Plano de contingência. Plano de continuidade dos negócios. Sites de contingência – Cold site, Warm site e Hot site.

Apresentar a importância do plano de Continuidade dos negócios, que vai muito além de ter um plano de alta disponibilidade de recurso e backup. Apresentar os diversos tipos de planos existentes que interagem entre si para conseguir o objetivo maior que é a proteção dos dados e das informações da empresa, sendo no próprio local ou em um site alternativo.

Em consequência da crescente concorrência dentro do mercado mundial, as empresas cada vez mais apostaram na tecnologia como um item diferenciador para a melhoria dos seus produtos e dos seus processos empresariais.

Isso fez com que elas ficassem dependentes, de uma forma absurda, de toda a infraestrutura de computadores e equipamentos de tecnologia da informação.

Com o advento da internet, as empresas começaram a se conectar entre si para poder realizar seus negócios, bem como interagir com seus fornecedores.

Frente a esse cenário, as empresas investiram pesado na alta disponibilidade e segurança dos seus ativos de informação, porém como não existe segurança 100 %, são necessárias implementações de planos de ações que visem à continuidade do negócio em uma situação em que os controles de segurança implementados não conseguiram impedir a concretização de um incidente.

O que é importante para a empresa é que ela tenha uma forma de continuar suas operações, mesmo que seja de forma parcial, até que todo o restante possa voltar à normalidade.

Existem vários planos que ajudaram a empresa nesse processo de restabelecimento do seu negócio, e alguns deles serão descritos a seguir.

Um plano de contingência de negócio não é apenas um plano que protege a era de tecnologia, mas sim todos os elementos que fazem parte do negócio da empresa e que envolvem processos, pessoas e máquinas. Uma sigla muito conhecida no mercado de tecnologia da informação, quando o assunto é continuidade de negócio, é a sigla PCN. Na realidade essa sigla é uma abreviação para Plano de Continuidade dos Negócios, que também pode ser vista como BCP, abreviação para Business Contingency Plan, em inglês. No PCN o foco principal são os negócios da organização e as pessoas durante e após a interrupção das atividades da empresa.

O PCN pode ser elaborado para restabelecer um negócio específico ou todos os negócios-chave da organização. Em razão disso, costuma-se afirmar que o PCN nem sempre inclui a recuperação de todos os processos e o retorno às operações originais, uma vez que é pensado primeiramente restabelecer os processos estritamente necessários à continuidade dos negócios da organização, deixando para os outros planos cobrirem os procedimentos de retorno das outras atividades.

Como estamos falando em recuperação do negócio, para a confecção desse plano é importante que outras atividades prévias tenham sido feitas, como a análise de risco e a BIA (esse termo é novo e em breve detalharemos).

A análise de risco, como visto anteriormente, é o processo de verificar quando um certo contexto de insegurança pode ser aceito ou não pela organização. Dessa forma, são feitas várias atividades buscando identificar os principais processos da empresa e os ativos de informação que os suportam. Com base nessas informações, são descobertos também os equipamentos de TI fundamentais para a execução das principais tarefas. Agora se faz necessário identificar os pontos fracos para verificar se as possíveis ameaças podem agir contra o ativo específico. Pronto, agora basta verificar qual o melhor controle a ser implementado para que a probabilidade da realização do risco diminua.

Não basta apenas fazer a análise de risco, pois teremos que identificar qual seria o impacto no negócio, caso aquele incidente de segurança viesse a ocorrer. Essa atividade que é feita de forma estruturada pelo mercado é conhecida como BIA.

A palavra BIA é uma abreviação para as palavras Business Impact Analysis (Negócios Impacto Analise), ou seja, dessa forma esse termo também é conhecido como AIN (Análise de Impacto nos Negócios), que é a tradução de BIA.

O principal objetivo da BIA/AIN é identificar o grau de relevância entre os processos que farão parte do escopo de contingência dentro de um plano de continuidade dos negócios, além de avaliar o tempo máximo de tolerância que a empresa consegue sobreviver sem eles.

O processo de BIA atua de forma a poder complementar o processo anteriormente feito de Análise de Riscos, em que o foco eram os riscos e impactos internos, enquanto isso a BIA procurará identificar os impactos Financeiro e Jurídico, bem como itens intangíveis como abalo da imagem da empresa e possíveis prejuízos.

Após os ataques terroristas ocorridos nas torres gêmeas dos Estados Unidos, em 2001, esse assunto ficou muito em evidência, pois algumas empresas haviam implementado os seus planos de continuidade de negócios, principalmente a parte relacionada à TI, na mesma localização do site principal. O que queremos dizer é que algumas empresas tinham os seus sistemas críticos duplicados na torre ao lado do site principal. Quando o desastre ocorreu, essas empresas ficaram sem nenhuma capacidade de operar, e algumas delas, depois do incidente, já deixaram de existir pela ausência de um plano de continuidade de negócios.

Antes de continuar, é importante que alguns termos fiquem bem claros para melhorar o entendimento dos planos de continuidade de negócios.

Quando for citada a informação sistemas críticos, estamos nos referindo aos sistemas cuja indisponibilidade seja por qualquer motivo representará para empresa perdas irreversíveis de cunho financeiro ou jurídico. Já quando nos referirmos a um desastre, o que temos de pensar é que se trata de qualquer tipo de anormalidade dentro de um ambiente e que impede a realização de alguma atividade por parte de alguém ou algum processo, requerendo que as partes envolvidas tenham de reproduzir repostas em conjunto para a resolução desse problema.

Outra função do PCN é a preservação da integridade física dos funcionários da empresa, e a redução dos prejuízos causados pelo incidente de segurança.

A continuidade operacional que é tratada dentro de um PCN se dá por meio da adoção de uma série de estratégias e ferramentas que devem funcionar de forma integrada e de acordo com prioridades que foram estabelecidas durante a elaboração do plano.

Ainda quando o assunto estiver relacionado à continuidade dos negócios, as variáveis tempo de recuperação X necessidade do negócio X o que eu perdi X o que eu tenho de Backup devem ser analisadas. Dessa forma, duas siglas entraram no cenário da discussão, o RTO e o POR.

- **RTO – Recovey Time Objectives** – geralmente é um tempo pré-definido no qual um processo estará disponível após a decretação da contingência, sendo esse tempo o máximo aceitável antes que a indisponibilidade do sistema afete a organização drasticamente.
- **RPO – Recovery Points Objectives** – é o ponto no tempo em que os dados devem ser restaurados para que o processamento seja reiniciado após a ocorrência de um desastre. Desse modo, ele está diretamente relacionado com o processo e frequência de geração de cópias de Backup do ambiente de TI. Um PCN é composto por outros subplanos relacionados a seguir:
- **PAC** – Programa de Administração de Crise – seu principal foco é garantir de forma mais eficaz a administração e o funcionamento das equipes que aturaram no processo durante a ocorrência da crise. Para isso serão elaborados documentos que definirão onde e como serão tomadas as ações que ajudarão a empresa a criar um centro de comando para fazer a gestão de crises, e, a partir daí, definir e distribuir as tarefas necessárias de coordenação da empresa durante o período da crise.
- **PRD** – Plano de Recuperação de Desastres – o foco está em avaliar, mapear e planejar a recuperação e restauração dos processos de negócio após a ocorrência da situação de emergência, mas ao contrário do PCN faltam procedimentos para garantir a continuidade dos processos críticos durante uma emergência ou interrupção. Nesse plano são detalhadas as ações relativas ao site alternativo. Esse plano fará parte do PCN/BCP e terá como meta final restabelecer o ambiente nas mesmas condições que estava antes do incidente de segurança. Esse tipo de plano também é conhecido como **DRP** (Desaster Recovery Planing) e tem a característica de ser focado em TI. Suas ações são direcionadas para recuperar o operacional dos sistemas, aplicações e computadores.

- **PCO** – Plano de Continuidade Operacional – o foco é estabelecer um conjunto de procedimentos que ajudem a implementar mediadas de contingencias relacionadas aos ativos que suportam os processos de negócio. A ideia principal é a redução do tempo de indisponibilidade para que a situação não traga tanto impacto para o negócio da empresa.
- **Plano de contingência de TI / plano de suporte de continuidade** – como vimos durante o processo de análise de risco, existem vários processos que são críticos para as atividades da organização e cada um desses processos possuem ativos de tecnologia de informação que os ajudam na realização das suas atividades. O plano de Contingencia de TI deve ser elaborado para cada aplicação crítica da empresa e acaba por gerar múltiplos planos para serem mantidos dentro do plano de contingência de negócio.
- **Plano de comunicações de crise** – em uma situação de emergência é muito comum que as pessoas fiquem desorientadas. Se as informações importantes a respeito da empresa forem passadas de forma indevida para o público, faz-se necessário que exista dentro do PCN um plano específico para esse caso. Dentro do PCN, o PCC (Plano de Comunicações de Crise) terá a responsabilidade de preparar seus procedimentos internos e externos de comunicação para o desastre e deverá ser desenvolvido pelo órgão responsável pelo contato com o público interno e externo. Isso se faz necessário para garantir que somente as declarações aprovadas pela empresa sejam divulgadas ao público e aos envolvidos. Todas as ações e procedimentos devem ser coordenados com todos os outros planos do PCN.

Estratégias de contingência

Sites alternativos

O plano de continuidade dos negócios considera que a empresa possa ficar com o seu site totalmente indisponível, embora interrupções de longos períodos de tempo sejam raras, mas se isso acontecer, a empresa necessita continuar operando-o de forma completa ou parcial, ou pelo menos ter um lugar para iniciar as suas operações de recuperação. Dessa maneira, o plano deve considerar a inclusão de um local alternativo para que a empresa possa recuperar e executar as suas atividades.

A recuperação dos dados atingidos por um desastre pode ser feita por meio da utilização de backup no próprio site, quando possível, ou em site externo:

- Com recursos próprios em prédios e infraestrutura dedicados.
- Com recursos contratados em prédios e infraestrutura contratados.
- Com recursos mistos em prédios próprios e infraestrutura alugada ou prédios alugados e infraestrutura própria.
- Por meio de acordos de reciprocidade.

Tipos de sites alternativos

- **Cold sites** – Esse tipo de site está relacionado a um local separado da organização, em que já se tenha disponível apenas a infraestrutura básica para colocar os servidores e sistemas em operação. Quando falamos em infraestrutura, estamos nos referindo à rede elétrica, conexões de telecomunicações e controles de acesso, climatização, nobreaks e equipamento de combate a incêndio, itens esse fundamentais para abrigar os servidores e os sistemas de informação.

  Nesse local não existirá equipamentos de TI e, por isso, o teste e verificação se tudo vai funcionar conforme o planejado é quase impossível. O nome do site **"Cold"** por si só já dá a ideia de que esse local tem que entrar em funcionamento (aquecer) para que a continuidade esteja em funcionamento.

- **Warm sites** – Já nesse tipo de site existe um gasto maior, pois existirá a necessidade de investimento em recursos de TI e que ficaram em funcionamento em paralelo com o site principal.

Esse local possuirá espaços parcialmente equipados com os equipamentos que possuem baixa tolerância à indisponibilidade, geralmente os mais críticos para que a empresa continue operando parcialmente no caso de um incidente de segurança. Como o próprio nome diz, **"Warm"** (Morno), esse local estará parcialmente funcionando, bastando mudança e alocação de alguns itens para que tudo volte a funcionar normalmente depois do incidente. Os sistemas serão recuperados e, quando for o caso, reconfigurados e instalados novamente, bem como serão restaurados os backups existentes para que a situação volte à normalidade**.**

- **Hot sites** – Nesse modelo existirá um site igualzinho ao principal, só que em outra localidade, com os mesmos recursos de tecnologia da informação e infraestrutura que o site principal possui. Já de início dá para perceber que o custo desse local será alto, pois todos os servidores deverão ser duplicados, e deverá existir um processo de replicação e sincronismos dos dados para que quando a situação de continuidade for iniciada, as equipes necessitem apenas se dirigir para o site backup e continuar as suas operações com o mínimo de perda possível.

Fazendo a mesma comparação como foi feita com os outros dois tipos, pelo fato de ser **"Hot"** (quente), ele não necessitará aquecer para entrar em funcionamento, bastara apenas apertar a opção continuar.

Existem outros tipos de sites que podem ser contratados, porém não são de uso tão comum, dentre eles podemos citar um mobile site, que na realidade é uma variação do **Hotsite**, só que esse está construído em um veículo que possibilita a mobilidade para um local apropriado.

Dentre os tipos existe também uma modalidade conhecida como o Acordo de Reciprocidade, que pode ser estabelecido entre duas empresas possuidoras de similaridades em suas características físicas, de negócio e tamanho. A ideia é compartilhar o local do site de contingência e cada uma ocupar o local somente quando a situação de continuidade for necessária. O problema que pode ocorrer é se a indisponibilidade atingir as duas empresas ao mesmo tempo ou o período de ocupação do espaço da contingência for longo demais

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

objeto disponível apenas na versão web

objeto disponível apenas na versão web

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de segurança da informação: guia prático para elaboração e implementação.* Rio de Janeiro: Ciência Moderna, 2006.

GIL, Antônio de Loureiro. *Segurança em informática: ambientes mainframe e de microinformática, segurança empresarial e patrimonial, 200 questões sobre segurança.* 2. ed. São Paulo: Atlas, 1998.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL.* São Paulo: Novatec, 2007.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva.* Rio de Janeiro: Elsevier, 2003.