Disaster Recovery, um assunto que por mais indesejável, precisa fazer parte do repertório de competências de qualquer área de tecnologia.

Afinal de contas, problemas podem acontecer em qualquer organização.

Como já dizia o lendário Forrest Gump: “shit happens”!

Dentro desse contexto, nada mais natural e necessário do que estar preparado em pelo menos dois grandes sentidos:

a) – Ações de resiliência para reduzir as chances e casos de incidentes.

b) – Ações de mitigação, buscando reduzir o tamanho do impacto na eventualidade de uma ocorrência.

Abordagem tradicional de DR em Tecnologia

Em ambos os casos, é bem comum, ao menos para quem (como eu) é do mundo de IT, pensar imediatamente em temas relacionados com nosso universo usual de tecnologia.

Ou seja, me refiro aos temas comuns como infraestrutura, sistemas e processos para evitar as ocorrências e mitigar o tamanho do impacto caso ocorram.

Mas muitas vezes, as empresas negligenciam a parte de relações públicas de seus planos de DR, uma omissão que pode levar a consequências comerciais piores do que aquelas causadas pelo próprio desastre.

É ai que vale explorar a importância de integrar estratégias de comunicação eficazes em planos de DR e então tive a oportunidade de ler essa matéria da CIO Online:

https://www.cio.com/article/479996/the-dr-essential-it-leaders-cant-overlook.html

Uma outra abordagem: Comunicação

Achei muito interessante a abordagem dada à matéria por ela trazer um outro viés que as vezes nos passa desapercebido: o da Comunicação!

Olhando agora em retrospectiva, fica fácil lembrar de tantos e tantos casos de incidentes poderiam ser muito mais “serenamente” tratados e superados caso a comunicação tivesse sido mais sofisticada.

E não se engane, quando se fala em incidentes em IT não é uma questão de “se” eles vão acontecer, mas sim de “quando” e “quantas” vezes vão acontecer. Pode esperar que a sua vez ainda vai chegar.

Talvez seja apenas um incidente sem maiores consequências, como pode vir a ser algo bem mais grave, que mereça a alcunha de “Disaster”.

A importância de se comunicar

A comunicação eficaz em momentos de crise não apenas informa as partes

interessadas sobre o progresso da recuperação, mas também ajuda a manter a confiança do público e a evitar o pânico.

A falta de comunicação adequada pode levar a rumores e desinformação, resultando em danos significativos à reputação e às operações da empresa.

Quanto à questão da comunicação, acredito que ela fica exponencialmente mais relevante conforme aumenta o grau de “exposição” do incidente.

Pode ser de um pequeno sistema ou funcionalidade utilizada apenas internamente em IT.
Aumenta quando for de uso de um ou poucos usuários de negócio.

E vai aumentando conforme aumenta a quantidade de usuários internos, até “explodir” em barulho caso seja algo exposto para uso direto aos seus clientes externos!

Recomendações da matéria

Dentro dessa matéria são apontados alguns passos para a comunicação dentro dos planos de tratamento de Disaster Recovery:

- D**esenvolver um Script de Comunicação**: Inclua elementos básicos de mensagem no plano de DR para garantir consistência e clareza nas comunicações.
- **Definir uma Cadeia de Comando de Comunicação**: Estabeleça uma hierarquia clara para a disseminação de informações durante uma crise, evitando confusão e pânico desnecessário.
- **Identificar Porta-Vozes de Backup**: Garanta que haja substitutos designados para os porta-vozes principais, garantindo continuidade na comunicação em caso de ausência.
- **Identificar Canais de Comunicação**: Determine os canais de comunicação externa, como mídia local e redes sociais, para garantir uma divulgação eficaz das informações.
- **Treinar e Ensaiar o Plano de PR/DR**: Realize exercícios regulares para familiarizar os funcionários com o plano de comunicação de crise e garantir que esteja atualizado e eficaz.
- **Treinar Funcionários para Delegar Informações**: Eduque os funcionários sobre a importância de encaminhar consultas externas para os canais apropriados, reduzindo o risco de disseminação de informações

imprecisas.
- **Entender que a DR é uma Questão de Negócios, não de TI**: Reconheça que a recuperação de desastres é uma responsabilidade compartilhada por toda a organização, não apenas pelo departamento de TI.

Os impactos para além da Tecnologia

Caso tenha alguma dúvida do tamanho do barulho que um incidente pode gerar, sugiro instalar e utilizar o famoso DownDetector e observar o quanto basicamente todas as empresas que ofertam serviços e produtos ao mercado de consumo massivo estão expostas ao “escrutínio popular”.

Daí a importância de estruturar adequadamente seus processos e skills de comunicação em diversos níveis, como entre as pessoas e por parte da própria empresa junto ao mercado.

Como foi bem explorado na matéria, o tema de Disaster Recovery não é apenas uma questão de IT, mas sim uma questão de sobrevivência do próprio negócio!

Como é usualmente organizado um Plano de Disaster Recovery

Em um ambiente empresarial cada vez mais dependente de tecnologia, os planos de DR são essenciais para garantir a continuidade das operações em face de interrupções inesperadas.

Estes planos são complexos e multidimensionais, abrangendo desde a recuperação de dados e sistemas críticos até a gestão de comunicações durante crises.

Um plano de recuperação de desastres típico é composto por várias seções que cobrem todos os aspectos necessários para restaurar rapidamente a operacionalidade após um incidente.

A estrutura pode variar dependendo das necessidades específicas da organização, mas geralmente inclui os seguintes elementos:

- **Introdução**: Define o escopo, os objetivos e os princípios orientadores do plano.
- **Governança**: Estabelece a estrutura de comando e controle, incluindo os papéis e responsabilidades durante um desastre.
- **Análise de Risco e Impacto nos Negócios (BIA)**: Identifica as funções críticas de negócios e os recursos necessários para manter essas funções operando.
- **Estratégias de Recuperação**: Descreve as abordagens para a recuperação de sistemas, aplicações e dados.
- **Planos de Ação de DR**: Fornece procedimentos detalhados para a execução da recuperação em resposta a diferentes tipos de desastres.
- **Comunicação de Crise**: Detalha os processos de comunicação interna e externa.
- **Teste e Manutenção**: Descreve a frequência e os métodos para testar e atualizar o plano.

Componentes Chave de um Plano de DR:

- **Análise de Impacto nos Negócios (BIA)**: Este componente é vital para entender quais aspectos do negócio são mais críticos. A BIA ajuda a identificar e priorizar os sistemas e processos que necessitam de recuperação rápida para minimizar o impacto financeiro e operacional.
- **Identificação de Riscos**: Uma análise detalhada dos riscos potenciais que podem causar interrupções. Isso inclui desastres naturais, falhas de hardware, ataques cibernéticos e outros riscos relevantes.
- **Estratégias de Recuperação**: Definir claramente as estratégias para restaurar as operações de TI e negócios. Isso pode envolver a recuperação de dados, a substituição de equipamentos, o uso de sites alternativos e a contratação de serviços terceirizados.
- **Planos de Implementação**: Procedimentos passo-a-passo que devem ser seguidos durante um desastre para recuperar operações e serviços. Isso inclui a inicialização de sistemas em um site de recuperação e o restabelecimento de conexões de rede.
- **Comunicação**: Planos detalhados para informar as partes interessadas

internas e externas, incluindo empregados, clientes, fornecedores e a mídia sobre o estado das operações.
- **Testes e Exercícios**: Um componente crítico que envolve a realização regular de testes para garantir que o plano de DR é eficaz e que a equipe está preparada para agir em caso de desastre.
- **Revisão e Manutenção**: O plano deve ser revisado e atualizado regularmente para refletir mudanças no ambiente de negócios e tecnológico.

O alcance de um plano de DR varia amplamente dependendo da natureza e do tamanho da empresa.

Para algumas organizações, pode ser suficiente ter planos que cubram apenas os sistemas de TI críticos.

Para outras, especialmente aquelas em setores altamente regulamentados ou que lidam com grandes volumes de dados sensíveis, o alcance pode ser muito mais abrangente, incluindo:

- Recuperação completa do centro de dados: Capacidade de restaurar todas as operações de TI, incluindo servidores, redes, aplicações e bases de dados.
- Continuidade dos serviços essenciais: Garantir que as funções empresariais vitais possam continuar sem interrupções significativas, mesmo durante um desastre.
- Gestão da cadeia de suprimentos: Planos para manter ou restaurar rapidamente a logística e os suprimentos essenciais em caso de interrupção nas operações normais.
- Recuperação regulatória e de conformidade: Assegurar que todas as recuperações respeitem as regulamentações legais e normativas aplicáveis, evitando assim penalidades adicionais.

Importância da Flexibilidade e Adaptação

Dado que os desastres podem variar enormemente em escala e natureza, um plano de DR deve ser suficientemente flexível para se adaptar a diferentes circunstâncias.

Por exemplo, a resposta a uma falha de software pode ser muito diferente da necessária para um desastre natural como um terremoto.

Essa flexibilidade é alcançada através da criação de planos modulares e escaláveis que podem ser ajustados conforme necessário.

A Tecnologia como Facilitadora

Com o avanço das tecnologias de cloud computing, virtualização e armazenamento distribuído, as empresas têm agora ferramentas mais robustas para implementar planos de DR.

Essas tecnologias permitem não apenas uma rápida recuperação de dados, mas também a implementação de soluções de failover automáticas que podem reduzir significativamente o tempo de inatividade durante interrupções.

A Integração entre DR e Segurança Cibernética

A segurança cibernética tornou-se um componente inseparável da recuperação de desastres.

Muitos desastres são o resultado de ataques cibernéticos, que podem causar danos significativos aos sistemas de TI.

Um plano de DR robusto deve incluir estratégias para a mitigação de riscos cibernéticos, como backups criptografados, sistemas de detecção de intrusão e planos de resposta a incidentes.

CIO Codex Framework – Service Continuity & Disaster Recovery

A fim de oferecer alguma base teórica de conceitos e características, abaixo é apresentado um resumo do conteúdo do CIO Codex Framework que trata esse assunto.

A Service Continuity & Disaster Recovery Management representa uma capability

crítica no espectro do CIO Codex Capability Framework, a partir da macro capability On premises & Cloud Technical Operation e alinhada à camada de Service Excellence.

Esta capability é vital para assegurar a resiliência organizacional e a disponibilidade contínua dos serviços de TI.

Por meio de estratégias proativas e planos meticulosamente elaborados, esta função minimiza os efeitos negativos de interrupções inesperadas, fortalecendo a confiança e a dependência dos clientes e parceiros de negócios na capacidade da organização de manter operações ininterruptas.

Os conceitos fundamentais que permeiam a Service Continuity & Disaster Recovery Management incluem a continuidade de serviço, que é a habilidade da organização de manter funções essenciais de TI durante e após crises, recuperação de desastres, que engloba a restauração de sistemas e dados após ocorrências disruptivas, e testes de resiliência, que validam a eficácia dos planos de continuidade e recuperação por meio de simulações controladas.

Entre as características distintivas desta capability, salientam-se a análise de riscos, que mapeia potenciais ameaças aos serviços de TI, o desenvolvimento de planos de continuidade robustos, a implementação de sistemas de backup e restauração, o treinamento e a conscientização das equipes, a coordenação eficaz durante crises, e o monitoramento constante da disponibilidade de sistemas, preparando a organização para reagir prontamente a interrupções.

O propósito essencial da Service Continuity & Disaster Recovery Management é estabelecer e manter planos e processos robustos que assegurem a continuidade dos serviços de TI durante eventos disruptivos e permitam uma recuperação efetiva e ordenada após tais eventos. A natureza essencial desta capability reside na sua capacidade de sustentar a continuidade dos negócios e na sua contribuição para a eficiência operacional da organização.

Dentro do contexto do CIO Codex Capability Framework, os objetivos desta capability são claros: assegurar a eficiência operacional através da implementação de planos de continuidade de serviço e recuperação de desastres eficazes, fomentar a inovação tecnológica para aprimorar esses processos e sustentar a vantagem competitiva da organização, garantindo a confiança dos clientes através da demonstração de uma infraestrutura robusta e resiliente.

O impacto da Service Continuity & Disaster Recovery Management se estende por diversas dimensões tecnológicas, incluindo a infraestrutura de TI, que deve ser projetada com redundâncias, a arquitetura de TI, que deve incorporar considerações de recuperação de desastres em sua concepção, e os sistemas e aplicações críticas,

que devem ser capazes de rápida restauração.

Além disso, a cybersecurity é um componente integral, garantindo que os serviços de continuidade incorporem defesas contra ameaças cibernéticas e físicas, e o modelo operacional é reforçado para assegurar que as práticas de gestão de continuidade e recuperação estejam alinhadas com os padrões de segurança e compliance.

CIO Codex Framework – Cybersecurity

A fim de oferecer alguma base teórica de conceitos e características, abaixo é apresentado um resumo do conteúdo do CIO Codex Framework que trata esse assunto.

A cibersegurança, um campo crítico da tecnologia, evoluiu para se tornar uma complexa malha de práticas, soluções e regulamentos destinados a proteger sistemas, redes e programas de ataques digitais.

Em sua essência, a cibersegurança é a aplicação de tecnologias, processos e controles projetados para proteger sistemas, redes e dados de ciberataques.

Efetiva cibersegurança reduz o risco de ataques cibernéticos e protege contra a exploração não autorizada de sistemas, redes e tecnologias.

Alguns conceitos e características se destacam nesse tema, como os apontados a seguir:

Confidencialidade, Integridade e Disponibilidade (CID)

A CID é um modelo que guia as políticas de segurança da informação para proteger a privacidade dos dados, prevenir erros e inacessibilidade.

Criptografia

Um método essencial de proteger informações, transformando-as em um código para prevenir acessos não autorizados.

Segurança de Rede

Inclui medidas para proteger a infraestrutura de TI contra intrusões, como firewalls, anti-malware, e sistemas de detecção de intrusão.

Segurança de Aplicações

Foca no manter o software e os dispositivos livres de ameaças. Um aplicativo comprometido poderia Prover acesso a dados projetados para serem protegidos.

Recuperação de Desastres/Business Continuity Planning

Prepara a organização para responder a incidentes de cibersegurança e retomar as operações normais o mais rápido possível.

Características da Cibersegurança:

Adaptação Contínua

O campo exige uma adaptação e atualização contínua em resposta a novas ameaças e tecnologias emergentes.

Abordagem em Camadas

Segurança eficaz exige uma defesa em camadas, que inclui medidas físicas, técnicas e administrativas.

Treinamento e Conscientização

Fundamental para a cibersegurança é a educação contínua dos usuários sobre as melhores práticas de segurança.

Uso de Inteligência Artificial (AI)

AI e machine learning estão cada vez mais sendo incorporados para prever e identificar ameaças de forma proativa, analisando padrões de ataques e respondendo a eles mais rapidamente do que os humanos.

Regulamentações e Compliance

A cibersegurança é fortemente regulada por leis e normas que ditam como as informações devem ser protegidas. GDPR, HIPAA e outras regulamentações impõem padrões e penalidades para garantir a proteção de dados.

A cibersegurança moderna não só é definida pelo desenvolvimento e implementação de soluções defensivas, ela também incorpora uma abordagem proativa que inclui a simulação de ataques (pentesting) e a construção de ambientes resilientes capazes de se adaptar e responder a ameaças persistentes e evolutivas.

Ao mesmo tempo, os profissionais da área devem considerar as implicações éticas do uso de AI na cibersegurança, tanto para aprimorar as defesas quanto para antecipar e se proteger contra o uso mal-intencionado da AI por agentes adversários.

A intersecção entre AI e cibersegurança é um território rico em potencial para o desenvolvimento de sistemas mais inteligentes e autônomos, mas também carrega a necessidade de vigilância constante e atualização de conhecimento para enfrentar os desafios que surgem com a evolução tecnológica.

Concluindo

O desenvolvimento e a manutenção de um plano de recuperação de desastres abrangente são fundamentais para a resiliência empresarial.

Empresas de todos os tamanhos devem considerar o DR não apenas como uma necessidade operacional, mas como uma estratégia de negócio essencial que abrange tecnologia, pessoas e processos.

Com a implementação de um plano de DR bem estruturado e regularmente testado, as organizações podem enfrentar desastres com confiança, minimizando o impacto sobre as operações, a reputação e o desempenho financeiro.

Integrar uma estratégia de comunicação eficaz em planos de recuperação de desastres é essencial para minimizar os impactos de crises e manter a confiança do público.

Ao seguir os passos delineados acima e reconhecer a importância da comunicação em tempos de crise, as empresas podem estar melhor preparadas para enfrentar os desafios que surgem durante períodos de interrupção operacional.