Estruturação do Plano de Continuidade de Negócio: um estudo de caso

Clédson de Souza Magalhães[1], Letícia Ribeiro P. de Oliveira[1], Ivo Sócrates M. de Oliveira[2]

[1]Curso de Gestão de TI – Instituto Federal do Tocantins (IFTO)
Caixa Postal 151 – 77.600-000 – Paraíso do Tocantins – TO – Brasil

[2]Eixo de Informação e Comunicação – Instituto Federal do Tocantins (IFTO) e Instituto de Ciências Matemáticas e de Computação – Universidade de São Paulo (USP)
Caixa Postal 151 – 77.600-000 – Paraíso do Tocantins – TO – Brasil.

{cledsomagalhaes, lete1002}@gmail.com, ivosocrates@usp.br

Abstract. *Attacks on information systems (IS) have increased, coinciding with the emergence of new digital pests. So it's a challenge keep the information available uninterruptedly. With the purpose of prepare the organization for a possible attack of success is that it should be adopted a Business Continuity Planning (BCP). Therefore, this paper presents an analysis of a hospital public institution, in order to diagnose the threats that surround the institution and prepares it to recover quickly in the event of materialization of risks. This research allowed the formalization of a BCP, which enables improvements relevant to the organization. Beyond the comprehension of the values attributed to the institutional business.*

Resumo. *Os ataques aos sistemas de informação (SI) têm aumentado, coincidindo com o surgimento de novas pragas digitais. Portanto, é um desafio manter as informações disponíveis initerruptamente. Com o intuito de preparar a organização para um possível ataque de sucesso é que deve ser adotado um Plano de Continuidade de Negócio (PCN). Logo, o presente trabalho apresenta uma análise de uma instituição pública hospitalar, visando diagnosticar as ameaças que cercam a instituição e prepara-la para se recuperar rapidamente em caso de ocorrência de riscos. Tal pesquisa permitiu a formalização de um PCN, que viabiliza melhorias relevantes para a organização. Além da compreensão dos valores dos negócios institucionais.*

1. Introdução

Os diversos incidentes relacionados à segurança da informação têm despertado os interesses das organizações na preparação para situações adversas. A principal ação que é gerada no campo de segurança da informação é a prevenção da ocorrência dos riscos, tal prevenção pode ser acompanhada através de um lúcido relatório de gestão de riscos.

Porém, muitos riscos, mesmo que monitorados, podem se concretizar, caso se concretize o que fazer? O Plano de Continuidade de Negócios (*Business Continuity Planning*) possui o objetivo de responder tal questionamento e representa um diagnóstico contendo um conjunto de planos alternativos de ação para eventuais incidentes previamente identificados.

Um Plano de Continuidade de Negócio (PCN) tem como finalidade garantir que os serviços, bem como as informações essenciais à sobrevivência da organização sejam devidamente reestabelecidos sem que haja o comprometimento das atividades

eliminando ou minimizando os impactos destes sobre os negócios organizacionais (SILVA, 2011, p. 23).

Segundo a ABNT ISO/IEC 27002 (2005, p. 103), o PCN deve ser implementado objetivando a minimização dos impactos a um nível aceitável sobre a organização através da combinação de ações preventivas e de recuperação de perdas de ativos da informação, caso ocorram, independentemente do motivo pelo qual estes possam ser resultantes, como por exemplo: desastres naturais, acidentes, falhas de equipamentos ou até mesmo de ações intencionais.

Fontes (2008 *apud* JUNIOR, 2008, p. 27) apresenta que muitas organizações só compreenderam a importância da continuidade de negócio após os ataques terroristas ao World Trade Center, em 11 de setembro de 2001 em Nova Iorque, pelo fato de algumas organizações simplesmente deixarem de existir por não terem um PCN. A partir de então, a pergunta deixou de ser, "Qual a probabilidade disso acontecer?" e passou a ser, "E se isso acontecer?".

Uma dúvida que permeia entre alguns gestores é a diferenciação entre Gerenciamento de Riscos e Plano de Continuidade de Negócio. No primeiro, os esforços são específicos no sentido de se minimizar o risco da ocorrência de um incidente de segurança da informação. No segundo, o incidente já aconteceu.

O plano de contingência de um PCN pode ser composto pelos seguintes planos: Plano de Administração de Crises (PAC) – define passo a passo os procedimentos a serem executados pelos diretores da organização antes, durante e depois da ocorrência do incidente, permitindo que os executivos tenham maior controle sobre a organização durante a crise (MAGALHÃES e PINHEIRO, 2007, p. 437); Plano de Recuperação de Desastres (PRD) – Segundo Junior (2008, p. 31), trata-se de diretrizes que definam como deverão ser restauradas as funcionalidades dos ativos humanos, operacionais e tecnológicos voltados para o suporte dos negócios, tendo como objetivo o reestabelecimento do ambiente e suas condições operacionais originais no menor espaço de tempo possível prevendo os impactos possíveis de ser causado pelo incidente; Plano de Continuidade Operacional (PCO) – Junior (2008, p. 30), define PCO quais os procedimentos a serem tomados a fim de reestabelecer os ativos que suportam cada atividade, reduzindo o tempo de indisponibilidade bem como os impactos aos negócios da organização como um todo.

Um PCN bem elaborado garante de forma precisa a identificação de riscos e seus prováveis impactos possibilitando a elaboração de estratégias e planos de ação que possibilitem reduzir danos ao patrimônio, ao meio-ambiente e as pessoas envolvidas. Desta forma, ele poderá contribuir para a proteção da imagem da organização uma vez que favorece a minimização de ações judiciais e ainda coordena a comunicação com os vários públicos que fazem parte dos negócios organizacionais.

Existem diversos documentos, livros e estudos voltados para o assunto, porém o que melhor dispõe de informações precisas, claras e objetivas são as normas técnicas ABNT NBR 15999-1 (2007) (código de práticas) e ABNT NBR 25999-2 (2008) (requisitos), as quais foram elaboradas como um guia para a preparação de um PCN.

É comum encontrar organizações que insistam em afirmar ser totalmente segura. Porém, "*afirmar que uma organização está 100% segura é um grande erro*". Segundo Nakamura e Geus (2007, p. 63), isto ocorre principalmente quando o assunto é segurança da informação, tendo em vista a complexidade envolvida por meio dos

aspectos humanos, tecnológicos e tantos outros, o que faz com que não possa existir um modelo de segurança que possa assegurar cobertura total à organização.

Nesse aspecto, é indispensável que o PCN aborde pelo menos três características essenciais à continuidade de negócio, que são: disponibilidade, confiabilidade e recuperação. E segundo Alves (2007, p. 35-36) ele deve conter, pelo menos, os seguintes tópicos: sumário executivo, gerenciamento dos elementos de emergência, procedimentos de resposta à emergência, documentos de suporte, identificação de desafios e priorização de atividades.

O hospital público alvo da pesquisa não possui nenhum documento formalizado para regulamentar, direcionar ou até mesmo tornar obrigatória as práticas citadas anteriormente. Tal hospital foi implantado na década de 90 em uma das cidades do estado do Tocantins, sendo um dos 17 hospitais públicos da rede SESAU (Secretaria Estadual de Saúde), tendo como objetivo o atendimento de urgência e emergência à pacientes do sistema SUS (Sistema Único de Saúde) desta localidade, bem como de várias cidades circunvizinhas, possuindo para tal cerca de 450 colaboradores e disponibilizando 90 leitos para observação e internação.

Ainda está em fase de implantação um sistema ERP (*Enterprise Resource Planning*) no local. E a infraestrutura de hardware conta com uma pequena sala, onde funciona a Central de Processamento de Dados (CPD), de onde todos os ativos de informática são monitorados e controlados e, ainda, sendo utilizada para a manutenção de equipamentos em caso de danos aos mesmos.

A infraestrutura conta com uma rede interna baseada em *Switches* 10/100/1000, que interliga cerca de 5 servidores, sendo utilizados para o sistema ERP implantado (banco de dados e aplicativos), para o controle de domínio, *firewall/proxy* e *backups* de arquivos dos mais de 50 microcomputadores espalhados nos diversos setores que compõem toda a estrutura hospitalar.

O objetivo da pesquisa é o de realizar uma análise da segurança da informação em uma instituição pública hospitalar, visando diagnosticar as ameaças que cercam a instituição, para que ao final seja apresentado um Plano de Continuidade de Negócio, alinhado as necessidades da instituição.

O presente trabalho está organizado como se segue. Na seção 2, são apresentados os materiais e métodos da pesquisa. Na seção 3, são apresentados os resultados e discussões. Finalmente, na seção 4, são apresentadas as conclusões.

2. Materiais e Métodos

A abordagem metodológica foi qualitativa, por se tratar de um estudo de caso centrado em um único caso, através do contato direto com a realidade da instituição pesquisada. E quantitativa, por selecionar um grupo específico de funcionários para auxiliar no diagnóstico do caso. A pesquisa foi realizada em 1 dos 17 hospitais públicos do estado do Tocantins da rede SESAU, entre fevereiro a julho de 2013. A estrutura de coleta de dados foi com base na análise dos documentos, processos observados, questionários, entrevistas, além de sua complementação através da realização de pesquisas bibliográficas, ou seja, por meio de um estudo sistematizado com base em materiais publicados em livros, artigos, teses, dissertações, normas técnicas e a Internet. O questionário foi aplicado aos funcionários da organização pesquisada buscando identificar as opiniões dos funcionários quanto à percepção da segurança da informação. O questionário foi aplicado a todos os funcionários da organização pesquisada, que

possuíam contato direto com a Tecnologia da Informação (TI), buscando identificar as opiniões dos funcionários. Após responder os questionários, foram realizadas entrevistas presenciais com cerca de 15% dos funcionários, ou seja, 36 funcionários, que lidam com os processos com rotinas que possuem contato direto com os recursos de TI.

3. Resultados e Discussões

Os resultados da pesquisa foram obtidos através do confronto das técnicas utilizadas na organização, para a obtenção de um lúcido diagnóstico da organização, com as práticas, normas e conhecimentos teóricos obtidos através de uma extensa revisão de literatura, que permitiu propor um PCN ajustado para a organização.

No PCN proposto para a organização foram definidas estratégias e ações a serem adotadas com o objetivo de possibilitar a redução de danos às informações, e, portanto, ao patrimônio e as pessoas envolvidas, contribuindo para a proteção da imagem organizacional. Para tanto, tomou-se como base o diagnóstico feito através do Relatório de Gestão de Riscos, que forneceu insumos relevantes para elaboração do PCN, visto haver em seu contexto a identificação das principais vulnerabilidades e ameaças que expõem aos riscos as informações manuseadas e armazenadas pelos usuários da organização.

Somente a partir da identificação dos pontos críticos, os quais são apresentados a seguir, é que se fez possível a realização de um mapeamento que permitisse a identificação dos processos, atividades e informações afetadas por estes, caso viesse a ocorrer algum incidente. A partir de levantamentos, as ameaças que potencializam riscos na instituição pesquisada, bem como o levantamento do quantitativo de ocorrência destas são apresentadas no gráfico da Figura 1.

Foram identificados cerca de 75 riscos, pelos quais estão expostos os sistemas de informação da organização pesquisada, ocorrendo com menor frequência a destruição de recursos de hardwares e com a maior frequência a interrupção de serviços, que gerou 27% das ameaças, conforme apresentado na Figura 1.

Na fase de análise e avaliação dos riscos foram avaliados os fatores: aspecto, classificação, origem, razões de ocorrência e as prováveis consequências sofridas a partir de cada ameaça identificada, considerando a possibilidade de ocorrência. Um destes fatores que se destaca é o aspecto dos riscos detectados.

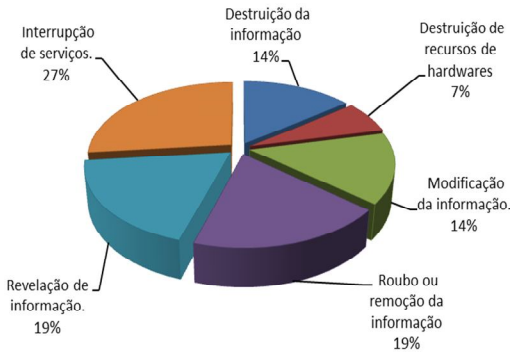

Figura 1. Gráfico das ameaças e suas respectivas ocorrências

Os aspectos dos riscos foram identificados como físicos, humanos, processuais e tecnológicos e ainda mensurados de acordo com suas ocorrências em todo o ambiente, sendo os resultados obtidos apresentados no gráfico da Figura 2.

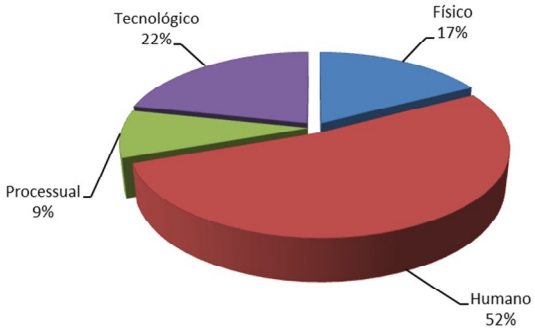

Figura 2. Gráfico dos aspectos e suas respectivas ocorrências

Para os aspectos dos riscos identificados, o processual foi o que menos se destacou obtendo uma pontuação de apenas 9% de ocorrências, porém, o risco humano obteve uma pontuação superior a 50% de ocorrências, conforme resultados apresentados na Figura 2.

No processo de elaboração da proposta levou-se em conta, desde o primeiro momento, a possibilidade de adoção e aplicação do mesmo não apenas naquela instituição, mas visando ainda que esta se estenda a qualquer outro hospital da rede SESAU do Estado do Tocantins, uma vez que todos possuem limitações e fatores idênticos ao da instituição pesquisada.

O ponto chave do processo de elaboração do PCN foi o de não subestimar quaisquer ameaças identificadas no Relatório de Gestão de Riscos. Por fim, o PCN foi construído, basicamente, através da sequência de passos apresentados a seguir: Identificação dos processos e ativos que necessitavam de proteção; Identificação dos potenciais desastres; Identificação do grau de exposição dos ativos ao desastre; Estimativa do impacto de cada desastre; Análise das medidas de proteção; e Estratégias para manter a produção perante um desastre, estratégias envolvendo comunicação, responsabilidades e papéis de controle, priorização de atividades, base de dados e base de conhecimento para suporte.

Assim sendo, foi elaborado e proposto um modelo de PCN para o hospital estudado, sendo sugerida à equipe de TI bem como à direção do mesmo a adoção de tal. Podendo o documento resultante de tal estudo, ou seja, o PCN proposto propriamente dito, ser visto na integra através da observação do Apêndice A, que se encontra na parte final deste artigo.

4. Conclusões

Um Plano de Continuidade de Negócios (PCN) não é um documento muito comum na maioria das organizações brasileiras, portanto após ocorrência de qualquer ataque é comum que os sistemas de informação fiquem dias sem operação para seus clientes, demonstrando o total despreparo da organização perante ação das ameaças.

A organização pesquisada não possuía um PCN, durante a fase de diagnóstico foi possível identificar as ameaças e, também, como a instituição estava despreparada para os mais diversos tipos de desastres, desde pequenos incidentes até os acidentes de maiores proporções.

A criação da proposta do PCN não apresentou grandes dificuldades, devido à colaboração dos funcionários e a presença de um Relatório de Gestão de Risco bem estruturado obtido na fase de diagnóstico.

Ao final da pesquisa os funcionários puderam identificar o valor que o PCN agregava. Conscientizaram também da necessidade de manter o mesmo atualizado, resguardando não só a imagem da organização, mas também, à própria imagem profissional. Possuindo rápida aderência pelos funcionários e gestores locais.

Espera-se que as propostas apresentadas continuem sendo utilizadas pela organização pesquisada para o fortalecimento institucional e que os resultados desta pesquisa possam servir de alerta para outras organizações.

Como trabalhos futuros espera-se elaboração de sistema de monitoramento para revisão do documento, reanálise perante grandes modificações no ambiente e monitoramento de melhorias e manutenção destas através da utilização de ferramentas e bibliotecas, tais como: ITIL, COBIT e outras que possam surgir.

Referências

Alves, R. M. e Zambalde, A. L. Segurança da Informação. 1ª ed. Lavras, MG: UFLA/FAEPE, 2007, 151 p.

ISO 15999-1. ABNT NBR ISO/IEC 15999-1:2007 – Gestão de continuidade de negócios – Parte 1: Código de prática. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2007.

ISO 25999-2. ABNT NBR ISO/IEC 25999-2:2008 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2008.

ISO 27002. ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

Junior, J. H. P. de P. Plano de Continuidade de negócios aplicado à segurança da informação. Porto Alegre, 2008. 60p. Monografia (Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores) – Universidade Federal do Rio Grande do Sul, 2008.

Magalhães, I. L. e Pinheiro, W. B. Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL. 1ª edição. Porto Alegre: Novatec, 2007. 672 p.

Nakamura, E. T. e Geus, P. L. Segurança de redes em ambientes cooperativos. São Paulo, SP: Novatec, 2007. 482 p.

Silva, E. Políticas de segurança e Planos de Continuidade de Negócios. Brasília, 2011. 45 p. (Pós-Graduação Latu Sensu em Segurança da Informação) – Faculdade de Tecnologia SENAC DF, Brasília, DF, 2011.

Apêndice

Apêndice A: Plano de Continuidade de Negócio Sugerido

Neste Apêndice é apresentado o PCN, propriamente dito, através da Tabela 1.

Tabela 1. Plano de Continuidade de Negócio Proposto para a Instituição Pública Hospitalar

Plano de Continuidade de Negócios - PCN			
Identificação de Incidentes		**Tratamento do Incidente**	
Incidente	**Causas**	**Plano de Continuidade (PCO)**	**Plano de Recuperação (PRD)**
Falta de energia elétrica	Externa	Acionamento imediato do gerador estacionário e rede elétrica alimentada por este até que seja reestabelecida a normalidade	Acionamento junto á prestadora de energia elétrica Solicitação do reestabelecimento dos serviços elétricos

	Interna	Uso de nobreaks nas principais máquinas, tais como switches, servidores e microcomputadores responsáveis pelos serviços crítico	Acionar o setor de manutenção elétrica do hospital para que seja feito reparos à rede elétrica do hospital, verificando o cabeamento, disjuntores, fusíveis e tomadas.
	Danos ao nobreak	Substituição do nobreak danificado por um reserva até que seja reparado o danificado	Levá-lo à manutenção para que seja feito reparos tais como: limpeza, trocas de baterias, ou conserto de placa.
Indisponibilidade dos serviços de redes	Danos a Switch	Substituição da switch danificada por um reserva até que seja realizados reparos	Levá-la à manutenção para que seja feito reparos tais como: limpeza e conserto.
	Danos ao cabeamento	Substituição do cabo danificado por outro já previamente preparado	Substituir ou reparar o cabo danificado
	Danos ao servidor de arquivos	Substituição do servidor ou dispositivo danificado e restauração do sistema e dos dados do mesmo através do último backup realizado	Encaminhar o servidor danificado para manutenção junto ao departamento específico da SESAU
	Danos ao servidor de domínio		Encaminhar o servidor danificado para manutenção junto ao departamento específico da SESAU
	Danos à placa de redes do computador	Substituição da placa danificada por uma reserva	Identificação das causas que ocasionaram o dano e correção para que não se repita
	Moderação acidental de dados	Reparo dos dados através da restauração de backup realizado anteriormente	Identificar meios pelos quais foram possíveis se fazer a moderação e tratá-los em conformidade com a Política de Segurança da Informação adotada
	Moderação proposital de dados		
	Remoção proposital de dados		Identificar meios pelos quais foram possíveis se fazer a remoção e tratá-los em conformidade com a Política de Segurança da Informação adotada
Indisponibilidade dos serviços de Internet	Danos à linha telefônica	Acionamento de um link extra diferente da tecnologia utilizada que permita a liberação de serviços nos pontos críticos que necessitam exclusivamente da Internet para realização de suas atividades até que os serviços normais sejam reestabelecidos	Acionar representante/consultor da prestadora de serviços de telecomunicação, o qual realizará o devido reparo ou troca do equipamento danificado
	Danos a algum ponto da fibra óptica		
	Danos ao Modem		
Vírus	Contaminação por vírus	Isolamento da máquina para evitar a proliferação às demais	Fazer atualização e varredura de antivírus e identificar os meios que possibilitaram a contaminação tratando-os segundo a Política de Segurança da Informação adotada.
Indisponibilidade de restauração de backups	Danos às mídias de armazenamento de backup	Dar continuidade aos serviços que não dependam das informações do backup até que estas sejam recuperadas	Fazer recuperação através de softwares e equipamentos específicos
Falha de Hardwares	Danos à impressora	Substituição da impressora danificada por uma reserva ou a configuração para impressão em uma outra impressora até que o reparo seja concluido	Acionar assistência técnica, que realizará o reparo ou troca do equipamento
	Danos ao microcomputador	Substituição da máquina danificada por uma reserva até que a danificada seja reparada	Caso não seja possível o conserto localmente, encaminhar a máquina danificada para manutenção junto ao departamento específico da SESAU
Falha de Softwares	Danos ao Sistema Operacional	Substituição da máquina danificada por uma reserva até que a danificada seja reparada	Identificar a causa do dano e fazer reparo e/ou reinstalação do Sistema Operacional danificado
	Danos Causados por atualização de softwares próprios	Reestabelecer os serviços através da restauração de backups	Identificar as causas do problema e saná-la
	Danos Causados por atualização de softwares de terceiros	Fazer isolamento do módulo danificado	Solicitar a imediata manutenção ao proprietário do software danificado
	Danos à Software utilitário	Nos casos dos departamentos que necessitem do sistema de atendimento, devem fazê-los manualmente para garantir o andamento de suas atividades até o reestabelecimento do aplicativo	Reparo através da restauração do sistema por meio de backup realizado anteriormente ou ainda a reinstalação e atualização do Software
		Casos como do eletrocardiograma e ultrassonografia que possuem seus aplicativos em máquinas específicas sem possibilidade de redundância,	

		devem ser avaliados e, se possível, encaminhados para outro hospital que realiza tais exames	
		Demais casos fazer uso de uma outra máquina ou aguardar seja feito o devido reparo	
Falta de refrigeração	Danos aos aparelhos de ar condicionado	Substituição do aparelho danificado por um reserva até que o danificado seja reparado	Acionar o setor de manutenção para que seja feito consertos ao mesmo
Danos causados às mídias de backups	Armazenamento inadequado	Fazer uso da penúltima cópia	Fazer cópias extras em mídias diferentes e armazená-las em um cofre de propriedade do hospital
Incêndio	Desconhecida	Nos casos dos departamentos que necessitem do sistema de atendimento, devem fazê-los manualmente para garantir o andamento de suas atividades até o reestabelecimento do aplicativo	Montagem de recursos de hardwares e softwares que permitam o reestabelecimento imediato dos serviços críticos da instituição
		Casos como do eletrocardiograma e ultrassonografia que possuem seus aplicativos em máquinas específicas, estas devem ser reconfiguradas para trabalho autônomo e liberado uso	
		Demais casos aguardar seja feito o devido reparo	