PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Leonardo Erlich

Plano de Continuidade de Negócios
Uma pesquisa exploratória na perspectiva estratégica no âmbito da segurança da informação

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas do Departamento de Administração da PUC-Rio.

Orientadora: Profa. T. Diana L. v. A. de Macedo-Soares, Ph.D.

Rio de Janeiro

Maio de 2004

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Leonardo Erlich

Plano de Continuidade de Negócios
uma pesquisa exploratória na perspectiva estratégica no âmbito da segurança da informação

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas do Departamento de Administração da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Profa. T. Diana L. v. A. de Macedo-Soares
Orientadora
Departamento de Administração, PUC-Rio

Prof. José Roberto Gomes da Silva
Departamento de Administração, PUC-Rio

Prof. Martius Vicente Rodrigues Y Rodrigues
Departamento de Administração, UFF

Prof. João Pontes Nogueira
Vice-Decano de Pós-Graduação do CCS, PUC-Rio

Rio de Janeiro, 13 de maio de 2004

Leonardo Erlich

Graduou-se em Engenharia de Computação na PUC-Rio em 2000. Foi o primeiro colocado na seleção para o Mestrado em Administração de Empresas da PUC-Rio em 2002. Possui diplomas de excelência acadêmica concedidos pela PUC-Rio em 1996 e 1997 e pela University of California em 1999 e 2000. Foi primeiro lugar no Concurso Nacional de Software, patrocinado pelo Ministério da Educação em 1998. Foi primeiro lugar nas Bolsas de Excelência Acadêmica IBM/PUC-Rio em 1998, 1999 e 2000. É Gerente de Projetos da Delage Consultoria & Sistemas. Atua há 9 anos na área de Tecnologia da Informação.

Ficha Catalográfica

Erlich, Leonardo

Plano de continuidade de negócios : uma pesquisa exploratória na perspectiva estratégica no âmbito da segurança da informação / Leonardo Erlich ; orientadora: T. Diana L. v. A. de Macedo-Soares – Rio de Janeiro : PUC, Departamento de Administração, 2004.

100 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Administração.

Inclui referências bibliográficas.

1. Administração – Teses. 2. Segurança da informação. 3. Plano de continuidade de negócios. 4. Restauração de atividades interrompidas. 5. Estratégia. I. Macedo-Soares, T. Diana L. v. A. de. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Administração. III. Título.

CDD: 658

À minha família pelo amor, apoio e confiança.

Agradecimentos

Agradeço aos colegas de turma pelos momentos de alegria e seriedade passados no Mestrado.

Agradeço aos amigos Felipe David Cohen e Luiz Mário de Farias pelo trabalho em conjunto realizado nos dois anos de Mestrado.

Agradeço a ajuda prestada no decorrer deste estudo por Gustavo Peixoto, Luiz Gutman, Marcos Sêmola, Francisco Gonçalves, Fernando Marinho, Audrey Holekamp e Rosane Peoples.

Agradeço muito às empresas e seus funcionários que colaboraram com esta pesquisa.

Faço um especial agradecimento à minha orientadora, Profa. T. Diana de Macedo Soares, por todo apoio e dedicação oferecidos na elaboração desta dissertação.

Agradeço fortemente ao IAG, à PUC-Rio, seus professores e funcionários por tudo o que me foi proporcionado.

Resumo

Erlich, Leonardo. **Plano de Continuidade de Negócios: uma pesquisa exploratória na perspectiva estratégica no âmbito da segurança da informação**. Rio de Janeiro, 2004. 100p. Dissertação de Mestrado – Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

Todos os dias, diversos sistemas são invadidos, muitas pessoas são vítimas de vírus, os mais variados dados são obtidos ilegalmente e muitas empresas ficam de uma hora para outra sem poder operar normalmente. A segurança da informação se ocupa exatamente da proteção dos recursos de informação de empresas e indivíduos. Dentre os diversos assuntos abrangidos pela segurança da informação, o plano de continuidade de negócios (PCN) é o objeto de estudo deste trabalho. Antes confinado à literatura especializada, o PCN ganhou projeção na mídia há pouco mais de dois anos, quando o mundo assistiu perplexo a queda das torres do World Trade Center. O plano de continuidade de negócios tem como objetivo principal evitar, ou reduzir sensivelmente, as perdas das empresas em casos de incidentes que afetem suas operações, além de restaurar suas atividades no espaço de tempo mais breve possível. O objetivo final deste estudo é estabelecer o retrato atual dos planos de continuidade de negócios das empresas brasileiras e propor sugestões para torná-las menos vulneráveis às ameaças internas e externas, sejam novas, antigas ou potenciais. Para atingir o objetivo proposto, foi realizada uma pesquisa com 112 empresas, levantando as percepções de seus executivos, por meio de questionários e entrevistas. A pesquisa demonstra que as empresas não estão preparadas para enfrentar incidentes que possam interromper suas atividades operacionais, estando sujeitas até mesmo à falência. Por fim, é recomendado às empresas que avaliem detalhadamente os riscos aos quais estão submetidas e as conseqüências que os incidentes podem causar. Os impactos podem justificar o investimento em um plano de continuidade de negócios.

Palavras-chave

Segurança da informação; plano de continuidade de negócios; contingência; incidentes; restauração de atividades interrompidas; estratégia.

Abstract

Erlich, Leonardo. **Business Continuity Plan: an exploratory research in the strategic perspective on information security**. Rio de Janeiro, 2004. 100p. MSc. Dissertation – Departamento de Administração, Pontifícia Universidade Católica do Rio de Janeiro.

Everyday, systems around the world are invaded by hackers, people fall victim to virus attacks, sensitive data are stolen, and firms find their operations screech to a halt. Information Security is responsible for the protection of the information resources of companies and people. The business continuity plan (BCP), one of the many issues that fall under the label of Information Security, is the object of this study. Previously confined to esoteric research journals, BCP gained significant coverage in the mainstream media in the wake of the attacks on the World Trade Center. The primary goal of a business continuity plan is the avoidance, or substantial reduction, of losses that a firm might suffer as a result of security incidents. Put simply, a BCP's goal is to keep firms operating as normal as possible during a disaster and get the firm back to standard operations as quickly as possible. The purpose of this study is to illustrate the current utilization of business continuity plans in Brazilian businesses and suggest how to make them less vulnerable to internal and external threats, regardless of whether they are old, new, or as yet undiscovered. To achieve this objective, 112 companies were selected and the executives could express their perceptions filling the surveys and through interviews. The research demonstrates that firms are not prepared to face incidents which may cause interruptions of their activities. Finally, the research recommends that companies to evaluate carefully the risks involved in their businesses and what consequences the security incidents may cause. The impacts can certainly justify the investments in Business Continuity Plan.

Keywords

Information security; business continuity plan; contingency; incidents; recovery of interrupted activities; strategy.

SUMÁRIO

LISTA DE ABREVIATURAS

AR – Análise de riscos.

B2B – Business to Business. Comércio eletrônico entre empresas.

B2C – Business to Consumer. Comércio eletrônico entre empresas e consumidores finais.

BIA – Business Impact Analysis ou Análise de Impacto no Negócio.

CERT – Computer Emergency Response Team. Centro de pesquisas em segurança na internet da Universidade de Carnegie Mellon. Site: http://www.cert.org/

CIO – Chief Information Officer. Principal responsável por tudo que concerne informação em uma empresa.

CSO – Chief Security Officer. Principal responsável pela área de segurança da informação de uma empresa.

DNS – Domain Name Server. Sistemas responsáveis por localizar fisicamente os endereços de uma rede.

GAO – Agência de Contabilidade Geral dos Estados Unidos.Site: http://www.gao.gov/

IETF – Internet Engineering Task Force. Organismo internacional que congrega profissionais e pesquisadores atuantes na internet. Site: http://www.ietf.org/

INFOSEC – Information Security Office. Departamento de segurança da informação da Texas A&M University. Site: http://infosec.tamu.edu/

IEC – International Engineering Consortium. Organização que atua na promoção do desenvolvimento de novas tecnologias na indústria da informação. Site: http://www.iec.org/

ISO – International Organization for Standardization. Organização internacional responsável por criar padrões em diversas áreas do conhecimento. Site: http://www.iso.org/

ITS – Institute for Telecommunication Sciences. Instituto de pesquisa em telecomunicações, vinculado ao Departamento de Comércio dos Estados Unidos. Site: http://www.its.bldrdoc.gov/

MCT – Ministério da Ciência e Tecnologia. Site: http://www.mct.gov.br/

OECD – Organização para Cooperação e Desenvolvimento Econômico. Site: http://www.oecd.org/

PCN – Plano de continuidade de negócios.

PRD – Plano de recuperação de desastres.

SI – Segurança da informação.

TAMU – Texas A&M University. Site: http://www.tamu.edu/

TI – Tecnologia da informação.

LISTA DE FIGURAS

LISTA DE TABELAS

Alguns homens vêem as coisas como são e dizem 'Por que?'. Eu sonho com as coisas que nunca foram e digo 'Por que não?'.

Se eu tenho uma maçã e você tem uma maçã e nós trocarmos as maçãs, então nós ainda teremos uma maçã cada. Mas se você tem uma idéia e eu tenho uma idéia e nós trocarmos as idéias, então cada um de nós terá duas idéias.

George Bernard Shaw