arcserve®

eBook

COMO MONTAR UM PLANO DE RECUPERAÇÃO DE DESASTRES

PRÁTICAS RECOMENDADAS

COMO MONTAR UM BOM PLANO DE RECUPERAÇÃO DE DESASTRES

Não há dinheiro ou planejamento capaz de impedir que os desastres aconteçam. Mas um bom plano de recuperação de desastres (DR) pode reduzir o tempo de inatividade de uma semana ou dia para horas ou até mesmo minutos.

Como qualquer projeto importante, o sucesso de um DR começa pelo planejamento, seguido por modelos e procedimentos de práticas recomendadas, que por sua vez são implementados pelas ferramentas certas.

Identifique os aplicativos essenciais, as infraestruturas das quais eles dependem e as tarefas e os dados aos quais eles precisam ter acesso.

Sua empresa acumulou uma quantidade significativa de dados ao longo do tempo. Centenas de gigabytes, talvez terabytes ou até petabytes de dados. Mas só parte deles, geralmente uma pequena fração, precisa ficar disponível de novo rapidamente.

1º PASSO: Análise de impacto nos negócios

A Análise de impacto nos negócios (BIA) define quais recursos sua empresa não pode ficar sem. Esse é o primeiro passo para criar um plano de recuperação de desastres que funcione.

A alta gerência da empresa, e não de TI, deve se envolver nessa análise para identificar e definir a lista de aplicativos considerados essenciais. Caberá à gerência de TI mapear as tarefas relacionadas aos aplicativos, a respectiva infraestrutura e outros serviços necessários para executar e usar esses aplicativos.

Todos os principais interessados na empresa precisam participar da análise, para não descobrir depois, quando um site sair do ar, que havia outro aplicativo que um executivo considerava essencial.

2º PASSO: Avaliação de risco

A segunda etapa para montar um plano completo de recuperação de desastres inclui o mapeamento dos dois tipos de infraestrutura de TI:

1. A infraestrutura de TI que você controla, localizada nos seus escritórios ou em outras instalações.
2. A infraestrutura de TI que você não controla, como sites ou serviços web e na nuvem executados em um ambiente hospedado.

Depois que a infraestrutura de TI for mapeada, procure pontos únicos de falha, como um servidor com apenas uma placa de rede.

Esses são os primeiros lugares que devem ser "reforçados" com redundância.

O QUE PROVOCA OS DESASTRES DE TI?

A causa de um desastre de TI pode ser pequena e específica. Uma fonte de alimentação, CPU, placa de interface de rede, RAM, ventoinha ou outro componente em um servidor pode falhar. Uma breve oscilação de energia pode afetar os dados ou interromper o funcionamento de um programa.
É raro um datacenter inteiro parar, mas pode acontecer. O tempo pode afetar a energia ou o serviço de rede. Um incêndio, uma inundação ou danos em um edifício podem tirar do ar toda a sala de computadores ou o datacenter.

3º PASSO: Gerenciamento de riscos

Para reduzir o risco de ocorrer um desastre no ambiente de TI, reforce a proteção contra os problemas mais comuns e você estará de 90% a 95% seguro contra possíveis pequenos acidentes.

A redundância é uma boa medida para evitar, ou mesmo minimizar, vários incidentes de TI. Por exemplo, servidores, equipamentos de armazenamento e rede podem ser configurados com duas fontes de alimentação, conectadas a fontes de energia separadas. Servidores, firewalls, no-breaks e outros equipamentos, inclusive sites inteiros, podem ser duplicados. Os serviços de rede e energia podem ser fornecidos por duas empresas diferentes e por cabos separados. Os dados podem ser armazenados em vários discos rígidos.

4º PASSO: Teste de DR

Existem só duas maneiras de verificar se um plano de recuperação de desastres funciona.

Uma delas é quando acontece um desastre. É claro que esse é o momento errado para descobrir que você fez escolhas erradas ou que uma das suas ferramentas ou serviços falhou ou que não abrangia um aplicativo essencial.

A outra maneira é fazer testes periódicos. É melhor descobrir uma falha na infraestrutura testando cenários de falha em circunstâncias controladas.

As auditorias externas podem ajudar a identificar se existem partes do seu plano de DR que precisam ser melhoradas. Um dos motivos é que nem todas as empresas simulam um cenário completo de desastre ou seguem todos os procedimentos até o fim para verificar se a recuperação total acontece. Uma auditoria externa pode elevar o padrão que sua empresa definiu e realizar testes completos e rigorosos, obrigando vocês a adotar práticas recomendadas de TI.

Backup fora da empresa

Na maioria dos eventos de desastres de TI, a recuperação de desastres envolve a restauração dos dados, porque a cópia principal foi danificada, destruída ou ficou inacessível.

Para garantir que uma cópia dos seus dados esteja disponível se e quando ocorrer um desastre de TI, é essencial contar com um backup externo. Ele deve estar geograficamente distante o suficiente para garantir que um evento importante como incêndio, inundação, falta de energia, explosão ou terremoto não danifique ou isole o backup.

A fita dominou o mundo dos backups externos por décadas. Mas o backup em fita tem alguns inconvenientes:

- Leva-se um bom tempo para solicitar, localizar e recuperar as fitas armazenadas fora da empresa.
- Se uma fita estiver com defeito, você só descobrirá quando precisar dela.
- Para ler fitas de gerações mais antigas, é preciso ter um drive de fita compatível. Como seu local pode ficar inacessível, você também precisará de um local alternativo, o que aumenta os custos de infraestrutura.
- Talvez você precise percorrer a fita inteira só para recuperar alguns arquivos.
- Muitos backups em fita usam formatos proprietários e exigem um software específico para ler, outro custo recorrente.

No mundo online 24x7x365 de hoje, um backup que não está disponível de maneira rápida e fácil pode ser bom para preservar dados importantes da empresa, mas não é útil para recuperação de desastres. Atualmente, os RTOs são de horas ou mesmo minutos.

OBJETIVO DE PONTO DE RECUPERAÇÃO (RPO) E OBJETIVO DE TEMPO DE RECUPERAÇÃO (RTO)

Os dados que você quer que estejam novamente disponíveis em tempo hábil são chamados de Objetivo de Ponto de Recuperação (RPO).
Objetivo de Tempo de Recuperação (RTO) refere-se ao tempo que você deseja que esses dados estejam disponíveis de novo.
O tempo aceitável de inatividade de TI para aplicativos e dados essenciais depende de muitos fatores (principalmente custos) e varia de uma empresa para outra, mas, em geral, hoje, é de minutos a horas, em comparação com dias, uma semana ou mais de anos atrás.

APLICATIVOS DE HOSPEDAGEM X TERCEIRIZAÇÃO

Outro componente muito importante no gerenciamento de risco dos desastres de TI é avaliar se é o momento de terceirizar qualquer aplicativo e serviço de TI e movê-lo para a nuvem.

SOBRE A ARCSERVE

A Arcserve fornece soluções excepcionais para proteção dos ativos digitais de valor inestimável de empresas que precisam de proteção abrangente e em larga escala dos seus dados. Fundada em 1983, a Arcserve é o nome mais experiente do mundo em soluções para a continuidade dos dados que protegem infraestruturas de TI com aplicativos e sistemas de diferentes gerações em qualquer local, dentro da empresa e na nuvem. Empresas em mais de 150 países confiam na experiência, no conhecimento e nas tecnologias integradas e altamente eficientes da Arcserve para acabar com os riscos de perda de dados, inatividade prolongada e para reduzir em até 50% os custos e a complexidade de fazer backup e recuperar dados. Com sede em Minneapolis, Minnesota e presente em várias partes do mundo.

Explore mais em **arcserve.com/br**

DEIXE A DOCUMENTAÇÃO DE DR À DISPOSIÇÃO

Há muitas informações associadas a um plano de recuperação de desastres. Um exemplo são as informações de contato de provedores, funcionários, empresas de serviços públicos e outras empresas com as quais você pode precisar conversar. Outro são os inventários de equipamentos de TI, incluindo números de série e informações sobre garantia, identificação dos circuitos, plantas do edifício etc. Verifique se você possui cópias dessas informações que possam ser acessadas mesmo que todo o ambiente de TI, e possivelmente as redes telefônicas com e sem fio, fiquem fora do ar. Considere armazenar uma cópia online e mantenha outra cópia protegida no seu smartphone, tablet ou notebook e em um flash drive.