



Curso Plano de Continuidade de Negócios

Em um cenário mundial de alto risco e volatilidade, com uma interconexão e interdependência de todas as cadeias de suprimento, a segurança e continuidade dos negócios é cada mais importante nas organizações. Identificar o valor real do risco aos quais seus ativos estão expostos e definir medidas de contingência para a continuidade dos negócios é, sem dúvida, a maior justificativa para se realizar um Plano de Continuidade de Negócios.

O Plano de Continuidade de Negócios (PCN), ou “**Business Continuity Plan (BCP)**”, pode ser compreendido como uma abordagem de planejamento cujo foco é criar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre* indo até o retorno à situação normal de funcionamento da organização dentro do contexto do negócio do qual ela faz parte.

Pela ótica do PCN, o funcionamento de uma organização empresarial deve-se a duas variáveis: os componentes e os processos. Os componentes são todas as variáveis utilizadas para realização dos processos: energia, telecomunicações, informática, infra-estrutura, pessoas. Todas elas podem ser substituídas ou restauradas, de acordo com suas características. Os processos, por sua vez, são as atividades realizadas para operar os negócios da empresa.

Todo PCN deve contemplar três aspectos fundamentais:

- Administração de Crises;
- Recuperação de Desastres (“*Disaster Recovery Plan*”);
- Continuidade Operacional.

Estes planejamentos têm como objetivo principal a formalização de ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio da organização sejam afetados, já que se isto ocorrer, pode acarretar em perdas financeiras.

Qualquer que seja o tamanho da empresa, a sua Governança deve buscar garantir que seus dados e informações estejam protegidos da melhor forma possível. Caso a empresa já tenha se decidido por terceirizar o *data center*, por exemplo, é prioritário que a empresa terceirizada tenha um plano de recuperação de desastres. Assim, ainda que ocorra qualquer incidente, a recuperação de todo patrimônio intelectual e estratégico do cliente deverá estar assegurado. Caso contrário, a gestão dos negócios passará por um pesadelo.

A decisão em contratar um serviço de (*Disaster Recovery Plan*), ou seja, um plano de recuperação de desastres não é simples. Principalmente porque demanda tempo e investimento. Por outro lado, a perda das informações, quando acontece, tem um valor incalculável. No pior dos cenários, a empresa poderá abrir falência.

Em linhas gerais o PCN analisa cada área da empresa e aponta, inclusive, os locais mais vulneráveis. É importante indicar onde é possível contar com um armazenamento seguro para instalar, se for o caso, o sistema de garantia da recuperação das informações, facilitando o backup periódico, por exemplo.



Normalmente, o PCN deve oferecer:

- Garantia de continuidade operacional de todos os processos críticos de negócios;
- Mitigação dos riscos de todas as ameaças de interrupção;
- Desenho da topologia de todos os recursos de *Disaster Recovery*;
- Previsão dos custos e investimentos para implementação do plano;
- Dimensionamento dos postos de trabalho de contingência;
- Documentação e treinamento de todos os procedimentos de contingência e continuidade;
- Recomendação do plano de testes de contingência.

Objetivo

Este curso tem como objetivo prover conhecimento das melhores práticas de Planejamento e Continuidade de Negócios, capacitando o aluno para a formulação, planejamento e execução de um plano de continuidade de negócios, aprofundando o conhecimento do aluno nas áreas de Gestão de Risco, Resposta a Incidentes e Gerenciamento de crises.

Público alvo

Gestores, consultores e profissionais nas áreas de Segurança e Tecnologia da Informação, Auditoria, Sistemas e Compliance.

Benefícios

Fornecer subsídios para os alunos realizarem uma análise de riscos e posteriormente um plano de continuidade de negócios em suas organizações, agregando todos os benefícios inerentes à sua implantação. Aprimorar o funcionamento de tarefas críticas e aumento da credibilidade da empresa por contingenciar a entrega de seus serviços. Além disso, a análise que ocorre para a implantação de um PCN pode revelar atividades ineficientes ou desnecessárias para a organização.

Ao final deste treinamento o aluno estará apto para:

- Realizar uma análise de riscos e posteriormente um plano de continuidade de negócios em suas organizações;
- Contingenciamento de tarefas críticas e planos de ações detalhados;
- Saber mais sobre atividades ineficientes ou desnecessárias para a organização.

Metodologia de ensino

Exposição interativa com apresentação de estudo de casos e exercícios práticos. O curso tem como proposta preparar o participante para estar apto estruturar e gerenciar o plano de continuidade de negócios da organização. Através de abordagem teórica e prática, com a aplicação de exemplos e debates, propicia um suporte para elucidação de dúvidas durante e após o término imediato do curso.



Pré requisitos

Não há pré-requisito específico, mas, recomenda-se que o participante tenha conhecimentos básicos sobre Processos de Negócios, Segurança da Informação e Gestão de Riscos, Tecnologia da Informação e Gestão Empresarial.

Material Didático

Apostila fornecida com os slides do curso e espaço para anotações.

Conteúdo Programático

1. Introdução à ISO 15999

Estabelece o processo, princípios e terminologia da gestão da continuidade de negócios. Fornece um sistema baseado nas boas práticas de GCN, visando alinhar a GCN à estratégia organizacional e a gestão de riscos da organização.

- O que são as normas 15999;
- Diferenças entre as normas;
- Aplicações da norma.

2. Visão Geral

Aborda conceitos de Planejamento de continuidade de negócios e como a empresa deve encarar a implantação e analisar sua viabilidade. Auxilia no planejamento, escrita e testes de um PCN, além de auxiliar na criação de um plano interino, com diversas ações para contingenciar as operações mais críticas do negócio.

- Visão Geral de PCN;
- Escrita de um PCN;
- Testes e refinamentos do PCN;
- Criação de planos interinos.



3. Gestão de risco e impacto aos negócios:

Fornece o conhecimento necessário para que seja efetuada uma análise e avaliação dos riscos dentro de uma organização, passo fundamental para determinar quais ativos e operações de negócios serão priorizados nas ações de contingência.

- Avaliação e Análise de riscos;
- Camadas de risco;
- Classificação e priorização de riscos.

4. Gerenciamento de crises e incidentes:

Estabelece os procedimentos para a criação e manutenção do centro de operações de emergência, local central para coordenar os esforços de recuperação e para gerenciar as crises decorrentes após grandes desastres. Orienta a criação de um plano para a comunicação das decisões e da liberação de informações durante crises.

- Centro de operações de emergência;
- Planejamento e implementação de um COE;
- Comunicação durante crises.

5. Resiliência e Recuperação de TIC:

Fornece o conhecimento necessário para que seja efetuada uma análise e avaliação dos riscos considerando os ativos de TIC e pessoas da organização. Considera medidas específicas de contingência e recuperação para a salvaguarda destes ativos, essenciais para a operação das empresas na atualidade.

- Redes e computadores;
- Colaboradores, Clientes e Fornecedores;
- Telecomunicações;
- Recuperação de dados e documentos vitais;
- Vírus e malware.

6. Energia e refrigeração:

Fornece diretrizes para a criação, manutenção e implantação de um plano de mitigação para serviços elétricos e os cuidados necessário para o armazenamento de mídias e equipamentos no que diz respeito à sua refrigeração correta.

- Serviços elétricos;
- Refrigeração.



7. Segurança Física e Lógica:

Aborda detalhes da segurança física e lógica dentro da organização. Detalha, entre outros, o processo de evacuação de pessoas, transporte e armazenamento de produtos perigosos e os requisitos para a operação de um Data Center contingenciado.

- Requisitos de um Data Center;
- Segurança Ambiental;
- Segurança Humana;
- Controle de Acesso;
- Segurança em Sistema Operacionais;
- Segurança em Cloud Computing.

8. Tópicos avançados em Continuidade de Negócios:

Trata de tendências e eventos recentes que mudaram a forma como as empresas devem encarar um Plano de Continuidade de Negócios. Detalha como novas tecnologias e ferramentas podem auxiliar a empresa a estarem atualizadas e preparadas para os desafios mais recentes para o contingenciamento dos negócios.

- Mapeamento via Google Earth;
- Mapeamento de Ativos;
- Terrorismo;
- Pandemias: Prevenção, alertas e ações.

Referência e Bibliografia Recomendada

- * Desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização. Conseqüentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, ao passo que para outras empresas, mesma ocorrência pode não ser caracterizada como desastre.

Disaster Recovery Handbook – Michael Wallace e Lawrence Webber –
Ed. Amacom, 2004



Faciliatador:

MARCELO LAU,

Engenheiro pela EEM, pós-graduado em administração pela FGV e mestre em ciência forense pela POLI/USP. Atuou por mais de 12 anos em instituições financeiras em áreas de segurança da informação e prevenção a fraude.

Ocupa atualmente os seguintes cargos:

Diretor Executivo na Data Security.

Country Manager na I-SEC Brasil.

Coordenador e professor no curso de Pós-Graduação no curso de Segurança da Informação no SENAC/SP.

Professor no MBA de Segurança da Informação na FATEC-SP.

Professor em Cursos de Compliance na Febraban.

Atuou por mais de 3 anos como pesquisador da POLI/USP. Dezenas de Entrevistas em Rádio, TV, Mídia Impressa e publicações online nos mais diversos canais de comunicação de cobertura regional e nacional no Brasil e Argentina como TV Globo, SBT, Valor Econômico, Estado de São Paulo, entre outros. Dentre as quais podemos acessar a seguinte, concedida à Record News:

<http://www.recordnewstv.com.br/linkbrasil/>

E outras notícias de destaque:

<http://www.usp.br/agen/bols/2006/rede1927.htm>

<http://revistaepoca.globo.com/Epoca/0,6993,EPT1111045-1881,00.html>

<http://www.datasecur.com.br/noticia.htm>

<http://g1.globo.com/Noticias/Tecnologia/0,,AA1295104-6174,00.html>

<http://www.nic.br/imprensa/clipping/2005/midia36.htm>

<http://www.internetsegura.org/noticias/noticias.asp?temp=5&id=201>

http://gsisic.serpro.gov.br/noticias/Seguranca/20061002_01

<http://www1.folha.uol.com.br/folha/informatica/ult124u21892.shtml>



*Material desenvolvido para o
treinamento ministrado por
Marcelo Lau em parceria com o
GrupoTreinar. É proibida a
cópia deste conteúdo, no todo ou
em parte, sem autorização prévia.*
