UNIVERSIDADE FEDERAL DE SANTA CATARINA

PLANEJAMENTO DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS USANDO A METODOLOGIA OCTAVE NA ANÁLISE DE RISCOS

DENISE SANTIN EBONE

FLORIANÓPOLIS – SC

2011/2

UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

PLANEJAMENTO DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS USANDO A METODOLOGIA OCTAVE NA ANÁLISE DE RISCOS

DENISE SANTIN EBONE

Orientadora:
Professora Dra. CARLA MERKLE WESTPHALL

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação.

Florianópolis – SC

DENISE SANTIN EBONE

PLANEJAMENTO DA GESTÃO DE CONTINUIDADE DE NEGÓCIOS USANDO A METODOLOGIA OCTAVE NA ANÁLISE DE RISCOS

Trabalho de conclusão de curso apresentado como parte dos requisitos para obtenção do grau de Bacharel em Sistemas de Informação.

Orientadora:

_____

Professora Dra. Carla Merkle Westphall

Banca Examinadora:

_____

Professora Dr. Carlos Becker Westphall

_____

Professor Dr. Mário Antônio Ribeiro Dantas

Florianópolis, __ de novembro de 2011.

AGRADECIMENTOS

Aos meus pais pela compreensão incentivo e apoio em todos os momentos da minha vida.

À professora Carla Merkle Westphall pela competência na orientação deste trabalho.

Aos meus amigos pela compreensão nos momentos em que não pude estar presente.

“No one plans to fail; they just simply fail to plan”

Disaster Recovery Journal

SUMÁRIO

1. Introdução 12

1.1. Objetivos 13
1.2. Objetivos específicos 13
1.3. Justificativa 13
1.4. Delimitação do Escopo 14
1.5. Estrutura do Trabalho 14

2. Segurança da Informação 15

2.1. Conceitos Básicos 17
2.2. Principais Normas sobre Segurança da Informação 19

2.2.1. ABNT NBR ISO/IEC 27001:2006 19
2.2.2. ABNT NBR ISO/IEC 27002:2005 20
2.2.3. ABNT NBR ISO/IEC 27005:2008 22

2.3. Política de Segurança 23

2.3.1. Desenvolvimento da Política de Segurança 25

3. Plano de Continuidade do Negócio 26

3.1. Principais Normas sobre Continuidade de Negócio 28

3.1.1. BS25999-1:2006 28
3.1.2. BS25999-2:2007 30

3.2. Desenvolvimento do PCN 31

3.2.1. Planejamento 33

3.2.1.1. Análise de Impacto 33
3.2.1.2. Análise de Riscos 34
3.2.1.3. Método OCTAVE 37

3.2.2. Implementação 39

3.2.2.1. Plano de Continuidade Operacional 40
3.2.2.2. Plano de Contingência 41
3.2.2.3. Plano de Recuperação de Desastres 41

3.2.2.4. Testes 43

3.2.3. Monitoração 43

3.2.4. Manutenção 44

3.3. Trabalhos Relacionados 45

4. Estudo de Caso 47

4.1. Descrição da organização 47
4.2. Escopo da Análise 47
4.3. Análise do Ambiente da GERED 49

4.3.1. Fase 1 - Construção de um perfil de ameaça 49

4.3.2. Fase 2 - Identificação das vulnerabilidades 51

4.3.3. Fase 3 - Desenvolvimento de estratégias de segurança 60

5. Considerações Finais 62

5.1. Trabalhos Futuros 63

6. Referências Bibliográficas 64
Apêndice A 68

LISTA DE FIGURAS

Figura 1. Propriedades de Segurança da Informação 16
Figura 2. Processo de Gestão de Riscos 22
Figura 3. Política de segurança de informações e seus relacionamentos 24
Figura 4. Fases do desenvolvimento de uma política 26
Figura 5. Ciclo de vida da GNC. 29
Figura 6. Modelo PDCA aplicado ao ciclo GCN. 31
Figura 7. Fases OCTAVE 38
Figura 8. Planos de Continuidade. 39
Figura 9. Organograma da GERED 48

LISTA DE TABELAS

Tabela 1. Modelo PDCA aplicado aos processos do SGSI. 20
Tabela 2. Estrutura do desenvolvimento de um PCN. 32
Tabela 3. Classificação de relevância dos processos da organização 34
Tabela 4. Critérios para definir cada risco. 36
Tabela 5. Escala de valores das ameaças. 37
Tabela 6. Quantitativos vs Qualitativos 37
Tabela 7. Escala de Impacto 51
Tabela 8. Processos da GERED 51
Tabela 9. Escala de Probabilidade de uma ameaça ocorrer 52
Tabela 10. Política da Segurança da Informação 52
Tabela 11. Segurança Física e do Ambiente 53
Tabela 12. Segurança de Equipamentos 54
Tabela 13. Proteção contra códigos maliciosos 56
Tabela 14. Cópias de Segurança 56
Tabela 15. Controle de Acesso à Rede 57
Tabela 16. Controle de Acesso os Sistema Operacional 58
Tabela 17. Tabela de Risco 59
Tabela 18. Nível de Risco da GERED 60

LISTA DE ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas
BIA	*Business Impact Analysis*
BSI	*British Standards Institution*
CPD	Centro de Processamento de Dados
GCN	Gestão da Continuidade de Negócio
GERED	Gerência de Redes e Banco de Dados
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
MPSC	Ministério Público de Santa Catarina
OCTAVE	*Operationally - Critical - Threat - Asset - Vulnerability – Evaluation*
PCN	Plano de Continuidade de Negócio
PDCA	*Plan - Do - Check – Act*
SGCN	Sistema de Gestão de Continuidade de Negócio
VPN	*Virtual Private Network*

RESUMO

As organizações dependem cada vez mais de seus processos informatizados já que praticamente todas as informações são capturadas, armazenadas e acessadas em formato digital. Infelizmente essa dependência também expõe as organizações a uma variedade de novas ameaças que podem afetar a continuidade do negócio. Apesar disso, as organizações falham na prevenção dos riscos, agindo apenas quando o desastre ocorre. Em vista disso, um plano de continuidade de negócios (PCN) é um conjunto de procedimentos que visa garantir a continuidade dos processos vitais de uma organização. Esse plano permite que em caso de desastre ou paralisação dos sistemas de informação os processos continuam funcionando sem perda de informação. Este trabalho utiliza as normas de segurança da informação e as normas de continuidade de negócio para estruturar as etapas de desenvolvimento de um PCN, após foi realizado um estudo de caso utilizando o método OCTAVE para analisar os riscos da Gerência de Redes de Banco de Dados (GERED) do Ministério Público de Santa Catarina (MPSC) que é responsável pela administração e segurança da rede de computadores de todas as promotorias de justiça do estado de Santa Catarina, portanto a GERED é responsável por garantir a disponibilidade e a integridade das informações do MPSC. Dessa forma, o objetivo desta monografia é pesquisar as principais referências sofre segurança da informação e analisar o ambiente da GERED usando o método OCTAVE realizando a primeira etapa do desenvolvimento de um PCN.

Palavras chave: plano de continuidade de negócios, segurança da informação, OCTAVE, ISO 27002, BS 25999.

ABSCTRACT

Organizations increasingly rely on their computerized processes as virtually all information is captured is captured, stored and accessed in digital format. Unfortunately, this dependence also exposes organizations to a variety of new threats that may affect business continuity. Nevertheless, organizations fail to prevent risks, acting only when the disaster strikes. As a result, a business continuity plan (BCP) is a set of procedures aimed at ensuring the continuity of the vital processes of an organization. This plan allows in case of disaster or interruption of information systems, processes continue to function without loss of information. This paper uses the standards of information security and business continuity for structuring the development stages of a BCP, after was made a case study using the OCTAVE method to analyze the risks of Gerência de Redes e Banco de Dados (GERED) of the Ministério Público de Santa Catarina (MPSC) which is responsible for administration and security of the computer network of all prosecution offices of the state of Santa Catarina, so GERED is responsible for ensuring the availability and integrity of information of MPSC. Thus, the purpose of this monograph is to research the main references of information security and analyze the GERED's environment using the OCTAVE's method performing the first step in the development of an BCP.

Keywords: business continuity plan, information security, OCTAVE, ISO 27002, BS 25999.

1. Introdução

A sobrevivência de uma organização depende do funcionamento de seus processos e da integridade das suas informações. Se houver uma interrupção dos processos mesmo que temporária pode causar danos irreparáveis na organização.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação (ABNT NBR ISO/IEC 27002:2005, p. ix).

Desastres acontecem com muito mais frequência do que as pessoas imaginam. Os grandes desastres que acabam nos noticiários não são frequentes, mas há uma infinidade de incidentes menores, que podem fazer tanto dano quanto. Exemplos: falha nos computadores, vazamento de água em arquivos de papel, falha de energia, etc. Não é uma questão de se vai acontecer alguma coisa, mas quando isso vai acontecer (WALLACE; WEBBER, 2004, p. xii).

A Gerência de Redes e Banco de Dados (GERED) do Ministério Público de Santa Catarina (MPSC) administra a rede das promotorias de Justiça do estado de Santa Catarina, portanto a GERED é responsável por garantir a disponibilidade e a integridade das informações do MPSC. O blecaute na ilha de Florianópolis em 2003 que durou 55 horas é um exemplo de um desastre que paralisou as operações da GERED e por consequência afetou as promotorias de justiça do estado.

O Plano de Continuidade de Negócios (PCN) visa prevenir a ocorrência de desastres, minimizar o impacto se um desastre acontecer e viabilizar a rápida ativação de processos alternativos na indisponibilidade dos processos usuais. Desta forma o plano visa minimizar o impacto de desastres eventuais sobre os negócios (SALDANHA, 2000, p. 16).

Este trabalho apresenta um estudo de caso, o qual analisa o ambiente da GERED usando o método OCTAVE realizando a primeira etapa do desenvolvimento de um PCN. São utilizadas também as principais normas de segurança da informação ISO 27000 e as normas de continuidade de negócio BS 25999.

1.1. Objetivos

O objetivo geral desse projeto é analisar o ambiente da GERED utilizando o método OCTAVE realizando a primeira etapa do desenvolvimento de um PCN.

1.2. Objetivos específicos

Neste projeto, espera-se atingir os seguintes objetivos específicos:

- Realizar um estudo sobre as principais bibliografias sobre segurança da informação e sobre continuidade de negócios;
- Apresentar as etapas de desenvolvimento de um PCN;
- Aplicar o método OCTAVE na GERED.

1.3. Justificativa

Apesar da crescente dependência do MPSC com os seus sistemas de informação, existe pouca preocupação e investimento para garantir a continuidade do negócio.

Frequentemente ocorre algum tipo de interrupção no fluxo da informação do MPSC, muitos colaboradores são vitimas de vírus, ocorrem falhas de atualização e de backup, ocasionando a paralisação da organização de uma hora para outra.

O PCN é fundamental para a sobrevivência de uma organização, faz parte desse plano os procedimentos necessários para garantir a proteção e integridade dos sistemas de informação de uma organização.

O presente trabalho se justifica por analisar o ambiente da GERED utilizando o método OCTAVE e as principais normas da segurança da informação e continuidade de negócios para garantir a disponibilidade dos sistemas e integridade dos dados do MPSC.

1.4. Delimitação do Escopo

O escopo deste trabalho consiste na utilização do método OCTAVE para analisar os riscos presentes no ambiente da GERED. Não faz parte do escopo deste trabalho o desenvolvimento do PCN.

1.5. Estrutura do Trabalho

O presente trabalho está dividido em seis capítulos, nos quais são abordados diversos aspectos relacionados à continuidade de negócios.

- Capítulo 1 – é apresentada uma introdução sobre o assunto a ser tratado, os objetivos e as justificativas.
- Capítulo 2 – é apresentado o referencial teórico que inclui conceitos básicos sobre segurança da informação, principais normas e política de segurança.
- Capítulo 3 – é apresentada a definição de continuidade de negócios, principais normas e o desenvolvimento de um PCN.
- Capítulo 4 – é apresentado o estudo de caso realizado na GERED.
- Capítulo 5 – são apresentadas as considerações finais e os trabalhos futuros.

2. Segurança da Informação

A informação é um dado com um valor atribuído e com uma interpretação lógica ou natural dada ao dado por quem usa a informação (REZENDE; ABREU, 2008, p. 36). Pode-se dizer então que a informação é todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou indivíduo.

As redes de computadores mudaram as formas de como se usa os sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas, assim como os riscos à privacidade e integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (LAUREANO, 2004, p. 11).

Desse modo a informação é um ativo da organização, ou seja, um bem que deve ser protegido do mesmo modo que os bens físicos, tendo em vista sua importância para a própria existência da organização (CAMPOS, 2006, p. 4). Sendo a informação o principal patrimônio de uma empresa consequentemente a informação necessita ser protegida.

Sêmola (2003, p.43) define a Segurança da Informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

O governo federal definiu a Segurança da Informação no decreto Nº 3.505 (Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, 2000) como a

> proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Segundo Ferreira e Araújo (2008, p. 73) a função básica da área de Segurança da Informação "é proteger o ativo de informação, minimizando os riscos a níveis aceitáveis".

Como ficou estabelecido nas definições apresentadas no texto, à informação é fundamental para o negócio[1] da organização e a segurança da mesma pode garantir a sobrevivência da organização.

Um sistema de segurança da informação baseia-se em três propriedades básicas (Figura 1): a confidencialidade, a integridade e a disponibilidade (LANDWEHR, 2006, p. 2).

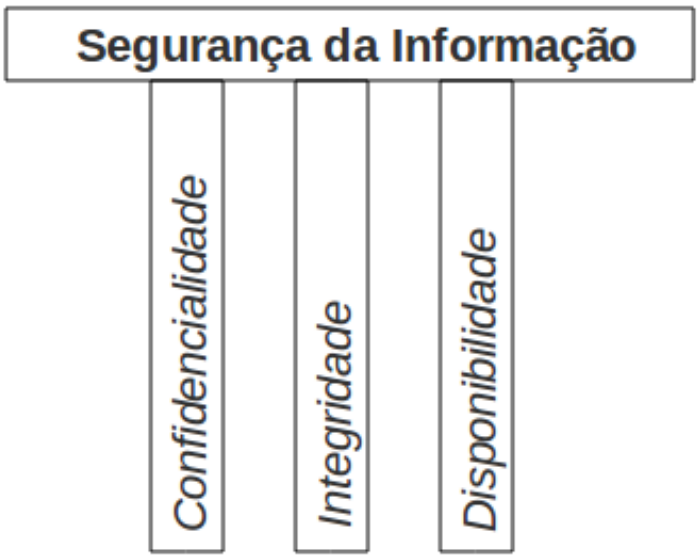

Figura 1. Propriedades de Segurança da Informação (CAMPOS, 2006, p.5).

Campos (2006, p. 6) define cada um dessas propriedades:

> O principio da confidencialidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.
>
> O principio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto confiável.
>
> O princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Ao analisar essas propriedades, observa-se que a confidencialidade oferece suporte a prevenção de acesso não autorizado às informações. Já a integridade previne a modificação não autorizada de informações. E a disponibilidade provê suporte a um acesso prontamente disponível as informações. Isto implica em dados e sistemas disponíveis e confiáveis.

[1] A referência a "negócio" deve ser interpretada, de modo geral, tendo em vista as atividades que são essenciais aos objetivos de existência da organização (ABNT NBR ISO/IEC 27001:2006, p. 1).

Em adição, Ferreira e Araújo (2008, p. 45) dividem a segurança em 4 grandes aspectos:

> Segurança computacional: conceitos e técnicas utilizados para proteger o ambiente informatizado contra eventos inesperados que possam causar qualquer prejuízo.
>
> Segurança lógica: prevenção contra acesso não autorizado.
>
> Segurança física: procedimentos e recursos para prevenir acesso não autorizado, dano e interferência nas informações e instalações físicas da organização;
>
> Continuidade de negócios: estrutura de procedimentos para reduzir, a um nível aceitável, o risco de interrupção ocasionada por desastres ou falhas por meio da combinação de ações de prevenção e recuperação.

A definição de Segurança da informação que será utilizada neste trabalho será do autor Sêmola (2003), por afirmar que os ativos de informação devem ser protegidos utilizando as três propriedades da segurança: confidencialidade, integridade e disponibilidade.

2.1. Conceitos Básicos

Para facilitar a compreensão do texto, serão definidos alguns termos utilizados nos demais capítulos.

Informação: "representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da organização" (SÊMOLA, 2003, p. 39).

A informação deve ser classificada conforme o seu grau de importância dentro da organização. Ferreira e Araújo (2008, p. 81) classificam a informação em 3 níveis:

> Informação pública: são aquelas que não necessitam de sigilo algum, podendo ter livre acesso para os colaboradores. São informações que, se forem divulgadas fora da organização, não trarão impactos para os negócios.
>
> Informação interna: o acesso externo às informações deve ser evitado. Entretanto, se esses dados se tornarem públicos, as consequências não serão críticas.
>
> Informação confidencial: as informações desta classe devem ser confidenciais dentro da organização e protegidas do acesso externo. Se alguns desses dados forem acessados por pessoas não autorizadas, as operações da organização poderão ser comprometidas, causando perdas financeiras e de competitividade.

Ativo: “qualquer coisa que tenha valor para a organização” (ABNT NBR ISO/IEC 27001:2006). Ativos da informação seriam todos os elementos usados para armazenar, transmitir e processar a informação.

Vulnerabilidade: são as fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais das três propriedades de segurança da informação (CAMPOS 2006, p. 11). As vulnerabilidades estão presentes em todos os ambientes da organização e se apresentam nas mais diversas áreas, como mostrado nos exemplos a seguir:

- Computadores sem proteção contra vírus e spywares;
- Rede local acessível por senha padrão ou pública;
- Acesso à informação por terceiros e prestadores de serviços;
- Ausência de mecanismos contra incêndio.

Ameaça: “causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização” (ABNT NBR ISO/IEC 27002:2005). É um agente externo ao ativo de informação que explora as vulnerabilidades desse ativo.

Sêmola (2003, p. 47) divide as ameaças em 3 grupos:

> Naturais – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.
>
> Involuntárias – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causados por acidentes, erros, falta de energia, etc.
>
> Voluntárias – Ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Incidente: é a ocorrência de um evento que possa causar interrupções nos processos do negócio em consequência da violação de um ou mais das três propriedades de segurança da informação (CAMPOS, 2006, p. 14).

Risco: “combinação da probabilidade de um evento e de suas consequências” (ABNT ISO/IEC Guia 73:2009). É o potencial de um incidente acontecer.

Impacto: “são as potenciais consequências que um incidente possa causar a organização” (CAMPOS, 2006, p.15). Tem que ser levado em consideração que o impacto de um mesmo incidente de segurança da informação pode ser diferente para organizações diferentes, dependendo de suas estratégias de negócio, dos processos afetados pelo incidente e da capacidade de resposta ao incidente de cada organização.

2.2. Principais Normas sobre Segurança da Informação

Uma das primeiras normas definidas sobre segurança da informação foi a BS7799 – *Code of Practice for Information Security Management*, criada pela *British Standard Institute* (BSI). Ela divide-se em duas partes: as recomendações de como implementar a Segurança da informação, chamada de BS7799:1995-1, e o conjunto de controles que devem ser implementados para garantir que as recomendações sejam seguidas, chamada de BS7799:1998-2 (INFORMATION SECURITY, 2002).

A ISO 17799 é a versão internacional equivalente a BS7799, homologada pela *Internacional Standardization Organization* (ISO) em 2000 (INFORMATION SECURITY, 2002). Em 2005, a ISO decidiu reunir as diversas normas de segurança da informação criando a série de normas ISO 27000. As principais normas sobre segurança da informação utilizadas neste trabalho são apresentadas a seguir.

2.2.1. ABNT NBR ISO/IEC 27001:2006

A norma ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos – é a tradução da norma internacional ISO/IEC 27001:2005.

Esta norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) documentado dentro do contexto dos riscos de negócio globais da organização (ANBT ISO/IEC 27001:2006, p.1).

Esta norma adota o modelo conhecido como “Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar todos os processos do SGSI. A Tabela 1 mostra os processos do modelo PDCA.

Tabela 1. Modelo PDCA aplicado aos processos do SGSI (ANBT ISO/IEC 27001:2006, p. vi).

PLAN (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (Agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

O modelo PDCA pode ser utilizado para melhorar os estágios de qualquer sistema de gestão, usado de forma contínua para o gerenciamento dos processos de uma organização.

2.2.2. ABNT NBR ISO/IEC 27002:2005

A norma ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação - é a tradução da norma internacional ISO/IEC 27002:2005.

Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização (ABNT NBR ISO/IEC 27002:2005, p.1).

Esta norma está estruturada em 11 seções de controles de segurança da informação, a seção com o controle que trata da Gestão da Continuidade de Negócios (GCN) é o A.14. O objetivo deste controle é "não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso" (ABNT ISO/IEC 27002:2005, p. 103). O controle A.14 possui cinco controles de segundo nível apresentados a seguir:

A.14.1.1 – Incluindo segurança da informação no processo de gestão de continuidade de negócio: convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.

A.14.1.2 – Continuidade de negócios e análise/avaliação de risco: convém identificar os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as consequências para a segurança de informação.

A.14.1.3 – Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação: convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.

A.14.1.4 – Estrutura do plano de continuidade do negócio: convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

A.14.1.5 – Testes, manutenção e reavaliação dos planos de continuidade do negócio: convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

2.2.3. ABNT NBR ISO/IEC 27005:2008

A norma ABNT NBR ISO/IEC 27005:2008 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança de informação – é a tradução da norma internacional ISO/IEC 27005:2008.

Esta norma fornece as diretrizes para o processo de gestão de riscos de segurança da informação. Esta norma foi elaborada para facilitar a implementação satisfatória da segurança da informação tendo como base a gestão de riscos (ABNT NBR ISO/IEC 27005:2008, p. 1).

De acordo com a norma, o processo de gestão de riscos de um sistema de informação é composto pelas seguintes atividades (Figura 2): análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos, a comunicação de riscos e o monitoramento e análise crítica de riscos.

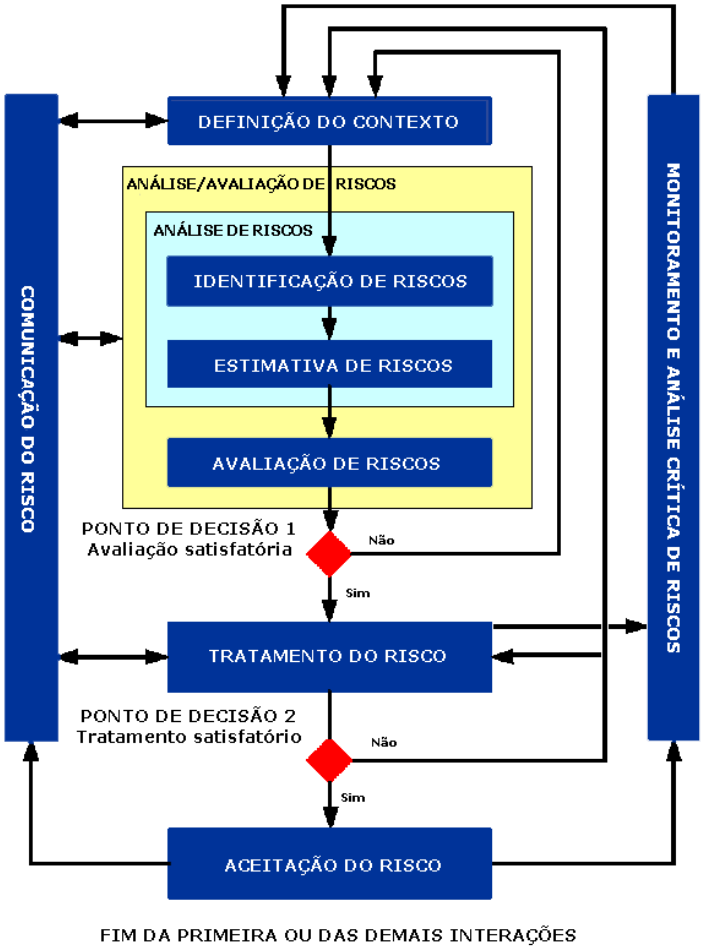

Figura 2. Processo de Gestão de Riscos (ABNT NBR ISO/IEC 27005:2008, p. 5).

Como pode ser observado na figura 2, primeiramente é estabelecido o contexto, nesta etapa são coletadas todas as informações relevantes sobre a organização.

Na fase análise/avaliação estão incluídas as tarefas de identificação dos riscos e análise da sua probabilidade e dos eventuais efeitos que os riscos possam ter. Posteriormente, o risco é avaliado e caso se considere não aceitável, deverá ser mitigado que consiste no tratamento do risco.

A atividade de aceitação do risco tem de assegurar que os riscos residuais[2] sejam explicitamente aceitos pelos gestores da organização. É importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados.

2.3. Política de Segurança

Para proteger a organização contra ameaças a segurança da informação é necessário escrever uma boa política de segurança.

Ferreira e Araújo (2008, p.36) definem a política de segurança como um "conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação devendo ser formalizada e divulgada a todos os usuários que fazem o uso dos ativos da informação".

Campos (2006, p. 99) define a política como um "conjunto de regras que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação".

A política de segurança provê uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ABNT NBR ISO/IEC 27002:2005).

Ferreira e Araújo (2008, p.41) definem que a especificação da política deve ser

> breve, utilizar palavras simples e formalizar o que é esperado dos funcionários da organização. Deve fornecer aos leitores informações suficientes para saber se os procedimentos descritos na política são aplicáveis a eles ou não. Deve descrever sua finalidade, por exemplo, se é orientada a pessoas, departamentos, equipamentos, etc.

[2] Risco residual é o risco que uma organização enfrenta se optar por não aplicar qualquer tipo de proteção (HARRIS, 2008, p. 106).

Ao atribuir direitos e responsabilidades a serem seguidos pelos usuários que lidam com os ativos de informação, os usuários passam a saber quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham.

Nenhuma política de segurança pode ser estabelecida sem considerar as penalidades e os processos disciplinares. A política como lei, deve indicar alguma forma de punição para aqueles que a desrespeitarem ou, do contrário, ela simplesmente será ignorada (CAMPOS, 2006, p.111).

Uma vez que a política seja de conhecimento de todos, não será admissível que as pessoas aleguem o desconhecimento das regras nela estabelecidas a fim de se livrar da responsabilidade sobre as violações cometidas (FERREIRA; ARAÚJO, 2008, p.154)

Por fim, segundo Sêmola (2006, p. 87) "a política de segurança deve ser personalizada", já que a política deve ir além dos aspectos relacionados com sistemas de informação ou recursos computacionais, a política de segurança deve estar integrada com as políticas institucionais da organização, as metas de negócio e ao planejamento estratégico da empresa (Figura 3).

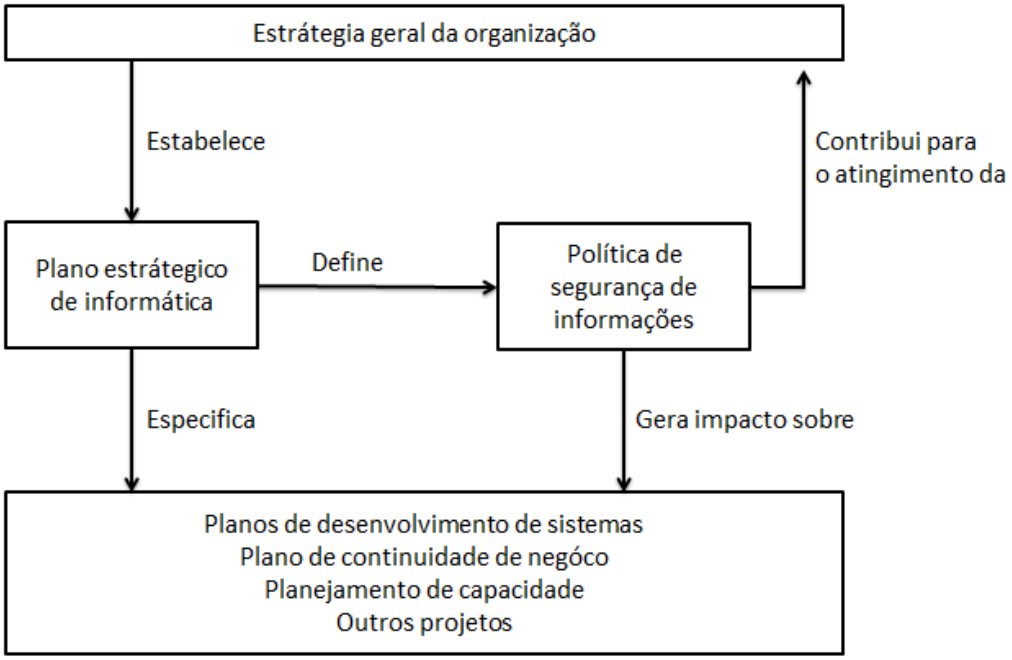

Figura 3. Política de segurança de informações e seus relacionamentos (DIAS, 2000, p.49).

2.3.1. Desenvolvimento da Política de Segurança

O desenvolvimento de uma política de segurança, segundo Ferreira e Araújo (2008, p.86) deve capacitar a organização com instrumentos jurídicos, normativos e processuais. Esses instrumentos devem abranger as estruturas físicas, tecnológicas e administrativas, de forma a garantir a confidencialidade, integridade e disponibilidade das informações corporativas.

Desta forma, a política assume uma grande abrangência e, por conta disso, é subdividida em três blocos: diretrizes, normas e procedimentos, sendo destinados respectivamente, às camadas estratégicas, tática e operacional.

Diretrizes: possuem papel estratégico e devem expressar a importância que a organização dá aos ativos de informação, além de comunicar aos funcionários seus valores (FERREIRA; ARAÚJO, 2008, p.86).

Exemplo: toda a informação confidencial recebida, produzida, armazenada, distribuída e descartada em resultado das operações da organização, deve ser protegida.

Normas: com caráter tático, as normas são o segundo nível da política, detalhando situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações (SÊMOLA, 2003, p. 105).

Exemplo: toda a mensagem confidencial enviada do correio eletrônico deve ser criptografada.

Procedimentos: está presente na política em maior quantidade por seu perfil operacional. Os procedimentos descrevem detalhadamente sobre como atingir os resultados esperados (FERREIRA; ARAÚJO, 2008, p.86).

Exemplo: toda mensagem confidencial enviada do correio eletrônico deve ser criptografada seguindo os seguintes passos:

1. Na mensagem, na guia Mensagem, no grupo Opções, clique no botão Criptografar o Conteúdo e os Anexos da Mensagem.
2. Redija sua mensagem e envie-a.

Segundo Ferreira e Araújo (2008, p. 36) o desenvolvimento e a implementação das diretrizes, normas e procedimentos da política de segurança da informação podem ser divididos nas 4 fases apresentadas a seguir (Figura 4):

Fases	Descrição
Fase I	Levantamento de Informações
Fases II	Desenvolvimento do Conteúdo da Política e Normas de Segurança
Fases III	Elaboração dos Procedimentos de Segurança da Informação
Fases IV	Revisão, Aprovação e Implantação das Políticas, Normas e Procedimentos de Segurança da Informação

Figura 4. Fases do desenvolvimento de uma política (FERREIRA; ARAÚJO, 2008, p. 38).

Na primeira fase o levantamento de requisitos pode ser feito através de questionários, onde serão obtidas informações sobre o ambiente de negócios e o ambiente tecnológico da organização. Na segunda fase serão atribuídas as regras e responsabilidades para os usuários da informação e serão definidos os critérios para classificação das informações. Na terceira fase serão formalizados os procedimentos de segurança da informação para integrá-los às políticas da organização. Na quarta fase serão revisadas e implantadas as diretrizes, normas e procedimentos de segurança da informação.

Segundo Ferreira e Araújo (2008, p. 111) a política de segurança também deve "assegurar a existência de um plano de continuidade capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, incluindo também as atividades de teste e manutenção do plano".

3. Plano de Continuidade do Negócio

O plano de continuidade de negócios (PCN) tem como objetivo possibilitar o funcionamento da organização em situações de contingência onde há interrupção dos ativos de informação.

Sêmola (2003, p. 98) define o plano como "garantir a continuidade de processos e informações vitais à sobrevivência da empresa, em menor espaço de tempo possível, com o objetivo de minimizar os impactos no negócio".

Wallace e Webber (2004, p. xi) definem que “este é o plano que permite que o seu negócio continue funcionando, mesmo a um nível reduzido durante e imediatamente após emergência”.

Dias (2000, p.111) afirma que uma das metas do plano de continuidade é “minimizar o tempo de parada dos sistemas para reduzir os impactos nos negócios e proteger as informações institucionais”.

Segundo Saldanha (2000, p. 18) o plano de continuidade é composto pelo

> conjunto de atividades que deverão ser adotadas antes, durante e depois da ocorrência de um desastre. Estas ações têm que ser definidas e documentadas com antecedência e devem implicar no menor número possível de tomadas de decisão no decorrer e após o desastre.

O PCN deve ser elaborado com o claro objetivo de contingenciar situações de incidentes de segurança que não puderam ser evitados (SÊMOLA, 2003, p. 98).

O benefício real de um PCN é forçar a organização a olhar para seus pontos fracos e fortalecê-los antes que uma tragédia ocorra. A análise exigida no desenvolvimento do plano irá ajudar a organização a compreender melhor o seu negócio, e quase sempre leva a descoberta de atividades ineficientes ou desnecessárias dentro da organização (WALLACE; WEBBER, 2004, p. xvi).

É importante entender que o PCN precisa se tornar um processo da organização, e não uma ação imediata e temporária. Precisa ser contínua, evoluir com a organização e estar sob responsabilidade de alguém. Em outras palavras, a continuidade do negócio precisa ser gerida como todo e qualquer processo organizacional (CAMPOS, 2006, p.170).

Um PCN deve resultar num conjunto de documentos onde estarão descritas as ações que deverão ser tomadas em caso de indisponibilidade dos ativos de informação.

Para construir o plano, as seguintes perguntas serão feitas repetidamente (WALLACE; WEBBER, 2004, p. xv).

- Quais são os meus ativos críticos?
- Quais são os riscos para esses ativos?
- Como posso reduzir a probabilidade da ocorrência de uma ameaça?
- Como posso minimizar o dano, se é inevitável?
- O que a equipe faz quando isso acontece?

Dessa forma, o PCN não deixa de ser um gerenciamento de risco e, portanto, também procura avaliar e controlar os riscos existentes na organização. No entanto, o foco principal é a elaboração de planos de como proceder diante dos riscos que foram aceitos.

3.1. Principais Normas sobre Continuidade de Negócio

A continuidade de negócios possui como principal referência à série normativa BS25999, elaborada pelo BSI (BS 25999 BUSINESS CONTINUITY), que é segmentada em duas normas: BS25999-1:2006 - *Business Continuity Management – Code of Practice* e BS25999-2:2007 *Specification for Business Continuity Management*. Estas normas foram lançadas no Brasil em 2008 respectivamente como ABNT ISO/IEC NBR 15999-1 e ANBT ISO/IEC NBR 15999-2.

3.1.1. BS25999-1:2006

A norma BS25999-1:2006 - Gestão de Continuidade de Negócios – Código de Prática, estabelece o processo, os princípios e a terminologia da Gestão da Continuidade de Negócios (GCN). E tem como objetivo fornecer uma base conceitual para entender, desenvolver e implementar a continuidade de negócios em uma organização.

Esta norma apresenta o ciclo de vida da GCN (Figura 5), este ciclo é composto por uma serie de atividades de continuidade de negócios que cobrem todos os aspectos da GCN.

Figura 5. Ciclo de vida da GNC (BS25999-1:2006, p. 9).

O ciclo de vida da gestão da continuidade é composto por seis elementos, descritos a seguir:

a) Gestão do Programa de GCN

- Atribuição de responsabilidades;
- Implementação da continuidade do negócio na organização;
- Gestão contínua da continuidade do negócio.

b) Entendendo a Organização

- Identificar os objetivos da organização,
- Identificar as atividades, os ativos, e os recursos;
- Análise de impacto no negócio (BIA);
- Análise de riscos.

c) Determinando as estratégias de continuidade de negócios

- Escolha das estratégias de continuidade de negócio.
- Implementar soluções adequadas para minimizar a ocorrência de um incidente e/ou reduzir os efeitos de um potencial incidente;

d) Desenvolvendo e implementando uma resposta de GCN

- Desenvolvimento e implementação dos planos de continuidade conforme a análise e identificação dos riscos.
- Definir a responsabilidade das pessoas envolvidas durante e após o incidente, assim como os seus papéis;

e) Testando, mantendo e analisando criticamente os preparativos de GCN

- Elaborar um programa de testes de forma a garantir e validar os preparativos para a GCN.
- Analisar criticamente todos os procedimentos de continuidade.

f) Incluindo a GCN na cultura da organização

- Desenvolvimento de um programa para incorporar a cultura do GCN na organização.
- Treinamento das pessoas relacionadas à GCN.

3.1.2. BS25999-2:2007

A norma BS 25999-2:2007 - Especificação da Gestão de Continuidade de Negócios, especifica os requisitos para estabelecer e gerenciar um Sistema de Gestão de Continuidade de Negócios (SGCN) definido por um programa de GCN.

Esta norma utilizado o modelo PDCA (Figura 6) da norma ISO 27001:2005 aplicado a todas as partes do ciclo de vida da GCN, de forma a garantir que a continuidade do negócio esteja devidamente gerenciada e aprimorada numa organização. Dessa forma, o modelo de SGCN é um instrumento para a melhoria do ciclo de vida da GCN.

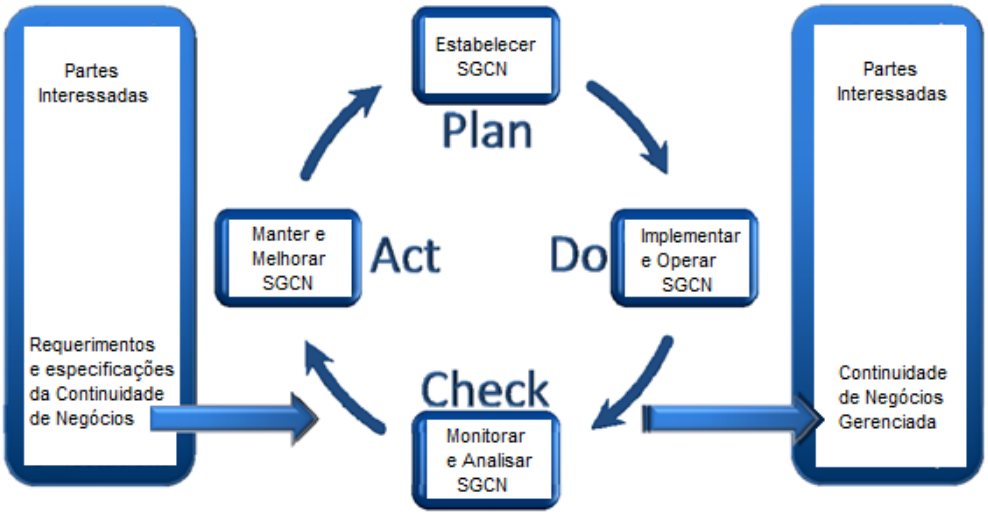

Figura 6. Modelo PDCA aplicado ao ciclo GCN (BS25999-2:2006, p. v).

3.2. Desenvolvimento do PCN

O desenvolvimento do PCN segue o modelo PDCA da norma BS25999-2:2007 que consistente na melhoria contínua, evidenciando as etapas de Planejamento, Implementação, Monitoração e Manutenção. Segue também o ciclo de vida da GCN da norma BS25999-1 e os controles de continuidade de negócio da norma ISO 27002:2005. A Tabela 2 mostra como o desenvolvimento do PCN pode ser estruturado conforme as normas.

Tabela 2. Estrutura do desenvolvimento de um PCN.

BS25999-2:2007 PDCA SGCN	**BS25999-1:2006 GCN**	**ISO 27002:2005 Controle A.14**
PLAN Planejamento	a) Gestão do Programa de GCN b) Entendendo a Organização	A.14.1.1 – Incluindo segurança da informação no processo de gestão de continuidade de negócio A.14.1.2 – Continuidade de negócios e análise/avaliação de risco
DO Implementação	c) Determinando as estratégias de continuidade de negócios d) Desenvolvendo e implementando uma resposta de GCN e) Testando, mantendo e analisando criticamente os preparativos de GCN	A.14.1.3 – Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação A.14.1.4 – Estrutura do plano de continuidade do negócio A.14.1.5 – Testes, manutenção e reavaliação dos planos de continuidade do negócio
CHECK Monitoração	e) Testando, mantendo e analisando criticamente os preparativos de GCN	A.14.1.5 – Testes, manutenção e reavaliação dos planos de continuidade do negócio
ACT Manutenção	e) Testando, mantendo e analisando criticamente os preparativos de GCN f) Incluindo a GCN na cultura da organização	A.14.1.5 – Testes, manutenção e reavaliação dos planos de continuidade do negócio

3.2.1. Planejamento

O planejamento possibilita a identificação das reais necessidades da organização e de cada processo crítico. O planejamento visa definir o escopo e a estratégia de estruturação do PCN. Para estas definições devem ser avaliados o ambiente interno, o ambiente externo, as possíveis perdas em função do impacto de um desastre, as demandas dos serviços críticos e as restrições financeiras (SALDANHA, 2000, p. 36).

3.2.1.1. Análise de Impacto

Essa primeira etapa tem por objetivo levantar o grau de relevância entre os processos ou atividades que fazem parte do escopo do plano. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que suportam cada um deles, para então apurar os impactos que poderiam ser gerados com a sua paralisação total ou parcial (SÊMOLA, 2003, p.100).

O impacto dos riscos varia bastante de acordo com o que acontece com quem e quando. Sua reação a um desastre que paralisa toda a empresa será bastante diferente do que o inconveniente de uma única pessoa (WALLACE; WEBBER, 2004, p. 34).

Segundo Campos (2006, p. 56) o impacto deve ser analisado quanto

> ao prejuízo potencial que pode ser gerado para a organização, levando-se em conta o prejuízo causado pela própria ocorrência do incidente, o tempo e o custo necessário para a reabilitação do ativo, prejuízos à imagem da organização, prejuízos a terceiros nos casos de roubo de informações de clientes ou fornecedores, entre outros.

Para essa etapa pode ser utilizada a análise de impacto aos negócios (BIA - *Business Impact Analysis*), ele serve para identificar os impactos de um possível desastre sobre as operações de uma organização (Tabela 3). Quanto maior o impacto decorrente de uma paralisação de um processo, mais crítico será este processo (SALDANHA, 2000, p.38).

Tabela 3. Classificação de relevância dos processos da organização (SÊMOLA, 2003, p. 100).

Processos de Negócio Escala	PN1	PN2	PN3	PNn
Não considerável				
Relevante	X			
Importante			X	
Crítico		X		
Vital				

De posse desta análise, torna-se possível definir as prioridades de contingência, os níveis de tolerância à indisponibilidade de cada processo e, ainda, agrupar os ativos em função de sua natureza e relação de dependência que mantêm com os processos. A partir de então, tem-se uma visão da funcionalidade dos processos, restando definir as ameaças que se quer contingenciar. A escolha das ameaças a se considerar para cada processo está diretamente ligada à probabilidade de um incidente (SÊMOLA, 2003, p.100).

A análise de impacto indicará os processos críticos que deverão ser alvo prioritário da análise de risco (SALDANHA, 2000, p. 51). Para cada processo crítico deverão ser identificados os ativos que poderão ser alvo de uma ameaça. Os ativos que forem considerados vitais para a continuidade dos processos da organização deverão ser alvo da análise de riscos.

3.2.1.2. Análise de Riscos

Segundo Campos (2006, p.44) a análise de risco possibilita identificar o grau de proteção que os ativos de informação de cada processo da organização precisam, permitindo assim proporcionar a proteção em grau adequado para o negócio.

Wallace e Webber (2004, p. 32) definem a análise de riscos como um processo que identifica as prováveis ameaças para o seu negócio.

Dias (2000, p. 54) define o objetivo da análise de riscos como

> medir ameaças, vulnerabilidades e impactos em um determinado ambiente, de forma a proporcionar a adoção de medidas apropriadas tanto às necessidades de negócio da instituição, ao proteger seus recursos de informação, como aos usuários que precisam utilizar esses recursos, levando em consideração justificativas de custos, nível de proteção e facilidade de uso.

A identificação das potenciais ameaças existentes exige cuidadosa análise e conhecimento não só do negócio em questão, mas também do meio ambiente no qual ele se encontra (SALDANHA, 2000, p.55).

Existem, fundamentalmente, duas linhas metodológicas para orientar uma análise de riscos: quantitativa e qualitativa (HARRIS, 2008, p. 92).

Quantitativa: a análise quantitativa tenta atribuir números reais e significativos para todos os elementos do processo de análise de risco (valor dos ativos, frequência das ameaças, danos causados por impactos, etc.). Cada elemento dentro da análise é quantificado e entra em equações para determinar os riscos totais e residuais.

As principais etapas para fazer uma análise quantitativa são mostradas a seguir:

Etapa 1: Atribuir valor aos ativos

- Qual é o valor deste ativo para a organização?
- Quanto custa para manter este ativo?
- Quanto lucro este ativo gera para a organização?
- Quanto custaria para recriar ou recuperar este ativo?
- Qual o dano para a organização se o ativo for comprometido?

Etapa 2: Estimar a perda potencial por ameaça

- Que dano a ameaça pode causar e quanto isso custaria?
- Qual é o custo de recuperação desta ameaça?
- Qual é a expectativa de perda para cada ativo?

Etapa 3: Faça uma análise das ameaças.

- Coletar informações sobre a probabilidade de cada ameaça acontecer.

- Calcular a taxa anual de ocorrência da ameaça, que é quantas vezes a ameaça pode ocorrer em um período de 12 meses.

Etapa 4: Obter o potencial de perda anual por ameaça

- Calcular a expectativa de perda anual por ameaça usando as informações calculadas nas primeiras três etapas.
- Escolha medidas corretivas para neutralizar cada ameaça.
- Realizar análise/custo benefício nas medidas corretivas identificadas.

Etapa 5: Reduzir, Transferir, Evitar, ou Aceitar o risco (Tabela 4)

Tabela 4. Critérios para definir cada risco.

Evitar	Não adotar tecnologias ou processos que ofereçam riscos ao negócio.
Reduzir	Implementação de controles para diminuir as vulnerabilidades dos ativos que suportam os processos.
Transferir	Há casos em que é recomendado transferir o risco para outra pessoa ou organização. Uma forma de fazer isso é contratar um seguro que garanta a cobertura dos prejuízos envolvidos em um incidente de segurança da informação.
Aceitar	Riscos podem ser aceitos se for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a organização.

Qualitativa: não atribui números e valores aos ativos e perdas. Em vez disso, o método qualitativo percorre diferentes cenários de risco e classifica a gravidade das ameaças e a validade das medidas corretivas com base em opiniões. Técnicas de análise qualitativa incluem melhores práticas, intuição e experiência. Exemplos de técnicas qualitativas para coletar dados são brainstorming, storyboards, grupos de discussão, pesquisas, questionários, e entrevistas.

As ameaças com alta probabilidade de concretização podem ser classificadas segundo Saldanha (2000, p. 60) de acordo com uma escala de valores (Tabela 5).

Tabela 5. Escala de valores das ameaças.

Não Aplicável	A ameaça não é relevante para o caso em questão.
Baixa	Não há registro desta ameaça ter se concretizado no passado e não há indicativos de que ela venha a se concretizar.
Média	Há registros no passado de ocorrências da ameaça, e ela pode vir a se concretizar novamente.
Alta	Existe uma significativa frequência de ocorrência da ameaça e ela tem boa possibilidade de voltar a ocorrer.

Enfim, as análises quantitativa e qualitativa têm suas vantagens e desvantagens e cada uma se aplica melhor a determinadas situações do que a outra. Cabe à organização determinar qual método que melhor se aplica a sua situação. A Tabela 6 pode ser usada para ter uma visão melhor da diferença entre os métodos.

Tabela 6. Quantitativos vs Qualitativos (CAMPOS, 2006, p.45).

Quantitativo	Qualitativos
Resultados baseados em valores objetivos	Resultados baseados em valores subjetivos
Cálculos complexos	Cálculos simples
Valores financeiros são atribuídos ao risco	Não há valoração do risco
Grande tempo e esforço são necessários para atribuir as taxas de risco.	Menor trabalho para atribuir as taxas de risco
Facilita o cálculo de custo/benefício	Dificulta o cálculo de custo/benefício

3.2.1.3. Método OCTAVE

Uma das principais metodologias de análise de risco que foca na segurança da informação é a OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), desenvolvida pela Universidade de Carnegie Mellon em 2001. As fases da OCTAVE podem ser vistas na Figura 7.

Figura 7. Fases OCTAVE

As fases são definidas por Dorofee e Alberts (2001, p. 20) responsáveis pelo desenvolvimento desse método.

Fase 1. Construção de um perfil de ameaça: onde se deve conhecer a estrutura da rede e organização das informações. O que é importante para organização (informações relacionadas com os ativos) e o que atualmente está sendo feito para proteger esses ativos. O resultado são os ativos mais importantes para a organização (ativos críticos).

Fase 2. Identificação das vulnerabilidades: nesta fase deve-se avaliar a infraestrutura e levantar pontos de vulnerabilidades. Identificar os pontos fracos que podem levar a ação não autorizada contra ativos críticos.

Fase 3. Desenvolvimento de estratégias de segurança: nesta fase é desenvolvido o plano de ação para a análise de risco. Definição das estratégias de proteção para a organização e planos de mitigação para enfrentar os riscos que podem atingir os ativos críticos.

3.2.2. Implementação

Uma vez que foram compreendidos os riscos que envolvem os ativos de informação é possível então decidir o que fazer em relação a esse risco identificado (CAMPOS, 2006, p. 68). Nesta etapa os planos de continuidade são desenvolvidos e implementados.

O PCN tem um alto nível de complexidade, podendo assumir diversas formas em função do objeto a ser contingenciado e a abrangência de sua atuação. Diferente do que muitos imaginam uma empresa não possuirá um plano único, mas diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos (SÊMOLA, 2003, p. 99).

Sêmola (2003, p. 99) define que o PCN é composto por 3 planos: o Plano de Continuidade Operacional, o Plano de Contingência e o Plano de Recuperação de Desastres (Figura 8).

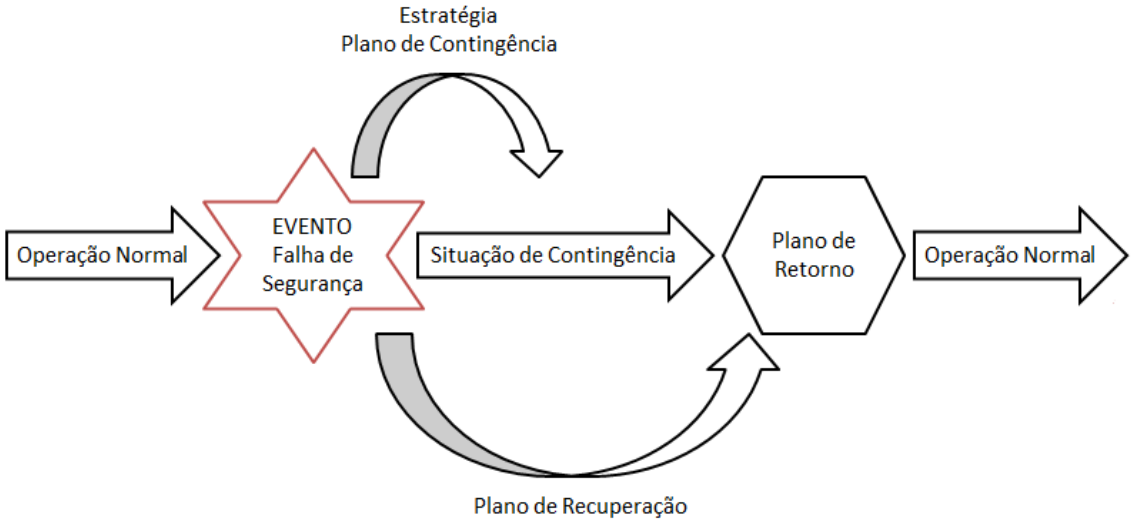

Figura 8. Planos de Continuidade (SÊMOLA, 2003, p. 99).

3.2.2.1. Plano de Continuidade Operacional

O plano de continuidade operacional é um conjunto de ações previamente documentadas que tem como objetivo minimizar o impacto de um desastre nas funções vitais de uma organização.

Um dos seus objetivos é diminuir a quantidade de ações improvisadas e a necessidade de tomada de decisões em circunstâncias extremamente adversas. As ações do plano têm como função reduzir ao máximo as consequências de um desastre (SALDANHA, 2000, p. 101).

Para cada tipo de desastre deve ser preparado um plano de continuidade operacional, o plano é acionado apenas na eminência do desastre. Para estruturar o plano 4 etapas podem ser seguidas (SALDANHA, 2000, p.106):

Etapa 1 – Cada desastre selecionado deverá ser analisado de acordo com a viabilidade de ser contemplando com um plano de continuidade operacional. O principal fator a ser considerado é a viabilidade do mesmo ser acionado em tempo útil.

Etapa 2 – Identificado o desastre, deve ser elaborado um resumo de ações a serem adotadas. Com base neste resumo devem ser identificadas as equipes operacionais que deverão executar as atividades do plano.

Etapa 3 – Cada equipe deve desenvolver os procedimentos emergenciais de acordo com o desastre especificado.

Etapa 4 – Cada equipe deverá descrever seus procedimentos conforme o padrão definido pelo gestor do PCN.

Seguindo essas etapas o documento final deve ser composto por procedimentos que tenham instruções objetivas, onde estejam identificados:

- O objeto da ação;
- Os responsáveis pela sua execução;
- Os recursos necessários para sua realização;
- O tempo necessário para sua concepção.

3.2.2.2. Plano de Contingência

O plano de contingência visa "estabelecer formas alternativas de operação dos processos críticos que viabilizem a continuidade produtiva das operações e serviços vitais impactados por um desastre, ainda que com uma degradação de seu desempenho" (SALDANHA, 2000, p. 115).

Um plano de contingência mais elaborado geralmente envolve uma localidade alternativa que possui uma infraestrutura menor ou semelhante ao site principal, esse plano tem um custo elevado porque envolve duplicar os processos críticos da organização. Os locais alternativos podem ser exclusivos da organização ou poderão ser terceirizados.

Os tipos de localidades alternativas segundo Ferreira (2003, p. 107) podem ser categorizados conforme sua prontidão para atender a uma situação emergencial.

Cold Site: ambiente com recursos mínimos de infraestrutura e telecomunicações. Recomendado para situações com grande tolerância de indisponibilidade. A organização fica responsável pela disponibilização de equipamentos, hardware e software, bem como instalação e configuração.

Warm Site: parcialmente equipado com alguns recursos de hardware, software e equipamentos de telecomunicações. Esta localidade deverá estar preparada para receber os recursos necessários, bem como os profissionais que realização suas configurações e operações.

Hot Site: completamente equipado, possui disponibilidade de recursos, como hardware, software, equipamentos de telecomunicações, segurança física e ambiental. Existem profissionais alocados nesta localidade, eles deverão estar sempre de prontidão para ativar os recursos necessários, assim que forem notificados que o plano de contingência foi ativado.

3.2.2.3. Plano de Recuperação de Desastres

O plano de recuperação de desastres é o conjunto de procedimentos a serem executados de forma a recuperar as condições de normalidade operacional

(SALDANHA, 2000, p. 116). Podem ser ações que visam o restabelecimento das condições existentes antes do desastre ou serem ações de reconstrução que necessariamente não estarão reconstruindo uma situação existente e sim uma nova situação.

Sêmola (2003, p.104) define que o plano de recuperação de desastres tem o propósito de criar um projeto de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

Um plano de recuperação de desastres tem o objetivo de realizar a completa recuperação dos sistemas e infraestrutura dentro de um prazo definido e com perda mínima de dados (NICKOLETT; SCHMIDT, 2001, p. 2).

A recuperação de desastres originalmente era baseada na realização de cópias de segurança, ou seja, eram feitos backups dos principais dados da organização. O objetivo era minimizar o período de tempo em que as bases de dados ficavam fora de operação.

Atualmente, o planejamento para recuperação de desastre compreende um conjunto mais amplo de objetivos: objetiva a recuperação de funções críticas da empresa ao invés de somente a restauração das operações de processamento de dados. Isto ocorre devido às mudanças no ambiente em que os planos para recuperação de desastre são desenvolvidos. A descentralização das funções de processamento de dados, o aumento dos computadores conectados através de uma rede, são apenas algumas das mudanças ambientais que forçaram alterações contextuais no campo do planejamento para recuperação de desastre (TOIGO, 1990, p. 83).

As atividades da fase de recuperação focam nas medidas para reparar danos nos sistemas originais e restaurar as atividades operacionais, novamente, na localidade principal. No final desta fase, os sistemas deverão estar adequadamente recuperados e realizando suas devidas funções (FERREIRA, 2003, p. 118).

Dias (2000, p.118) diz que para garantir a efetiva restauração dos sistemas e que todos os componentes necessários para restaurá-los estão sendo recuperados corretamente, todos os procedimentos de recuperação precisam ser testados periodicamente.

3.2.2.4. Testes

Um plano de continuidade não pode ser considerado completo sem que o mesmo tenha sido testado (SALDANHA, 2000, p. 191). Antes do teste o plano não passa de um conjunto de documentos. O teste é a única maneira de garantir a efetividade dos planos de continuidade.

Dias (2000, p. 127) define 3 metodologias de teste:

Teste Integral: situação bem próxima da realidade. Envolve a transferência de pessoas e dos processos críticos para um local alternativo. Esta metodologia de teste é provavelmente a mais eficaz e certamente mais cara.

Teste parcial: são testados apenas algumas partes do plano, determinadas atividades ou aplicativos. Seus custos são baixos, mas sua abrangência é menor.

Teste simulado: envolve a representação da situação emergencial. Os colaboradores praticam as atividades que devem desempenhar no caso de um desastre.

Após o teste será realizada uma avaliação, onde deverão ser registrados todos os resultados e problemas ocorridos durante os testes.

3.2.3. Monitoração

A organização deve, em intervalos regulares, analisar criticamente o PCN, de forma a assegurar sua permanente atualização e efetividade. A análise deve verificar se o PCN está em conformidade com todas as leis, normas, estratégias, estruturas e diretrizes da organização (BS 25999-1:2006, p. 38).

A análise pode assumir a forma de auditorias internas ou externas, ou auto-avaliações. Uma auditoria ou auto-avaliação do PCN da organização deve verificar se:

- todos os processos críticos da organização foram identificados e incluídos no PCN;
- as soluções do PCN são eficazes, atualizadas e apropriadas para o nível de risco enfrentado pelo organização;
- a manutenção e os testes do PCN foram efetivamente implementadas;

- a organização tem um programa de treinamento e conscientização do PCN;
- os procedimentos do PCN foram comunicadas para todas as pessoas-chave e que elas compreenderam seus papéis e responsabilidades.

Ao ser verificado que houve mudanças nas atividades do negócio e que essas mudanças ainda não estão contempladas no PCN, então deve ser feito uma atualização do plano.

3.2.4. Manutenção

A maioria dos processos e procedimentos de um negócio muda com frequência, tornando o PCN um produto altamente perecível. Para mantê-lo em perfeitas condições é necessário que se esteja atento a todas as mudanças internas e externas e que estas mudanças sejam refletidas no PCN através de adequações e aperfeiçoamentos (SALDANHA, 2000, p. 201).

Os planos atualizados devem ser distribuídos e reforçados por análises críticas periódicas do plano como um todo (ABNT ISO/IEC 27002:2005, p. 119). As manutenções devem ser realizadas quando:

- Identificar durante as auditorias que são necessárias ações corretivas de modo a eliminar as causas da não-conformidade com os procedimentos de continuidade de negócios.
- Mudanças nas atividades de negócios que ainda não tenham sido contempladas nos planos de continuidade de negócio.

Após a atualização do plano é necessária que os planos atualizados sejam documentados e distribuídos para a organização.

É essencial realizar o treinamento dos colaboradores, esse treinamento começa com a distribuição do PCN para cada um dos componentes. Cada colaborador, especialmente aqueles com responsabilidades específicas em caso de desastre, deve estar consciente de suas responsabilidades durante uma emergência, sabendo exatamente que atividades desempenhar.

Normalmente o treinamento envolve teoria e prática de procedimentos de emergência e recuperação. As normas técnicas da ABNT determinam que esse tipo de treinamento seja feito periodicamente para relembrar os funcionários mais antigos e educar os recém-contratados (DIAS, 2000, p. 126).

3.3. Trabalhos Relacionados

Como trabalhos relacionados à continuidade de negócios, podem ser citados:

- Em "Plano de continuidade de negócios para a empresa Alfa: uma proposta com base na NBR 15999, no ITIL e no COBIT" (SILVEIRA, 2009), Patrícia Marques da Silveira desenvolveu um trabalho semelhante em seu trabalho de conclusão de curso. O objetivo principal do trabalho é definir um Plano de Continuidade de Negócio baseado nas práticas mais utilizadas pelas organizações, que permita à empresa qualificar as suas operações e atender as expectativas dos clientes internos e externos. O trabalho apresenta uma revisão da literatura sobre a importância da segurança da informação, gerenciamento da continuidade de negócios segundo o ITIL e o COBIT. Foi realizado um estudo exploratório de natureza qualitativa, através de entrevistas semiestruturadas e observações. Posteriormente foi realizada análise das informações coletadas e apresentada as propostas para a continuidade de negócio. Como conclusão do trabalho foi destacada a necessidade de difundir na organização a importância de se ter um plano de continuidade de negócio, fazendo com que a empresa adote as práticas da gestão de continuidade de negócio para gerenciar de forma eficiente e eficaz o PCN. Verificou-se que a NBR15999 apresentou as informações sobre a gestão da continuidade de negócios até os detalhamentos sobre as informações contidas nos planos e controles que devem ser adotados. O COBIT teve sua contribuição nos requisitos essenciais para a elaboração e controle do PCN, e o ITIL apresentou de uma forma geral os objetivos do PCN e a sua contribuição para organização.

- Em "Gestão da continuidade de negócio: o caso de uma empresa de

telecomunicações" (SOUZA, 2010), Diego Muller Cardeal de Souza desenvolveu um trabalho semelhante em sua dissertação de mestrado. O objetivo principal do trabalho é desenvolver uma proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios numa empresa do setor de telecomunicações. O trabalho apresenta uma revisão da literatura de gerenciamento de riscos e gestão de continuidade de negócios inseridos no contexto da governança corporativa. Foi realizado um estudo de caso em uma empresa de telecomunicações e feita à análise crítica da estrutura de gestão de continuidade de negócios da empresa, com o objetivo de identificar as principais dificuldades observadas na implantação dessa estrutura bem como as principais não-conformidades do modelo com relação às práticas previstas na norma BS25999-1. Posteriormente foi desenvolvida a proposta de estrutura de apoio à implantação de um sistema de gestão de continuidade de negócios na empresa. Como conclusão do trabalho foi destacada a estrutura de apoio proposta através de um diagrama segmentado em quatro etapas principais e seus elementos de implantação. Em casa elemento foram apresentadas as sugestões para a implantação de um sistema de gestão de continuidade de negócios aplicado às particularidades do cenário da companhia.

- No artigo "Projetando uma Política de Segurança de acordo com a BS 7799 usando a metodologia OCTAVE" (PAULINA; MAREK, 2007), os autores descrevem como a metodologia OCTAVE melhora a tomada de decisão no processo de proteção da informação. Este artigo ilustra as etapas do método incluindo exemplos e referências as normas de segurança.

4. Estudo de Caso

A seguir será apresentado o estudo de caso sobre a aplicação do método OCTAVE na primeira etapa de desenvolvimento de um plano de continuidade de negócios, e os principais resultados obtidos.

4.1. Descrição da organização

O Ministério Público é uma instituição independente do Poder Judiciário, Executivo e Legislativo. Sua função é fiscalizar o cumprimento da lei, defendendo os direitos da sociedade. Para isso defende as causas que são de interesse coletivo, e não aquelas que possam beneficiar apenas uma pessoa ou um grupo isolado de pessoas (Guia do Ministério Público de Santa Catarina, 2009).

O negócio do Ministério Público de Santa Catarina, segundo estabelecido no seu planejamento estratégico, é o de "promover a defesa dos direitos da população", e a missão é a de "promover a defesa dos direitos da população, visando à redução dos conflitos e à construção da paz social" (Plano Geral de Atuação, 2011).

Com esse entendimento, o Ministério Público definiu como visão estratégica "ser uma instituição que sirva de referencial pelos padrões de eficiência e regularidade na geração de resultados úteis à sociedade e na garantia dos direitos do cidadão" (Plano Geral de Atuação, 2011).

4.2. Escopo da Análise

O escopo da análise escolhido foi os processos da Gerência de Redes e Banco de Dados (GERED) por ser o centro das atividades que envolvem a segurança da informação do MPSC.

As atividades da GERED estão subordinadas à Procuradoria-Geral de Justiça e à Secretaria-Geral do Ministério Público. A Figura 9 mostra a hierarquia à qual a GERED está subordinada.

Figura 9. Organograma da GERED (www.mp.sc.gov.br)

O estudo de caso foi executado na GERED com o objetivo de analisar o ambiente através do método OCTAVE realizando a primeira etapa do desenvolvimento de um Plano de Continuidade de Negócio (PCN), para assim garantir a integridade e disponibilidade dos dados do MPSC. Neste trabalho foi realizada uma pesquisa do tipo exploratório com uma abordagem qualitativa.

De acordo com Ciribelli (2003, p. 54) a pesquisa exploratória "proporciona maiores informações sobre o tema que o pesquisador pretende abordar; auxilia-o a delimitá-lo; ajuda-o a definir objetivos e a formular suas hipóteses de trabalho e também a descobrir uma forma original de desenvolver seu assunto". A pesquisa exploratória pode ser feita através de documentos, bibliografias, entrevistas, observações, estudo de caso e visitas.

O estudo de caso (SCHOLZ; TIETJE, 2002, p. 9) é uma investigação empírica que investiga um problema. A compreensão do problema e sua solução requerem a integração de variáveis mutuamente dependentes ou elementos de prova que possam ser recolhidos pelo menos parcialmente, através da observação pessoal.

A abordagem qualitativa segundo Reis (2010 p. 67) tem como objetivo "interpretar e dar significados aos fenômenos analisados sem empregar os métodos e as técnicas estatísticas como base do processo de análise de um problema". Isso significa que nessa abordagem de pesquisa os resultados não são traduzidos em números, unidades de medidas, como é o caso da abordagem quantitativa.

4.3. Análise do Ambiente da GERED

Para realizar a primeira etapa do desenvolvimento de um PCN foi utilizado o método OCTAVE, por ser um método de análise voltado para área de tecnologia da informação. A seguir são apresentadas as fases do método e os resultados da análise.

4.3.1. Fase 1 - Construção de um perfil de ameaça

Nesta fase, são analisados os principais recursos da GERED e os requisitos de segurança necessários para proteger esses recursos. Foram entrevistados os colaboradores da GERED para determinar a importância da proteção dos dados, bem como descrever os impactos potenciais que poderia surgir em caso de perda de dados vitais.

A GERED é reponsável por várias atividades dentro da estrutura do MPSC, as principais são:

- Agilizar a troca de informações entre Procuradoria Geral de Justiça e as promotorias de justiça espalhadas por 120 cidades do estado de Santa Catariana.
- Segurança, por se tratar de uma rede onde trafegam dados sigilosos;
- Disponibilidade dos serviços;

- Integridade dos dados;
- Dar suporte na infraestrutura de rede das promotorias de justiça.
- Prover serviços como: correio eletrônico, diretório de arquivos, hospedagem de site da instituição, backup dos arquivos.

Os recursos da GERED considerados mais importantes para organização são classificados nas seguintes categorias:

- Pessoas: inclui suas habilidades, treinamento, conhecimento e experiencias.
- Hardware/Software: inclui os dispositivos de tecnologia da informação e os serviços.
  - 16 servidores;
  - 2 storages;
  - 2.600 estações de trabalho;
  - 520 notebooks;
  - 68 máquinas virtuais;
  - 86 serviços;
  - 1800 caixas de e-mail.
- Informações: documentos armazenados em papel ou digitalemente.
- Redes: dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos (dados, impressoras, entre outros), mediante meios de acesso, protocolos e requisitos de segurança.

A organização irá sofrer um grande impacto se os requisitos de segurança desses ativos são violados. Para analisar os impactos é necessário realizar a atividade de Análise de Impacto (BIA) através de um questionário aplicado aos principais colaboradores da GERED (Apêndice A). O objetivo foi o levantamento do impacto que uma interrupção nos processos críticos pode causar a organização. Para classificar os impactos foram usadas as informações da Tabela 7:

Tabela 7. Escala de Impacto

Escala	Grau do Impacto
1	Irrelevante
2	Pequeno
3	Moderado
4	Grande
5	Catastrófico

A partir do questionário é possível ter uma visão dos principais processos da organização e o impacto que a sua perda ou indisponibilidade causaria a organização. Na Tabela 8 foram listados os processos identificados, o grau de impacto e os períodos de interrupção identificados pelos entrevistados.

Tabela 8. Processos da GERED

Processos	RTO	RPO	Impacto
Servidor de arquivos	1 Hora	1 hora	Catastrófico
Serviço de e-mail	1 Hora	1 hora	Catastrófico
Backup dos dados	1 Hora	1 hora	Grande
Portal / Intranet	2 Horas	2 horas	Moderado
Serviço de internet	4 Horas	2 horas	Moderado
Geração de Login e E-mail	4 Horas	2 horas	Pequeno
Monitoramento da rede	4 Horas	4 horas	Irrelevante
RTO (Recovery Time Objective): período de tempo máximo que o negócio pode suportar sem a solução tecnológica. **RPO** (Recovery Point Objective): quantidade aceitável de perda de dados medidos em tempo.			

Todos os entrevistados classificaram como catastrófico a perda do servidor de arquivos e do serviço de e-mail, já que a indisponibilidade desses serviços impossibilitaria a continuidade de negócios da organização.

4.3.2. Fase 2 - Identificação das vulnerabilidades

Nessa fase é desenvolvida a atividade de Análise de Risco, com o objetivo de analisar as vulnerabilidades existentes nos processos críticos. Foi realizado um

levantamento dos possíveis riscos que pudessem vir a ocorrer e cada risco foi avaliado segundo a Tabela 9:

Tabela 9. Escala de Probabilidade de uma ameaça ocorrer

Escala	Probabilidade da ameaça ocorrer
0,10	Improvável
0,25	Baixa
0,50	Média
0,75	Provável
0,95	Alta

Foram feitas perguntas ao gerente da GERED sobre os controles existentes no ambiente segundo alguns pontos de auditoria recomendados pela norma ISO 27002. Esses controles foram escolhidos por serem os principais controles necessários para garantir a segurança da informação na GERED. A partir das respostas foi feita a análise da probabilidade das possíveis ameaças a continuidade dos negócios.

I. Política de Segurança da Informação

O primeiro controle analisado refere-se à política de segurança (Tabela 10) que é um fator crítico para o sucesso da implementação da segurança da informação dentro de uma organização.

Tabela 10. Política da Segurança da Informação

A.5.1.1	Documento da política de segurança da informação	Controle Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

Pergunta 1: Que tipo de controles existem na organização para orientar e apoiar a direção para a segurança da informação de acordo com os requisitos de negócios e com as leis e regulamentações relevantes?

Resposta: Não há um documento que formalize a política de segurança da GERED. Existem algumas regras de segurança que são comunicadas aos colaboradores, mas não a uma verificação do cumprimento das regras.

Análise: Não existe uma política de segurança, não ha uma formalização das regras, por esse motivo os colaborados não sabem dos seus direitos e deveres em relação à segurança da informação, portanto a probabilidade da ameaça de uso inadequado dos ativos de informação é considerada provável.

II. Segurança Física e do Ambiente

O segundo controle analisado refere-se à segurança física e do ambiente (Tabela 11), esse controle tem por objetivo verificar se as instalações de processamento das informações críticas ou sensíveis estão em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados.

Tabela 11. Segurança Física e do Ambiente

A.9.1.1	Perímetro de segurança física	Controle Devem ser utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação.
A.9.1.2	Controles de entrada física	Controle As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
A.9.1.3	Segurança em escritórios salas e instalações	Controle Deve ser projetada e aplicada segurança física para escritórios salas e instalações.
A.9.1.4	Proteção contra ameaças externas e do meio ambiente	Controle Deve ser projetada e aplicada proteção física contra incêndios, enchentes, terremotos, explosões, perturbações de ordem pública e outras formas de desastres naturais ou causados pelo homem.

Pergunta 2: Que tipo de controles existem na organização para prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações?

Resposta: Na organização MPSC existe o controle através de câmeras de monitoramento de todas as entradas e dentro do próprio CPD, o controle é feito através de chaves, cada pessoa tem a sua chave. O CPD fica isolado em um andar onde somente o pessoal autorizado pode acessar. Possui sistema contra incêndio.

Análise: O acesso de pessoas não autorizadas a GERED é dificultado pela presença 24 horas da policia militar, câmeras de monitoramento e o uso obrigatório do crachá para todos os colaboradores do MPSC, portanto a probabilidade da ameaça de uma pessoa não autorizada acessar a GERED é considerada baixa.

No quesito desastres naturais, a região de Florianópolis é atingida frequentemente por inundações, mas em toda história do MPSC numa houve uma inundação que atingisse a GERED, portanto a probabilidade da ameaça de um desastre natural atingir a GERED é considerada improvável.

O sistema contra incêndio do MPSC consiste na presença de extintores, de alarmes de incêndio e portas corta-fogo entre os andares, portanto a probabilidade da ameaça de um incêndio atingir a GERED é considerada baixa.

III. Segurança de Equipamentos

O terceiro controle analisado refere-se à segurança dos equipamentos (Tabela 12), esse controle tem por objetivo verificar se os equipamentos estão protegidos contra ameaças físicas e do ambiente. A proteção dos equipamentos é necessária para reduzir o risco de acesso não autorizado às informações e para proteger contra perdas ou danos.

Tabela 12. Segurança de Equipamentos

A.9.2.1	Instalação e proteção do equipamento	Controle Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.
A.9.2.2	Utilidades	Controle Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

A.9.2.3	Segurança do cabeamento	Controle O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou dados.
A.9.2.4	Manutenção dos equipamentos	Controle Os equipamentos devem ter manutenção correta, para assegurar sua disponibilidade e integridade permanente.

Pergunta 3: Que tipo de controles existem na organização para impedir perdas, danos, furtos ou comprometimentos de ativos e interrupção das atividades?

Resposta: O CPD possui no-break com a capacidade de 30 minutos de parada, além disso, possui uma unidade geradora de energia, capaz de funcionar 12 horas sem parada do serviço. Toda a conexão que alimenta o CPD tanto elétrica como lógica, é totalmente independente da infraestrutura do prédio. Os equipamentos possuem garantia em caso de falha é acionado a garantia do equipamento para sua substituição.

Análise: O histórico da região de Florianópolis mostra que a falha de energia pode durar mais de 12 horas, portanto a probabilidade da ameaça de falha de energia atingir a GERED é considerada provável.

Devido ao alto nível de segurança das instalações do MPSC, visto no controle Segurança Física e do Ambiente, podemos considerar a probabilidade da ameaça de roubo de equipamentos como improvável.

Os equipamentos da GERED possuem garantia, mas não possuem uma manutenção periódica, portanto a probabilidade da ameaça de falha de equipamentos é considerada provável.

IV. Proteção Contra Códigos Maliciosos

O quarto controle analisado refere-se à proteção contra códigos maliciosos (Tabela 13), esse controle tem por objetivo prevenir e detectar a introdução de códigos maliciosos não autorizados. Os recursos de processamento da informação e os softwares são vulneráveis à introdução de código malicioso, tais como vírus de computador, worms de rede, cavalos de Tróia. Convém que os usuários estejam conscientes dos perigos do código malicioso.

Tabela 13. Proteção contra códigos maliciosos

A.10.4.1	Controle contra códigos maliciosos	Controle Devem ser implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Pergunta 4: Que tipo de controles existem na organização para proteger a integridade do software e da informação?

Resposta: Para garantir a integridade dos dados é utilizado software de antivírus em todas as estações, anti-spam, para impedir que softwares maliciosos cheguem por e-mail, e orientado o usuário através de cartinhas sobre o uso consciente da Internet.

Análise: A GERED possui um sistema de antivírus e anti-spam, porém novos vírus surgem rapidamente e com a Internet a propagação do vírus é muito rápida, portanto a probabilidade da ameaça ocasionada por vírus de computador é considerada provável.

V. Cópias de Segurança

O quinto controle analisado refere-se às cópias de segurança (Tabela 14), que tem por objetivo manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

Tabela 14. Cópias de Segurança

A.10.5.1	Cópias de segurança das informações	Controle Cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente, conforme a política de geração de cópias de segurança definida.

Pergunta 5: Que tipo de controles existem na organização para manter a integridade e disponibilidade da informação e dos recursos de processamento de informação?

Resposta: As cópias de segurança são feitas todos dos dias em disco e fita, são divididos em dados diários, semanais e mensais. As fitas são guardadas em um cofre

contra incêndio, as fitas semanais e mensais são copiadas e levadas para outro edifício do MPSC e colocadas num cofre.

Análise: O backup dos dados do MPSC é realizado diariamente e armazenado em diferentes mídias e locais, portanto a probabilidade da ameaça de perda de backup é considerada baixa.

Porém o backup é realizado uma vez no dia, começa às 20 horas e termina às 5 horas da manhã, se uma pane acontece após o expediente, digamos às 19 horas, toda a informação gerada durante o dia será perdida, portanto a probabilidade da ameaça de perda de informações do servidor é considerada provável.

VI. Acesso à Rede

O sexto controle analisado refere-se ao controle de acesso à rede (Tabela 15), que tem por objetivo prevenir acesso não autorizado aos serviços de rede.

Tabela 15. Controle de Acesso à Rede

A.11.4.1	Política de uso dos serviços de rede	Controle Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.
A.11.4.2	Autenticação para conexão do usuário	Controle Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.
A.11.4.2	Identificação de equipamento em redes	Controle Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.

Pergunta 7: Que tipo de controles existem na organização para prevenir o acesso não autorizado aos serviços de rede?

Resposta: O link entre sede e comarcas é feito através de VPN, e a rede possui 3 firewall para garantir a segurança dos dados. No momento em que o usuário é criado no sistema de RH, ele é automaticamente provisionado na rede com sua atual lotação, no momento em que ele é colocado como inativo no sistema o seu usuário fica

desabilitado. Caso o usuário necessite de um direito de acesso em algum diretório o responsável da área deve autorizar esse acesso.

Análise: A VPN é uma forma segura de transferência de dados e o firewall bloqueia o acesso a determinados conteúdos, tentativas de invasão à rede e downloads de sites considerados inseguros. E cada usuário possui um perfil de acesso às informações, esse perfil é definido no momento da contratação e desabilitado no momento do desligamento do colaborador da organização, portanto a probabilidade da ameaça de acesso não autorizado aos serviços da rede é considerada baixa.

VII. Acesso ao Sistema Operacional

O sétimo controle analisado refere-se ao acesso ao sistema operacional (Tabela 16), tem como objetivo prevenir acesso não autorizado aos sistemas operacionais. Os recursos de segurança da informação devem ser usados para restringir o acesso aos sistemas operacionais para usuários autorizados.

Tabela 16. Controle de Acesso os Sistema Operacional

A.11.5.1	Procedimentos seguros de entrada no sistema (log-in)	Controle O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (log-on).
A.11.5.2	Identificação e autenticação de usuários	Controle Todos os usuários devem ter identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.
A.11.5.3	Sistema de gerenciamento de senha	Controle Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.
A.11.5.4	Desconexão de terminal por inatividade	Controle Terminais inativos devem ser desconectados após um período definido de inatividade.

Pergunta 8: Que tipo de controles existe na organização para prevenir o acesso não autorizado à informação contida nos sistemas operacionais?

Resposta: Controlado por logon, cada usuário possui o seu login e senha de rede. A cada 5 minutos de inatividade é bloqueada a estação automaticamente. Os terminais sem inatividade por 2 horas são desconectados automaticamente.

Análise: As senhas fornecidas pela GERED aos novos colaborados são padronizadas o sistema não obriga o usuário a trocar a senha periodicamente, tornando a senha facilmente descoberta através da engenharia social, portanto a probabilidade da ameaça de acesso não autorizado ao sistema operacional é considerada média.

A partir dos questionários Análise de Impacto e Análise de Riscos é possível calcular o tipo de risco que cada processo pode sofrer. A tabela de risco (Tabela 17) mostra o cálculo entre o impacto e a probabilidade da ameaça ocorrer, resultando no nível de risco.

Tabela 17. Tabela de Risco

Matriz Probabilidade X Impacto

Probabilidade					
Alta	0,95	1,90	2,85	3,80	4,75
Provável	0,75	1,50	2,25	3,00	3,75
Média	0,50	1,00	1,50	2,00	2,50
Baixa	0,25	0,50	0,75	1,00	1,25
Improvável	0,10	0,20	0,30	0,40	0,50
	Irrelevante	Pequeno	Moderado	Grande	Catastrófico
			Impacto		

Nives de Risco
Alto
Médio
Baixo

Na Tabela 18 é mostrado o resultado das análises realizadas na GERED, é possível ver os riscos, a sua probabilidade e o impacto que causariam na organização se os riscos viessem a ocorrer.

Tabela 18. Nível de Risco da GERED

Recursos	Risco	Probabilidade	Impacto	Nível crítico
Pessoas	Uso inadequado dos ativos de informação	Provável	Moderado	
Instalações	Acesso não autorizado	Baixa	Grande	
	Desastres naturais	Improvável	Catastrófico	
	Incêndio	Baixa	Catastrófico	
Equipamentos	Falha de equipamentos	Provável	Grande	
	Falha de energia	Provável	Grande	
	Roubo de equipamento	Improvável	Moderado	
Informação	Vírus de computador	Provável	Moderado	
	Perda de backup	Baixa	Grande	
	Perda de informações do servidor	Provável	Catastrófico	
	Falha nos serviços (e-mail, arquivos, etc.)	Média	Catastrófico	
Rede	Falha no link externo de rede	Baixa	Moderado	
	Acesso não autorizado ao sistema operacional	Média	Grande	
	Acesso não autorizado aos serviços da rede	Baixa	Grande	

A partir dessa análise é possível desenvolver as estratégias de continuidade priorizando as estratégias para os processos considerados de alto nível de risco.

4.3.3. Fase 3 - Desenvolvimento de estratégias de segurança

Nesta fase as informações coletadas nas fases anteriores são usadas para desenvolver as estratégias de segurança. Foram sugeridas algumas estratégias de segurança para os recursos considerados críticos.

1. Pessoas

Desenvolvimento de um documento com a política de segurança que será aprovado pela direção, publicado e comunicado para todos os colaboradores.

Todos os colaboradores devem conhecer e compreender a política de segurança da informação visando garantir que todas as pessoas tenham consciência da importância da mesma e a pratiquem na organização.

2. Instalações

As instalações do MPSC foram classificadas como suscetíveis a falhas de equipamentos e de energia, portanto sugere-se a implantação de um site backup contendo os serviços críticos como uma estratégia de continuidade no caso de um desastre atingir as instalações da GERED.

Além da implantação do site backup devem ser realizadas vistorias periódicas do site principal e do site backup para que a manutenção dos equipamentos seja feita antes da interrupção do negócio.

3. Informações

Os entrevistados identificaram as informações armazenadas nos servidores como os ativos mais importantes, portanto sugere-se a realização de backups incrementais de uma em uma hora, principalmente dos serviços de e-mail e arquivos.

Esse backup deve ser armazenado no storage da organização e no site backup, no caso de um desastre que afete as instalações principais não haverá perda de informações ao transferir os negócios para o site backup.

4. Rede

Na política de segurança deve constar o procedimento de troca de senhas periódicas. Quando a senha expirar, o usuário será direcionado para a tela de alteração da senha. Para troca da senha alguns critérios de complexidade deverão ser utilizados, por exemplo, senha com mais de 8 caracteres, contendo números e letras ou caracteres especiais.

A execução do método OCTAVE cumpriu com a realização da primeira etapa de desenvolvimento de um PCN, após essa etapa é possível realizar a implementação dos planos de continuidade de negócios e posteriormente sua monitoração e manutenção, cumprindo com as etapas de desenvolvimento de um PCN.

5. Considerações Finais

A segurança da informação pode ser considerada fundamental para sobrevivência da organização, em decorrência da importância que as informações possuem para a continuidade dos negócios.

As principais referências pesquisadas sobre segurança da informação foram as normas da série ISO 27000 que mostram os conceitos sobre segurança da informação, o modelo Plan-Do-Check-Act (PDCA) e a gestão de riscos. E as principais referências de continuidade de negócio foram as normas da série BS 25999 que mostram o ciclo de vida da gestão de continuidade do negócio e as etapas da sua implementação em uma organização.

A semelhança entre este trabalho e os principais trabalhos relacionados apresentados está no uso das normas de segurança da informação e das normas de continuidade de negócios. A principal diferença é que este trabalho utilizou o método OCTAVE para realizar a análise de riscos.

Neste trabalho foi realizado um estudo de caso no Ministério Público de Santa Catarina (MPSC) na Gerência de Redes e Banco de Dados (GERED) que é responsável pela disponibilidade e integridade dos dados do MPSC. Foi analisado o ambiente da GERED utilizando o método OCTAVE, realizando a primeira etapa do desenvolvimento de plano de continuidade de negócios (PCN).

A partir desse estudo foi constatada a importância dos processos da GERED e por consequência a necessidade do desenvolvimento de um PCN. Focando principalmente no desenvolvimento de uma política de segurança da informação e a implantação de um site backup para garantir a integridade e disponibilidade das informações do MPSC.

Por fim, o desenvolvimento deste trabalho contribuiu com os conhecimentos relacionados à segurança da informação, como a análise de riscos, a política de segurança da informação e o plano de continuidade de negócio, proporcionando uma visão maior da importância da implementação de um plano de continuidade de negócios para a sobrevivência da organização.

5.1. Trabalhos Futuros

Como sugestões para trabalhos futuros que venham a contribuir para a melhoria do processo de continuidade de negócios podem ser citados os seguintes itens:

a) Desenvolvimento da política de segurança da informação;
b) Desenvolvimento do plano de continuidade de negócio;
c) Elaboração de um programa de Governança de TI para o aperfeiçoamento dos processos de TI.

6. Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança de informação**. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO GUIA 73:2009: Gestão de Riscos - Vocabulário**. Rio de Janeiro, 2009.

BRITISH STANDARD. **BS 25999-1:2006 Business continuity management – Part 1: Code of practice**. Londres, 2006.

BRITISH STANDARD. **BS 25999-2:2007 Business continuity management — Part 2: Specification**. Londres, 2007.

BS 25999 BUSINESS CONTINUITY. **Overview**. Disponível em <http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/> acesso em 19/6/2011

CAMPOS, André L. N. **Sistemas de Segurança da Informação – Controlando os Riscos**. Florianópolis: Visual Books, 2006.

CIRIBELLI, Marilda Corrêa. **Como elaborar uma dissertação de mestrado através da pesquisa científica**. Rio de Janeiro: 7Letras, 2003.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

DOROFEE Audrey J; ALBERTS Christopher J. **OCTAVE Criteria Version 2.0.** Pittsburgh: Carnegie Mellon Software Engineering Institute, 2001.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação – Guia Prático pra Elaboração e Implementação**. Rio de Janeiro: Ciência Moderna Ltda, 2008.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna Ltda, 2003.

Guia do Ministério Público de Santa Catarina. Florianópolis, 2009. Disponível em < http://portal.mp.sc.gov.br/portal/conteudo/guia_web.pdf> acesso em 22/08/2011.

HARRIS, Shon. **CISSP All-in-One Exam Guide**. New York: The McGraw Hill Companies, 2008.

INFORMATION SECURITY. **Press Realease**. 2002. Disponível em <http://www.bsigroup.com/en/About-BSI/News-Room/BSI-News-Content/Disciplines/Information-Security/Information-security/> acesso em 19/6/2011.

LANDWEHR, Carl E. **Computer security**. Virginia: Springer-Verlag 2001.

LAUREANO, Marcos Aurélio Pchek. **Gestão de Segurança da Informação**. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> Acesso em: 10 de maio de 2011.

NICKOLETT, Chip; SCHMIDT, Jason. **Business Continuity Planning Description and Framework**. Brookfield Comprehensive Solutions, 2001.Disponível em: <http://www.comp-soln.com/BCP_whitepaper.pdf> Acesso em: 15 de maio de 2011.

PAULINA, Januszkiewicz; MAREK, Pyka. **Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology.** Poland: Academy of Business in Dąbrowa Górnicza, 2007.

Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. 2000. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm> acesso em 6/19/2011.

Plano Geral de Atuação. Florianópolis, 2011. Disponível em < http://portal.mp.sc.gov.br/portal/conteudo/arte/pga_2011_web.pdf> acesso em 22/08/2011.

REIS, Linda G. **Produção de Monografia da Teoria a Pratica**. Distrito Federal: Senac-DF, 2010.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas, 2008.

SALDANHA, Fernando. **Introdução a Planos de Continuidade e Contingência Operacional**. Rio de Janeiro: Papel Virtual, 2000.

SCHOLZ, Roland W.; TIETJE, Olaf. **Embedded case study methods: integrating quantitative and qualitative knowledge.** Londres: Sage Publications, 2002.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma Visão Executiva**. Rio de Janeiro: Elsevier, 2003.

SILVEIRA, Patrícia Marques. **Plano de continuidade de negócios para a empresa Alfa: uma proposta com base na NBR 15999, no ITIL e no COBIT**. Pontifícia Universidade Católica do Rio Grande do Sul. Faculdade de Administração de Empresas. Dissertação de Conclusão de Curso. 2009.

SOUZA, Diego Muller Cardeal de. **Gestão da continuidade de negócio: o caso de uma empresa de telecomunicações**. Universidade Federal do Rio Grande do Sul. Faculdade de Engenharia de Produção. Dissertação de Mestrado. 2010.

TOIGO, Jon William. **Recuperação de Sistemas de Informação**. Rio de Janeiro: Livros Técnicos e Científicos, 1990.

WALLACE, Michael; WEBBER, Lawrence. **The Disaster Recovery Handbook - A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets**. NewYork: Amacom, 2004.

Apêndice A

Questionário - Análise de Impacto						
Processo de negócio:						
Período de funcionamento (horário-dias):						
Quais os recursos e tempos de recuperação para o processo de negócio?						
Recurso		Tempo de Recuperação		Ponto de Recuperação		
Tempo de inoperância suportável (sem que haja conseqüências para a empresa)						
Minutos:			Dias:			
Horas:			Não pode parar:			
Impactos na organização:						
			1	2	3	4	5
Impacto na imagem da organização							
Interrupção no fluxo de trabalho							
Interrupção total no processo de negócio da organização							
Interrupção de prestação/fornecimento de serviços							
Suspensão de atendimento ao cliente							
Perda de ativos							

Legenda: 1 - Irrelevante; 2 – Pequeno; 3 – Moderado; 4 – Grande; 5 - Catastrófico

Tempo de Recuperação: tempo máximo que o negócio pode suportar sem a solução tecnológica.

Ponto de Recuperação: a quantidade aceitável de perda de dados medidos em tempo

Planejamento da Gestão de Continuidade de Negócios Usando a Metodologia OCTAVE na Análise de Riscos

Denise Santin Ebone

Centro Tecnológico - Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 476 - 88.040-970 - Florianópolis - SC - Brasil

denyebone@gmail.com

Abstract*. Organizations increasingly rely on their computerized processes because virtually all information is captured, stored and accessed in digital format. This dependence exposes organizations to a variety of new threats that may that may affect business continuity. This article presents a business continuity management process which uses the OCTAVE methodology. The results indicate that the method is efficient to evaluate the organization's information security environment, assisting in the process of risk analysis and decision making.*

Resumo*. As organizações dependem cada vez mais de seus processos informatizados porque praticamente todas as informações são capturadas, armazenadas e acessadas em formato digital. Essa dependência expõe as organizações a uma variedade de novas ameaças que podem afetar a continuidade do negócio. Este artigo apresenta um processo para gestão da continuidade de negócio através da metodologia OCTAVE. Os resultados indicam que o método é eficiente para avaliar o ambiente de segurança da informação de uma organização, auxiliando no processo de análise de risco e tomada de decisão.*

1. Introdução

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação (ABNT NBR ISO/IEC 27002:2005).

O Plano de Continuidade de Negócios (PCN) visa prevenir a ocorrência de desastres, minimizar o impacto se um desastre acontecer e viabilizar a rápida ativação de processos alternativos na indisponibilidade dos processos usuais. Desta forma ele visa minimizar o impacto de desastres eventuais sobre os negócios (SALDANHA, 2000).

Este artigo propõe um método para o desenvolvimento de um PCN através da utilização das normas de segurança da informação e das normas de continuidade de negócio.

O assunto está dividido em cinco seções. A primeira seção apresenta a introdução ao artigo. A segunda sessão apresenta os conceitos sobre segurança da informação, as principais normas e a política de segurança. A terceira sessão apresenta os conceitos sobre continuidade de negócios, as principais normas e o desenvolvimento

do PCN. A quarta sessão apresenta um estudo de caso aplicado em uma organização para verificar a eficácia dos conceitos apresentados. A quinta sessão apresenta as considerações finais.

2. Segurança da Informação

Segurança da informação pode ser defina como a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade (SÊMOLA, 2003). Ativos da informação seriam todos os elementos usados para armazenar, transmitir e processar a informação.

A *International Organization for Standardization* (ISO) reuniu as diversas normas de segurança da informação existente e criou a serie de normas ISO 27000. As principais normas sobre segurança da informação utilizadas neste artigo são:

ISO/IEC 27001:2006 - especifica os requisitos para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI). Esta norma adota o modelo conhecido como "Plan-Do-Check-Act" (PDCA), que é aplicado para estruturar todos os processos do SGSI.

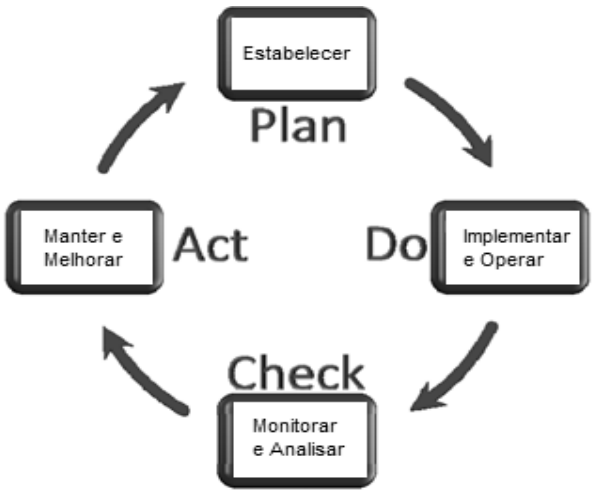

Figura 1. Modelo PDCA

ISO/IEC 27002:2005 - estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização.

ISO/IEC 27005:2008 - fornece as diretrizes para o processo de gestão de riscos de segurança da informação. De acordo com a norma, o processo é composto pelas seguintes atividades: análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos, a comunicação de riscos e o monitoramento e análise crítica de riscos.

A primeira atividade a ser desenvolvida para garantir a segurança da informação segundo a norma 27001 é o desenvolvimento de uma Política de Segurança. A política de segurança é um conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação devendo ser formalizada e divulgada a todos os usuários que fazem o uso dos ativos da informação (FERREIRA; ARAÚJO, 2008).

O desenvolvimento de uma política de segurança deve capacitar a organização com instrumentos jurídicos, normativos e processuais. Esses instrumentos devem

abranger as estruturas físicas, tecnológicas e administrativas, de forma a garantir a confidencialidade, integridade e disponibilidade das informações corporativas.

3. Plano de Continuidade do Negócio – PCN

O PCN tem como objetivo possibilitar o funcionamento da organização em situações de contingência onde há interrupção dos ativos de informação.

O PCN garante a continuidade de processos e informações vitais à sobrevivência da empresa, em menor espaço de tempo possível, com o objetivo de minimizar os impactos no negócio (SÊMOLA, 2003).

A continuidade de negócios possui como principal referência à série normativa BS 25999, elaborada pelo *British Standards Institution (*BSI), que é segmentada em duas normas:

BS25999-1:2006 - estabelece o processo, os princípios e a terminologia da Gestão da Continuidade de Negócios (GCN). E tem como objetivo fornecer uma base conceitual para entender, desenvolver e implementar a continuidade de negócios em uma organização.

Figura 2. Ciclo de vida da Gestão de Continuidade de Negócios

BS25999-2:2007 - especifica os requisitos para estabelecer e gerenciar um Sistema de Gestão de Continuidade de Negócios (SGCN) definido por um programa de GCN. Esta norma utilizado o modelo PDCA da norma 27001 aplicado a todas as partes do ciclo de vida da GCN, de forma a garantir que a continuidade do negócio esteja devidamente gerenciada e aprimorada numa organização.

Dessa forma o desenvolvimento do PCN segue o modelo PDCA da norma BS25999-2:2007 que consistente na melhoria contínua, evidenciando as etapas de Planejamento, Implementação, Monitoração e Manutenção.

Etapa 1. Planejamento - possibilita a identificação das reais necessidades da organização e de cada processo crítico. O planejamento visa definir o escopo e a estratégia de estruturação do PCN. Para estas definições devem ser avaliados o ambiente interno, o ambiente externo, as possíveis perdas em função do impacto de um desastre, as demandas dos serviços críticos e as restrições financeiras (SALDANHA, 2000).

Etapa 2. Implementação - nesta etapa os planos de continuidade são desenvolvidos e implementados. O PCN tem um alto nível de complexidade, podendo

assumir diversas formas em função do objeto a ser contingenciado e a abrangência de sua atuação. Por isso, uma empresa não possuirá um plano único, mas diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos (SÊMOLA, 2003). Podemos dividir o PCN em 3 planos:

Plano de Continuidade Operacional: este documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio.

Planos de Contingência: são desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencentes ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência.

Plano de Recuperação de Desastres: este documento tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados pelo incidente que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

Etapa 3. Monitoração - a organização deve, em intervalos regulares, analisar criticamente o PCN, de forma a assegurar sua permanente atualização e efetividade. A análise deve verificar se o PCN está em conformidade com todas as leis, normas, estratégias, estruturas e diretrizes da organização (BS 25999-1:2006). A análise pode assumir a forma de auditorias internas, externas, ou auto-avaliações.

Etapa 4. Manutenção - a maioria dos processos e procedimentos de um negócio muda com frequência, tornando o PCN um produto altamente perecível. Para mantê-lo em perfeitas condições é necessário que se esteja atento a todas as mudanças internas e externas e que estas mudanças sejam refletidas no PCN através de adequações e aperfeiçoamentos (SALDANHA, 2000).

4. Estudo de Caso

Um estudo de caso foi realizado para aplicação da primeira etapa de desenvolvimento de um PCN usando a metodologia OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), desenvolvida pela Universidade de Carnegie Mellon em 2001. Esse método foi escolhido por ser um método de análise voltado para área de tecnologia da informação.

A organização avaliada foi o Ministério Público de Santa Catarina (MPSC), especificamente a Gerência de Redes e Banco de Dados (GERED) por ser responsável pela disponibilidade e integridade das informações do MPSC. O método OCTAVE é composto por 3 fases:

Fase 1 - Construção de um perfil de ameaça - nessa fase são analisados os principais recursos da organização e os requisitos de segurança necessários para proteger esses recursos. Foram realizadas entrevistadas na GERED para mapear os principais processos e o impacto que uma interrupção nesses processos pode causar a organização.

Fase 2 - Identificação das vulnerabilidades - nessa fase é analisado as vulnerabilidades existentes nos processos críticos. Foi realizado um levantamento dos possíveis riscos que pudessem vir a ocorrer.

Foram feitas perguntas ao gerente da GERED sobre os controles existentes no ambiente segundo alguns pontos de auditoria recomendados pela Norma 27002. A partir das respostas foi feita a análise da probabilidade de uma ameaça atingir a organização e afetar a continuidade do negócio.

A partir desses questionários foi possível calcular o tipo de risco que cada processo pode sofrer.

Tabela 1. Nível de risco da GERED

Recursos	Risco	Probabilidade	Impacto	Nível crítico
Pessoas	Uso inadequado dos ativos de informação	Provável	Moderado	ALTO
Instalações	Acesso não autorizado	Baixa	Grande	MÉDIO
	Desastres naturais	Improvável	Catastrófico	BAIXO
	Incêndio	Baixa	Catastrófico	MÉDIO
Equipamentos	Falha de equipamentos	Provável	Grande	ALTO
	Falha de energia	Provável	Grande	ALTO
	Roubo de equipamento	Improvável	Moderado	BAIXO
Informação	Vírus de computador	Provável	Moderado	ALTO
	Perda de backup	Baixa	Grande	MÉDIO
	Perda de informações do servidor	Provável	Catastrófico	ALTO
	Falha nos serviços (e-mail, arquivos, etc.)	Média	Catastrófico	ALTO
Rede	Falha no link externo de rede	Baixa	Moderado	MÉDIO
	Acesso não autorizado ao sistema operacional	Média	Grande	ALTO
	Acesso não autorizado aos serviços da rede	Baixa	Grande	MÉDIO

Fase 3 - Desenvolvimento de estratégias de segurança - nesta fase as informações coletadas nas duas fases anteriores são usadas para desenvolver as estratégias de segurança. As estratégias sugeridas no caso da GERED são:

- Desenvolvimento de uma política de segurança da informação;
- Implantação de um site backup;
- Realização de backups incrementais de uma em uma hora;
- Troca de senhas periódicas.

A execução do método OCTAVE cumpriu com a realização da primeira etapa de desenvolvimento de um PCN, após essa etapa é possível realizar a etapa de implementação dos planos de continuidade de negócios e posteriormente a monitoração e manutenção.

5. Considerações Finais

A segurança da informação pode ser considerada fundamental para sobrevivência da organização, em decorrência da importância que as informações possuem para a continuidade do negócio.

As principais referências pesquisadas sobre segurança da informação foram as normas ISO 27000 que mostram os conceitos sobre segurança da informação, o modelo Plan-Do-Check-Act (PDCA) e a gestão de riscos. As principais referências de

continuidade de negócio foram as normas da BS 25999 que mostram o ciclo de vida da gestão de continuidade do negócio.

O estudo de caso apresentado analisou o ambiente da GERED resultando em algumas estratégias de continuidade. A partir desse estudo foi constatada a importância dos processos da GERED e por consequência a necessidade do desenvolvimento de um plano de continuidade de negócio. Focando principalmente no desenvolvimento de uma política de segurança da informação e a implantação de um site backup para garantir a integridade e disponibilidade das informações do MPSC.

6. Referências

ABNT NBR ISO/IEC 27001:2006: Tecnologia da informação – Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2006.

ABNT NBR ISO/IEC 27002:2005: Tecnologia da informação — Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27005:2008: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança de informação. Rio de Janeiro, 2008.

BRITISH STANDARD. BS 25999-1:2006 Business continuity management – Part 1: Code of practice. Londres, 2006.

BRITISH STANDARD. BS 25999-2:2007 Business continuity management — Part 2: Specification. Londres, 2007.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação – Guia Prático pra Elaboração e Implementação. Rio de Janeiro: Ciência Moderna Ltda, 2008.

SALDANHA, Fernando. Introdução a Planos de Continuidade e Contingência Operacional. Rio de Janeiro: Papel Virtual, 2000.

SÊMOLA, Marcos. Gestão da Segurança da Informação – Uma Visão Executiva. Rio de Janeiro: Elsevier, 2003.