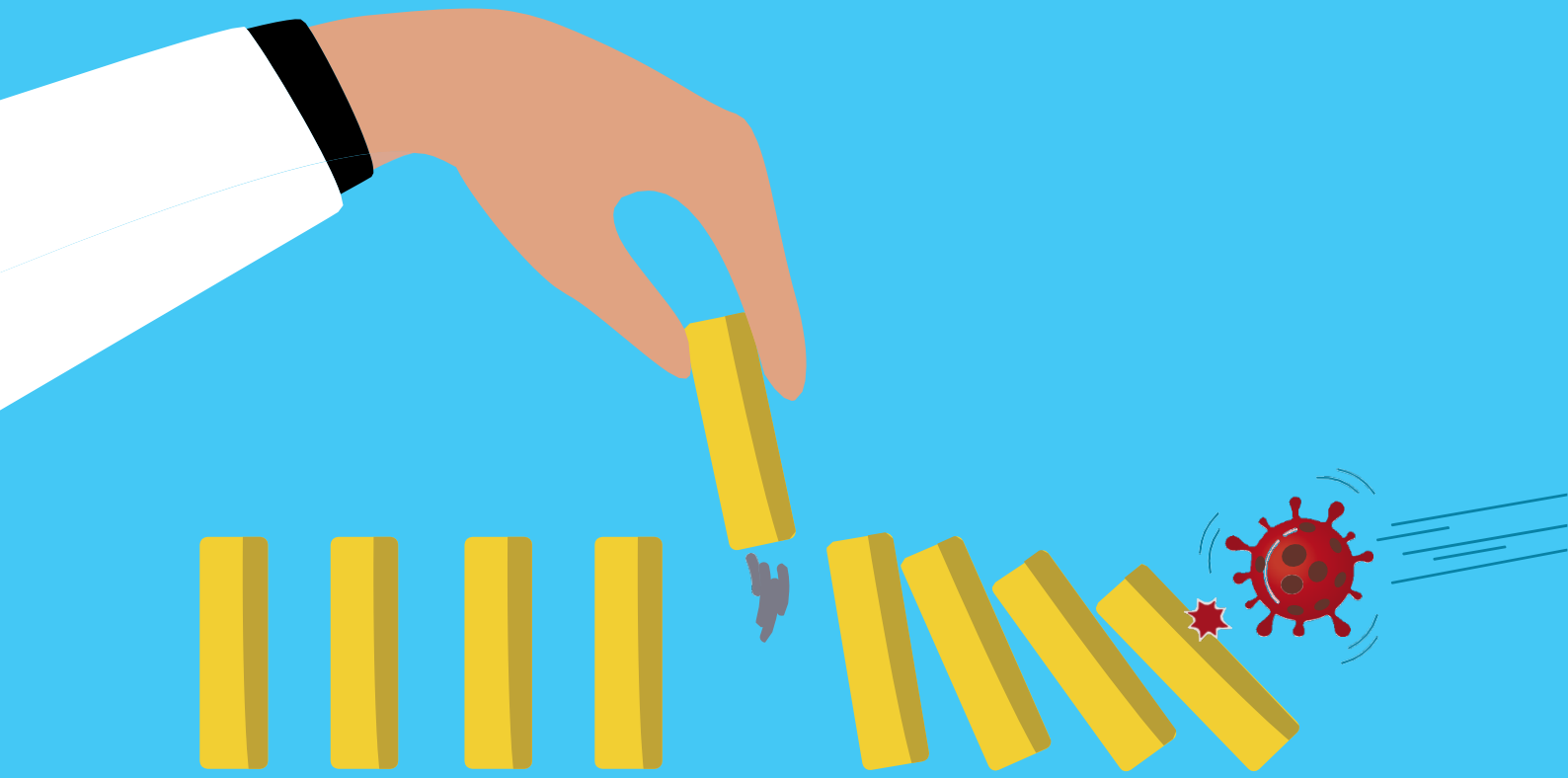
MANUAL DE CONTINUIDADE DOS NEGÓCIOS E RECUPERAÇÃO

Como a Zoho Corp responde a desastres e faz negócios como de costume

Apresentando

- Estrutura de BCDR para empresas.
- Um estudo de caso da Covid-19: Lidando com o novo normal de negócios – trabalhando de casa



“Não é possível prever a próxima catástrofe, mas você pode estar preparado para ela!”

Glossário de termos

ARMC	Comitê de auditoria e gerenciamento de riscos
BC	Continuidade dos negócios
BCC	Coordenador de continuidade dos negócios
BCDR	Continuidade dos negócios e recuperação de desastres
BCM	Gerenciamento de continuidade dos negócios
BCDRC	Comitê de continuidade dos negócios e recuperação de desastres
BIA	Análise do impacto nos negócios
Covid-19	Comumente conhecida como coronavírus; uma pandemia global que é uma síndrome respiratória aguda grave
DR	Recuperação de desastres

Abra o manual e encontre

Capítulo 01

Introdução

História:
A realização

Tsunami em 2004

Antes e durante a década de 90, a cidade de Chennai era um refúgio de paz e não era vulnerável a desastres naturais. Entretanto, na última década, testemunhamos desastres naturais em todas as formas: furacão, terremoto, tsunami e a recente pandemia viral global de Covid-19.

Em 2004, um terremoto de magnitude 9.1 atingiu o oceano índico perto da Indonésia, gerando um enorme tsunami que ocasionou cerca de 8.000 mil mortes na costa de Chennai. As ondas gigantes inundaram as áreas à beira-mar provocando danos patrimoniais e ativos a muitas empresas de TI e telecomunicações da região. Nosso escritório da Zoho não foi afetado pelo tsunami; no entanto, a empresa foi afetada por ausências de funcionários naquele momento.

Chennai fica inundada em 2015

Em 2015, vimos a pior queda de chuvas em Chennai (1.049 mm, a maior quantidade registrada desde novembro de 1918), seguida por inundações sem precedentes que deixaram milhares de cidadãos presos tentando passar pelas águas profundas. As chuvas castigaram Chennai por um mês.

Estávamos mais bem preparados para enfrentar a devastação da água e seus efeitos prejudiciais em 2015. O edifício Estancia Tower foi completamente evacuado, e as operações foram fechadas por alguns dias devido ao alagamento de alguns andares, resultando em danos consideráveis com água e vidros quebrados. Invocamos um esforço de recuperação e algumas de nossas equipes essenciais de atendimento ao cliente foram transferidas para nossos escritórios em Tenkasi, Tamil Nadu e Bangalore, Karnataka, os locais alternativos para operações contínuas em 2015. Também asseguramos que nossos funcionários recebessem acomodações residenciais para sua segurança e continuidade dos negócios; alguns de nossos funcionários trabalharam produtivamente em suas casas.

Esse incidente abriu nossos olhos e nos ajudou a perceber como a falta de planejamento pode representar um sério risco para qualquer organização moderna como a nossa. Formamos um comitê de continuidade dos negócios e recuperação de desastres (BCDRC) na Zoho para desenvolver nosso plano de continuidade dos negócios e recuperação de desastres (BCDR), dois componentes essenciais de nossos negócios. Acreditamos que a invocação deste plano nos ajuda a estar preparados para todos os desastres. Modificamos nossas ações com base no impacto e na natureza do desastre.

15 anos após o tsunami.

Como a Zoho Corp evoluiu como uma empresa na continuidade dos negócios, resiliência e resposta?

Nossa jornada de BCDR

Por que BCDR?

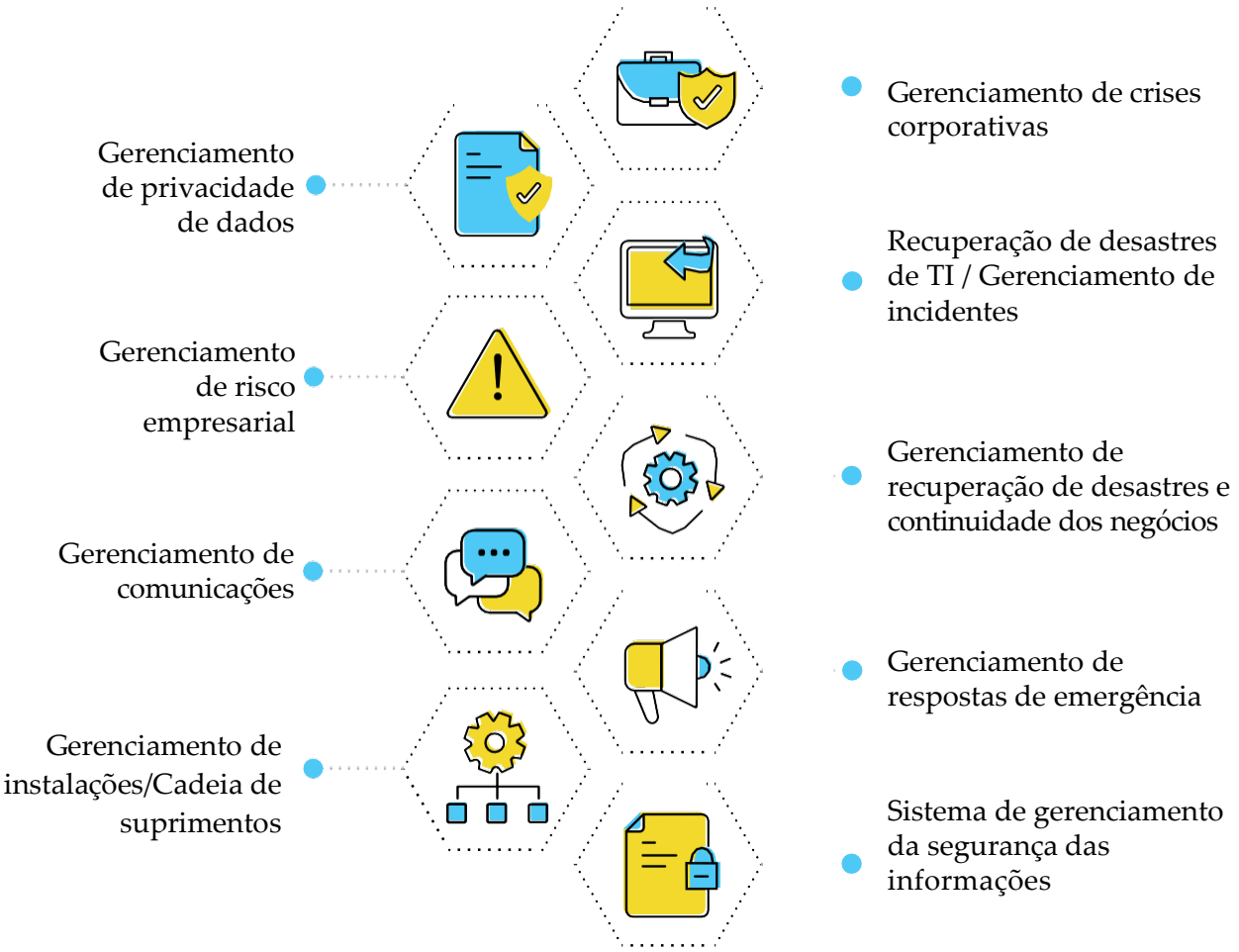
O maior teste para a reputação de uma organização é sua capacidade de lidar com uma crise. Descobrimos que nem todas as crises são iguais. Sua intensidade e longevidade podem diferir e, portanto, não há uma fórmula para lidar com uma crise.

O segredo para sair ileso é se preparar. Para isso, temos um amplo leque de gerenciamento de crises para determinar uma resposta adequada para cada tipo de crise. Nossos esforços de gerenciamento de crises e continuidade dos negócios, orientados por nosso BCDRC, integram as disciplinas de gerenciamento de crises corporativas, gerenciamento de resposta a emergências, gerenciamento de incidentes/recuperação de desastres de TI (continuidade da tecnologia), gerenciamento da continuidade dos negócios (organizacional/operacional) e gerenciamento de segurança das informações.

BCDR é a sua própria disciplina, por isso devemos tratá-lo dessa forma. BCDR e a preparação devem chegar ao nível de base e serem considerados um dos principais processos em conjunto com a melhoria contínua.

– Rajesh Ganesan
Vice-presidente, ManageEngine

Estrutura de gerenciamento de crises



Nas últimas décadas, os desastres naturais tornaram-se mais comuns e dispendiosos, destacando a necessidade de a continuidade dos negócios estar pronta para ser implantada no caso de um desastre. Como empresa, a Zoho entende perfeitamente que nossa BCDR é vital para ajudar nossa organização a evitar e reduzir os riscos associados a qualquer interrupção das operações.

Um desastre pode afetar as organizações de forma diferente – um furacão pode derrubar o telhado do edifício de uma organização, inundar outro e deixar um terceiro sem danos. Embora alguns desastres naturais, como um furacão, possam causar perda de vidas ou ferimentos significativos, outros desastres, como um grande incidente de TI, apesar de parecer menos dramáticos, podem impactar significativamente as operações de negócios.

Na Zoho, acreditamos que a preparação é a chave para lidar com todos os tipos de desastres de forma eficaz e para garantir a continuidade dos negócios. (Se você está gerenciando uma empresa, então também deve acreditar na preparação!)

Nossa BCDR registra uma abordagem empresarial orientada a processos que abrange as habilidades operacionais de nossos data centers, operações de TI, sistemas, funções de atendimento ao cliente e estratégias de comunicação. Tudo isso é fundamental para a resiliência e operações bem-sucedidas da Zoho, mesmo em circunstâncias imprevistas.

O plano de BCDR foi criado Com base nestes princípios orientadores:

Princípios	Raciocínio
Integrar os principais processos de negócios	Garantir que a BCDR e o gerenciamento de riscos sejam parte integrante dos principais processos.
Reunir as melhores e mais confiáveis informações.	Coletar informações de várias fontes de dados: • Internos: As partes interessadas e o conselho administrativo fornecem decisões baseadas em evidências. • Externos: Órgãos governamentais e aplicação da lei
Fazer uma abordagem que prioriza as pessoas.	• Garantir a segurança de nossa força de trabalho.
Garantir uma recuperação ágil e rápida.	• Operar de forma eficiente durante emergências e garantir que nossos produtos e serviços não sejam interrompidos por nossos clientes. • Dar uma resposta imediata e eficaz para manter a credibilidade aos olhos de nossos clientes, parceiros e partes interessadas.
Preparar-se de forma eficaz para lidar com todos os tipos de desastres.	• Garantir que nossa BCDR resolva a interrupção dos negócios resultante de vários tipos de desastres. (Consulte a seção abaixo para entender as categorias de desastres).
Melhorar continuamente	• Registrar os aprendizados de eventos problemáticos para identificar lacunas na BCDR, para que possamos nos preparar melhor para responder a eventos futuros.

Então, as organizações devem começar com a BCDR imediatamente?

A resposta é um retumbante SIM. Nenhum negócio é imune a desastres. A história do planejamento da continuidade está repleta de exemplos de empresas que saem dos negócios após um desastre. Mais empresas estão agora mudando seu foco na continuidade dos negócios, entendendo que o tempo de inatividade, especialmente se durar muito tempo, pode resultar em riscos e custos substanciais para sua organização.

MENSURÁVEL 	INTANGÍVEL 
Receita adiada ou perdida	Danos à credibilidade e à reputação
Aumento da rotatividade de clientes; insatisfação do cliente	Perda de cortesia com parceiros e clientes
Menos produtividade dos funcionários	Perda de moral dos funcionários e perda de confiança na organização
Penalidades devido á não conformidade dos acordos de serviço (SLAs; Service-Level Agreements)	Perda de vantagens competitivas

Uma BCDR abrangente é fundamental para lidar com eventos imprevistos e com o tempo de inatividade resultante, permitindo que as organizações eliminem pontos de falha, garantam planos de backup e restaurem operações rapidamente. No entanto, embora algumas empresas tenham dificuldade para desenvolver e executar um plano, outras expressam incontáveis desculpas para evitar o desenvolvimento de um:

“Nosso pessoal saberá o que fazer durante uma emergência.”

O que seus funcionários farão quando algo acontecer em sua localização física? Sim, contratamos as pessoas mais inteligentes e intuitivas, mas permitir que os funcionários respondam e ajam por conta própria só aumentará o caos existente. Um plano de continuidade dos negócios bem documentado, políticas relevantes e treinamento com as simulações em tempo real podem garantir que a força de trabalho está preparada para desastres e mantê-la concentrada em permanecer o mais produtiva possível.

“Isso não vai acontecer conosco.”

Agradecemos o otimismo. No entanto, é sempre melhor esperar o inesperado, pois a falta de backups, planos de recuperação de desastres ou esforços de continuidade suficientes podem deixar qualquer empresa paralisada, caso o pior aconteça.

“Temos seguro. Não há com o que se preocupar!”

Estamos no mercado há mais de 20 anos e sofremos alguns golpes ao longo do caminho. É assim que sabemos que, embora o seguro faça parte de uma estratégia de continuidade dos negócios, ele não pode cobrir os danos periféricos e intangíveis resultantes de um evento como perda de clientes, participação de mercado ou contratempos no desenvolvimento de um novo produto.

“Não é nossa prioridade. Não temos tempo para isso.”

Aconteceu conosco; dificilmente víamos a continuidade como uma prioridade até que se tornou um requisito catastrófico. No caso de um desastre, a continuidade dos negócios tem sido o fator-chave para manter nossos negócios funcionando. Acreditamos que a capacidade de atender aos clientes durante e imediatamente após um evento pode melhorar a credibilidade com os clientes e garantir sua sustentação.

“BCDR é para grandes empresas. Podemos relaxar.”

Muitas pequenas e médias empresas (PMEs) acreditam que são muito pequenas e que ter uma BCDR em vigor pode ser um exagero. Infelizmente, o impacto nas startups e nas PMEs é mais brutal durante os desastres, pois normalmente elas têm menos reservas de dinheiro para gerenciar quedas repentinas. Ter uma BCDR pode impedir que pequenas empresas incorram em mais perdas, permitindo-lhes atingir o ponto de equilíbrio até que a situação se estabilize.

Por que nossa estrutura?

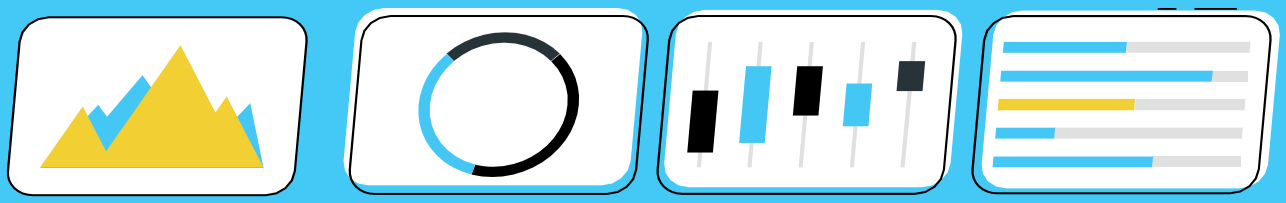
Somos um provedor de Software como um serviço (SaaS) com mais de 20 anos de experiência em desenvolvimento de software, e com 12 escritórios em todo o mundo e 10 data centers. Nossa sede nos EUA atualmente fica em Pleasanton, Califórnia. O campus de pesquisa e desenvolvimento e a sede global ficam no Estancia IT Park em Chennai, Índia, com uma infraestrutura de classe mundial que hospeda uma força de trabalho de quase 10.000 pessoas trabalhando no desenvolvimento de produtos de software inovadores. Cerca de 50 milhões de clientes em todo o mundo confiam em nossas aplicações para suas necessidades de negócios e de TI.

A estrutura futura apresenta o modelo de continuidade dos negócios e recuperação de desastres da Zoho, que inclui recursos, ações, processos, listas de verificação, práticas recomendadas e informações. Foi criada, testada e projetada para ser resiliente para nos ajudar a evitar a interrupção das operações diante de um evento.

Esse modelo ajudou a Zoho a minimizar o impacto, manter funções essenciais e retornar às operações normais o mais rápido possível após qualquer cenário de desastre, independentemente da causa e da duração. Registra nossos aprendizados na última década e pode servir como um plano para simplificar e desmistificar os processos de recuperação de desastres e continuidade dos negócios para todas as organizações de TI desenvolverem seus próprios esforços de BCDR com base em seu modelo de negócios.

Combina a experiência do Comitê de continuidade dos negócios e recuperação de desastres (BCDRC) que inclui o conselho administrativo e a alta gerência, tornando-o uma leitura essencial para as equipes de continuidade dos negócios, gerentes de TI, gerentes de risco, auditores e líderes.

Se isso despertar o seu interesse, prossiga para nossa estrutura de BCDR abaixo.



Um esquema para manter sua empresa funcionando durante um desastre

Resiliência. Recuperação. Contingência

Capítulo 02

Um esquema de BCDR para empresas

Estrutura de BCDR da Zoho

Finalidade e escopo

- Defina propósito e escopo
- Governança da BCDR
- Funções e responsabilidades

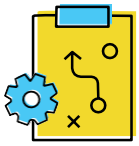
Avaliação de riscos

- Identificação de riscos
- Análise de riscos
- Avaliação de riscos
- Tratamento de riscos

Análise do impacto nos negócios

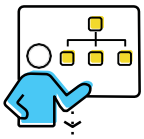
- Conduzir entrevistas de BIA
- Criar relatórios de BIA
- Aprovação do BCDRC

Planejamento de BCDR



- Procedimentos de recuperação de desastres
- Procedimentos de continuidade dos negócios
- Aprovação do BCDRC

Implementação e treinamento



- Treinamento e educação
- Documentação da BCDR

Melhoria contínua

- Planejamento da revisão e manutenção

Finalidade

O plano de BCDR estabelece as etapas e procedimentos que a Zoho e a ManageEngine seguirão antes, durante e na sequência de desastres, por exemplo, desastres naturais, eventos causados pelo homem, pandemias etc. Somos resilientes como empresa, e estamos comprometidos em garantir a máxima funcionalidade durante qualquer emergência e retornar nossas operações ao normal no menor tempo possível.

Principais elementos da BCDR:

- **Resiliência:** Resistir a interrupções dos negócios em virtude de condições adversas
- **Recuperação:** Voltar aos negócios o mais rápido possível após um desastre
- **Contingência:** Ter um conjunto abrangente de medidas e controles em vigor para uma recuperação completa
- **Melhoria contínua:** Revisar continuamente o plano, fazer as revisões necessárias e manter o plano atualizado

Escopo

A eficácia de uma BCDR depende de um escopo bem definido. Como a Zoho é uma grande empresa e tem equipes distribuídas, esse processo é compreensivelmente complexo. Há muitas perguntas que fazemos, respondemos e registramos ao determinar o escopo de uma BCDR:

- Ele cobrirá todos os locais de trabalho, locais propensos a desastres ou o centro de produção?
- Ele cobrirá todos os clientes ou apenas uma porcentagem deles?
- Ele cobrirá um desastre local ou desastres disseminados, como furacões e pandemias?
- Quais são nossos produtos e serviços essenciais?
- Quais são os processos críticos e as unidades de negócio que DEVEM funcionar no caso de um desastre? Exemplo: Equipes de atendimento ao cliente.

Em seguida, validamos determinadas suposições. Por exemplo: recursos qualificados, líderes de equipe ou alternativas que estarão disponíveis após um desastre.

Governança da BCDR

Muitas organizações encarregadas de desenvolver uma BCDR começam imediatamente a escrever um plano. No entanto, a experiência nos diz que uma boa estrutura de governança é fundamental para direcionar nossos esforços de criação e garantir que não haja becos sem saída e armadilhas nos processos.

Temos um sistema de controle ou governança que é composto por nosso conselho administrativo e executivos da alta gerência da Zoho e da ManageEngine. O BCDRC é contratado desde o início para orientar nossos esforços e garantir que, a) os indivíduos certos estejam nas funções certas para maximizar nossos esforços de continuidade dos negócios, e b) a BCDR esteja sempre pronta e relevante.

A tabela a seguir destaca as funções e responsabilidades de nosso BCDRC.

As funções e responsabilidades de nosso BCDRC

CONSELHO ADMINISTRATIVO	ALTA GERÊNCIA
Compreende e comunica o valor da BCDR e os riscos na ausência de uma BCDR	A equipe de alta gerência tem um conhecimento sólido das práticas de BCDR e riscos de negócios.
Analisa a BCDR da organização anualmente.	Mantém o conselho administrativo e os membros da diretoria informados sobre quaisquer mudanças significativas nos planos de continuidade dos negócios.
Obtém atualizações frequentes da equipe de alta gerência para quaisquer novas políticas e procedimentos de continuidade dos negócios.	Define os objetivos de gerenciamento de negócios da Zoho, fornece informações estratégicas e designa os coordenadores de continuidade dos negócios (BCCs).
Direciona e aprova o planejamento, a implementação, os testes e outros objetivos estratégicos da BCDR.	Revisa e aprova, durante a criação e a atualização de processos críticos, os procedimentos operacionais padrão (POP) e exercícios de planejamento de nossa BCDR para todas as unidades de negócio.
Orienta o comitê de auditoria a se preparar para auditorias externas.	Apoia e comunica a importância do planejamento, do treinamento e dos testes de BCDR a todas as partes interessadas.
Direciona o plano de comunicação externa para investidores, clientes, mídia e autoridades de aplicação da lei.	Atribui os gerentes intermediários apropriados para executar os principais procedimentos e exercícios relacionados à BCDR.

Outras funções e responsabilidades

QUEM ?	FAZ O QUÊ?
Os coordenadores de continuidade dos negócios (BCC) são como coordenadores de incidentes (consulte o processo de IM aqui). O BCC cria e mantém a BCDR e trabalha em estreita colaboração com outras funções críticas de negócios para entender seus processos, identificar riscos e também ajudar a gerenciar e minimizar esses riscos.	• Gerenciam, comunicam e controlam todas as atividades associadas à BCDR e à recuperação de funções de negócios críticas. • Ativam a BCDR para departamentos afetados. • Mantêm o gerente de incidentes informado sobre os esforços de continuidade/ recuperação de desastres (consulte o processo de IM aqui). • Atendem à gerência intermediária para analisar e priorizar os processos críticos de suas respectivas unidades de negócio. • Recebem atualizações dos gerentes intermediários e ajustam os planos, conforme necessário. • Trabalham com a equipe de comunicações e fornecem informações para ajudar a elaborar o plano de comunicações. • Quando a empresa volta ao normal, recebem o feedback da gerência intermediária para identificar lacunas e registrar os aprendizados para melhorar continuamente a BCDR. • Mantêm a documentação da BCDR, e garantem a confidencialidade e a privacidade.
Gerência intermediária (Proprietários de empresas)	• Entrevista com o BCC para determinar os processos críticos de suas unidades de negócio. • Avaliar os riscos específicos de suas unidades de negócio. • Recomenda as etapas para o BCDRC para abordar os riscos identificados relacionados a suas unidades de negócio individuais. • Colabora com a equipe de gerenciamento de TI e o BCC para projetar e implementar a BCDR com base na avaliação de riscos e na BIA.

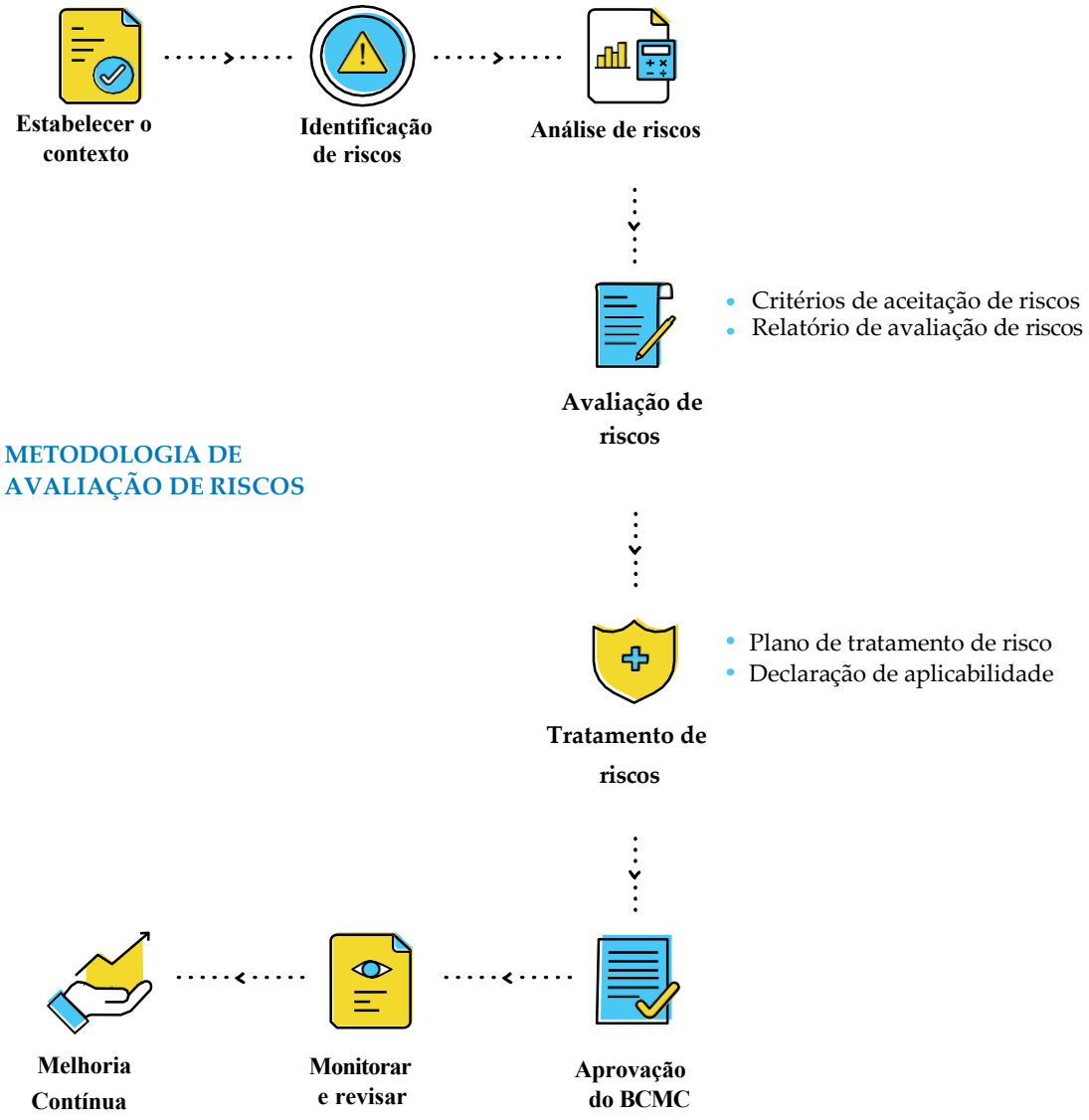
Outras funções e responsabilidades

QUEM?	FAZ O QUÊ?
Gerência intermediária (Proprietários de empresas)	• Realiza testes adequados para garantir a exatidão dos procedimentos de operabilidade dos negócios de acordo com a BCDR.
Comitê de auditoria e gerenciamento de riscos (ARMC)	• Realiza auditorias internas de conformidade. • Revisa e reporta ao BCDRC sobre a eficácia da BCDR.
Equipe de gerenciamento de riscos	• Os proprietários de riscos são, em última análise, responsáveis por garantir que o risco seja gerenciado adequadamente.
Conselho jurídico	• Identifica os riscos legais e aconselha o BCDRC. • Supervisiona todas as investigações internas durante emergências. • Toma medidas proativas de conformidade para o Zoho. • Trabalha com porta-vozes/equipe de comunicações para elaborar nossa comunicação externa.
Outras partes interessadas	• Relatam suas preocupações na avaliação de riscos e na BIA de suas respectivas unidades de negócio. • Familiarizam-se com a BCDR e os contatos de emergência. • Participam de sessões de teste e treinamento e fornecem um feedback à gerência intermediária.

Avaliação de riscos

A primeira e principal etapa da BCDR é a avaliação dos riscos. Risco é a incerteza de atingir os objetivos, o que afeta nossos negócios de uma forma adversa. Os riscos são percebidos quando:

- O objetivo do negócio não é alcançado.
- Não há conformidade com as políticas e os procedimentos da organização, ou com a legislação e regulamentação externas.
- Os recursos da empresa não são utilizados de maneira eficiente e eficaz.
- Há uma violação da Confidencialidade, integridade e disponibilidade (CIA) das informações.



É importante que a Zoho tenha uma abordagem de todos os perigos para os processos de avaliação e controle de riscos em vigor para garantir que os possíveis impactos não se tornem reais ou, se isso acontecer, haja um plano de contingência em vigor para lidar com eles. Também é importante que o processo seja claro para que as avaliações sucessivas produzam resultados consistentes, válidos e comparáveis, mesmo quando realizadas por pessoas diferentes.

Estabelecer o contexto

O escopo da avaliação de riscos é definido com base em fatores como:

- Localização geográfica: Data centers distribuídos e configuração de escritório
- Unidades de negócio ou departamentos Processo(s) de negócios
- Serviços, sistemas e redes de TI
- Clientes, parceiros, produtos ou serviços

O ambiente geral no qual a avaliação de riscos é realizada deve ser identificado e racionalizado. Isso incluirá uma descrição do contexto interno e externo e quaisquer alterações recentes que afetem a probabilidade e o impacto dos riscos em geral.

CONTEXTO INTERNO	CONTEXTO EXTERNO
Governança, estrutura organizacional, funções e responsabilidades	Ambientes cultural, social, político, jurídico e regulatório
Políticas, objetivos e estratégias	Ambientes financeiros, tecnológicos, econômicos, naturais e competitivos
Capital, tempo, pessoas, processos, sistemas e tecnologias	Ambientes internacionais, nacionais, regionais ou locais
Sistemas de informação, fluxos de informação e processos de tomada de decisão	Principais motivadores e tendências que afetam os objetivos da organização
Relações com as, percepções e valores das, partes interessadas internas	Relações com as, e percepções e valores das, partes interessadas externas
A cultura da organização	
Padrões, diretrizes e modelos adotados pela organização	
Forma e extensão das relações contratuais	
O(s) tipo(s) de serviços em nuvem fornecidos	

Identificação de riscos

Embora haja uma infinidade de desastres, os efeitos resultantes são semelhantes para a maioria, e é para eles que planejamos. Eles resultam em cenários como perda de infraestrutura ou falha sustentada de TI. A preparação para o pior cenário ajuda a cobrir muitos cenários e riscos em um único plano.

Nossa equipe de avaliação de riscos identifica, classifica e avalia uma ampla gama de desastres, sobretudo aqueles com potencial de impacto extremamente alto, e depois caracteriza seus efeitos sobre os negócios para melhorar a preparação, a resposta e a resiliência.

Natural		Intencional	Acidental
Subcategoria			
Geofísico	Terremoto	Ameaça de bomba	Derramamento de produto químico
	Erupção vulcânica	Atividade terrorista	Contaminação por radiação
	Deslizamento de terra	Desordem civil	Falha nos sistemas de aquecimento ou no ar-condicionado
	Desabamento de pedras	Explosão de bomba	Falha de telecomunicações
Meteorológico	Tempestade	Armas biológicas	Falha na rede
	Tempestade de neve com raios	Desperdício desastroso	Vazamento de gás
	Nevasca	Greve de funcionários	Incêndio (interno)
	Tornado	Ataque cibernético	Incêndio (externo)
Hidrológico	Inundação	Funcionários descontentes sabotam os sistemas de uma organização	
	Tsunami		
	Avalanche		
Climatológico	Seca		
	Onda de calor/onda fria		
	Incêndios florestais/terrestres		
Biológico	Epidemia		
	Pandemia		

A maioria das empresas tem planos de resiliência para desastres geofísicos, intencionais e acidentais, e para recuperação de desastres de TI. Esses planos, que são eficazes para várias interrupções nos negócios, podem falhar durante uma pandemia global, como a Covid-19.

É importante que as empresas compreendam as diferenças significativas entre desastres naturais e epidemias pandêmicas para que possam ir além das estratégias tradicionais de continuidade dos negócios. Na Zoho, estabelecemos políticas e estratégias de comunicação específicas para pandemias para minimizar as interrupções nos negócios.

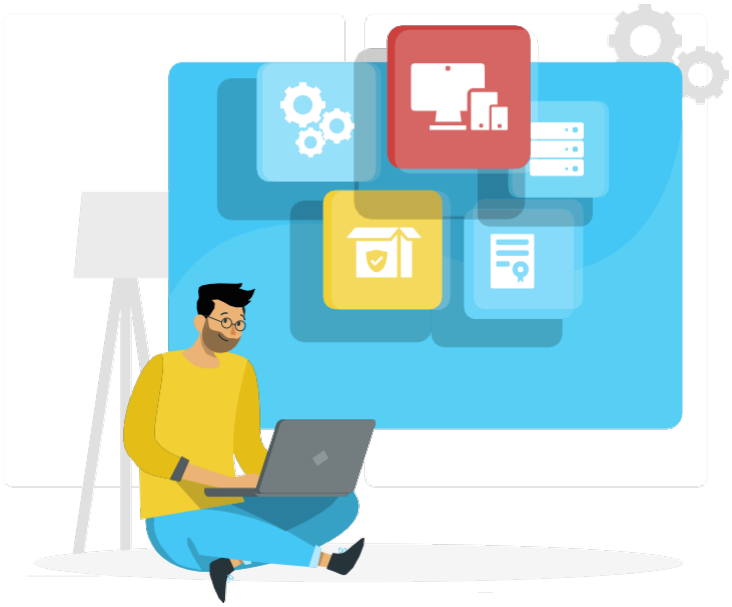
Embora desastres naturais com fenômenos físicos sejam limitados a uma determinada geografia, desastres biológicos, como pandemias virais, se espalham globalmente. A tabela abaixo lista as diferenças entre as interrupções devido a desastres naturais e pandemias.

Diferenças de interrupções entre desastres naturais e biológicos

Fatores distintivos	Natural	Biológico
Impacto	Afeta a organização, a instalação, a força de trabalho e terceiros.	Um evento sistêmico que afeta todos globalmente, incluindo a organização e sua força de trabalho, clientes, fornecedores e concorrentes.
Exposição	Pode ser contido e isolado assim que a causa for identificada.	Um contágio que se espalha rapidamente pelas geografias com impactos graves.
Duração	Duração mais curta. Varia de algumas horas a uma semana.	Maior duração. Uma pandemia viral pode durar vários meses.
Força de trabalho	Escassez temporária e realocação da força de trabalho.	Escassez significativa da força de trabalho que precisa de outras alternativas, como o teletrabalho.
Comunicação externa	As emergências devem ser relatadas às autoridades de aplicação da lei apropriadas e à assistência médica (p. ex., departamento de polícia, corpo de bombeiros, serviço de ambulância).	Alto grau de coordenação com o governo local, aplicação da lei, assistência médica.
Infraestrutura	Afeta a disponibilidade da infraestrutura pública, como eletricidade, telecomunicações e Internet.	Afeta a cadeia de suprimentos global.

Compilar/manter o inventário de ativos:

A definição de um ativo é "qualquer coisa que tenha valor para a organização" e precisa ser protegida. Um inventário completo de ativos é compilado e mantido pela Zoho usando a aplicação ServiceDesk Plus. Isso inclui os dados do cliente que a Zoho armazena e processa em sua função como um provedor de serviços em nuvem.



Os dois principais tipos de ativos são identificados como:

- Ativos primários – informações, e processos e atividades de negócios
- Ativos de suporte – hardware, software, rede, pessoal, local e estrutura organizacional

A lista de ativos é mantida no documento Informações sobre o Inventário de Ativos e na aplicação ServiceDesk Plus. Dentro do inventário, cada ativo recebe um valor que deve ser considerado como parte do estágio de avaliação de impacto desse processo. Cada ativo também tem um proprietário que deve estar envolvido na avaliação de risco. Quando apropriado para fins de avaliação de risco, os ativos de dados de clientes em nuvem podem ser de propriedade de uma função interna e o cliente consultado sobre o valor. Para fins de avaliação de riscos, recomenda-se agrupar ativos com requisitos semelhantes para que o número de riscos a serem avaliados permaneça gerenciável.

Para cada ativo (ou grupo de ativos), as ameaças que podem ser razoavelmente esperadas para serem aplicadas serão identificadas. Elas variam de acordo com o tipo e podem ser eventos acidentais, como incêndio, inundação, impacto no veículo ou ataques mal-intencionados, como vírus, roubo ou sabotagem. As ameaças se aplicarão a uma ou mais das CIA (Confidencialidade, integridade e disponibilidade).

Cenários de risco:

A identificação de cenários de risco é realizada por uma combinação de discussões em grupo e entrevistas com partes interessadas, como:

- Gerente(s) da unidade de negócio responsável(is) por cada atividade crítica de negócios
- Representantes das pessoas que normalmente realizam cada aspecto da atividade
- Fornecedores dos insumos para a atividade
- Destinatários das produções da atividade
- Terceiros apropriados com conhecimento relevante
- Representantes dos que prestam serviços e recursos de apoio à atividade
- Qualquer outra parte que seja sentida para fornecer informações úteis sobre o processo de identificação de risco

Os riscos identificados, juntamente com uma descrição, são registrados para avaliar a probabilidade e o impacto dos riscos.

Desastres e cenários de risco identificados na última década

PERIGOS	CENÁRIOS DE RISCO
Terremotos Inundações Tsunami Pandemia Ransomware Ataques de DDoS Falha de telecomunicação Falha na rede	Danos irreversíveis à infraestrutura de TI Metade das principais unidades de negócio de geração de receita Perda do centro de produção da Zoho (Edifício Zoho Estancia) e data centers Perda de dados críticos do cliente Absenteísmo de funcionários críticos Perda de acesso aos nossos sites mundiais Interrupção da cadeia de suprimentos

Análise de riscos

Esse processo envolve a atribuição de um valor numérico para a) probabilidade e b) impacto de um desastre. Esses valores são então multiplicados para chegar a um nível de classificação alto, médio ou baixo para o desastre.

Avaliação da probabilidade:
É feita uma estimativa da probabilidade de ocorrer um desastre. Isso deve considerar se o desastre ocorreu antes na Zoho ou em organizações semelhantes, ou no local e se há motivo, oportunidade e capacidade suficientes para que uma ameaça seja realizada.

A probabilidade de cada desastre é avaliada em uma escala numérica de 0 (baixa) a 3 (alta). Ao avaliar a probabilidade de um desastre, os controles existentes são considerados e isso significa que uma avaliação deve ser feita sobre a eficácia dos controles existentes. A lógica para registrar as notas atribuídas a um risco de desastre é auxiliar na compreensão e ajudar em avaliações futuras.

PROBABILIDADE		
POSSIBILIDADE	**EXPLICAÇÃO**	**PONTUAÇÃO**
BAIXA	Um evento que nunca ocorreu	**0**
	Um evento que é altamente improvável de ocorrer ou ocorre raramente (talvez uma vez a cada 3 anos)	**1**
MÉDIA	Um evento que provavelmente ocorrerá com pouca frequência, talvez uma vez ao ano	**2**
ALTA	Um evento que é provável e que pode ocorrer várias vezes ao ano	**3**

Avaliação do impacto:

É fornecida uma estimativa do impacto que o risco de desastre pode afetar a confidencialidade, integridade ou disponibilidade na organização. Isso considerará os controles existentes que reduzem o impacto, se esses controles forem considerados eficazes. O impacto será levado em consideração no seguinte:

- Clientes
- Financeiro
- Saúde e segurança
- Reputação
- Efeitos secundários, indiretos ou cumulativos dentro da organização
- Obrigações legais, contratuais ou organizacionais

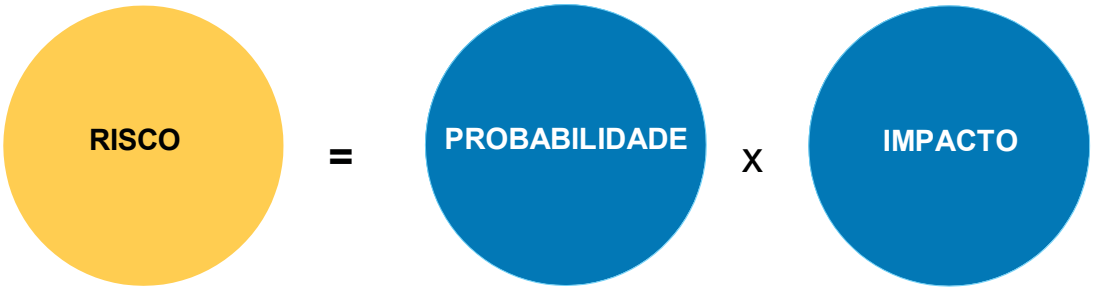
O impacto de cada risco é avaliado em uma escala numérica de 0 (baixa) a 3 (alta).

POSSIBILIDADE	EXPLICAÇÃO	PONTUAÇÃO
BAIXA	Nenhum impacto	0
	Impacto insignificante ou menor com menos esforço de reparo	1
	Os danos à reputação ou a perda de receita são mínimos	
MÉDIA	Danos tangíveis, esforço extra necessário para reparar	2
	Os danos à reputação ou a perda de receita são significativos	
ALTA	A despesa significativa de recursos requer e compromete o sistema	3
	Os danos à reputação e a perda de receita são altos	

Classificações dos riscos:

Com base na avaliação da nota de probabilidade e impacto, uma pontuação é calculada para cada risco multiplicando-se os dois números (probabilidade X nível do impacto). Essa pontuação resultante é usada para decidir a classificação do risco com base na matriz

Fórmula de risco:



Cada risco receberá uma classificação com base em sua pontuação, como segue:

VALOR DO RISCO	NÍVEL DO RISCO	CÓDIGO DE CORES
0-3	BAIXA	
4-6	MÉDIA	
7-9	ALTA	

Observação: Com base em nosso apetite de risco, alteramos a definição de classificações alta, média e baixa. Por exemplo: Podemos decidir que apenas riscos com uma pontuação de 16 ou mais

Avaliação de riscos

Critérios de aceitação de riscos:

O tratamento de risco não será feito para os riscos classificados no nível do risco "Baixo". Se o valor for classificado como 3, nenhuma ação será tomada. Se o valor for classificado como >= 4, as ações serão iniciadas. O tratamento de risco ainda pode ser feito para a categoria de risco "Baixo", caso o BCDRC decida fazê-lo.

Avaliamos os riscos para decidir sobre os que podem ser aceitos e os que precisam ser tratados. Isso deve considerar os critérios de aceitação de riscos. A matriz acima mostra as classificações de riscos, em que o verde indica que o risco está abaixo do limite aceitável e pode ser considerado "seguro". As áreas laranja e vermelha geralmente indicam que um risco não atende aos critérios de aceitação e precisa ser tratado. Os riscos serão priorizados para o tratamento de acordo com sua pontuação e classificação, portanto, recomenda-se que os riscos de pontuação alta sejam tratados antes daqueles com níveis mais baixos de exposição para a organização.

Relatório de avaliação de riscos:

Os resultados derivados da avaliação de riscos são capturados no relatório de avaliação de riscos com as seguintes informações:

- Ativos (somente avaliação de risco baseada em ativos)
- Ameaças
- Vulnerabilidades
- Descrições do cenário de risco (somente avaliação de risco baseada no cenário)
- Controles atualmente implementados
- Probabilidade (incluindo lógica)
- Impacto (incluindo lógica)
- Pontuação de risco
- Classificações dos riscos
- Proprietário do risco
- Se o risco é recomendado para aceitação ou tratamento
- Prioridade dos riscos para o tratamento

Observação: O relatório de avaliação de riscos contém as informações para a fase de tratamento de risco do processo e é aprovado pelo BCDRC antes de prosseguir, particularmente os riscos recomendados para aceitação.

Tratamento de riscos

O tratamento de riscos é um processo para desenvolver uma gama de opções para atenuar os riscos que são acordados como inaceitáveis. Aplicamos as seguintes medidas para tratar os riscos:

1. Modificar o risco aplicando controles apropriados para diminuir a probabilidade e/ou o impacto do risco.
2. Evitar o risco executando ações que não se aplicam mais.
3. Compartilhar o risco com outra parte. Por exemplo: seguradora ou fornecedor.

Usamos nosso julgamento para decidir qual curso de ação seguir com base em um conhecimento sólido das circunstâncias que envolvem o risco. Exemplo: Estratégia de negócios, considerações regulatórias e legislativas, questões técnicas, questões comerciais e contratuais.

Observação: O revisor de riscos garante que todas as partes interessadas ou que estejam envolvidas no tratamento do risco sejam consultadas, incluindo o proprietário do risco.

Plano de tratamento de riscos:

Ao avaliar as opções de tratamento, o plano de tratamento de riscos é criado com os seguintes detalhes:

- Riscos que exigem tratamento
- Proprietário do risco
- Opção de tratamento recomendada
- Controle(s) a ser(em) implementado(s)
- Responsabilidade pelas ações identificadas
- Prazos para ações
- Níveis de risco residual após a implementação dos controles.

Declaração de aplicabilidade (SOA):

A SOA define os controles padrão que foram selecionados e os motivos para sua seleção. Também detalha aqueles que foram implementados e identifica todos os que foram explicitamente excluídos, juntamente com os motivos da exclusão.

Aprovação do BCDRC

Em cada estágio do processo de avaliação de riscos, o BCDRC é mantido informado sobre o progresso, incluindo a aprovação formal dos riscos residuais propostos. O BCDRC aprova os seguintes documentos:

1. Relatório de avaliação de riscos
2. Plano de tratamento de riscos
3. Declaração de aplicabilidade (SOA)

A aceitação ou o tratamento de cada risco será aprovada(o) pelo proprietário do risco relevante.

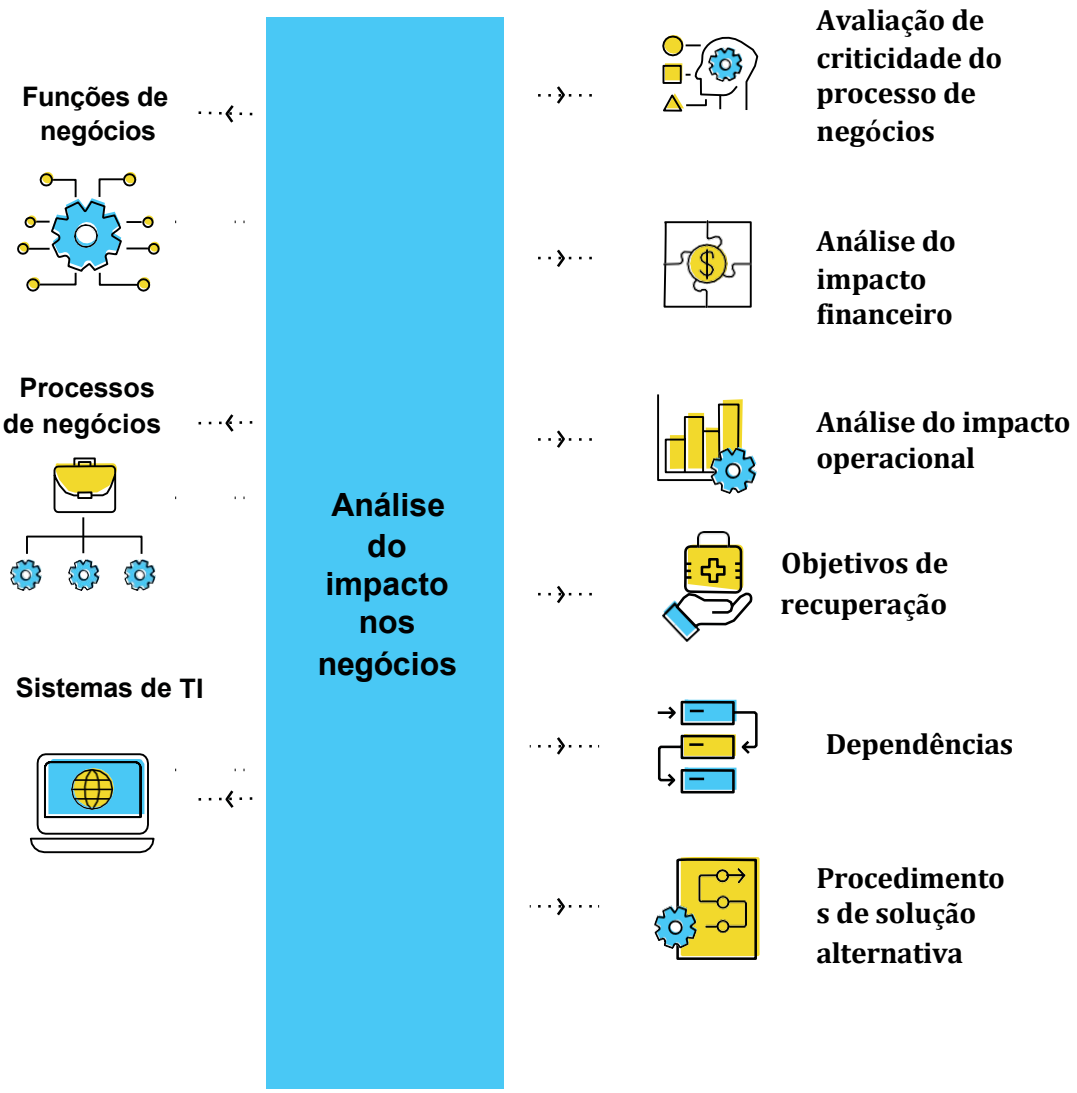
Monitoramento e geração de relatórios de riscos

Como parte da implementação de novos controles e da manutenção dos existentes, os indicadores-chave de desempenho (KPIs) são identificados, o que permite medir o sucesso dos controles de risco relevantes. Esses indicadores são relatados regularmente e as informações sobre tendências são produzidas para que situações excepcionais sejam identificadas e tratadas como parte do processo de revisão do BCDRC.

Revisões regulares

Além de uma revisão anual completa do ARMC, as avaliações de risco são avaliadas regularmente para garantir que permaneçam atualizadas, e os controles aplicados sejam válidos e relevantes. As avaliações de risco relevantes também são analisadas em relação a grandes mudanças nos negócios, como mudanças de escritórios, fusões e aquisições, ou introdução de serviços de TI novos ou alterados.

Análise do impacto nos negócios



Embora algumas funções de negócios possam ser relativamente pouco importantes, algumas são fundamentais para os negócios em andamento. O processo de BIA facilita a identificação das funções de negócios mais críticas, suas interdependências e se elas devem ser consideradas para inclusão na estratégia de continuidade dos negócios. Também nos ajuda a identificar como essas funções principais podem ser afetadas por desastres e estabelece a base para planos de recuperação mais sistemáticos e lógicos.

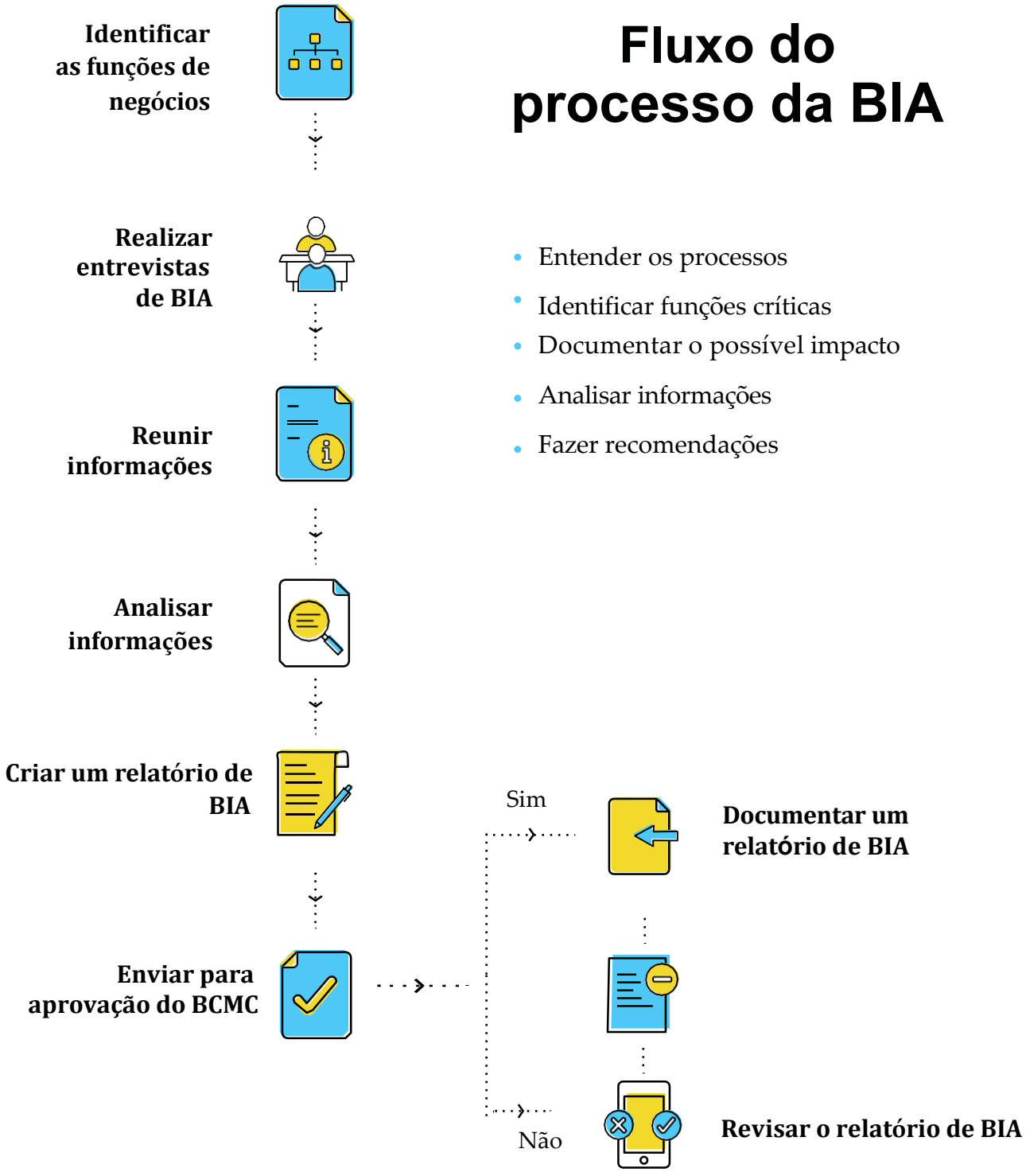
A realização dessa análise nos torna mais confiantes e seguros em relação às nossas decisões de negócios, sabendo que nossas decisões são baseadas em uma sólida compreensão dos componentes mais essenciais de nossa empresa.

Os principais objetivos da BIA são os seguintes:

- Priorizar unidades ou departamentos críticos para os negócios, produtos e serviços que devem ser protegidos.
- Criar um inventário das atividades de negócios essenciais e dos recursos mínimos necessários para conduzir os negócios em um estado normal ou quase normal.
- Estabelecer períodos de tempo de recuperação ou objetivos de tempo de recuperação para ajudar a priorizar planos de tratamento de riscos e selecionar as estratégias apropriadas de resposta e recuperação.

Conforme mostrado no diagrama de atividade do processo abaixo, BIA é um processo multifásico realizado pelo BCC.

Fluxo do processo da BIA



- Entender os processos
- Identificar funções críticas
- Documentar o possível impacto
- Analisar informações
- Fazer recomendações

Entrevistas de BIA

O BCC faz o estoque de todas as unidades de negócio e reúne algumas informações básicas antes da entrevista real usando um formulário da Zoho Creator. Um link com o questionário é enviado como um e-mail em nome de um líder de departamento, juntamente com uma nota sobre o que o BCC está tentando realizar por meio deste exercício e por que ele é importante. Uma quantidade razoável de tempo (cerca de 2 semanas) é dada às equipes atribuídas para concluir a tarefa. Este trabalho prévio prepara o palco para entrevistas de BIA mais focadas e eficazes e reduz o tempo.

O BCC inicialmente faz as perguntas abaixo:

- Nome da unidade de negócio?
- O que a unidade de negócio faz?
- Quantos recursos a unidade de negócio tem?
- Onde está localizada a unidade de negócio?
- Quantas horas são de operação? Isso envolve turnos?

Coletar informações:

O BCC realiza uma reunião inicial para entregar o questionário aos líderes de departamento e articular claramente o objetivo de todo o exercício. O questionário abrange todos os pontos de dados necessários, pois o resultado final da BIA depende desta etapa. Veja abaixo um exemplo de questionário do BCC:

Amostra de questionário do BCC

Pontos de dados	Perguntas	Perguntas relacionadas á TI
Unidade e processos de negócios	Descreva sua unidade de negócio e seus processos?	Quais sistemas e aplicações de TI esta unidade de negócio usa?
Dependências	Quais são suas dependências com outras unidades de negócio? Uma interrupção desta unidade de negócio teria impacto sobre as outras? Como e quando essa interrupção em outras unidades ocorreria?	Quais são os sistemas de TI que afetam ou são afetados por esta unidade de negócio?
Dependências de recursos	Esta unidade de negócio depende de alguma função importante? Em caso afirmativo, qual é a função e até que ponto esta unidade de negócio depende dela? Qual é o número mínimo de recursos necessários para que esta unidade de negócio funcione?	Quais são os sistemas secundários, se houver, necessários para essas funções de trabalho?
Dependências de experiência	Essa unidade de negócio depende do conhecimento e da experiência de um trabalhador qualificado? Em caso afirmativo, descreva a função e a experiência do trabalhador qualificado e o impacto nos negócios na ausência dele.	
Operacional	Se essa unidade de negócio não funcionasse, como isso impactaria os negócios?	Se esta unidade de negócio não funcionasse, como isso afetaria as operações de TI?

Amostra de questionário do BCC

Pontos de dados	Perguntas	Perguntas relacionadas à TI
Tolerância a blecautes	Em face de um desastre, como a perda do centro de produção (Zoho Estancia), quanto tempo a unidade/os sistemas de negócios podem ser sustentados antes que a perda afete a organização, suas partes interessadas e seus fornecedores?	
Requisitos mínimos de infraestrutura	Quais são os requisitos de infraestrutura para a sua unidade de negócio: espaço físico, material de escritório, rede, comunicação, mobiliário, iluminação, climatização, água e suprimentos de alimentos?	
Outros	Quais são as outras preocupações, se houver, que podem afetar a recuperação da sua unidade de negócio?	
Processos e recursos de negócios alternativos	Quais são as soluções alternativas atualmente em vigor para seus processos de negócios? Quais indivíduos são os recursos alternativos ou de backup designados?	
Documentação crítica	Onde você armazena seus documentos críticos? Mencione o tipo de documentos, local e os locais alternativos (se houver)	

Amostra de questionário do BCC

Pontos de dados	Perguntas	Perguntas relacionadas à TI
Períodos de recuperação	Quais são os possíveis problemas de recuperação para sua unidade de negócio? Qual é o período mínimo de recuperação? Quais indivíduos são os recursos essenciais são necessários para restaurar as operações para um estado quase normal?	
Impacto financeiro	Se essa unidade de negócio não funcionasse, qual seria o impacto financeiro nos negócios? Quando o impacto seria percebido? Será um impacto único ou recorrente?	
Período de recuperação	Qual é o período mínimo necessário (em horas, dias, semanas, meses) para recuperação desta unidade de negócio?	Quanto tempo vai demorar para recuperar ou substituir os sistemas/ aplicações de TI relacionados a esta unidade de negócio?
Contrato de nível de serviço (SLAs)	Existe algum SLA em vigor para esta unidade de negócio? Na eventualidade de qualquer desastre, qual seria o impacto nos SLAs? Quais são as principais métricas associadas aos SLAs?	Como a TI é afetada durante a interrupção desta unidade de negócio?
Aplicações de TI	Quais aplicações de software são necessárias para esta unidade de negócio?	Quais ativos de TI são necessários para executar essas aplicações e dar suporte a esta unidade de negócio?
Desktops, notebooks, estações de trabalho	Quantos desktops, notebooks e estações de trabalho são necessários para esta unidade de negócio?	Quais são os dados de configuração desses sistemas?
Servidores e redes	Esta unidade de negócio requer sistemas de back-end e rede?	

Amostra de questionário do BCC

Pontos de dados	Perguntas	Perguntas relacionadas à TI
Soluções alternativas	Esta unidade de negócio tem algum processo de solução alternativa que foi desenvolvido e testado? Em caso afirmativo, esses processos facilitariam a operação tranquila desta unidade de negócio durante um evento? Em caso negativo, é viável desenvolver essas soluções alternativas?	Existem soluções alternativas relacionadas à TI para esta unidade de negócio? Em caso afirmativo, quais são essas soluções alternativas e como elas podem ser implementadas?
Remoto	Esta unidade de negócio poderá funcionar a partir dos locais de recuperação de backup da Zoho? Ou os membros da unidade de negócio podem trabalhar remotamente de casa?	O que a TI deve fazer para habilitar o acesso remoto a esta unidade de negócio?
Registros vitais	Onde esta unidade de negócio armazena documentos críticos? É feito backup desses documentos? Em caso afirmativo, onde e com que frequência a unidade de negócio faz backup dos documentos?	Onde os backups de documentos são armazenados? A estratégia atual de backup de documentos é adequada o suficiente?
Experiência anterior de interrupção nos negócios	Esta unidade de negócio enfrentou alguma interrupção anteriormente? Em caso afirmativo, qual foi o cenário e a duração da interrupção? Há algum aprendizado que possa ser incorporado à BCDR para se preparar para futuras interrupções?	A TI está envolvida nesse cenário de interrupção? Em caso afirmativo, como o departamento de TI solucionou essa interrupção?
Impacto competitivo	Qual seria o impacto competitivo para a Zoho se esta unidade de negócio enfrentasse uma interrupção significativa? Qual porcentagem de clientes perderíamos?	

O BCC realiza entrevistas de acompanhamento para validar as informações coletadas e preencher quaisquer lacunas.

Analisar as informações:

O questionário é criado para coletar informações sobre os impactos financeiros e não financeiros, prazos de recuperação, recursos e requisitos de aplicações. O BCC compila e analisa as respostas para fornecer as informações necessárias para desenvolver estratégias de recuperação e continuidade em toda a empresa.

A tabela abaixo captura algumas das categorias de impacto mais importantes que consideramos. Esta tabela pode ser usada como um checklist por outras organizações de TI ao conduzir uma BIA.

Categorias de impacto	Natural
Impacto financeiro	• Perda de receita devido à perda de vendas • Penalidades devido à não conformidade dos SLAs • Aumento das despesas operacionais, de alívio e de recuperação
Exposição	• Danos à produção/data centers • Acesso restrito a locais de trabalho • Danos aos sistemas de TI • Danos a outros ativos físicos • Perda de dados • Perda de rede, energia, sistemas de telecomunicação • Interrupção da cadeia de suprimentos
Recurso	• Faltas • Baixo moral do funcionário
Saúde e segurança	• Saúde comprometida dos funcionários (pandemias) e segurança dos trabalhadores (incêndio) • Danos ambientais

Categorias de impacto	Natural
Jurídico	• Incapacidade de cumprir os SLAs • Incapacidade de cumprir as normas
Estratégico	• Atraso em novas iniciativas de negócios • Falta de inovação devido ao menor engajamento dos funcionários resultante da interrupção.
Intangível	• Clientes insatisfeitos • Defeito do cliente • Danos à reputação comercial da Zoho • Perda de cortesia com os parceiros • Perda de moral dos funcionários

As informações coletadas nas entrevistas de BIA são usadas para:

- Identificar as unidades de negócio e os processos críticos
- Definir o objetivo de tempo de recuperação (RTO) para cada processo de negócio.
- Definir o objetivo de ponto de recuperação (RPO) para cada processo de negócio
- Fazer a previsão dos requisitos de recursos

Identificação de funções críticas:

No panorama geral, qual é a importância de cada unidade de negócio e seus processos para a capacidade de operação da Zoho? Um sistema de classificação de três pontos ajuda o BCC a atribuir uma "classificação de criticidade" a uma unidade de negócio e suas funções.

CATEGORIAS	CRITICIDADE	CÓDIGO DE CORES
1	**Crítico** (UNs e processos de missão crítica)	
2	**Importante** (UNs e processos necessários)	
3	**Menor** (UNs e processos desejáveis)	

Categoria 1:

As unidades e os processos de negócios críticos são aqueles que são:

- mais sensíveis ao tempo de inatividade,
- mantêm o fluxo de caixa,
- cumprem os SLAs e
- desempenham um papel fundamental na manutenção da reputação de negócios da Zoho.

O BCDR concentra mais tempo e recursos nas unidades de negócio e funções críticas primeiro, seguido pelas unidades de negócio e funções importantes.

Categoria 2:

As operações de negócios da Zoho a curto prazo normalmente não são afetadas por unidades de negócio e processos não funcionais. No entanto, se a situação continuar a longo prazo, as unidades de negócio e os processos não operacionais podem interromper as operações.

Categoria 3:

As unidades de negócio e os processos menores ou desejáveis não causam interrupção significativa nos negócios. Seus impactos geralmente são abordados nas etapas posteriores da recuperação dos negócios.

Objetivo de tempo de recuperação (RTO)

Depois que os dados de impacto são analisados, o BCC define o RTO, que é o momento em que um processo de negócios deve ser restaurado após uma interrupção. Isso depende da criticidade de uma unidade de negócio, processo e aplicação e varia em qualquer lugar entre nenhum tempo de inatividade e vários dias ou semanas. Resumindo: "Quanto tempo podemos ficar inativos?"

Esse período pode variar de acordo com a organização. Para algumas organizações de TI, o tempo de recuperação dos processos pode ser de até 0 minutos.

CATEGORIAS	CRITICIDADE	CÓDIGO DE CORES
1	**Crítico** (UNs e processos de missão crítica)	**12 horas ou menos**
2	**Importante** (UNs e processos necessários)	**48 horas ou menos**
3	**Menor** (UNs e processos desejáveis)	**< 3 dias**

Objetivo de ponto de recuperação (RPO):

O RPO define a perda máxima de dados aceitável que pode ser tolerada por um processo de negócios crítico. Em resumo, se os sistemas de TI que dão suporte a um processo de negócios crítico falharem, quantos dados podem ser recuperados? Usamos três períodos aqui e isso também pode variar de acordo com a organização.

RPO 0 – sem perda de dados (backups em tempo real)
RPO 1 – menos de 4 horas de perda de dados
RPO 2 – perda de dados de 24 horas

Identificando requisitos e dependências de recursos:

O BCC documenta cada departamento e processo juntamente com o(s) recurso(s) responsável(is) pelos processos de uma unidade de negócio. Uma lista de recursos de backup para o processo também é identificada caso os recursos principais estejam indisponíveis durante uma emergência.

Ele também identifica os sistemas, aplicações (seja um CRM, folha de pagamento ou software de RH) e o nível de acesso necessário para realizar seus trabalhos. O nível de confiança de uma unidade de negócio nesses sistemas e aplicações é classificado como alto, médio ou baixo para garantir a disponibilidade de sistemas e aplicações cruciais durante uma emergência.

Uma compreensão completa das interdependências entre as unidades de negócio, suas funções e os sistemas de TI é crucial para a recuperação de desastres e para a continuidade dos negócios. Se o Sistema A estiver inativo durante um evento, é inútil que nossas equipes de TI passem uma semana tentando restaurar o Sistema B enquanto o Sistema A não estiver funcional. O BCC documenta e destaca essas interdependências nesta fase para garantir a eficácia da continuidade dos negócios.

Relatório de BIA

Os resultados da BIA são documentados com recomendações de estratégias de recuperação e apresentados ao BCDRC para aprovação. O relatório de BIA também é devidamente incorporado aos nossos planos de gerenciamento de incidentes e recuperação de desastres de TI. Aqui está um exemplo de relatório de BIA de uma de nossas unidades de negócio e operações de rede.

Informações da unidade de negócio:

Nome da unidade de negócio: Centro de operações de rede (NOC)
Líder da unidade de negócio: Pabhu Ponnukumaraswamy
ID do e-mail: xxxx@zohocorp.com
Celular: +919999999999

Número de funcionários

50

Prioridade

Crítico

Prioridade

- Crítico

Funções da unidade de negócio

- Monitoramento de rede.
- Resposta a incidentes.
- Fornecer conectividade de rede, WAN, VPN e LAN 24 horas por dia, 7 dias por semana, com 99,999% de tempo de atividade.
- Fornecer suporte a aplicações de hardware e software aos funcionários.
- Gerenciar a infraestrutura de TI da Zoho.

Impacto da interrupção da unidade de negócio

A interrupção do NOC afetará diretamente todas as unidades de negócio e a produtividade da Zoho. A interrupção dessa unidade de negócio significa que a Zoho não será capaz de conduzir os negócios e o tempo de inatividade será diretamente proporcional à perda de dólares.

RTO	RPO
15 minutos.	Zero

Dependências internas

Recursos Humanos, Financeiro, Instalações e Segurança.

Dependências externas

- Dependência de fornecedores e técnicos de servidores físicos externos
- ISP para conectividade de rede

Recomendações

- O local de backup deve estar a uma distância segura do centro de produção. (Tenkasi)
- É seguro contratar dois fornecedores de ISP externos para conectividade de rede

Aprovações do BCDRC

O relatório de BIA é enviado ao BCDRC para sua perspectiva e aprovação, pois os resultados da BIA são usados para formular estratégias de recuperação e planejamento de continuidade. A BIA passa por um processo de aprovação de várias etapas. O primeiro nível de aprovação é conduzido pelo proprietário da BIA, e o último passo adiante é dado pelo BCDRC.

Planejamento de BCDR

A maior parte do nosso trabalho no desenvolvimento do nosso plano de BCDR está concluída neste momento. Esta seção é onde tudo se reúne: a avaliação de riscos nos forneceu os dados para nos ajudar a identificar o impacto desses riscos nos negócios. Todos esses dados agora nos ajudam a identificar as estratégias de resposta, mitigação e recuperação de desastres, bem como as pessoas, os recursos e as atividades de que precisamos para um plano de BCDR eficaz.

O plano de BCDR inclui duas fases:

- Procedimentos de resposta a emergências que todos os locais de trabalho da Zoho seguirão conforme apropriado para desastres como incêndios, inundações e terremotos para proteger a vida dos funcionários e limitar danos.
- Atividades de recuperação de desastres e continuidade dos negócios conduzidas após a interrupção para a restauração das operações de negócios.

Funções e responsabilidades

Uma das etapas cruciais na resposta e recuperação de emergência é atribuir funções e responsabilidades. Quando os desastres atingem, as equipes de resposta em cena são nossa primeira linha de proteção.

Essas equipes ajudam a conter o impacto do desastre e a realizar uma recuperação oportuna antes que os socorristas, como policiais ou bombeiros, cheguem ao local do desastre.

Abaixo estão as equipes de resposta e as responsabilidades.

BCDR	
Funções	Responsabilidades
Equipe de emergência	• Envolver a equipe de emergência treinada para atuar como segurança durante o desastre e ajudar a EMT na evacuação imediata. • Notificar a equipe de segurança • Informar os serviços de emergência externos na chegada sobre o tipo e o local da emergência, resumir os danos, por exemplo, mínimo, pesado, destruição total, e o status da evacuação • Notificar a equipe de segurança do edifício quem estabelecerá a segurança na instalação e não permitirá acesso ao local, a menos que notificado pelo BCDRC
Equipe de segurança	• Em caso de emergência, as operações de proteção e segurança são um dos primeiros pontos de contato do BCDRC • Entrar em contato com a agência nacional de serviço de emergência apropriada • Ativar o alarme de evacuação seguido de um anúncio verbal para todos os funcionários para evacuar o edifício • Fora do horário comercial, a equipe de segurança permanece em contato para notificar o BCDRC e gerenciar uma emergência • Fornecer resposta de emergência a todas as emergências no local • Fornecer recursos de segurança e trabalhar com todas as equipes de recuperação, conforme necessário • Entrar em contato com serviços externos de emergência
Líder de instalações	• Responsável pelas medidas de segurança de vida dos funcionários, incluindo alarmes de incêndio, extintores, iluminação de emergência, sistemas de detecção de incêndio, saídas de emergência e outros sistemas de advertência • Fornecer plantas de emergência no andar mediante solicitação • Certificar-se de que todos os funcionários evacuem as instalações e se encontrem no local externo designado (ponto de encontro) e sigam as instruções fornecidas pela equipe de emergência • Atuar como uma ligação entre a Zoho e fornecedores de serviços essenciais, como os de climatização, eletricidade e encanamento

BCDR	
Funções	Responsabilidades
Médicos internos	• Os médicos internos são mobilizados durante emergências
Serviço de ambulância	• Fornecer transporte para os funcionários feridos
Funcionários	• Familiarizar-se com os procedimentos padrão de emergência • Responder a emergências • Seguir as instruções das equipes de emergência e segurança • Manter todas as saídas de emergência desobstruídas e evitar pânico durante emergências
Equipe de recuperação de desastres	• Coordenar com EMT e BCDRC para ações de recuperação apropriadas • Notificar todos os líderes de departamento da empresa e aconselhá-los a ativar seus planos, se aplicável, com base na situação de desastre • Determinar as necessidades de recuperação • Estabelecer áreas de centro de comando e de reunião • Avaliar os danos no local e/ou ativos afetados • Fornecer recursos de segurança e trabalhar com todas as equipes de recuperação, conforme necessário • Entrar em contato com fornecedores/prestadores de serviços de equipamentos instalados para obter suas opiniões de especialistas sobre a condição dos equipamentos • Documentar os resultados da avaliação usando o formulário de avaliação • Inspecionar as áreas afetadas para avaliar danos a cópias físicas essenciais de registros (arquivos, manuais, contratos, documentação etc.) e dados eletrônicos

BCDR	
Funções	**Responsabilidades**
Equipe de recuperação de desastres	• Reunir informações sobre danos a outros locais de trabalho, por exemplo, condições ambientais, integridade da estrutura física, mobiliário e acessórios da equipe de resposta a desastres (DRT) • Desenvolver uma lista de prioridades de restauração, identificando instalações, registros vitais e equipamentos necessários para a retomada de atividades que poderiam ser operacionalmente restauradas e recuperadas rapidamente • Preparar o relatório de debriefing pós-desastre
Equipe de gerenciamento de emergências	• Avaliar quais ações de recuperação devem ser invocadas e ativar as equipes de recuperação correspondentes • Avaliar e analisar os achados da avaliação de danos • Definir a prioridade de restauração com base nos relatórios de avaliação de danos • Fornecer informações de status contínuas à alta gerência • Agir como um canal de comunicação para as equipes corporativas e os principais clientes • Trabalhar com fornecedores e com a DRT para desenvolver um cronograma de reconstrução/reparo
Tecnologia da informação	• Facilitar as atividades de recuperação e restauração de tecnologia, fornecendo orientação sobre equipamentos de substituição e sistemas de TI • Coordenar a remoção de equipamentos recuperáveis nos locais de desastres que podem ser usados para operações alternativas do local

Procedimentos de notificação

- Durante o horário comercial padrão: Na observação ou notificação de uma situação potencialmente grave, o funcionário que identifica o incidente (denominado "repórter") chama o líder da unidade de negócio. Se o líder da unidade de negócio estiver inacessível ou incapacitado, o repórter ligará para o backup, um gerente sênior.

- O líder/backup da unidade de negócio notifica a equipe de emergência no local, que realiza os procedimentos padrão de emergência e evacuação, se necessário, bem como EMT e a DRT.

- Fora do horário comercial: A equipe do sistema de gerenciamento de edificações (BMS) notifica EMT e DRT.

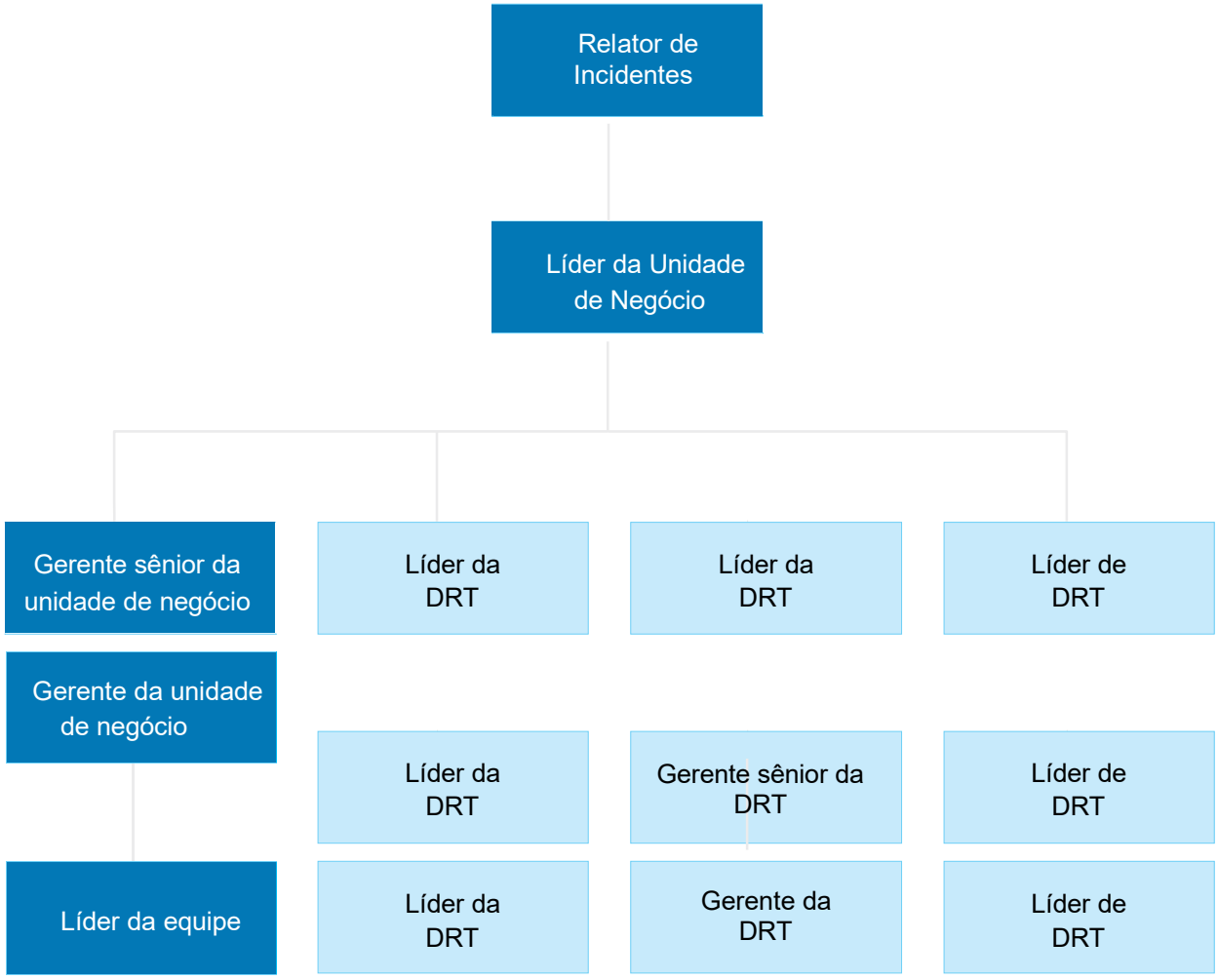
- EMT, DRT e outras equipes de resposta atuam, com base nas diretrizes especificadas pelo BCDRC.

- Quando um desastre é declarado, EMT notifica a TI imediatamente para mobilização. A DRT entrará em ação conforme necessário e fará o acompanhamento.

- A pessoa autorizada a declarar um desastre no BCDRC tem um backup que também está autorizada a declarar um desastre quando necessário. Por exemplo: CEO = autoridade primária, COO = autoridade secundária.

Uma árvore de chamadas é uma técnica de notificação geral que usamos para listar os números de contato principais e alternativos da equipe principal, bem como os números da equipe de backup se a equipe principal não puder ser alcançada. A lista de contatos inclui o nome, o departamento, a função, o número do celular, o número residencial, e o endereço da equipe principal e de backup.

O que está em jogo para a Zoho



Declaração de desastre:

Um desastre é declarado somente quando a emergência provavelmente não será contida e resolvida dentro de prazos predefinidos. O BCDRC é responsável por declarar um desastre e deve estar bem informado sobre os eventos geográficos, políticos, sociais e ambientais que podem representar uma ameaça às operações de negócios da Zoho. Para evitar alarmes falsos, o BCDRC identificou instituições que fornecem previsões de desastres oportunas e significativas que permitem que a Zoho responda e recupere de forma eficaz. Abaixo estão algumas instituições identificadas que o ajudam com monitoramento de desastres para locais de trabalho regionais.

Tipo de desastre	Sistemas de aviso/previsão antecipado(a) (Para locais de trabalho regionais)
Ciclones e terremotos	Departamento meteorológico indiano e sensores de terremoto
Tsunami	Centro nacional indiano para serviços de informação oceânica
Inundações	Abastecimento de água central

Invocando o plano

Como todas as organizações de TI, esperamos nunca ter de invocar o BCDR. No entanto, as emergências podem surgir a qualquer momento e acreditamos na prontidão. O BCDR é reservado para desastres significativos e interrupção nos negócios e é invocado pelo BCDRC.

Independentemente das circunstâncias de interrupção do serviço ou da identidade do(s) indivíduo(s) no BCDRC que foram notificados pela primeira vez sobre o desastre, EMT e DRT são ativadas imediatamente nos seguintes casos:

- O centro de produção de Estancia está inativo devido a um desastre natural como inundação, terremoto etc.
- Qualquer interrupção nos sistemas de TI ou nas instalações de rede que possa causar tempo de inatividade simultâneo no centro de produção por mais de três horas.

Comunicação interna:

Uma comunicação interna eficaz é fundamental para garantir que os funcionários fiquem bem informados, apoiados, tranquilizados e, o mais importante, seguros durante um desastre. O ideal é que uma comunicação presencial seja eficaz para transmitir mensagens aos interessados durante um desastre. Na Zoho, uma publicação do fórum do CEO e do RH com mensagens importantes sobre o desastre e o BCDR no Zoho Connect é um canal de comunicação eficaz. Ele é um software de colaboração, como uma aplicação interna semelhante ao Facebook, que conecta todas as partes interessadas e permite comunicações bidirecionais durante um desastre. As opções de comunicação alternativas incluem WhatsApp e SMS.

Além dos fóruns no Zoho Connect das equipes de BCDRC e RH, os líderes da unidade de negócio são os pontos focais para seus departamentos para fornecer atualizações sobre o progresso de seus esforços de recuperação de desastres e continuidade dos negócios e como eles podem contribuir para os esforços de recuperação.

Resposta inicial

Pode parecer óbvio, mas o BCDR prioriza nossos funcionários e suas vidas em relação aos ativos.

Os procedimentos de resposta a emergências realizados nos minutos iniciais de uma emergência são essenciais para salvar a vida de nossos funcionários. Nossos procedimentos de emergência capturam quatro ações de proteção: evacuação, abrigo, abrigo no local e lockdown. Essas ações de emergência se aplicam a todos os funcionários (incluindo a equipe de gerenciamento) e a todos os locais de trabalho da Zoho Corporation.

Autoridade:

As instruções e orientações fornecidas pela equipe de emergência treinada da Zoho regem a estrutura de subordinação. Essa autoridade é concedida à equipe de emergência para garantir que a vida e a segurança dos funcionários tenham precedência sobre os sistemas de TI, outros ativos e a produção durante uma emergência.

Ponto de encontro

O plano de BCDR identifica dois pontos de encontro dentro e fora das instalações da Zoho, onde os funcionários devem se reunir após a evacuação. Essas áreas de evacuação têm espaço suficiente para acomodar todos os funcionários da Zoho e estão longe de edifícios, redes de energia, árvores, gasodutos, postes e veículos.

O plano de BCDR identifica dois pontos de encontro de evacuação

- Primário – Terreno aberto atrás da Zoho.
- Secundário – Terreno aberto na rua em frente à Zoho.

Ação de proteção e procedimentos de emergência por tipos de desastre

TIPO DE DESASTRE	AÇÃO PROTETIVA	PROCEDIMENTOS
Incêndio/fumaça	Evacuação	1. Se houver incêndio ou fumaça na instalação, avalie a situação e determine a gravidade, categorize o incêndio como "primário" ou "secundário" 2. No caso de incêndios secundários (p. ex., um único componente de hardware ou incêndios em papel), os funcionários tentam apagar o incêndio com os extintores de incêndio portáteis localizados em todas as instalações da Zoho. Qualquer outra situação de incêndio ou fumaça deve ser tratada pelo pessoal qualificado do edifício até que o corpo de bombeiros local chegue 3. Em caso de incêndio grave, o sistema de alarme de incêndio deve ser ativado imediatamente e tocar continuamente por 60 segundos 4. A pessoa que relata o incêndio deve fornecer às equipes de recuperação seu nome, extensão, local de trabalho (bloco, andar, ID da estação de trabalho) e a natureza da emergência. Eles devem seguir todas as instruções fornecidas 5. A pessoa que relata o incêndio deve ligar para EMT e DRT em seus números de celular 6. A equipe de emergência auxilia os funcionários (dando o máximo de atenção aos portadores de deficiência) na saída segura do edifício. Elevadores não podem ser usados 7. Todos os funcionários devem se reunir no local externo ou no ponto de encontro designado e seguir as instruções fornecidas pela equipe de emergência 8. Após a evacuação, uma contagem de funcionários será feita para garantir que todos os indivíduos sejam contabilizados 9. O ponto de encontro deve ser monitorado e os funcionários devem ser tranquilizados sobre sua segurança 10. Os primeiros socorros adequados serão concedidos pelos médicos internos a todos os indivíduos feridos até que a EMT chegue
Danos por inundação/água	Evacuação	1. Interrompa as operações e o uso de equipamentos elétricos e vá para um terreno mais alto

TIPO DE DESASTRE	AÇÃO PROTETIVA	PROCEDIMENTOS
Danos por inundação/água	Evacuação	2 Se a água estiver pingando de uma unidade de ar-condicionado e não estiver colocando em risco os sistemas de TI e outros ativos, entre em contato com a equipe de reparo da tubulação e climatização imediatamente 3 Se a inundação for grave, ative o sistema de alarme/advertência para os funcionários e notifique imediatamente as equipes de EMT/DRT, a equipe de emergência e implemente os procedimentos de desligamento 4 Enquanto os procedimentos de desligamento estiverem em andamento, evacue a área e siga as instruções do BCDRC 5 Evacue o edifício do local de trabalho, se necessário, e prossiga para o ponto de encontro de emergência. Siga os procedimentos de evacuação 6 A DRT liga para o número de emergência nacional imediatamente e espera ajuda externa
Tornado/ ciclones	Abrigo	7 Ative o sistema de alarme para avisar os funcionários 8 Notifique as equipes de EMT/DRT 9 Siga as instruções da equipe de emergência e vá para o porão, andares inferiores e o lado mais forte do edifício 10 Se não houver porão, vá para um hall/sala no nível mais baixo do edifício 11 Afaste-se de janelas de vidro, prateleiras grandes, decorações de teto e outros objetos potencialmente perigosos 12 Uma falha de energia pode ocorrer. Tenha estoques de água, alimentos não perecíveis, primeiros socorros, baterias, lanternas e outras necessidades com base na duração prevista do tornado ou ciclone 13 Os funcionários devem permanecer dentro do campus até que o ciclone ou tornado passe 14 Os líderes das unidades de negócio devem fazer uma contagem dos funcionários e notificar a equipe de emergência em caso de indivíduos ausentes

TIPO DE DESASTRE	AÇÃO PROTETIVA	PROCEDIMENTOS
Terremotos	Abrigo no local	1 Interrompa as operações e o uso de equipamentos elétricos e vá para um terreno mais alto 2 Se a água estiver pingando de uma unidade de ar-condicionado e não estiver colocando em risco os sistemas de TI e outros ativos, entre em contato com a equipe de reparo da tubulação e climatização imediatamente 3 Se a inundação for grave, ative o sistema de alarme/advertência para os funcionários e notifique imediatamente as equipes de EMT/DRT, a equipe de emergência e implemente os procedimentos de desligamento 4 Enquanto os procedimentos de desligamento estiverem em andamento, evacue a área e siga as instruções do BCDRC 5 Evacue o edifício do local de trabalho, se necessário, e prossiga para o ponto de encontro de emergência. Siga os procedimentos de evacuação 6 A DRT liga para o número de emergência nacional imediatamente e espera ajuda externa
Ataque terrorista	Lockdown	1 Quando há suspeita de um ataque terrorista e se ouvem tiros, a principal rota de evacuação não é segura. Todos os funcionários, incluindo a equipe de emergência, devem encontrar locais seguros para se esconder e permanecer em silêncio 2 Os dispositivos móveis devem ser silenciados desativando as funções de toque e vibração 3 Todos os funcionários devem trabalhar juntos como uma equipe e acompanhar todos os colegas acometidos pelo pânico pela segurança de todos 4 A equipe de segurança deve ligar para a linha direta de emergência regional 5 Depois que a ameaça for eliminada, com base nas informações recebidas das autoridades locais, siga os procedimentos de evacuação da equipe de emergência

Contatos de emergência

Em caso de emergências, solicitamos ajuda, informações e os serviços destas linhas de emergência.

LINHAS DIRETAS DE CRISES DE EMERGÊNCIA (REGIONAL)	
Linha direta de emergência nacional	
Serviços de gerenciamento de desastres	
Ambulância aérea	
Cruz Vermelha	
Linha direta de notificação de vazamento de gás	
Corpo de bombeiros	
Departamento de polícia	
Hospital	
Serviços médicos (móveis)	
Serviços de ambulâncias	
EMPRESAS DE SERVIÇOS PÚBLICOS	
Provedor de rede	
Gás	
Encanamento	
Climatização	
Companhia de eletricidade	

Atividades de BCDR

Veja como é um cenário de emergência na Zoho quando as atividades de recuperação são realizadas. Os exemplos abaixo são algumas das atividades de recuperação em caso de incêndio, inundação e terremotos e, é claro, variam dependendo da natureza da emergência e de seu impacto nos negócios.

Como a Zoho está preparada para eventualidades?

CRONOGRAMA	ATIVIDADES
Primeiras 3-4 horas	**Comunicação externa:** Nossa equipe de comunicações coleta informações de fontes confiáveis e cria mensagens importantes (antes, durante e depois do desastre), além de garantir uma mensagem consistente em todos os canais: site, blog, mídia, divulgação de notícias, mídias sociais etc. A equipe mantém uma lista de públicos-alvo externos em potencial para entrar em contato conforme necessário: serviços médicos de emergência, bombeiros, polícia, governo local, fornecedores e vendedores com seus números de contato. Dois porta-vozes oficiais, o presidente/vice-presidente da Zoho e da ManageEngine, com uma experiência sólida no trabalho com a mídia impressa e de radiodifusão, serão os contatos principais para todas as perguntas da mídia. O porta-voz normalmente realiza todas as conferências de imprensa e dá à maioria das entrevistas para analistas e parceiros durante uma crise. Todas as comunicações externas incluirão detalhes do desastre, incluindo a data e a hora da ocorrência, uma descrição indicando o impacto do desastre nos negócios, as etapas que estão sendo tomadas para atenuar os riscos, a recuperação e a continuidade dos negócios e o tempo estimado para recuperação. Centros de comando de emergência (ECC): Nossos centros de comando de emergência são os centros de coordenação para a resposta a desastres. O pessoal do BCDRC e das equipes de resposta coleta informações críticas, coordena atividades de resposta e recuperação, e gerencia os funcionários conforme as demandas de emergência desses centros. Centro de comando de emergência 1: Estancia IT Park, Chennai, Índia Centro de comando de emergência 2: Tenkasi, Índia Locais alternativos: Em caso de perda temporária ou permanente de uma instalação atingida por desastres, os 12 escritórios espalhados por diferentes países atuam como locais alternativos. Mudamos nossas funções comerciais críticas para locais alternativos que são equipados para fornecer ambientes de trabalho semelhantes.

CRONOGRAMA	ATIVIDADES
Primeiras 3-4 horas	Os locais alternativos podem incluir (mas não se limitar a): • Local(is) alternativo(s) da Zoho listado(s) aqui que não foi(ram) afetado(s) por desastres. Os locais mais próximos do local afetado podem hospedar os recursos essenciais e ajudar na recuperação de operações de negócios. • Locais de trabalho temporários: Locais de trabalho temporários são montados em caso de emergências com sistemas mínimos de TI, telecomunicações e outros equipamentos. • Teletrabalho: Os funcionários trabalham remotamente de casa ou locais alternativos de sua escolha conforme a Zoho é executada em aplicações em nuvem. Equipes e recursos críticos: Na fase de BIA deste plano, identificamos as equipes críticas e os funcionários que são considerados essenciais durante uma emergência ou desastre. Essas unidades de negócio críticas, como as equipes de atendimento ao cliente (pré-vendas, vendas, suporte ao cliente) e seus recursos são movidos para locais alternativos. Recursos mínimos de outras unidades de negócio críticas, como RH e instalações, reportam-se ao trabalho independentemente das condições. Disponibilidade: Os dados das aplicações são armazenados em uma memória resiliente que é replicada nos centros de dados. Os dados no data center primário são replicados quase em tempo real no data center secundário. Em caso de falha do data center primário, o data center secundário assume o controle e as operações continuam sem problemas, com perda mínima ou nenhuma de tempo. Ambos os data center estão equipados com múltiplos ISPs. Temos sistemas de energia de emergência, controle de temperatura e proteção contra incêndio como medidas físicas para garantir a continuidade dos negócios. Essas medidas nos ajudam a obter resiliência. Os dados de status ao vivo e de histórico (30 dias) dos serviços de nuvem podem ser vistos em status.zoho.com / status.zoho.eu / status.zoho.in / status.zoho.com.au. Backups de dados prontos para desastres: O backup e a recuperação de dados são essenciais para a recuperação de dados durante desastres naturais. Na Zoho, realizamos backups completos e adicionais para preservar informações corporativas. Esses backups são realizados regularmente para registros de auditoria e arquivos considerados críticos. A mídia de backup é armazenada em um data center externo seguro, geograficamente separado do original.

CRONOGRAMA	ATIVIDADES
5-24 horas	**Plano de sucessão:** Em caso de vítimas, ative o plano de sucessão que lista quem substitui o BCDRC, gerentes seniores, gerentes, líderes de equipe durante uma emergência se eles não estiverem disponíveis para executar suas responsabilidades. **Estabilize a situação:** A situação de desastre é estabilizada para salvar vidas e geralmente é realizada no estágio de resposta. No entanto, algumas atividades de estabilização, como remover registros do local do desastre e isolar sistemas afetados, são realizadas antes da avaliação de danos para evitar danos adicionais aos registros e informações, bem como a outros ativos. **Avaliação de danos:** Depois que um desastre é declarado, a DRT deve ser mobilizada. A avaliação de danos é realizada tão rapidamente quanto as condições permitem pela DRT (sob a direção das autoridades locais) para avaliar os danos: • Aos registros impressos essenciais (arquivos, manuais, contratos, documentação etc.) e dados eletrônicos. • Ao(s) local(is), por exemplo, condições ambientais, integridade da estrutura física, mobiliário e acessórios. A avaliação de danos nos ajuda a medir a extensão: o que pode ser substituído, recuperado ou reconstruído. Os resultados da avaliação de danos são documentados no formulário de avaliação e análise de danos. (Consulte a seção de formulários abaixo para obter uma lista completa dos que usamos durante emergências). Isso ajuda a desenvolver uma lista de prioridades de restauração, identificar instalações, registros vitais e equipamentos necessários para a retomada das atividades. EMT e DRT reúnem todas as informações sobre o evento e enviam para revisão do BCDRC. A decisão de mudar para a fase de continuidade dos negócios é tomada neste momento. Se a situação não garante essa ação, então EMT e DRT continuam a abordar a situação no(s) local(is) afetado(s). Cadeia de suprimentos: Em tempos de desastre, nossas cadeias de suprimentos que estavam funcionando bem podem sofrer interrupções significativas. Identificamos uma lista dos principais fornecedores de backup para todos os equipamentos e suprimentos essenciais para que possamos mudar para esses fornecedores caso o fornecedor principal também seja afetado pelo desastre.

CRONOGRAMA	ATIVIDADES
Dias 2-4	Operações de recuperação no local do desastre: As operações de recuperação começam agora para sistemas de TI, móveis, estações de trabalho e registros danificados com procedimentos apropriados. As atividades incluem: • Isolar e remover sistemas, móveis e outros equipamentos afetados do local do desastre. • Enviar os sistemas e equipamentos para recuperação aos respectivos fornecedores para reparo. • Organizar o equipamento de sistemas sem danos • Limpar todas as estações de trabalho, incluindo móveis, sistemas de TI sem danos e outros equipamentos. • Remover detritos e certificar-se de que a instalação seja restaurada ao normal. Mover os recursos críticos de volta para o local principal: Assim que o local principal for estabilizado e reparado, os recursos críticos são movidos de volta para o local principal.
Dias 5-14	Fazendo negócios como de costume: No caso de destruição total das instalações, os esforços começam a ser totalmente reconstruídos, enquanto os funcionários críticos continuam trabalhando em locais alternativos e outros funcionários trabalham em casa. No caso de dano parcial, a instalação é reconstruída no menor tempo possível e todos os funcionários são movidos para a instalação principal. Assim que todos os sistemas de TI, registros, dados, suprimentos forem restaurados e as operações normais retornarem para a organização, a comunicação externa será enviada aos clientes, parceiros, imprensa e autoridades envolvidas.

Formulários

Formulário de desastre:

No caso de um desastre, o pessoal em serviço faz as entradas iniciais em um formulário de desastre. Este formulário captura um registro cronológico do impacto nos negócios relatado durante o evento. Ele é então encaminhado para o ECC, onde é continuamente atualizado. O log em execução permanece ativo até que o desastre termine e os negócios voltem ao normal.

Formulário de desastre

Data e hora	Tipo de evento	Localização	Problemas de acesso ao edifício	Impacto projetado nas operações	Log em execução (eventos em andamento)

Formulário de avaliação e análise do status de equipamentos críticos

Data e hora	Tipo de evento	Localização	Equipamento	Condição	Recuperação	Comentários

Formulário de status de equipamentos críticos:

OK – Não danificado
DBU – Danificado, mas utilizável
DS – Danificado, requer recuperação antes do uso
D – Destruído, requer reconstrução

Aprovações do BCDR

Uma vez concluído o plano de BCDR, incluindo os custos estimados para recuperação, ele é submetido para aprovação formal do BCDRC. O BCC obtém o apoio e a adesão da alta gerência para enfatizar o seu compromisso com o processo de BCDR e sua importância.

Implementação e treinamento

Criamos um plano de BCDR e agora ele faz parte de nossos processos e políticas principais. A última etapa é treinar aqueles que usarão o plano, incluindo os que não fazem parte de seu desenvolvimento. O treinamento pode incluir passo a passo, simulações de desastres ou testes de componentes.

As equipes de DRT e EMT escolhem cenários de desastres que podem acontecer de forma realista. Por exemplo, eles podem construir um cenário em torno de um acidente de incêndio para realizar simulações de incêndio. As simulações de incêndio são realizadas a cada seis meses para verificar a reação dos funcionários, a eficiência dos sistemas de alarme e combate a incêndio, a execução dos procedimentos de evacuação pela equipe de emergência, e as atividades de resposta e recuperação a desastres.

Também treinamos nossas equipes de TI e de segurança em atividades de resposta a desastres e recuperação – como exercícios de ataque de phishing –, diagnóstico de primeiro nível —como manutenção de dispositivos —, para que elas fiquem mais rápidas, pois são essenciais para manter nossos sistemas disponíveis e acessíveis em uma emergência.

Mais de 8.000 funcionários, espalhados por todos os 12 escritórios em diversos países, atendendo mais de 50 milhões de usuários em todo o mundo.

Ainda assim, a Zoho fez uma transição repentina para o trabalho remoto em apenas 3 dias!

Como fizemos essa mudança inimaginável?

Estudo de caso da Covid -19

Capítulo 03

Covid-19

Um estudo de caso

Mensagem do CEO e aviso

Sridhar Vembu
Feb 25, 03:28 pm

OPENHOUSE

Preparing for the virus hitting India

PLEASE READ THIS POST - THIS IS IMPORTANT.

So far, life has been normal in India. But in the global backdrop with the Covid-19 virus is extremely worrying. The WHO is preparing for a global pandemic, which many virologists now consider inevitable. India's healthcare systems will likely not be able to cope with the load. So we must help ourselves.

As a company, we must prepare ourselves for the inevitable and I would be very happy if the worst never arrives.

Here are the steps we are taking:

1. **We have to be prepared for the eventuality that we have to shut down our offices entirely and everyone has to stay home and work from home.** We have started some work-from-home trials in some teams. We will broaden them over the course of this week and next.

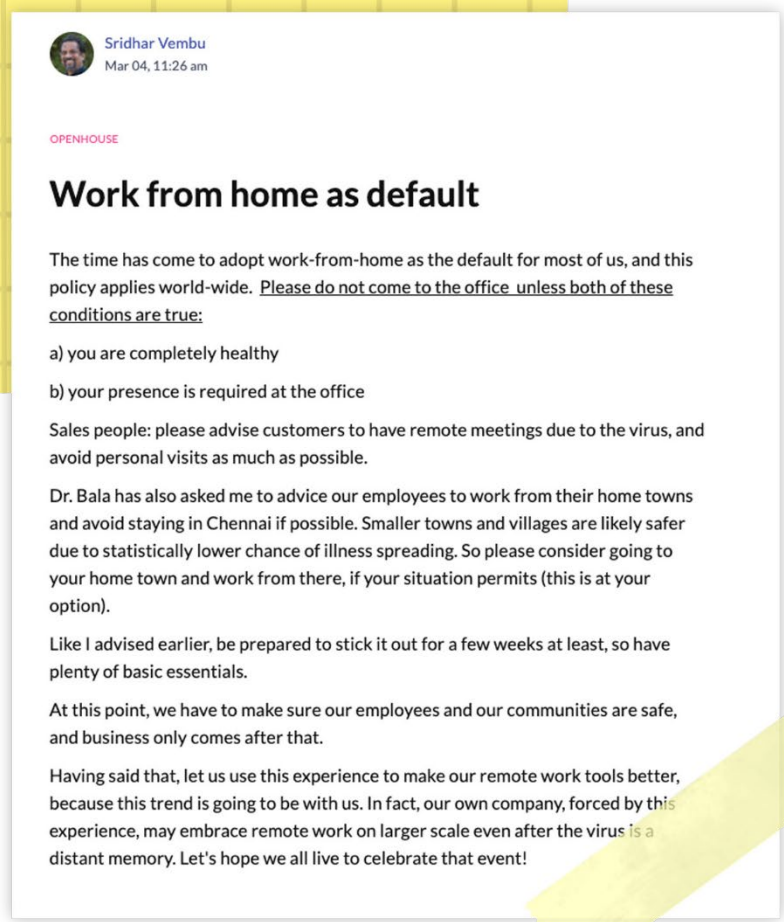
2. We are reviewing all our travels. ***As a first step, if you are not comfortable traveling, feel free to drop out of travel.*** We may adopt a broad "no travel on Zoho business" policy if the situation warrants - we are evaluating this on a daily basis. The trouble is that the virus seems to spread from a non-symptomatic carrier to infect people around them. This is one major reason leading virologists think a global

Em fevereiro de 2020, enfrentamos um surto global de Covid-19 que destacou o risco substancial de grandes interrupções operacionais globais.

25 de fevereiro de 2020 15h28 PM (IST):

No final de fevereiro, recebemos uma mensagem de nosso CEO solicitando que a força de trabalho de mais de 10.000 funcionários se preparasse para o pior e para oferecer o melhor. Ele também deu a entender a esperada crise econômica que continuaria na maior parte de 2020 e observou que o maior desafio seria manter um nível significativo de operação nos próximos seis a nove meses. A mensagem também listou as medidas oportunas que precisam ser tomadas considerando a pandemia e como parte de nosso BCDR escrito.

O grande anúncio, após uma decisão



04 de março de 2020 11h26 AM (IST):

No dia 04 de março, nosso CEO disse que era hora de abraçarmos a cultura do trabalho remoto.

Nossa força de trabalho de mais de 8.000 pessoas, espalhada por 12 escritórios em diversos países, atendendo a mais de 50 milhões de usuários em todo o mundo, fez o salto para a cultura de trabalho remoto parecer impossível, mas também foi uma decisão revolucionária – da qual não nos arrependemos! A Zoho foi uma das primeiras empresas de tecnologia a mudar para o modelo de trabalho em casa diante da Covid-19.

Expulsando a Covid-19

A Zoho é uma empresa centrada nas pessoas. A saúde e a segurança de nossos funcionários vêm em primeiro lugar. Como mencionado anteriormente, agimos cedo. Nos últimos dois anos, nossos funcionários têm viajado muito para reuniões, workshops, seminários e feiras. Também temos nossas equipes de suporte e pré-vendas nos locais dos clientes. Nosso primeiro passo foi chamar todos os nossos funcionários de volta para casa, para o nosso escritório Estancia em Chennai, Índia.

Também colocamos em prática várias medidas, incluindo o aumento de precauções em nossas instalações com base nas recomendações da OMS e do governo local. Estamos constantemente monitorando a situação, seguindo as diretrizes do governo, e nossas equipes de RH e administração estão frequentemente comunicando atualizações a nossos funcionários em todo o mundo.

Diretrizes que seguimos:

- O campus deve estar operacional no modo de acesso restrito, e somente recursos críticos, como administradores de sistemas de TI e outros recursos NOC, serão permitidos dentro do campus. Esses recursos podem acessar o campus com o consentimento por escrito da equipe de RH.
- Áreas comuns, como salas de conferência, academias e áreas recreativas, devem permanecer fechadas.
- Todos os eventos da Zoho e da ManageEngine, e viagens de negócios (nacionais e internacionais) devem ser cancelados (até segunda ordem) e antes que o governo anuncie proibições de voo, se possível.
- Os funcionários que retornarem de viagens de países de alto risco deverão ficar em quarentena por 14 dias corridos (mesmo quando não tiverem mostrado nenhum sintoma) e não devem entrar em contato físico com outros funcionários durante esse período. Depois do período de quarentena, o funcionário será testado pelo médico interno e receberá uma nota dizendo que esse funcionário não apresenta nenhum risco antes de poder voltar ao trabalho no campus.
- Salas de isolamento são montadas e as medições de temperatura ajudam a proteger as pessoas no campus.
- O médico interno irá monitorar a saúde dos funcionários que estão trabalhando. Se esses funcionários tiverem sintomas, como tosse ou febre, eles deverão trabalhar em casa.
- Álcool em gel e máscaras N95 serão mantidos em locais de destaque dentro das instalações da Zoho.
- Todos os funcionários serão submetidos a verificações de temperatura com scanners térmicos, estar de máscara o tempo todo e usar álcool em gel à vontade.

Quando um funcionário testa positivo e apresenta sintomas da doença, fornecemos suporte contínuo e monitoramos a sua condição de saúde. Também aplicamos o uso de formulários de rastreamento de contatos para ajudar a rastrear indivíduos que entraram em contato com o funcionário afetado usando um software low code que fornece uma maneira de criar formulários e aplicações on-line facilmente distribuíveis. O funcionário, incluindo os contatos, deve se colocar em quarentena por um período obrigatório de 14 dias. Eles devem retornar à Zoho somente após uma recuperação completa e com uma nota do médico confirmando sua recuperação. Fechamos imediatamente o local de trabalho para higienizar e descontaminar todas as áreas, incluindo as áreas comuns (lavatórios, refeitório, despensa) que o funcionário pode ter acessado.

Após isso, uma comunicação externa é enviada ao governo local, às autoridades de saúde, às partes interessadas, aos parceiros e à mídia.

A Zoho é executada na Zoho

Nos últimos meses, temos apoiado os clientes, desenvolvendo novos recursos de produtos, realizando correções de produtos, planejando lançamentos futuros, oferecendo service packs e muito mais utilizando nosso trabalho do modelo doméstico. Temos realizado isso o mais próximo possível da maneira como nossa organização operava antes do surgimento da pandemia.

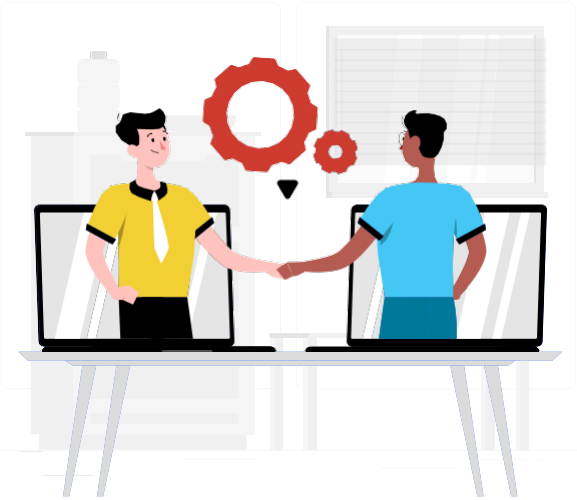
Surpreendentemente, para uma empresa do nosso porte, não usamos software de negócios de terceiros. Sempre realizamos todas as nossas operações na nuvem – vendas, marketing, suporte ao cliente, financeiro, jurídico, TI etc. – usando nosso próprio pacote de mais de 45 aplicações. Aqui está um resumo de algumas das ferramentas mais importantes que nos permitem liderar o ataque à cultura remota.

Comunicação e colaboração:

Nós nos reunimos on-line para colaborar em tempo real usando o Zoho Connect, o Cliq e o Mail, e trabalhamos como se ainda estivéssemos no mesmo edifício. Quase todas as nossas conversas acontecem no Connect para que qualquer pessoa possa ouvir e acompanhar o que está acontecendo em outras equipes e departamentos. As equipes de diferentes fusos horários podem facilmente ganhar contexto e retomar de onde os outros pararam. O RH e a equipe de administração usam essas aplicações para transmitir o trabalho de casa e anúncios da Covid 19, e para manter todos informados.

Quando a comunicação começa a ficar um pouco confusa, podemos rapidamente pular para a videoconferência da mesma maneira que faríamos para ir ao cubículo de um membro da equipe em nosso escritório. Embora nada se aproxime das reuniões presenciais, o Zoho Meeting e o ShowTime ajudam a espelhar essa interação e nos permitem ter conversas significativas e esclarecer quaisquer contratempos.

Seja descrevendo as políticas da Covid-19 ou criando este e-book, o Zoho WorkDrive nos permite realizar nosso trabalho. É uma fantástica plataforma de colaboração de conteúdo que nos permite escrever, editar, comentar e compartilhar simultaneamente a partir de um espaço de trabalho aberto e compartilhado, independentemente dos fusos horários.



Gerenciamento de projetos:

Muitas de nossas equipes de produtos usam o Zoho Projects para atribuir, acompanhar o progresso e permanecer no controle de nossos projetos, especialmente de nossos lançamentos de produtos. Sem o Projects, nossas equipes estariam correndo em círculos e perdendo prazos importantes. Também é uma bênção para nossos gerentes, pois os ajuda a saber que as pessoas não estão relaxando.

E mais! Nossas equipes de vendas e marketing usam o Zoho Campaigns, o CRM e o Zoho Social. Nossas equipes de suporte atendem aos clientes usando o Zoho Desk. Contratamos pessoas com o Zoho Recruit, os gerenciamos com o Zoho People e equilibramos nossos livros usando o Zoho Books.

Zorro salva o dia (mais uma vez!)

Nossa infraestrutura de TI é a espinha dorsal de nossas operações de negócios. Zorro, nossa equipe de administração de rede, trabalha constantemente nos bastidores muito tempo depois de sairmos. Quando não estão corrigindo nossos notebooks ou recuperando arquivos perdidos, eles estão combatendo um grande incidente. As coisas que eles fazem para manter nosso negócio funcionando são quase sobre-humanas. A Zorro geralmente lida com um pequeno número de trabalhadores remotos em uma base ad hoc. Desta vez, mais de 8.000 funcionários de nossa força de trabalho (incluindo o CEO) passaram a trabalhar remotamente do dia para a noite. A Zorro se empenha todos os dias para:

Proteger nossos dados

Usamos vários dispositivos (smartphones, notebooks, tablets e desktops) e vários sistemas operacionais (iOS, Android, Windows e Chrome). Fazer o trabalho remoto significa que nossos dispositivos estão fora da parede. Se nossos dispositivos estão fora e on-line, nossos dados estarão em risco.

Hoje, o gerenciamento de endpoints remoto e a segurança são a prioridade da Zorro. Eles dão suporte a nossos funcionários que têm controle remoto total sobre os dispositivos de propriedade dos funcionários e da empresa para fornecer atualizações seguras, gerenciar patches, implantar software e gerenciar licenças, tudo isso enquanto mantêm o controle de atividades mal-intencionadas nesses endpoints.

Redes privadas virtuais (VPNs) são instaladas para estabelecer uma conexão segura entre a rede de nossos funcionários e a rede interna da Zoho. Uma vez conectados, nossos funcionários podem acessar os recursos em nossa rede da mesma forma que seus dispositivos que estavam fisicamente conectados no escritório usando seu próprio nome de usuário e senha exclusivos e confidenciais.

Todas as aplicações em nuvem da Zoho usam um mecanismo de logon único (SSO) altamente confiável. Enquanto desfrutamos da experiência do SSO, a Zorro gerencia todas as contas de usuário, monitora nossas atividades em tempo real e aprimora a segurança em várias partes da organização. Além disso, a autenticação multifator (MFA) permite um processo de verificação em duas etapas em todas as aplicações. Uma etapa extra ao fazer login em nossas contas nos salva de pesadelos de segurança para sempre.

Monitorar e responder a incidentes

Como mencionado anteriormente, os invasores cibernéticos não estão descansando durante a pandemia. Enquanto estamos distraídos tentando conter o vírus, a Zorro e nossas equipes de NOC estão mais cautelosas do que nunca. O NOC está sempre monitorando nossa rede, sites, servidores e aplicações para tomar as medidas necessárias quando um evento crítico, como uma interrupção de rede, ocorre.

Solucionar problemas

A mudança do cubículo para o sofá nos deu todo o tempo para preparar o almoço, lavar roupa entre as tarefas ou passear com nossos animais de estimação. Até que a realidade se ajuste. Em um dia de trabalho regular, podemos receber uma mensagem de "conta bloqueada", não conseguir fazer uma campanha ao vivo, descobrir que nossa licença do Adobe expirou, enfrentar problemas no navegador ou não conseguir configurar a VPN, que são solicitações regulares de TI. Mas a nova complicação agora é que todos trabalham de casa. Por isso, nossos técnicos da Pitstop de TI agora pedem nossa permissão para assumir o controle de acesso remoto de nossos dispositivos para solucionar problemas e corrigir todos os nossos problemas técnicos.

Gerenciar o influxo de tickets de TI

Ainda precisamos de equipamentos de nossos locais de trabalho em quarentena (notebooks, carregadores, telefones celulares, mouse ou, às vezes, até mesmo itens pessoais esquecidos em nossas estações de trabalho). Os nossos técnicos da Pitstop de TI recolhem os dados necessários: modelo do notebook, tipo de carregador, IDs de estações de trabalho etc., utilizando a nossa ferramenta ITSM. Com mais contexto, eles podem responder aos tickets facilmente. Eles também transmitem informações como a senha do portão e o ponto de contato para coletar nossos equipamentos e pertences usando essa ferramenta.

A Zorro também fez várias melhorias no fluxo de trabalho com base na ITSM para as equipes de negócios: RH, financeiro, jurídico e assim por diante para colaborar e trabalhar melhor.

Habilitar redefinições de senha

Sejamos honestos. Duas semanas é o suficiente para esquecermos nossas senhas. Ainda conseguimos bloquear nossas contas, mas os nossos técnicos da Pitstop nos ajudam a redefinir nossas senhas de forma segura e a desbloquear as nossas contas no conforto das nossas casas.

Identificar e gerenciar vulnerabilidades

À medida que os ataques cibernéticos aumentaram após a Covid-19, a Zorro está constantemente à procura de novas ameaças. Quando uma vulnerabilidade é identificada, a Zorro corrige rapidamente as falhas antes que elas levem a uma violação protegendo, no processo, a Zoho de se tornar uma vítima de ataques cibernéticos.

Gerenciar o acesso privilegiado

Algumas de nossas contas de usuário têm mais importância do que as outras e têm superprivilégios. Seus recursos e acesso elevados colocam essas contas em um risco maior de serem comprometidas. A Zorro monitora todas as contas privilegiadas, alertando a alta gerência se alguma atividade suspeita for executada a partir dessas contas.

Algumas das atividades ou tarefas, como alterações importantes nas configurações do servidor ou da rede, também precisam de acesso privilegiado.

Gerenciar ativos

Como a maioria de nossos funcionários mudou para suas cidades durante o lockdown, eles levaram os ativos da empresa (smartphones, notebooks etc.) alocados a eles. A Zorro deve manter um inventário de ativos e gerenciar licenças, portanto, após a Covid-19, quando nossos funcionários estiverem de volta ao escritório, podemos garantir que os ativos sejam contabilizados.

Compartilhar conhecimentos

Com o trabalho de casa se tornando o novo normal, alguns de nossos funcionários distribuídos tornaram-se mais autossuficientes. Eles estão acessando os recursos internos da Zorro para encontrar artigos relacionados a VPNs ou problemas de firewall antes de entrar em contato com técnicos Pitstop de TI.

Estamos nessa juntos

Nossa força de trabalho

A mudança para o trabalho remoto mudou nossas vidas. Continuamos sentindo falta do encontro casual na despensa, dos bate-papos ao lado da máquina de café e do acesso a uma boa comida. No entanto, também existe um lado positivo: menos trajetos longos, opções de roupa sem julgamento, mais tempo com a família e, é claro, mais produtividade.

É isso mesmo. Notamos um aumento na produtividade depois de mudar para o modelo de trabalho remoto, e somos gratos a todas as nossas equipes de negócios e funcionários.

Retribuir para os nossos clientes

Para facilitar um trabalho tranquilo a partir da transição para casa, o TI precisa de acesso a sistemas críticos na infraestrutura, como servidores, aplicações, bancos de dados e dispositivos de rede. No entanto, alguns de nossos clientes de pequenas e médias empresas têm preocupações de segurança e não estão abertos para acesso remoto. Entendemos o lado deles.

Reunimos recursos essenciais de trabalho remoto para as equipes de TI gerenciarem sua infraestrutura de TI e habilitarem o trabalho remoto para suas forças de trabalho distribuídas. Todas as nossas ferramentas da ManageEngine ajudam os clientes a criarem várias camadas de segurança para permitir o acesso remoto seguro a sistemas críticos de forma segura e eficaz.

No lado comercial, lançamos o Zoho Remotely, um pacote de aplicações em nuvem que ajudará na comunicação, colaboração, rastreamento de trabalho e assistência remota.

Capítulo 04

CONCLUSÃO

BCDR de avaliação

Se sua organização enfrentar uma emergência hoje, você tem os processos necessários de resposta, recuperação e continuidade dos negócios para lidar com isso? Resumimos os indicadores em que nossos esforços de BCDR se baseiam.

O checklist abaixo é um ponto de partida para que a TI e outras organizações elaborem um plano de BCDR abrangente. O processo será, obviamente, diferente com base na sua cultura organizacional, nos sistemas, ambientes, na natureza e gravidade do desastre.

Checklist de BCDR para empresas	
Propósito e escopo	↬ Qual é a finalidade e o escopo do seu plano de BCDR? ↬ Ele abrange todas as suas unidades de negócio críticas, funções, recursos, partes interessadas (incluindo clientes) e os vários tipos de desastres?
Governança e funções	↬ Você tem uma equipe de alta gerência que controla e aprova o plano? ↬ Você identificou a equipe que cria e modifica o plano? ↬ Você identificou outras equipes que precisam estar envolvidas nos processos de planejamento, criação, treinamento e aprovação de BCDR?
Avaliação de riscos	↬ Você identificou os riscos para sua organização? É uma falta de segurança de TI, estrutura de construção ruim, desastres (como terremotos, inundações e pandemias), acidentes causados pelo homem (como incêndio) e falhas de infraestrutura (como falta de energia)? ↬ Você avaliou a probabilidade dos desastres e avaliou os riscos? ↬ Você identificou as medidas para controlar e atenuar esses riscos? ↬ Você documentou todos os seus dados de avaliação de riscos?
Análise do impacto nos negócios	↬ Você identificou as unidades de negócio críticas e suas funções? ↬ Você identificou as interdependências entre essas unidades de negócio e funções? ↬ Você identificou os recursos críticos para as unidades de negócio e seus backups? ↬ Você identificou os sistemas de TI críticos? ↬ Você estabeleceu o RTO e o RPO? ↬ Você identificou os requisitos mínimos de infraestrutura, sistemas e recursos para manter sua empresa funcionando?

Checklist de BCDR para empresas	
Análise do impacto nos negócios	↬ Você identificou o impacto financeiro em sua organização? ↬ Você identificou o que está em jogo para sua empresa caso o desastre dure semanas/meses, como uma pandemia? ↬ Você documentou o impacto e criou um relatório de BIA?
Planejamento de BCDR	Resposta ↬ Você identificou as equipes de resposta a emergências (incluindo TI) e o pessoal? ↬ Você estabeleceu a estratégia de notificação com base em sua hierarquia e estrutura organizacional? ↬ Você identificou os pontos de encontro em caso de desastre? ↬ Você tem procedimentos de resposta de emergência para todos os tipos de desastres? Todos os acordos de TI estão em vigor, como proteção de equipamentos de TI, backup de energia alternativo e conexão de rede alternativa? O backup dos dados é feito regularmente? Os sistemas de alarme de incêndio estão instalados? ↬ Você identificou as linhas diretas de emergência locais? ↬ Você documenta cada etapa e tem formulários em vigor para capturar todos os detalhes, como em um formulário de desastre? Comunicação ↬ Você tem uma equipe de comunicação para criar seu plano de comunicação? ↬ Você tem uma estratégia de comunicação interna e externa bem definida em vigor? Recuperação ↬ Você criou um cronograma de suas atividades de recuperação? O que você fará nas primeiras 3-4 horas do desastre, 5-24 horas, 2-4 dias, 5-14 dias? Você identificou os centros de comando de emergência e locais alternativos para operações de negócios contínuas?

Checklist de BCDR para empresas	
Planejamento de BCDR	↬ Quais são as medidas de continuidade dos negócios para garantir a disponibilidade: procedimentos de recuperação e backup de dados, resiliência do data center, data centers secundários, vários ISPs, backup de energia, sistemas de controle de temperatura e sistemas de prevenção de incêndio implementados? ↬ Sua organização tem um plano de sucessão para tomar decisões importantes durante desastres? ↬ Como você estabilizará a situação de desastre? ↬ Você realiza uma avaliação de danos durante um desastre para determinar danos a ativos críticos? ↬ O que você faz para garantir a continuidade dos suprimentos? Você identificou fornecedores de backup?
Implementação e treinamento	↬ Você fornece treinamento regular a toda a equipe de emergência? ↬ Você realiza simulações de incêndio e de segurança de TI, como ataques de phishing etc., com simulações ao vivo? ↬ Você estabeleceu os prazos e a frequência dessas simulações? ↬ Você documenta os resultados do treinamento para aprimoramento contínuo?
Planejamento da revisão e manutenção	Você revisa e atualiza regularmente seu plano de BCDR para garantir que o plano permaneça atualizado com as informações e alterações mais recentes em termos de sistemas de TI, recursos, infraestrutura e políticas?

Melhores práticas de BCDR

Entendemos como é difícil pensar claramente sob a intensa pressão de um desastre repentino. Uma das melhores maneiras de responder a uma emergência é manter a calma e não entrar em pânico. Aqui estão algumas práticas recomendadas a serem consideradas em sua jornada de BCDR.

- Sejamos honestos. Não importa quantas vezes o plano é testado e improvisado, sempre haverá algumas últimas revisões/adições durante uma emergência real. É aí que entra em jogo o nosso pensamento rápido e a nossa criatividade. Na Zoho, fizemos algumas revisões de última hora em nosso plano de BCDR, como atualizar o contato dos provedores de serviços de emergência que mudaram para um novo local, alterar rotas de evacuação ou reatribuir responsabilidades e tarefas dos funcionários no último minuto. Acontece com o melhor de nós, e não há razão para entrar em pânico.

- É uma prática recomendada envolver e pedir sugestões sobre como melhorar o plano da auditoria interna, do contador e das equipes jurídicas. O conselho jurídico também deve ser solicitado a revisar os esforços de planejamento de BCDR para verificar se há problemas de violação. Esta é uma etapa crucial que pode salvar as organizações de implicações legais e multas enormes.

- Durante a fase inicial da BIA, um modelo de coleta de dados que consome menos tempo e está mais alinhado com a forma como você trabalha em sua organização é melhor. Qualquer esforço que não faça parte de suas principais atividades comerciais, como continuidade dos negócios, recuperação de desastres e conformidade, geralmente é de baixa prioridade para suas unidades de negócio e recursos. Todas as etapas que você tomar para reduzir o esforço de coletar os dados podem valer a pena.

- É melhor ter data centers em diferentes locais geográficos e, de preferência, em áreas menos propensas a desastres.

- Teste o plano de BCDR de uma forma realista com todos os recursos envolvidos para garantir que ele funcione e, em seguida, faça os ajustes necessários.

- Por fim, garanta que o plano seja acessível a todas as partes envolvidas, mesmo em caso de desastre.

Últimas palavras

De certa forma, concordaríamos que a Covid-19 é um alerta para a maioria das organizações. Foi comprovado que o desastre poderia ocorrer a qualquer momento, e o impacto pode ser sentido em todo o mundo.

Supondo, então, que as equipes de alta gerência estejam todas definidas para garantir a continuidade dos negócios e que as equipes de negócios estejam se preparando para criar ou intensificar um plano existente, esperamos que este manual seja útil para todos vocês e desejamos boa sorte em seus esforços de BCDR.

Até a próxima!