CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA – FATEC – AM

SEGURANÇA DA INFORMAÇÃO

Gisele Guarino Guimarães

PLANO DE CONTINUIDADE DE NEGÓCIOS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO APLICADA EM PEQUENAS E MÉDIAS EMPRESAS

Americana

2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA – FATEC – AM

SEGURANÇA DA INFORMAÇÃO

Gisele Guarino Guimarães

PLANO DE CONTINUIDADE DE NEGÓCIOS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO APLICADA EM PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação do Professor Doutor Alexandre Mello Ferreira.
Área de Concentração: Gestão em Segurança da Informação

Americana, SP

2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Guimarães, Gisele Guarino
G976p Plano de continuidade de negócios e políticas de segurança aplicada em pequenas e médias empresas. / Gisele Guarino Guimarães. – Americana: 2014.
81f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. Alexandre Mello Ferreira

1. Segurança em sistemas de informação I. Ferreira, Alexandre Mello II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Gisele Guarino Guimarães

PLANO DE CONTINUIDADE DE NEGÓCIOS E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO APLICADA EM PEQUENAS E MÉDIAS EMPRESAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Gestão em Segurança da Informação.

Americana, 05 de dezembro de 2014.

Banca Examinadora:

Alexandre Mello Ferreira (Presidente)
Doutor
FATEC - Americana

José William Pinto Gomes (Membro)
Graduado
FATEC - Americana

Clerivaldo José Roccia (Membro)
Mestre
FATEC - Americana

AGRADECIMENTOS

Ao professor Alexandre Mello Ferreira pela orientação, compreensão e incentivo dispensado ao desenvolvimento deste trabalho.

Aos demais professores pela amizade, companheirismo e principalmente pelo suporte no aprendizado da segurança da informação.

E principalmente à minha família que tanto me apoiou no decorrer de todo o curso e conclusão deste trabalho.

DEDICATÓRIA

À

Minha Família

Em especial ao meu marido e filhos.

RESUMO

Toda organização está suscetível a interrupções das suas atividades críticas ocasionadas por ameaças que podem afetar os objetivos estratégicos do negócio. Este trabalho apesenta um estudo sobre a introdução de uma Gestão de Segurança da Informação e Gestão de Continuidade de Negócios em uma empresa de médio porte do setor varejista com o propósito de que a mesma possa responder de maneira eficiente aos cenários de incidentes e manter a continuidade dos serviços considerados mais críticos. Inicialmente são definidos alguns conceitos sobre segurança da informação, gestão de riscos e melhores práticas. Por fim, é realizada uma análise de maturidade da situação atual da empresa em relação aos controles de segurança de suas informações através da aplicação de um teste de verificação. Logo em seguida, é feita uma análise de risco onde são demonstradas as principais ameaças, vulnerabilidades e probabilidades de ocorrência com o levantamento dos riscos que mais impactam nos objetivos do negócio para, então, apresentar diretrizes que serão utilizadas na elaboração de um novo modelo de Plano de Continuidade de Negócios.

Palavras Chave: gestão de continuidade de negócios; segurança da informação; análise de risco; plano de continuidade de negócios.

ABSTRACT

Every organization is susceptible to interruptions in their critical activities due to threatens that may affect the business strategic goals. This essay presents a study about the introduction of Management Information Security and Business Continuity Management in a medium-sized company on the retail department with the purpose of the company can respond effectively to risky situations and that it can maintain continuity in services considered most critical. Initially are determined some concepts about information security, risk management and better practices. Finally, an analysis of the maturity of the company's current situation is done. This analysis is relative to the security controls of its information through the application of a proofing test. In sequence, a risk analysis is performed when the main threats, vulnerabilities and probabilities of occurrence with valuation of the risks that most impact the business objectives are demonstrated, for then guidelines that will be used in developing of a new model of the Business Continuity Plan are presented.

***Keywords**: business continuity management*; i*nformation security*; *risk analysis*; *continuity business plan.*

SUMÁRIO

1 INTRODUÇÃO 14
2 SEGURANÇA DA INFORMAÇÃO 16
2.2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO 19
2.2.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO 22
2.2.2 AUDITORIA 25
2.2.3 GESTÃO DE RISCO 27
2.3 NORMAS E MELHORES PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO 28
2.3.1 NBR ISO/IEC 17799 29
2.3.2 A FAMÍLIA ISO/IEC 27000 30
2.3.3 ABNT NBR ISO/IEC 27001 32
2.3.4 ABNT NBR ISO/IEC 27002 33
2.3.5 ABNT NBR ISO/IEC 27005 35
2.3.6 CobIT - O FRAMEWORK RISK IT E VAL IT 36
3 CONTINUIDADE DE NEGÓCIO 42
3.1 GESTÃO DE CONTINUIDADE DE NEGÓCIOS 42
3.2 PLANO DE CONTINUIDADE DE NEGÓCIO 44
3.2.1 MODELO DE MATURIDADE 47
3.3 NBR ISO/IEC 22301 48
4 ESTUDO DE CASO 52
4.1 A EMPRESA 52
4.2 TESTE DE VERIFICAÇÃO QUANTO A SEGURANÇA DAS INFORMAÇÕES 54
4.3 ESTRATÉGIA DE CONTINGÊNCIA 55
4.3.1 ANÁLISE DE RISCO E DE IMPACTO NA EMPRESA X 56
4.4 DIRETRIZES PARA A CONSTRUÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS PARA A EMPRESA X 60
4.5 MODELO DE PLANO DE CONTINUIDADE DE NEGÓCIO 63
5 CONSIDERAÇÕES FINAIS 65
REFERÊNCIAS 67
APÊNDICE A 70
APÊNDICE B 72
APÊNDICE C 77

LISTA DE FIGURAS

Figura 1: Modelo PDCA aplicado aos processos do SGSI 21

Figura 2: Visão geral do Modelo do Cobit 37

Figura 3: Modelo PDCA aplicado aos processos do SGCN 50

Figura 4: Análise de Riscos 58

LISTA DE TABELAS

Tabela 1: Distribuição Organizacional e de TI 53

Tabela 2: Tabela de pontuação – teste de controle de segurança 54

Tabela 3: Ameaças e vulnerabilidades com alto impacto ao negócio 57

LISTA DE GRÁFICOS

Gráfico 1: Resultado da análise de verificação de controle de segurança 55

LISTA DE SIGLAS E ABREVIAÇÕES

ABNT – Associação Brasileira de Normas Técnicas

BCM – Business Continuity Management

BIA – Business Impact Analysis.

BS– British Standard

BSI – British Standards Institution

CCSC – Commercial Computer Security Centre

COBIT – Control Objectives for Information and Related Technology

COSO ERM Committee of Sponsoring Organizations - Enterprise Risk Management

CPD – Centro de Processamento de Dados

DTI – Diretoria de Tecnologia de Informação

GCN – Gestão da Continuidade do Negócio.

ID – Identificador

IEC – International Electro technical Commission

ISACA – Information Systems Audit and Control Association

ISO – International Organization for Standardization

ITGI – IT Governance Institute

NBR– denominação de norma da Associação Brasileira de Normas Técnicas

PCN – Plano de Continuidade de Negócios.

PDCA – Plan (Planejar), Do (Fazer), Check (Verificar), Act (Agir).

PIB – Produto Interno Bruto

SGCN – Sistemas de Gestão de Continuidade de Negócio

SGSI – Sistema de Gestão de Segurança da Informação

SLA – Service Level Agreement

TI – Tecnologia da Informação.

1 INTRODUÇÃO

Atualmente a informação tornou-se o ativo mais importante de uma organização, já que para se alcançar os objetivos estratégicos, ela é essencial, desde que esteja disponível, apresente-se com qualidade, segurança e tenha fácil acesso.

Sendo assim, TI não é mais vista apenas como infraestrutura, mas como parte integrante do planejamento estratégico corporativo, gerando informações para a tomada de decisões, criando oportunidades de novos negócios, como ferramenta de aquisição de novos clientes, entre outros. Oliveira (2007, p.140) define tecnologia da Informação em uma organização como sendo “o conjunto de conhecimentos que são utilizados para operacionalizar as atividades da empresa para que seus objetivos possam ser alcançados”.

Como o mundo corporativo é sempre muito competitivo e sofre constantes mudanças, essas não devem interferir no bom andamento institucional. Então, as informações precisam estar protegidas contra vulnerabilidades e ameaças, ou seja, deve ocorrer o gerenciamento dos riscos e detecção daqueles que mais impactam nos objetivos dos negócios.

A elaboração de um plano de continuidade de negócios e plano de recuperação de desastre é necessária para que não ocorra a interrupção das atividades empresariais, perda de seus dados, ou até mesmo evitar fatos como os que ocorreram no dia 11 de setembro, quando grandes instituições se extinguiram pela falta de normas e procedimentos adequados quanto à segurança de suas informações.

A Gestão de Continuidade dos Negócios (GCN) fornece uma estrutura que permite identificar ameaças potenciais à organização e constrói a capacidade para lidar com elas, para que, dessa forma, a empresa possa responder às ameaças e proteger os interesses da alta direção, sua reputação e marca (ISO 22301,2013).

Este trabalho tem o propósito de apresentar conceitos e melhores práticas utilizadas na implementação de um plano de continuidade de negócio aplicado à

segurança da informação com foco nas médias empresas, as quais são consideradas de grande importância ao nosso país por apresentarem um alto índice de empregabilidade. Segundo o Portal do Brasil (2012) “Pequenas e médias empresas brasileiras representam 20% do PIB e são responsáveis por 60% dos 94 milhões de empregos no País”.

Muitas empresas, consideradas de grande porte já incorporam o plano de continuidade de negócios e gerenciamento de crises no projeto corporativo, pois é fundamental que os investidores tenham confiança e credibilidade nos negócios aos quais estão depositando seus consideráveis valores.

Já as empresas de médio e pequeno porte geralmente não apresentam preocupação nesse sentido. Desconsideram, algumas vezes, a importância da implantação de um plano que ajude a impedir ou deter a perda de seus dados ou a interrupção de suas atividades, as quais podem causar prejuízos consideráveis à instituição. Com seus pensamentos retrógrados de que TI é considerada geradora de gastos, não existe alinhamento desta área com o planejamento estratégico definido pela direção organizadora.

Neste trabalho, primeiramente são definidos alguns conceitos sobre segurança da informação, gestão de segurança da informação, suas normas e melhores práticas.

A seguir, são apresentadas as etapas do gerenciamento de riscos segundo a norma 27005 (ABNT, 2008) e conceitos sobre a gestão de continuidade de negócios, com foco na elaboração de um plano de continuidade de negócio.

Por fim, é feito um estudo de caso em uma empresa de médio porte onde é realizada uma análise de maturidade de sua atual situação em relação aos controles de segurança de suas informações com a aplicação de um teste de verificação. Logo em seguida, é feita uma análise de risco onde são apresentadas as principais ameaças, vulnerabilidades, probabilidades de ocorrência com o levantamento dos riscos que mais impactam nos objetivos do negócio, para só a partir daí, então, apresentar as diretrizes para elaboração do modelo de um Plano de Continuidade de Negócios.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação não se resume apenas à compra de equipamentos e softwares como, firewalls, sistemas de detecção de intrusos ou antivírus, ou ainda não se trata somente da adoção de Políticas de Segurança e do estabelecimento de responsabilidades. Nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconsequente.

Segurança da Informação não é uma ciência exata. Se fôssemos classificá-la, ela estaria no campo da gestão de riscos. E para gerir riscos é preciso conjugar vários verbos; Conhecer, Planejar, Agir, Auditar, Educar, Monitorar, Aprender e Gerenciar são apenas alguns deles.

Caruso e Steffen (1999) afirmam que o bem mais valioso de uma empresa pode não ser o produto fabricado pela mesma ou o serviço prestado ao cliente, mas as informações relacionadas a esse bem de consumo ou serviço.

A segurança da informação diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização (empresa) ou um indivíduo.

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

Segundo Fontes (2006) Segurança da informação é conjunto de orientações, normas procedimentos, políticas e demais ações com o objetivo de proteger as informações de uma organização, para que seu negócio seja realizado e sua missão alcançada.

A ISO/IEC 17799 (2005) define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Para Fontes (2006) proteger a informação significa garantir:

- Disponibilidade: a informação deve ser acessível para o funcionamento, alcance de objetivos e missão da organização;
- Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida;
- Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização;
- Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como os princípios éticos seguidos pela organização e sociedade;
- Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.

Com a finalidade de garantir um nível de proteção adequado para os ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança (BEAL, 2005).

Dessa forma, as organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos, levando-se em conta os riscos reais a que estão sujeitos esses ativos (BEAL, 2005).

É preciso cercar o ambiente de informações com medidas que garantam sua segurança efetiva, a um custo aceitável, visto ser impossível obter-se segurança absoluta, já que a partir de um determinado ponto, os custos se tornam inaceitáveis (CARUSO; STEFFEN, 1999).

Para Beal (2005), devido à alta complexidade e ao alto custo de manter os ativos da informação salvos de ameaças com relação à sua confidencialidade,

integridade e disponibilidade, é importante a empresa adotar um enfoque de gestão baseado nos riscos específicos para o negócio.

Assim, a gestão do risco é o conjunto de processos que permite às organizações identificarem e implementarem as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (BEAL, 2005).

Existem diversos elementos e terminologias que compõem o cenário da segurança, sendo que os principais são (ALVES, 2006):

Ativo: Tudo o que representa valor para o negócio da instituição.

Exemplos:

- Humanos (Pessoas);
- Tecnológicos (Software, hardware);
- Físicos (Escritórios, CPD);

Ameaças: Causas potenciais responsáveis por um incidente de segurança; exploram falhas (vulnerabilidades).

Exemplos:

- Hackers;
- Crackers;
- Agentes naturais;
- Vândalos;

Vulnerabilidades: Falha e/ou conjunto de falhas que podem ser exploradas por ameaças.

Exemplos:

- Contas sem senha;
- Falhas em programas;

Impacto: Resultado de um incidente de segurança, que poderá acarretar perdas ou danos pequenos, médios ou grandes.

Exemplo: Comprometimento de um site de comércio eletrônico na Internet e a posterior divulgação deste incidente pelos meios de comunicação.

Risco: A avaliação dos riscos permite identificar as ameaças dos ativos, as vulnerabilidades e a sua probabilidade de ocorrência, além de seus impactos sobre a organização. Quanto maior for o conhecimento sobre os riscos, mais fácil será decidir como tratá-los.

Segundo Moraes, Terence e Escrivão Filho (2004), nenhuma empresa pode escapar dos efeitos da revolução causada pela informação. Dessa forma, deve-se ter consciência de que a informação é um requisito tão importante quanto os recursos humanos, pois dela depende o sucesso ou fracasso das tomadas de decisões diárias.

2.2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Segundo Fontes (2008), o termo governança foi utilizado inicialmente para Governança Corporativa logo após ações administrativas fraudulentas e/ou irresponsáveis. Para implementar a Governança Corporativa é necessário aplicá-la em diversas áreas da organização como, por exemplo, na área da Segurança da Informação e ne área da Tecnologia da Informação.

De acordo com o autor, governança é a gestão da gestão e, para a Segurança da Informação, devemos considerar os seguintes aspectos:

É preciso existir a Gestão da Segurança da Informação. O primeiro requisito a ser implementado é uma pessoa responsável pelo processo de segurança da informação. Em segundo lugar, é necessário que haja recursos financeiros, de tempo e operacionais, e, em terceiro lugar, a decisão da existência de um processo de segurança deve partir da alta administração da organização, pois este processo interfere em pessoas, na cultura e no poder que as pessoas possuem dentro da organização.

É preciso entender de Gestão de Segurança da Informação. Aqueles que forem tratar da Gestão de Segurança da Informação devem entender do processo e ter experiência prática no assunto.

Ter autonomia. A autonomia é necessária para que não haja limitações, pois algumas pessoas se sentirão incomodadas pela medição de alguns indicadores que antes estavam implícitos.

Planejar, executar, avaliar e melhorar. Este processo é um ciclo que possibilitará a continuidade das ações de Gestão em Segurança da Informação.

Alinhamento e sincronismo com o negócio da organização. A gestão em Segurança da Informação deverá ser feita para possibilitar que o negócio se realize (alinhamento) dentro do tempo planejado (sincronismo). Quando a direção estiver definindo a estratégia para o negócio deve considerar a segurança como um elemento que pode alcançar ou limitar essa estratégia.

Ser um elemento da Governança Corporativa. Sem uma Governança Corporativa será mais difícil a existência de uma Governança em Segurança da Informação.

Fazer Governança porque é necessário. A existência da Governança em Segurança da Informação deve ser motivada pela necessidade de se realizar tarefas e controles de segurança e não pela simples divulgação de sua existência na empresa.

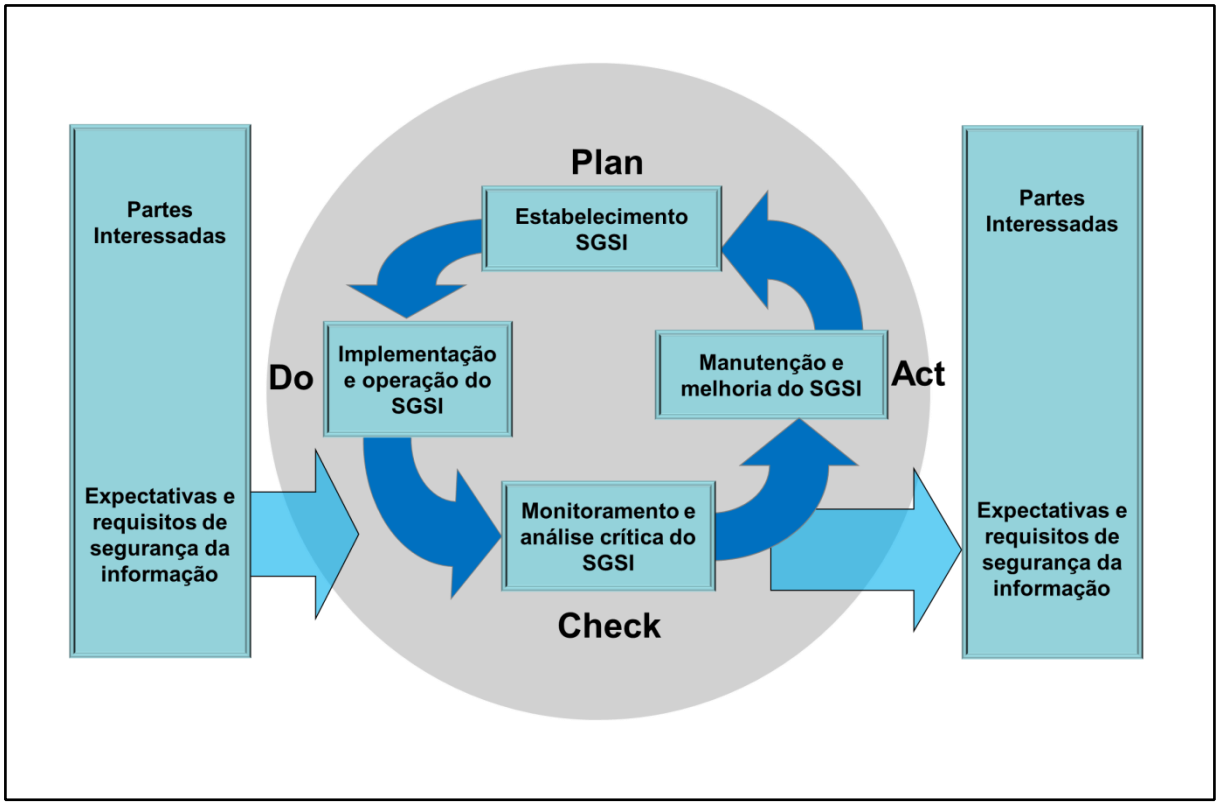
Garantir uma avaliação contínua. A Governança em Segurança da Informação deve garantir a existência de uma avaliação contínua dos **riscos**, **políticas** e **procedimentos** em Segurança da informação. A definição de indicadores pode explicitar o nível de qualidade da gestão na definição de prioridades de ações para garantir o alinhamento do negócio.

Garantir riscos em níveis aceitáveis. Havendo uma gestão de riscos, a Governança em Segurança da Informação deve garantir que esses riscos estejam mantidos em um nível aceitável para a organização.

Para se implementar a gestão da segurança da informação, Beal (2005) sugere o uso do método PDCA, modelo cíclico adotado por toda família ISO 27k e que está referenciada na Figura 1. O significado da sigla PDCA vem de:

- P = *Plan*, de planejar
- D = *Do*, de executar
- C = *Check*, de verificar, avaliar
- A = *Act*, de agir corretivamente

Figura 1: Modelo PDCA aplicado aos processos do SGSI.



Fonte: ABNT NBR ISO/IEC 27001 (2006).

Com o uso do método PDCA, a autora estipulou as seguintes etapas aplicadas à gestão da segurança da informação:

- Planejamento da segurança – começando do nível mais alto, identificam-se os processos críticos de negócio e dos fluxos de informação associados, para depois descer para o nível dos sistemas e serviços de informação e da infraestrutura de TI que dá suporte a tais sistemas e serviços;
- Implementação da segurança – são atividades necessárias para se colocar em prática aquilo que foi planejado para atender aos requisitos de segurança da organização;

- Avaliação e ação corretiva – nesta etapa, deve-se coletar o maior número possível de informações e averiguar se a segurança implantada atende aos requisitos da fase de planejamento;
- Análise crítica independente da segurança da informação – recomenda que seja feito, por auditoria interna ou prestador de serviços especializado na área, um levantamento que ajude a garantir que as práticas da organização permaneçam condizentes com sua política e adequadas para situação de risco existente.

Quando se implementa um processo de gestão da segurança da informação, procura-se eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível. (CARUSO: STEFFEN, 1999).

O importante é que a organização garanta que o processo de segurança da informação e sua gestão estarão sob controle e seguirão práticas que permitirão a continuidade dessa gestão ao longo do tempo de forma efetiva (FONTES, 2008).

2.2.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Para Ferreira e Araújo (2006), a Política de Segurança é definida 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 uso dos ativos de informação.

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e assume uma grande abrangência, encontrando-se subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégicas, tática e operacional. Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa (SÊMOLA, 2003).

Ferreira e Araújo (2006) ressaltam que as normas, políticas e procedimentos de segurança devem ser:

- Simples
- Compreensíveis (escritas de maneira clara e concisa);
- Homologadas e assinadas pela Alta Administração;
- Estruturadas de forma a permitir a sua implantação por fases;
- Alinhadas com as estratégias de negócio da empresa, padrões e procedimentos já existentes;
- Orientadas aos riscos (qualquer medida de proteção das informações deve direcionar para os riscos da empresa);
- Flexíveis (moldáveis aos novos requerimentos de tecnologia e negócio, dentre outros);
- Protetores dos ativos de informação, priorizando os de maior valor e de maior importância;
- Positivas e não apenas concentradas em ações proibitivas ou punitivas.

De acordo com Fontes (2008), as políticas, as normas e os procedimentos são os regulamentos que suportam e dão validade ao processo de segurança da informação e aos controles definidos que vão ser aplicados nos aspectos seguintes para:

a) **Garantir o acesso à informação.** Gestão da identidade do usuário e ciclo de vida dessa identidade. Gestão de autenticação do usuário. Gestão de autorização para acessar a informação.

b) **Classificar a informação.** Definição de níveis de sigilo da informação, do gestor da informação e do proprietário da informação.

c) **Enfrentar situações de contingência.** Definição da solução para o tempo suportável de indisponibilidade dos recursos de informação antes de impactos financeiros, operacionais ou de imagem que comprometa a continuidade da organização.

d) **Garantir a resiliência operacional.** A existência de gestão de problemas, gestão de mudanças, gestão de recursos e gestão de capacidade para

que não haja ruptura na operação do negócio, no que se refere nos recursos da informação.

e) **Proteger o ambiente físico e de infraestrutura.** Garantia de que o ambiente físico está controlado e protegido e que os elementos de infraestrutura, água, energia, temperatura, condições do ar estão adequados para o uso pelos recursos de informação.

f) **Desenvolver aplicações.** Existência de metodologia, requisitos de segurança, proteção do ambiente de desenvolvimento de sistemas, documentação para a garantia do conhecimento.

g) **Tratar incidentes de segurança.** Registrar incidentes, responder em tempo adequado e encaminhar para solução definitiva.

h) **Garantir informações para atividade forense.** Definição de ações preventivas, treinamento de usuário para tratar situações desse tipo, infraestrutura mínima de tecnologia, realização de análise forense de situações de fraude, erro ou recuperação de informação.

i) **Proteger recursos de tecnologia.** Proteção da rede da organização contra ataques externos e internos, proteção de cada computador, definição de autenticação entre recursos de tecnologia, garantia de utilização de produtos atualizados.

j) **Conscientizar e treinar os usuários.** Definir procedimentos para a conscientização, definir e implementar treinamentos necessários, garantir engajamento da direção e garantir o alinhamento com regulamento internos e externos.

k) **Definir área organizacional da segurança da informação.** Definição do escopo de atuação, definição da estrutura de pessoas e recursos, identificação das áreas gestoras de informação, identificação das áreas que utilizam a informação, identificação dos processos necessários para a gestão da segurança da informação, definição da posição organizacional.

l) **Evitar fraudes pela tecnologia.** Análise dos sistemas e processos de negócio, definição/avaliação das contramedidas, definição de monitoramento constante, definição de medidas preventivas, definição de maneiras de detecção de fraude, existência de respostas rápidas.

2.2.2 AUDITORIA

A auditoria tem como principal objetivo promover a adequação, revisão, avaliação e recomendações para o aprimoramento dos controles internos no sistema de informação de uma empresa, bem como avaliar a utilização de recursos humanos, materiais e tecnológicos envolvidos no processamento dos mesmos (SCHMIDT, 2006).

A auditoria de sistemas deve atuar em todos os sistemas da organização, seja no nível operacional, tático ou estratégico (LYRA, 2008).

Ainda segundo o autor, é possível pensar em uma metodologia de trabalho baseada nas melhores práticas e que seja flexível e aderente à todas as modalidades da auditoria de sistema da informação. Essa metodologia é composta pelas seguintes fases:

a) Planejamento e controle do projeto de auditoria de sistemas de informação

De acordo com as diretrizes da alta administração, estabelece-se o planejamento inicial das ações e recursos necessários, tendo como enfoque os sistemas a serem auditados.

b) Levantamento do sistema de informação a ser auditado

Uma vez delimitado o escopo de trabalho, ou seja, o sistema a ser auditado, inicia-se o processo de levantamento de informações relevantes sobre o sistema.

c) Identificação e inventário dos pontos de controle

Nessa etapa, busca-se identificar os diversos pontos de controle que merecem ser validados no contexto do sistema escolhido. A esse processo denominamos inventário de pontos de controle.

Cada ponto de controle deve ser relacionado juntamente com seus objetivos e funções que exercem no sistema como um todo. Devem ser identificados os seus parâmetros, suas fraquezas e técnicas de auditorias mais adequadas à sua validação.

d) Priorização e seleção dos pontos de controle do sistema auditado

Essa etapa consiste na seleção e priorização dos pontos de controle que foram inventariados na etapa anterior. A seleção dos pontos de controle pode ser efetuada com base em:

Grau de risco existente no ponto – verificação dos prejuízos que poderão ser acarretados pelo sistema a curto, médio e longo prazo. Prevê, com antecedência, quais as ameaças prováveis de um ponto.

Existência de ameaças – podemos auditar primeiramente os pontos que se encontram sob forte ameaça.

Disponibilidade de recursos – escolha dos pontos que podem ser alterados com recursos destinados.

e) Avaliação dos pontos de controle

Essa etapa consiste em realizar teste de validação dos pontos de controle, ou seja, devem-se aplicar técnicas de auditoria e ferramentas adequadas que evidenciem falhas ou fraquezas do controle interno. É auditoria propriamente dita

f) Conclusão da auditoria

É a fase em que são elaborados relatórios de auditoria contendo o resultado encontrado; diagnóstico da situação atual dos pontos de controle e, caso existam, as fraquezas do controle interno. Quando determinado ponto de controle apresentar fraqueza, transforma-o em Ponto de Auditoria, fazendo-se necessário apontar no relatório de auditoria recomendações para a solução ou mitigação dessa fraqueza.

g) Acompanhamento da auditoria

O acompanhamento da auditoria (follow-up) deve ser efetuado até que todas as recomendações tenham sido executadas e as fraquezas tenham sido eliminadas ou atinjam um nível tolerável pela organização.

2.2.3 GESTÃO DE RISCO

É através das informações que as organizações gerenciam seus produtos ou serviços e traçam suas estratégias de negócio. É por isso que os sistemas de informações se tornaram ativos críticos que necessitam serem protegidos contra ameaças que podem explorar as vulnerabilidades do sistema. Estas violações na segurança podem causar a perda da confidencialidade, integridade e disponibilidade das informações, gerando perdas financeiras e competitivas por parte das empresas afetadas (KROLL et al, 2010).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Gerenciar os riscos pode ser um processo complexo e oneroso, contribuindo para que as empresas não priorizem esse processo em projetos de segurança da informação (OLIVEIRA et al, 2009).

Segundo Beal (2005, p. 10):

> Toda a organização precisa adquirir uma visão sistêmica das suas necessidades de segurança, dos recursos a serem protegidos e das ameaças às quais está sujeita, para então poder identificar as medidas de proteção mais adequadas, economicamente viáveis e capazes de reduzir ou eliminar os principais riscos para o negócio.

Na visão de Peltier (2005), a gestão de riscos é um processo que, em geral, busca um equilíbrio entre a realização das oportunidades de ganhos e a minimização das vulnerabilidades e das perdas.

> Gestão de riscos é o processo pelo qual as medidas de segurança são selecionadas e implementadas para se atingir um nível aceitável de risco, previamente estabelecido, e a um custo razoável. Risco é também o potencial de dano ou perda a que um ativo ou grupo de ativos está sujeito. O nível baseia-se no valor atribuído pelo seu proprietário e no impacto e ou consequência causado por um evento adverso sobre aquele ativo. Risco é também a probabilidade de uma vulnerabilidade específica ser explorada por uma determinada ameaça (ROPER, apud Ohtoshi, 2008, p. 22).

Existem normas e metodologias que guiam o desenvolvimento de uma gestão de riscos, onde cada uma fornece um conjunto de diretrizes distintas para o gerenciamento dos riscos. Dentre os modelos de referência para gestão dos riscos que visam nortear as implementações necessárias está a ISO/IEC 27005 (2008). O processo descrito na norma forma um embasamento para a construção de metodologias para gestão de riscos.

.

2.3 NORMAS E MELHORES PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

As melhores práticas são as técnicas identificadas como as melhores em termos de eficácia, eficiência e reconhecimento de valor para os envolvidos e afetados direta e ou indiretamente na realização de determinadas tarefas, atividades, procedimentos, ou até mesmo, na realização de um conjunto de tarefas, atividades, procedimentos devidamente agrupados ou integrados por um objetivo comum.

“Normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia.” (BEAL, 2005, p. 36).

Sêmola (2003) diz “que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que deem uniformidade a um processo, produto ou serviço”.

Diante disso, é saudável que todas as empresas procurem uma base comum que facilite a interação e a confiança entre elas e busquem elementos que as protejam mais, conquistando diferenciais competitivos.

Atualmente existem algumas metodologias e melhores práticas em segurança da informação e governança para o ambiente de tecnologia, as quais são reconhecidas e utilizadas mundialmente como, por exemplo, a NBR ISO/IEC 177999:2005 e o CobIT (FERREIRA; ARAÚJO, 2006).

> Diferente da norma que se propõe a orientar todos no sentido de construir uma base comum de conduta, não haverá uma única e recomendada metodologia. Surgirão muitas delas simultaneamente pelas mãos de muitas empresas em diversos países, mas todas deverão estar alinhadas às diretrizes da norma sem deixar de serem adaptadas e contextualizadas a cada mercado, considerando a cultura local e as variáveis internas e externas que interferem na empresa (Sêmola, 2003, p. 74).

As melhores práticas de mercado surgiram como guias para unificar o conhecimento e a experiência de diversos executivos e gestores que atuaram durante anos para levar grandes organizações ao sucesso e para obter a maximização dos resultados do negócio. O grande diferencial não está em utilizar apenas um guia, mas sim em combinar o que cada um possui de melhor e criar uma solução customizada que seja capaz de atender às demandas de negócio de cada organização (FERREIRA; ARAÚJO, 2006).

2.3.1 NBR ISO/IEC 17799

Em 1987, o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (*Commercial Computer Security Centre*) que dentre suas atribuições tinha a tarefa de criar uma norma de segurança das informações para o Reino Unido. Assim, em 1995, este código foi revisado e publicado como uma British Standard, denominado BS7799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e crescimento da segurança da informação. (OLIVA: OLIVEIRA, 2003).

Esse documento foi disponibilizado em duas partes para consulta pública, a primeira denominada BS-7799-1, em 1995, e a segunda, a BS7799-2, em 1998. A BS7799-1 é a primeira parte da norma que contém uma introdução, definição de extensão e condições principais de uso da norma. Disponibiliza 148 controles divididos em dez partes distintas. É planejada como um documento de referência para implementar "boas práticas" de segurança na empresa. A BS7799-2 é a segunda parte da norma e tem por objetivo proporcionar uma base para gerenciar a segurança da informação dos sistemas das empresas.

Em Abril de 1999 as duas normas (a de 1995 e a de 1998) foram publicadas após uma revisão, com o nome de BS7799-1999 e estava sendo adotada por diversos outros países. A primeira parte da norma BS7799 foi submetida à "ISO" e, em maio de 2000, foi homologada como "ISO/IEC 17799:2000". Por fim, em setembro de 2001, a Associação Brasileira de Normas Técnicas – ABNT homologou a versão brasileira da norma, denominada NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação.

Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005 e finalmente incorporada na série de normas ISO 27001 e ISO 27002. As séries de normas ISO 27000 foram especificamente reservadas pela ISO para as questões de segurança da informação.

2.3.2 A FAMÍLIA ISO/IEC 27000

A família de normas ISO/IEC 27000 constitui um conjunto de normas internacionais para a gestão da segurança da informação desenvolvido pela *International Organization for Standardization* (ISO) em Genebra e a *International Electrotechnical Commission* (IEC). Estas normas fornecem um *framework* para gerenciamento de segurança da informação. As designações corretas para a maioria destas normas incluem o prefixo ISO/IEC, e todos eles devem incluir um sufixo, que é a data da publicação. O nome da maioria destas normas, no entanto, tende a ser

falado na forma abreviada. ISO/IEC 27001:2005, por exemplo, é muitas vezes denominado simplesmente ISO27001 (CALDER; WATKINS, 2008).

Abaixo estão algumas normas da família 27k:

- ISO/IEC 27000:2009 – SGSI – Visão Geral e Vocabulário
- NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação – Requisitos
- NBR ISO/IEC 27002:2005 – Código de Prática para a Gestão da Segurança da Informação
- NBR ISO/IEC 27003:2011 – Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação
- NBR ISO/IEC 27004:2010 – Métricas para a Gestão da Segurança da Informação
- NBR ISO/IEC 27005:2011 – Gestão de Riscos de Segurança da Informação
- ISO/IEC 27006:2007 – Requisitos para corpo de auditoria e certificação de SGSI
- ISO/IEC 27007– Diretrizes para auditoria de SGSI

Dentre as normas citadas acima, as mais conhecidas pelos profissionais que trabalham com a TI nas empresas são a ISO 27001 e a ISO 27002.

Segundo Palma (2011) a norma ISO 27001 “ajuda a empresa a adotar um sistema de gestão da segurança da Informação que permita mitigar os riscos de segurança atribuídos a seus ativos e adequar as necessidades a área de negócio”.

Para Palma (2011) a ISO 27002 “é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação, facilitando atingir os requisitos especificados pela Norma ISO 27001”.

Quando uma organização deseja obter uma certificação de gestão de segurança da informação ela recorrerá à ISO 27001. A certificação comprova que a

segurança da informação está sendo implementada da melhor maneira possível pelo gestor da organização.

A ISO 27002:2005 é uma norma "auxiliar" que fornece mais detalhes sobre como implementar os controles de segurança especificados na ISO 27001 (ABNT, 2005).

2.3.3 ABNT NBR ISO/IEC 27001

A norma ISO 27001:2005, que é a norma BS7799-2:2002 revisada, com melhorias e adaptações contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão já incorporaram (FERREIRA; ARAÚJO,2006).

O *framework* de segurança definido pela parte 2 da norma britânica BS7799 estabelece um SGSI – Sistema de Gestão de Segurança da Informação que, somado ao conjunto de controles sugeridos pela primeira parte da norma, serve de objeto para a certificação (SÊMOLA, 2003).

Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (ABNT NBR ISO/IEC 27001:2006).

Segundo Sêmola (2003), como ocorre na prática, o objeto da certificação não precisa necessariamente ser toda a empresa, devendo começar por um escopo restrito, normalmente um processo representativo para a natureza da atividade da empresa. Assim, os trabalhos se iniciam e desdobram em seis fases principais:

- Definição das diretrizes da política de segurança;
- Definição do SGSI – Sistema de Gestão de Segurança da Informação;
- Execução de uma análise de riscos;
- Definição de uma estrutura para gerenciamento de risco;
- Seleção dos objetos de controles e os controles aplicáveis;
- Preparação da Declaração de Aplicabilidade dos Controles.

2.3.4 ABNT NBR ISO/IEC 27002

A Norma NBR ISO/IEC 27002, originalmente publicada como NBR ISO/IEC 17799 e depois renomeada, é uma adaptação da norma britânica *BS 7799* – Parte 1 – *Código de prática para a Gestão da Segurança da Informação* e tem como objetivo fornecer recomendações básicas e mínimas para a gestão de segurança da informação (FONTES, 2008).

Esta Norma é equivalente à ISO/IEC 17799:2005, hoje publicada com a nomenclatura de ABNT NBR ISO/IEC 27002.

A Norma ISO/IEC 27002 possui uma estrutura com 11 seções de controle de segurança da informação, que totalizam, juntas, 39 categorias principais de segurança e uma seção introdutória que aborda a análise/tratamento de riscos. As 11 seções são:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;
- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gestão das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade do Negócio;
- Conformidade.

1. Política de Segurança da Informação: recomendações para a criação de uma política de segurança da informação alinhada aos objetivos do negócio. Contendo: diretrizes, princípios e regras que irão prover orientação e apoio para implantação e manutenção da segurança, com apoio da alta direção;
2. Organização da Segurança da Informação: orienta a direção da organização no planejamento, implementação e controle do gerenciamento da segurança da informação;

3. Gestão de Ativos: recomendações sobre a realização de inventário dos ativos informacionais e atribuição de responsabilidades pela manutenção dos controles necessários para protegê-los;

4. Segurança em Recursos Humanos: recomendações para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações;

5. Segurança Física e do Ambiente: recomendações para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis ao negócio contra acesso não autorizado, dano ou interferência;

6. Gestão das Operações e Comunicações: recomendações para garantir a operação correta e segura dos recursos de processamento de informações e proteger a integridade de serviços e informações;

7. Controle de Acesso: recomendações para a monitoração e o controle do acesso a recursos computacionais, para protegê-los contra abusos internos e ataques externos;

8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação: recomendações para o uso de controles de segurança em todas as etapas do ciclo de vida forçam que, com todos os esforços de TI, tudo seja implementado e mantido com a segurança em mente, usando controles de segurança em todas as etapas do processo;

9. Gestão de Incidentes da Segurança da Informação: recomendações para notificação de fragilidades e eventos de segurança da informação, responsabilidades e procedimentos e coleta de evidências;

10. Gestão da Continuidade do Negócio: recomendações para preparar a organização para neutralizar as interrupções às atividades comerciais e proteger os processos críticos em caso de ocorrência de falha ou desastre;

11. Conformidade: recomendações para a preservação da conformidade com requisitos legais (tais como direitos autorais e direito à privacidade), com normas e diretrizes internas e com os requisitos técnicos de segurança.

Estes controles podem compor o escopo do sistema de gerência de segurança tendo como foco os negócios da empresa (ALVES, 2006).

2.3.5 ABNT NBR ISO/IEC 27005

Esta Norma Internacional, criada em julho de 2008, fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001. Entretanto, esta Norma Internacional não inclui uma metodologia específica para a gestão de riscos de segurança da informação. Cabe à organização definir sua abordagem ao processo de gestão de riscos, levando em conta, por exemplo, o escopo do seu SGSI, o contexto da gestão de riscos e o seu setor de atividade econômica. Há várias metodologias que podem ser utilizadas de acordo com a estrutura descrita nesta Norma Internacional para implementar os requisitos de um SGSI (ABNT NBR ISO/IEC 27005, 2008).

Segundo a norma, o conhecimento dos conceitos, modelos, processos e terminologias descritos na ABNT NBR ISO/IEC 27001 e na ABNT NBR ISO/IEC 27002 é importante para um entendimento completo desta Norma Internacional.

A norma ABNT NBR ISO/IEC 27005 se aplica a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização (ABNT NBR ISO/IEC 27005, 2008).

As atividades de gestão de riscos de segurança da informação, apresentadas na Seção 6 da norma, são as seguintes:

- Definição do contexto,
- Análise/avaliação de riscos,
- Tratamento do risco,
- Aceitação do risco,
- Comunicação do risco,
- Monitoramento e análise crítica de riscos.

2.3.6 CobIT - O FRAMEWORK RISK IT E VAL IT

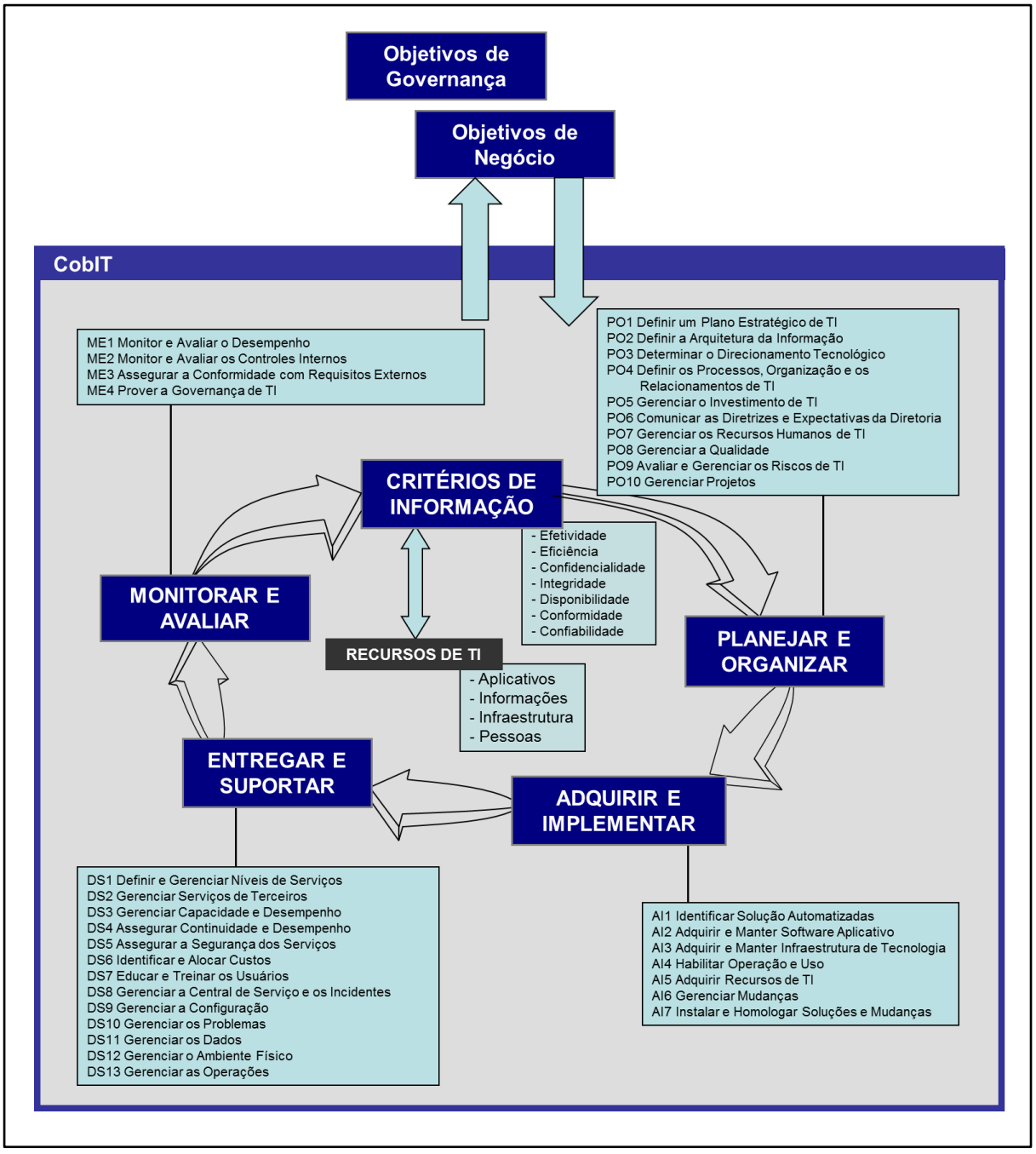
O CobIT, assim como as normas acima citadas, provê boas práticas para o gerenciamento dos processos de TI em uma estrutura lógica e gerenciável, encontrando as múltiplas necessidades do gerenciamento empresarial, interligando os gaps entre os riscos de negócio, assuntos técnicos, necessidades de controle e requisitos de medições de desempenho (NERY e PARANHOS, 2003).

> O CobIT (*Control Objectives for Information and Related Technology*), elaborado pelo ISACA (*Information Systems Audit and Control Association*), é um modelo de estrutura de controles internos orientado para o entendimento e o gerenciamento dos riscos associados ao uso da Tecnologia da Informação. Sua estrutura de controles possui padrões aceitos mundialmente como os melhores praticados para o estabelecimento de controles e padrões de segurança para a área de Tecnologia da Informação das empresas dos mais variados segmentos de negócio, principalmente do setor financeiro (FERREIRA; ARAÚJO, 2006, p. 32).

O CobIT possui 210 objetivos de controle divididos em 34 processos agrupados em 4 domínios (LAHTI, 2006). Na Figura 2 temos a demonstração de cada processo detalhado. São eles:

- Planejamento e Organização (PO)
- Aquisição e Implementação (AI)
- Entrega e Suporte (DS)
- Monitoração e Avaliação (ME)

Figura 2: Visão geral do Modelo do Cobit.



Fonte: *IT Governance Institute (*2002, p.22).

Planejamento e Organização (PO)

O domínio de Planejamento e Organização é composto de 10 processos e trata do desenvolvimento dos planos estratégicos de TI e fornece suporte aos objetivos e

metas empresariais. Os planos devem objetivar o futuro e estar alinhados com o planejamento da organização.

Aquisição e Implementação (AI)

O domínio de Aquisição e Implementação é composto de sete processos e trata da aquisição de novas tecnologias, contratação e desenvolvimento de uma equipe qualificada para executar os planos estratégicos de TI. A fase de Implementação foca a manutenção, teste, certificação e identificação das alterações que possam afetar a disponibilidade das informações.

Entrega e Suporte (DS)

O domínio de Entrega e Suporte é composto de treze processos e trata da entrega dos serviços de TI, assegurando que os serviços sejam executados conforme definido na implementação através de acordos de nível de serviço (SLA - *Service Level Agreement*). A fase de suporte prevê que os processos sejam executados de forma eficiente e efetiva.

Monitoração e Avaliação (ME).

O domínio de Monitoração e Avaliação é composto de quatro processos e foca o monitoramento, através dos SLAs, verificando se o que foi proposto está sendo realizado. Através de auditorias internas e externas são analisados os processos de negócio e o resultado da auditoria permite que os processos sejam ajustados para atender as expectativas da direção da organização.

O CobIT considera como requisitos para a informação: efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade. E como recursos de TI: pessoas, sistemas, tecnologia, infraestrutura e dados (Alves, 2006).

2.3.6.1 O FRAMEWORK RISK IT

Framework de processo é um modelo que integra uma série de guias, políticas e métodos que representam uma determinada abordagem a um determinado assunto.

A necessidade do tratamento específico de determinados assuntos que, ao longo dos anos, vem ficando cada vez mais complexos ensejou o desenvolvimento de *frameworks* de processos que hoje são de conhecimento comum, com focos específicos, tais como:

O *framework* RISK IT menciona três categorias de risco de TI: a primeira está relacionada à entrega de serviços de TI e diz respeito à área de operações, no que tange ao desempenho, disponibilidade, *compliance* e segurança das atividades diárias; a segunda trata da entrega das soluções de TI e em conexão aos programas e projetos da organização, tendo como componentes as oportunidades de negócio, investimento, custo, prazo e escopo: e, por fim, a terceira categoria é a dos benefícios e valor para a TI, na qual se analisam os riscos envolvidos na área de negócio, eficiência e eficácia e busca a melhoria de processos.

Assim, o risco de TI refere-se aos riscos corporativos que serão gerados se os serviços de TI não forem entregues, se novas soluções que aproveitam oportunidades de negócio não forem concretizadas ou se não houver benefícios para a organização gerados por TI.

Fischer (2009) analisa que o *framework* Risk IT está fundamentado em princípios para a gestão efetiva do risco de TI que possuem lastro em outros princípios geralmente aceitos para o gerenciamento do risco, como COSO ERM e a ISO 31000. Essas estruturas foram adaptadas para sua aplicação no domínio da TI, sendo os princípios do RISK IT relacionados a:

- Governança do Risco de TI;
- Alinhamento aos riscos do negócio;
- Alinhamento da gestão dos riscos de TI à gestão de riscos da organização;
- Realização de análise de custo/benefício do gerenciamento de riscos;
- Efetivação do gerenciamento de risco da organização;

- Promoção da comunicação aberta e honesta do risco de TI;
- Estabelecimento de estrutura de responsabilidade pelas operações por meio de níveis aceitáveis e bem definidos de tolerância a risco; e
- Promoção do gerenciamento do risco de TI como um processo diário e contínuo na vida da organização.

2.3.6.2 O FRAMEWORK VAL IT

Uma governança de TI não consegue sobreviver sem uma governança corporativa, e vice-versa, não apenas por estarem relacionadas, mas também pelo reconhecimento das empresas nos benefícios alcançados com a tecnologia da informação e a utilização destes para direcionar os valores das partes interessadas do negócio.

O Val IT considera a governança corporativa, ajudando os executivos a se concentrar em questões fundamentais relacionadas à governança de TI nas perspectivas de criação de valor e investimentos, sejam financeiros ou não financeiros.

O *framework* do CobIT e do Val IT apoiam as necessidades das empresas que lidam com a governança corporativa TI, como parte da governança corporativa da empresa. O *IT Governance Institute* (ITGI) define Governança Corporativa de TI como: “O conjunto de responsabilidades, bem como a liderança, as estruturas organizacionais e processos, exercidos pelo conselho de administração e gestores executivo para garantir que a TI gere valor para a empresa. Uma parte integrante da governança global da empresa, a governança corporativa de TI garante que TI sustente e estenda os crescentes objetivos das estratégias da empresa”.

A estrutura Val IT é apoiado por publicações e ferramentas operacionais e fornece orientação para:

- Definir a relação entre a TI e os negócios e as funções na organização com responsabilidades de governança;
- Gerenciar carteira de investimentos em negócios habilitados por TI de uma organização;

- Maximizar a qualidade de casos de negócios para investimentos em negócios habilitados por TI, com especial destaque para a definição de indicadores financeiros, a quantificação dos benefícios "soft" e a avaliação global do risco de queda.

Val IT aborda investimentos empresariais suposições, custos, riscos e resultados relacionados a um portfólio equilibrado de TI habilitados. Ele também fornece a capacidade de *benchmarking* e permite às empresas trocar experiências sobre as melhores práticas para a gestão de valor.

3 CONTINUIDADE DE NEGÓCIO

Qualquer evento que possa impedir a organização de atingir seus objetivos é uma ameaça. O risco é a possibilidade dessa ameaça se transformar em realidade. Realizar a escolha das ameaças de maior impacto e manter continuamente essa avaliação é realizar a gestão do risco (FONTES, 2008).

De acordo com o autor, antes do evento da ameaça se concretizar, são executadas ações preventivas que buscam minimizar os riscos e ações de flexibilidade operacional que possibilitam a organização enfrentar situações sem que haja interrupção do negócio.

Mas, toda organização deve estar preparada para enfrentar situações de contingência e de desastre que tornem indisponíveis recursos que possibilitam o uso de suas informações.

Continuidade de negócio é capacidade da organização em continuar a entrega de produtos ou serviços em um nível aceitável previamente definido após incidente de interrupção (ABNT/ISO 22301,2013).

3.1 GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Dentre as diversas definições sobre o processo de Gestão de Continuidade de Negócios encontradas na literatura, destaca-se, por sua abrangência e credibilidade acadêmica, a apresentada na norma ABNT/NBR ISO 22301 (2013, p.6), a qual veio substituir a ABNT NBR 15999-2:2010:

> Gestão de Continuidade de Negócios (GCN) é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder eficazmente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado.

Westerman e Hunter (2008) definem GCN como um processo que consiste em compreender e reduzir o potencial de eventos catastróficos para afetar processos

comerciais essenciais, sendo parte fundamental da gestão de risco e a base da pirâmide do risco de TI.

A Gestão de Continuidade de Negócio engloba toda a organização e incluem políticas, padrões e procedimentos para garantir que operações específicas possam ser mantidas ou recuperadas em tempo oportuno após um evento de interrupção (BIS apud FRIEDENHAIN, 2006).

A preocupação em ampliar a visão empresarial sobre este importante processo se deve ao fato de a GCN estar intimamente relacionada à estratégia organizacional, ajudando a garantir que as metas e objetivos não sejam afetados por interrupções inesperadas, garantindo a entrega de produtos e serviços dos quais dependem a reputação e sobrevivência da organização.

A implementação de um sistema de gestão de continuidade pode gerar diversos benefícios, exemplos disso incluem:

- Proteção de valor para os acionistas;
- Melhor compreensão do negócio, obtido através da identificação e análise de riscos;
- Resiliência operacional que resulta da implementação de redução de risco;
- O tempo de inatividade é reduzido quando processos alternativos e soluções alternativas são identificadas;
- Documentos e Registros vitais podem ser mantidos e protegidos;
- Melhora da eficácia operacional através de um programa de reengenharia de processos de negócios e/ou de TI;
- Preservação no mercado, garantindo a continuidade da prestação de serviços;
- Melhoria da segurança em geral.

Qualquer evento que comprometa o tempo máximo de indisponibilidade do processo de negócio, ou seja, tempo que o negócio pode ficar inoperante sem causar prejuízos significativos, é considerado um desastre a ser contido através do Plano de Continuidade de Negócios (LAWER; SZYGENDA, 2007).

3.2 PLANO DE CONTINUIDADE DE NEGÓCIO

O objetivo de um Plano de Continuidade de Negócio é garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre, ou seja, contingenciar situações e incidentes de segurança que não puderam ser evitados (SÊMOLA, 2003).

De acordo com o autor,

> Uma empresa possuirá diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos e, ainda, se preocupar com múltiplas ameaças potenciais. Esta segmentação é importante; afinal uma empresa tem processos cuja tolerância à falha é variável, os impactos idem, assim como o nível de segurança necessário à natureza das informações manipuladas (SÊMOLA, 2003, p. 99).

Fontes (2008) diz que a definição e desenvolvimento do plano de continuidade de negócio (PCN) devem ser específicos para cada organização, pois deve ser baseado em uma análise de impacto no negócio caso ocorra indisponibilidade dos recursos da informação.

O sucesso do PCN vai depender do conhecimento e treinamento de todas as pessoas envolvidas na sua elaboração e execução, inclusive da direção.

Segundo Sêmola (2003) a elaboração de um plano de continuidade de negócios segue algumas etapas, definidas como:

a) Análise de impactos no negócio

A primeira etapa para a elaboração de um plano de continuidade de negócios, conhecida mundialmente pela sigla BIA – *Business Impact Analysis*, é fundamental por fornecer informações do grau de relevância entre os processos ou atividades que fazem parte do escopo da contingência em função da continuidade do negócio. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que suportam

cada um deles, para então apurar os impactos quantitativos que poderiam ser gerados com a sua paralização total ou parcial.

b) Estratégias de contingência

Na definição do Dicionário Aurélio, contingência é: “ação ou situação imprevista e que não se consegue controlar; eventualidade”.

A escolha de qualquer uma das estratégias, a seguir, depende diretamente do nível de tolerância que a empresa pode suportar e ainda depende do nível de risco que a mesma está disposta a correr. Esta decisão pressupõe a orientação obtida por uma análise de riscos e impactos que gere subsídios para apoiar a escolha mais acertada.

Hot-site

Estratégia “quente” ou pronta para entrar em operação assim que uma situação de risco ocorrer. Exemplo: um servidor de banco de dados teria a tolerância de milissegundos para garantir a disponibilidade de seu serviço.

Warm-site

Esta estratégia se aplica a objetos com maior tolerância à paralisação, podendo permanecer indisponível por mais tempo, até o retorno operacional da atividade. Exemplo: serviço de e-mail que poderia ficar indisponível por minutos sem gerar impactos significativos

Relocação de Operação

Tem como objetivo desviar a atividade atingida pelo evento que provocou a quebra de segurança para outro ambiente físico, equipamento ou link. Exemplo: redirecionamento do tráfego de dados de um roteador ou servidor com problemas para outro que possua folga de processamento e suporte o acúmulo de tarefas

Bureau de Serviços

Esta estratégia considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado, fora dos domínios da empresa. Torna-se restrita a poucas situações por possuir um tempo de tolerância maior devido à reativação operacional da atividade e requer atenção especial quanto aos mecanismos de controles adotados para a segurança de suas informações.

Acordo de Reciprocidade

Conveniente para atividades que demandariam investimentos de contingência inviáveis ou incompatíveis com a importância da mesma. Esta estratégia propõe um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional. Apesar da redução significativa de investimentos, estas empresas precisam adotar procedimentos que reduzam a exposição das informações que estarão circulando em ambiente de terceirizado, principalmente quando se trata da concorrência.

Cold-site

Esta estratégia propõe uma alternativa de contingência a partir de um ambiente com recursos mínimos de infraestrutura e telecomunicações, sendo aplicável a situações com indisponibilidade ainda maior.

Autossuficiência

Muitas vezes a autossuficiência é a melhor ou a única estratégia possível para determinada atividade. Isso ocorre quando nenhuma outra é aplicável, quando os impactos não são significativos ou quando são inviáveis seja financeiramente, tecnicamente ou estrategicamente.

c) Planos de Contingência

São desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. É subdividido em três módulos distintos e complementares que tratam de cada momento vivido pela empresa.

Plano de Administração de Crise

Este documento tem o propósito de definir passo-a-passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente e os procedimentos a serem executados pela mesma equipe. A comunicação do ocorrido à imprensa é um exemplo típico de tratamento dado pelo plano.

Plano de Continuidade Operacional

Este documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio. Orientar as ações diante da queda de uma conexão à internet é um exemplo de desafio organizado pelo plano.

Plano de Recuperação de Desastre

Este documento tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, restabelecendo o ambiente as condições originais de operação.

Os três planos precisam passar por baterias severas de testes e homologação, a fim de garantir sua eficiência e permitir ajustes diante de previsíveis mudanças físicas, tecnológicas e humanas que ocorrem frequentemente no ambiente corporativo.

3.2.1 MODELO DE MATURIDADE

Segundo Pereira Júnior (2008), é fundamental que as organizações conheçam o status atual dos seus processos de negócio e definam qual o nível de gestão e controle que desejam oferecer aos seus clientes. Os modelos são utilizados para controle dos processos de negócio e fornecer um método eficiente para classificar o status atual da organização.

A seguir estão descritos os níveis do modelo de maturidade:

Nível zero (Inexistente) - Os riscos, vulnerabilidades e ameaças nos processos de TI não são conhecidos. A organização não reconhece a continuidade de negócios como um aspecto a ser considerado.

Nível um (Inicial) - A organização reconhece que a continuidade de negócios é necessária e deve ser considerada. As responsabilidades são informais e limitadas.

As soluções de contorno para resposta aos incidentes utilizam diversas abordagens reativas e inapropriadas.

Nível dois (Repetitivo) - Não existe um Plano de Continuidade de Negócios documentado apesar dos princípios serem conhecidos. Não há treinamento ou divulgação formal de procedimentos padronizados e, quanto às responsabilidades, existe um alto grau de dependência em relação ao conhecimento individual.

Nível três (Definido) - Os processos e procedimentos estão padronizados, documentados e divulgados através de treinamento, objetivando identificar, minimizar ou eliminar situações de indisponibilidade. A execução regular de testes e exercícios é realizada, de forma planejada, documentada e avaliada pelas partes usuárias.

Nível quatro (Administrado) - Existe uma forma para monitorar e mensurar o cumprimento dos processos e procedimentos. São realizados testes para avaliar a necessidade de constante manutenção das atividades e propiciar a adoção de melhores práticas. Os incidentes são classificados e conhecimentos por todos os envolvidos. Metas e métricas para a continuidade do negócio foram desenvolvidas e acordadas, mas de uma forma limitada.

Nível cinco (Otimizado) - Os processos e procedimentos são definidos ao nível de melhores práticas e com base no resultado de melhorias continuas e benchmarking de outras organizações. O Plano de Continuidade de Negócios é discutido pela direção e o gerenciamento de risco faz parte da cultura da organização. Os planos de procedimentos para assegurar a continuidade de negócio são atualizados e validados periodicamente.

3.3 NBR ISO/IEC 22301

A ISO 22301, primeira norma internacional a nível mundial para a Gestão de Continuidade de Negócios (BCM), foi desenvolvida para ajudar as organizações a minimizar o risco associado a acontecimentos disruptivos. A ISO lançou oficialmente a ISO 22301 “Segurança da sociedade – Sistemas de gestão de continuidade de negócios – Requisitos”, a nova norma internacional para Sistemas

de Gestão de Continuidade de Negócio (SGCN). Esta norma vem substituir a atual norma ABNT NBR 15999-2:2010.

Esta Norma especifica requisitos para estabelecer e gerenciar um eficaz Sistema de Gestão de Continuidade de Negócios (SGCN). Um SGCN reforça a importância de:

- entender as necessidades da organização e a imprescindibilidade de estabelecimento de política e objetivos para a gestão de continuidade de negócios;
- implementar e operar controles e medidas para a gestão da capacidade geral da organização para gerenciar incidentes de interrupção;
- monitorar e analisar criticamente o desempenho e a eficácia do SGCN; e
- melhorar continuamente com base na medição objetiva.

O SGCN, assim como outros sistemas de gestão, possui os seguintes componentes chave:

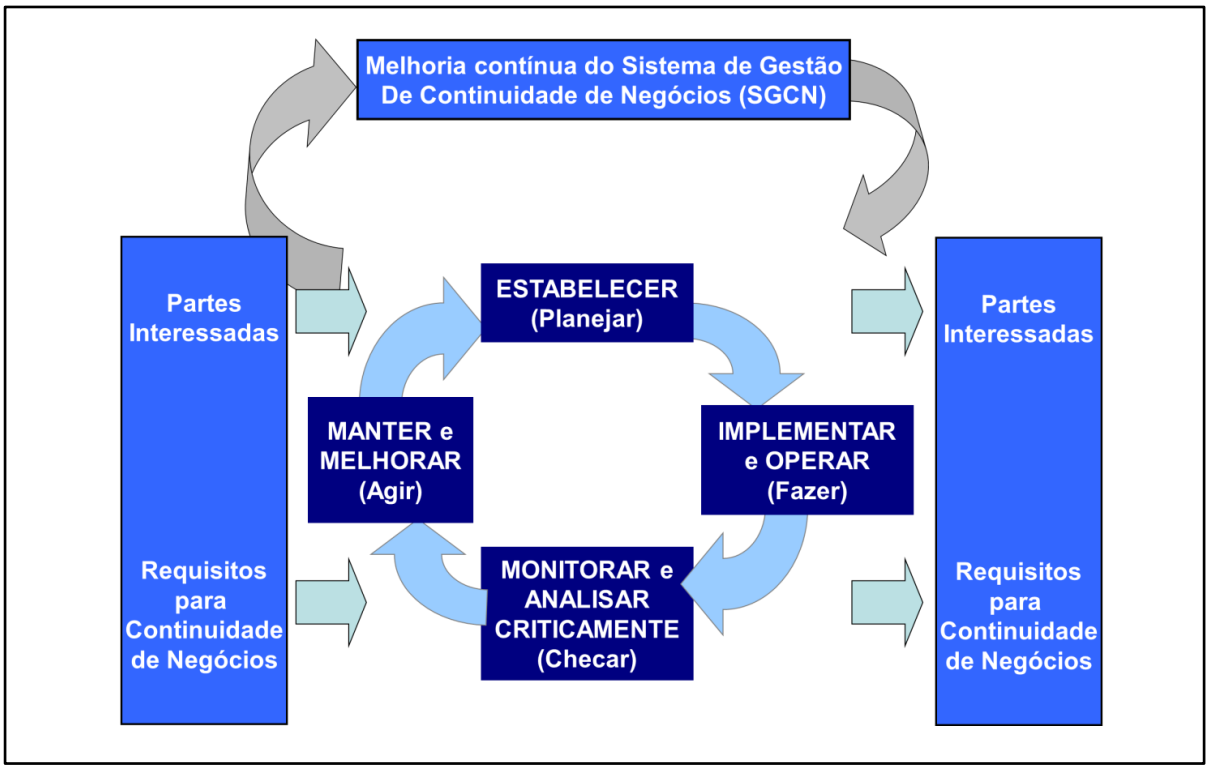
a) uma política;
b) pessoas com responsabilidades definidas;
c) processos de gestão relativos a:
    - política;
    - planejamento;
    - implementação e operação;
    - avaliação de desempenho;
    - análise crítica pela Direção e
    - melhorias.
d) documentação fornecendo evidências auditáveis; e
e) quaisquer processos de gestão da continuidade de negócios pertinentes à organização.

Esta Norma adota o modelo "*Plan-Do-Check-Act*" para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente a eficácia do SGCN de uma organização, suportando assim a

implementação consistente e integrada e a operação com sistemas de gestão relacionados.

A Figura 3 ilustra como um SGCN considera como entradas as partes interessadas e os requisitos de continuidade de negócios e, por meio de ações necessárias e processos, produz resultados de continuidade (por exemplo, continuidade de negócios gerenciada) que atendem aqueles requisitos.

Figura 3: Modelo PDCA aplicado aos processos do SGCN.



Fonte: ABNT NBR ISO 22301 (2013).

Os requisitos especificados na ISO 22301 são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do tipo, dimensão e natureza da organização. O campo de aplicação destes requisitos depende do ambiente de trabalho e complexidade da organização em causa.

As principais cláusulas da ISO 22301:2012 encontram-se organizadas da seguinte forma:

Cláusula 4: Contexto da organização
Cláusula 5: Liderança

Cláusula 6: Planeamento
Cláusula 7: Suporte
Cláusula 8: Operação
Cláusula 9: Avaliação de desempenho
Cláusula 10: Melhoria

Com a ISO 22301, você poderá:

- Estabelecer, implementar, manter e melhorar seu Sistema de Gestão de Continuidade dos Negócios;
- Cumprir os requisitos de sua política de continuidade de negócios;
- Dar às partes interessadas a confiança em seu compromisso com a conformidade para ser reconhecido internacionalmente nas melhores práticas;
- Alcançar a certificação BSI de seu Sistema de Gestão de Continuidade dos Negócios.

4 ESTUDO DE CASO

O estudo de caso foi feito em uma empresa familiar de médio porte, assim denominada por apresentar um faturamento anual acima de R$ 2,4 milhões. Pertencente ao setor varejista se encontra em considerável crescimento e atende ao escopo proposto e referenciado no Capítulo 1 deste trabalho, cujo questionamento inicial é o porquê este tipo de empresa geralmente não adota um plano de continuidade de negócio.

4.1 A EMPRESA

Por questões de confidencialidade de informações, a empresa objeto deste estudo será apresentada com o nome fictício de Empresa X.

A Empresa X atua há 20 anos como importadora e distribuidora de forros, divisórias, pisos laminados, painel wall e outros, e é composta por 95 funcionários, além de vendedores e fornecedores.

Na Tabela 1 podemos observar como se encontra a distribuição dos departamentos, seus funcionários e equipamentos de TI, os quais estão interligados por uma rede interna e externa, com comunicação via internet, responsável pela maioria dos negócios realizados.

Por ser uma empresa familiar, apresenta centralização na gestão do seu negócio, o que faz com que adiem ao máximo a decisão de investir em TI, principalmente no que diz respeito à segurança de seus dados e continuidade do negócio, fatos que não consideram tão relevantes para a sobrevivência da empresa.

Entretanto, eles já parecem cientes de que sua sobrevivência depende da melhoria nos seus processos internos, de um atendimento mais ágil aos clientes e de um melhor gerenciamento de resultados e informações estratégicas, mas não conseguem associar isso a disponibilidade, confidencialidade, integridade e auditabilidade, ou seja, a segurança de suas informações.

Embora já exista uma padronização e controle de tarefas, estes não são exercidos de forma competente pelos funcionários para as funções assumidas, gerando algumas vezes, insatisfação do consumidor final.

Tabela 1: Distribuição Organizacional e de TI.

Departamentos	Funcionários	Computadores	Impressoras
		1 servidor	
Vendas	30	30	3
Expedição/Estoque	5	4	
Departamento Pessoal	5	7	
Contabilidade	10	10	1
Faturamento	5	5	2
Caixa	3	3	
Logística	6	6	
Direção	3	3 Desktop / 2 Notebooks	1
Téc. Programação	3	3	
Motoristas	20	-	
Monitoramento	3	3	
Segurança	2	1	
Total	95	77	7

Fonte: Próprio autor.

Com relação à análise da existência de um plano de continuidade de negócio ou parte dele, a empresa se encontra no nível zero de maturidade, segundo o modelo apresentado na seção 3.2.1 do Capítulo 3. Os riscos, vulnerabilidades e ameaças nos processos de TI não são conhecidos. A organização não reconhece a continuidade de negócios como um aspecto a ser considerado.

O primeiro item a ser abordado é a conscientização corporativa sobre os riscos da falta de uma política de segurança e de um PCN, podendo estes levar a significantes perdas financeiras ou de imagem, impossibilidade de atender às solicitações dos clientes, impossibilidade de entrega de produtos, entre outros.

Embora a empresa atinja alto grau de lucratividade, devido ao bom preço de seus produtos em relação ao do mercado, pode ser extinta pela concorrência, ou pela perda de seus dados, ou ainda pode ter prejuízo de imagem e reputação quando não puder honrar seus compromissos.

4.2 TESTE DE VERIFICAÇÃO QUANTO À SEGURANÇA DAS INFORMAÇÕES

Foi elaborado um teste a fim de despertar a percepção da empresa quanto ao grau de conformidade em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ISO/IEC 27002 e demonstrados no Apêndice A. Na realidade, através dos índices obtidos com a pontuação final, será possível verificar o quão distante a empresa está do quem vem sendo considerado referência nacional e internacional de gestão de segurança da informação. Este teste foi elaborado seguindo o modelo sugerido por Sêmola (2003).

A Tabela 2 demonstra como deve ser adicionada a pontuação.

Tabela 2: Tabela de pontuação – teste de controle de segurança.

OPÇÃO	ADICIONAR
SIM	2 PONTOS
DESATUALIZADA	1 PONTO
NÃO	0 PONTOS

Fonte: Próprio autor.

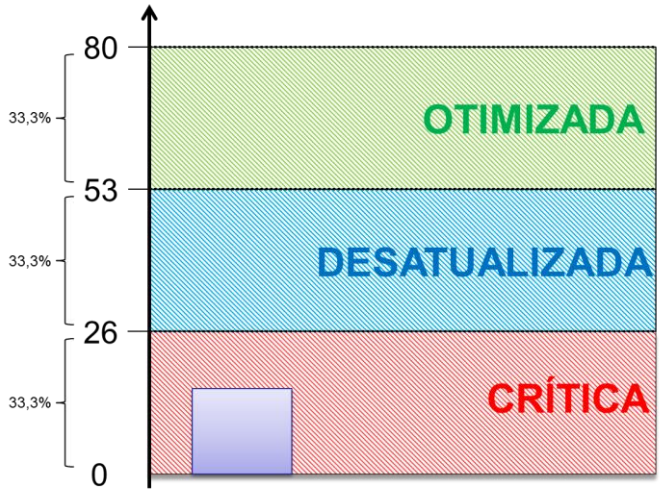
Se o resultado for entre 80 e 54, a empresa deve estar em destaque por conta da abrangência dos controles que aplica no negócio.

Se o resultado estiver entre 53 e 27, a empresa pode ter adotado a maioria dos controles, porém a maioria dos quesitos pode estar defasada, o que demonstra deficiência na gestão ou falta de recursos financeiros, ou ainda, falta de uma análise de risco para priorização das atividades.

Se o resultado estiver entre 26 e 0, significa que a segurança não está sendo tratada como prioridade e a pontuação indica ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser desconhecimento dos riscos, falta de sensibilização dos executivos ou, até mesmo, devem estar acontecendo ações isoladas entre departamentos que não distribuem uniformemente a segurança, diminuindo o nível de segurança do negócio.

A empresa estudada, como já era de se esperar, apresentou pontuação igual a 15, resultado abaixo de 26, considerado crítico, demonstrado no Gráfico 1.

Gráfico 1: Resultado da análise de verificação de controle de segurança.



Fonte: Próprio autor.

Mas o teste não fugiu do objetivo principal: análise de maturidade quanto à segurança da informação e conscientização da importância de uma análise de risco com priorização de ações.

4.3 ESTRATÉGIA DE CONTINGÊNCIA

Quando alguma situação de contingência ocorrer, ou seja, aquela impossível de ser controlada, é preciso escolher uma estratégia. Essa escolha depende do nível de tolerância quanto ao tempo da paralização e do nível do risco e impacto que a empresa está disposta a suportar. Como exemplo podemos citar o tempo de tolerância de paralização de um servidor de banco de dados comparado com o de um servidor de e-mails, onde o tempo de paralização provoca impactos diferentes, consequentemente, tempos de tolerâncias diferentes.

4.3.1 ANÁLISE DE RISCO E DE IMPACTO NA EMPRESA X

Nesta etapa foi feito o levantamento dos ativos críticos do negócio que poderão ser afetados por falhas e erros no processo, objetivando a proteção dos processos críticos de negócio e salvaguarda dos ativos da companhia, um elemento importante na prevenção de desastres.

Os objetivos principais desta fase são:

- Detectar os riscos existentes nas instalações;
- Identificação das ameaças e das vulnerabilidades existentes; e
- Qualificação dos riscos encontrados.

É preciso fazer a Análise de Risco indicando as vulnerabilidades encontradas e mensurar seus impactos de forma clara e objetiva, pois, só assim um PCN vai ter sucesso e será aceito e aprovado pela organização.

Na Tabela 3 podemos observar as ameaças e vulnerabilidades com alto impacto ao negócio e, igualmente, um grupo expressivo com alta e média probabilidade de ocorrer, definitivamente um cenário preocupante.

Tabela 3: Ameaças e vulnerabilidades com alto impacto ao negócio.

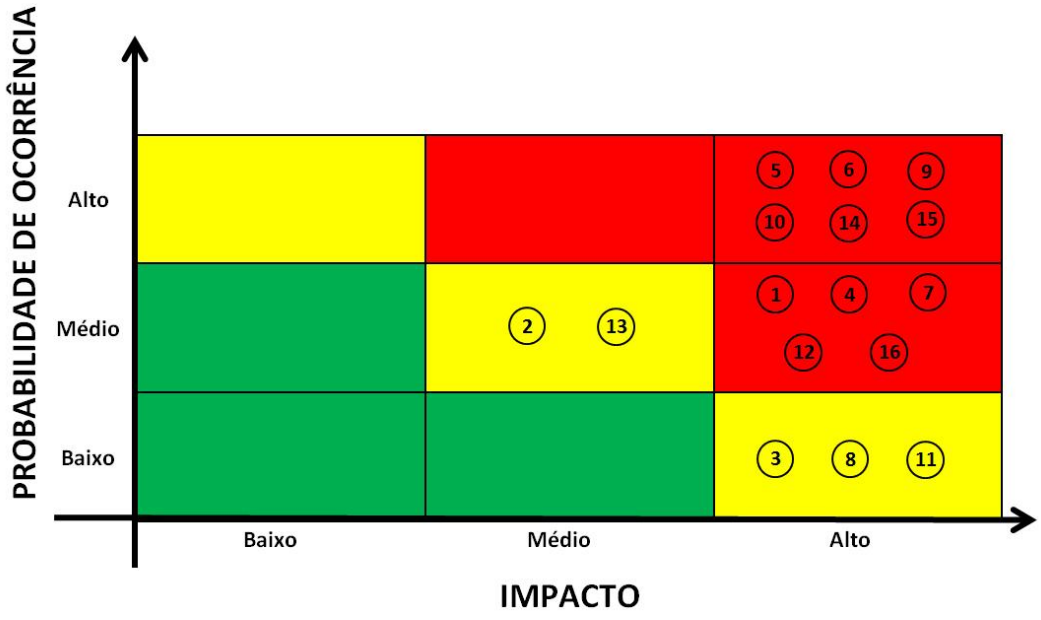
ID	Vulnerabilidade	Ameaça	Consequência	Probabilidade de Ocorrência	Impacto
1	Armazenamento não protegido	Furto de mídia ou documentos	Impossibilidade de acesso à informação		
2	Aparelho sem manutenção preventiva	Interrupção de funcionamento do equipamento	Interrupção de atividade		
3	Software amplamente distribuído	Comprometimento dos dados	Impossibilidade de acesso à informação		
4	Gerenciamento de senhas mal feito	Forjamento de direitos	Acesso não autorizado		
5	Inexistência de um controle eficaz de mudança	Defeito de software	Atraso na realização dos processos		
6	Inexistência de cópias de segurança (“back-up”)	Perda de dados	Inoperabilidade de atividades		
7	Inexistência de evidências que comprovem o envio ou o recebimento de mensagens	Repúdio de Ações	Não realização de um negócio		
8	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação	Indisponibilidade dos serviços		
9	Gerenciamento de rede inadequado (quanto à flexibilidade de roteamento)	Saturação do sistema de informação	Indisponibilidade dos serviços		
10	Falta de conscientização em segurança	Acesso não autorizado	Roubo de informações		
11	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de equipamentos	Atraso na realização de atividades		
12	Fornecimento de energia instável	Interrupção do suprimento de energia	Paralização dos servidores		
13	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de equipamentos	Prejuízo ao negócio		
14	Inexistência de um procedimento formal para o registro e a remoção de usuários	Abuso de direitos	Acesso não autorizado		
15	Inexistência de um plano de continuidade	Falha de equipamento	Atraso na entrega do produto		
16	Inexistência de política de uso de correspondência eletrônica (e-mail)	Erro durante o uso	Prejuízo de imagem da organização		

Fonte: Próprio autor.

Na Figura 4 temos a identificação do nível de risco dos itens acima (IDs) através da relação impacto e probabilidade. Os critérios de probabilidade e impactos definidos por Vargas (2009), seguem as seguintes regras:

- Probabilidade
  - Baixa – a probabilidade de ocorrência do risco pode ser considerada pequena ou imperceptível (menor do que 20%).
  - Média – existe uma probabilidade razoável de ocorrência do risco (probabilidade entre 20 e 60%).
  - Alta – O risco é iminente (probabilidade maior que 60%).
- Impacto
  - Baixo – O impacto do evento de risco é irrelevante para o projeto, tanto em termos de custo quanto de prazos, podendo ser facilmente resolvido.
  - Médio – O impacto do evento de risco é relevante para o projeto e necessita de um gerenciamento mais preciso, sob pena de prejudicar os seus resultados.
  - Alto – O impacto do evento de risco é extremamente elevado e, no caso de não existir uma interferência direta, imediata e precisa da equipe do projeto, os resultados serão seriamente comprometidos.

Figura 4: Análise de Riscos.



Fonte: Próprio autor.

O nível do risco deve atender a seguinte classificação, sendo impacto (IMP) x probabilidade (PROB): BAIXO (Verde), MÉDIO (Amarelo) e ALTO (Vermelho). Exemplos:

- $PROB_{(ALTO)}$ x $IMP_{(BAIXO)}$ = $AMARELO_{(MÉDIO)}$
- $PROB_{(MÉDIO)}$ x $IMP_{(ALTO)}$ = $VERMELHO_{(ALTO)}$

A partir da conclusão da Análise de Risco, inicia-se a elaboração da Análise de Impacto, onde serão calculados os prejuízos decorrentes caso um acidente venha a acontecer.

Conforme definido anteriormente a Análise de Impacto no Negócio é o processo que envolve a análise das funções de negócio e os efeitos que uma interrupção possa causar nelas. Neste ponto é essencial a participação de todas as áreas de negócios da empresa, as quais se apresentam da seguinte maneira: área de vendas; área de gerência de fornecedores e de contratos; área de logística; área de infraestrutura e área administrativa.

Para o desenvolvimento da análise de impacto dos negócios, aconselha-se a utilização de um roteiro de entrevista informal, de forma a poder entender o processo de negócio e o entrevistado entender o significado daquela atividade. Na entrevista podemos ter um roteiro com perguntas, como por exemplo:

- Em qual período do mês o processo fica mais crítico e por quê?
- Quais sistemas você usa para executar as atividades deste processo de negócio?
- Existe alguma atividade alternativa que você utiliza quando o sistema não está disponível?
- Quanto tempo é necessário para executar esta atividade alternativa sem o sistema estar disponível?
- Qual o período máximo de atraso dos dados aceitável para a execução das atividades críticas desse processo de negócio?

Na empresa em estudo estipulamos um cenário fictício de desastre, tomando como exemplo sua paralização por falta de energia durante 12 horas, causando as seguintes consequências:

- TI totalmente indisponível durante este período;
- nenhum acesso aos aplicativos e sistemas corporativos da organização;
- prejuízo financeiro, pois nenhuma venda foi realizada;
- atraso na entrega de mercadorias, pois caminhões de entrega ficaram parados esperando liberação.

A partir daí é possível elaborar uma análise de perdas e impactos financeiros anteriormente denominados como BIA e, ainda, estimar a perda intangível envolvida pela ausência de TI de acordo com o cenário usado. A análise financeira é classificada da seguinte maneira:

- Perda Financeira: é mensurada de imediato, exemplo: deixou de vender, deixou de produzir:
- Impacto Financeiro: existe a possibilidade de perder dinheiro, exemplo: pode não receber uma duplicata e, consequentemente, não pagar um fornecedor, não aplicar o valor, e assim por diante;
- Perda intangível: problema com a imagem, perda de clientes, e outros.

O conceito da valorização é que sustenta a inciativa do PCN e a empresa passa a aprovar o plano quando enxerga o tamanho do prejuízo que possa ter.

4.4 DIRETRIZES PARA A CONSTRUÇÃO DO PLANO DE CONTINUIDADE DE NEGÓCIOS PARA A EMPRESA X

As diretrizes para a construção do PCN estão a seguir especificadas e detalhadas abaixo:

Escopo

A definição do escopo e do cenário é fundamental e deve ser a primeira etapa a ser definida. A limitação de escopo e cenário tem por objetivo possibilitar a elaboração de versões de plano compatíveis com a maturidade da organização na questão continuidade de negócio, sendo que cada versão poderá ser mais completa do que a anterior.

O escopo deve estar disponível como informação documentada e nele a organização deve:

a) estabelecer as partes da organização a serem incluídas no plano;
b) considerar a missão da organização, objetivos, obrigações internas e externas (incluindo aquelas com as partes interessadas), bem como responsabilidades legais e regulatórias;
c) identificar produtos, serviços e todas as atividades relacionadas com o escopo;
d) levar em consideração as necessidades e interesses das partes interessadas, tais como clientes, investidores, acionistas, cadeia de suprimentos, expectativas e interesses públicos e/ou da comunidade.

Na empresa em estudo o escopo está mais voltado às atividades que envolvem a área de vendas e todas as outras que interferem nela.

Comprometimento da Direção

A Alta Direção, no caso o proprietário, deve garantir que papéis, responsabilidades e autoridades relevantes sejam atribuídos e comunicados dentro da organização.

Planejamento

Para alcançar seus objetivos de continuidade de negócios, a organização deve determinar quem serão os responsáveis; de preferência pessoas que sejam competentes com relação à educação apropriada, treinamento e experiência; o que deverá ser executado; quais serão os recursos necessários; quando a execução será concluída; e como os resultados serão avaliados. A organização deverá, ainda, realizar avaliações da capacidade de continuidade de negócios dos seus fornecedores.

Comunicação

A organização deve determinar as necessidades de comunicações internas e externas relevantes para o PCN, inclusive:

a) o que será comunicado;
b) quando comunicar;
c) para quem comunicar.

Além disso, deve garantir a disponibilidade dos meios de comunicação durante o incidente gerador de interrupção e garantir a operação e teste das capacidades de comunicação destinado a serem utilizados durante a interrupção dos meios normais de comunicação.

Informação documentada

Quando um PCN for criado ou atualizado, deve possuir uma descrição (por exemplo: um título, data, autor e número de referência), um formato (por exemplo: linguagem, versão de software, gráficos) e uma mídia (por exemplo: papel, eletrônico).

Planejamento e controle operacional

É preciso definir uma estratégia a partir da análise de impacto nos negócios e no processo de avaliação de riscos, e especificar os critérios para que estas informações sejam confidenciais e mantenham-se atualizadas.

Quanto ao impacto potencial de uma interrupção, devemos considerar os requisitos legais, fixar prazos de forma priorizada para a retomada destas atividades, em um nível mínimo de execução tolerável, levando em consideração o tempo em que os impactos desta interrupção torne-se inaceitável e identificar dependências e recursos que suportam estas atividades, incluindo fornecedores, terceiros e demais partes interessadas relevantes.

Quanto ao processo de avaliação de riscos, é preciso identificar riscos de interrupção das atividades prioritárias da organização, bem como os processos, sistemas, informações, pessoas, bens, parceiros terceiros, e outros recursos que os suportam. Além disso, devemos analisar sistematicamente o risco, ou seja, avaliar quais riscos de interrupção podem ser tratados, para só depois identificar os tratamentos alinhados com os objetivos de continuidade de negócios, e de acordo com o apetite de risco da organização.

Estrutura de resposta a incidentes

A organização deverá possuir uma estrutura de gestão para responder a uma interrupção, utilizando pessoal com a autoridade, responsabilidade e competência

necessária para gerenciar um incidente, ou seja, que seja capaz de identificar o ponto inicial de impacto que justifique o início da resposta formal, avaliar a natureza, a extensão e o impacto potencial de um incidente, acionar a resposta de continuidade de negócios adequada, ter processos e procedimentos para a ativação, operação, coordenação e comunicação da resposta, ter recursos disponíveis para apoiar os processos e procedimentos para a gestão de um incidente, a fim de minimizar o impacto, e comunicar com as partes interessadas e as autoridades, bem como os meios de comunicação.

Recuperação

A organização deve possuir procedimentos documentados para restaurar e retornar as atividades de negócios das medidas temporárias adotadas, e atender aos requisitos de negócios normais após um incidente.

Teste e manutenção

A organização deve possuir e testar os procedimentos de continuidade de negócios, para garantir que estes são compatíveis com os seus objetivos de continuidade e produzir relatórios formalizados que contemplem os resultados, recomendações e ações para implementar melhorias.

Avaliação de desempenho

A organização deve determinar o que precisa ser monitorado e medido, os métodos para monitoramento, medição, análise e avaliação, quando o monitoramento e a medição devem ser realizados e quando os resultados do monitoramento e da medição devem ser analisados e avaliados.

4.5 MODELO DE PLANO DE CONTINUIDADE DE NEGÓCIO

O Plano de Continuidade de Negócios quando aplicado a grandes empresas é composto por outros três planos:

- Plano de Administração de Crise;
- Plano de Continuidade Operacional;

- Plano de recuperação de Desastre.

Atendendo aos objetivos propostos por este trabalho de graduação, o modelo sugerido no Apêndice B é um modelo novo e foi construído considerando as normas acima descritas.

Este plano simplificado converte os três planos em um único modelo, objetivando o sucesso de sua aplicabilidade num cenário real onde a empresa em questão dispõe de menos recursos humanos, tecnológicos, físicos ou financeiros.

Como finalização dos estudos, este modelo foi aplicado à interrupção de energia elétrica na Empresa X e apresentado no Apêndice C.

5 CONSIDERAÇÕES FINAIS

A proteção dos ativos e a continuidade do negócio são alguns dos principais objetivos da segurança da informação. Para garantir a continuidade das operações mesmo mediante cenários de desastres é fundamental que as organizações, independente do segmento ou porte, coloquem em prática um programa de gestão da continuidade de negócio.

A realização desta monografia permitiu conhecer melhor o processo de gerenciamento de risco utilizado para implementação de um plano de continuidade de negócios e o quanto é importante a utilização do plano no mapeamento das ameaças e riscos que os ativos de informação estão sujeitos. A ênfase dada à segurança da informação permitiu aprofundar os conhecimentos sobre as principais ameaças que a informação está exposta e aos mecanismos de defesa que devem ser implementados.

Ao ampliar a compreensão sobre GCN foi adquirida maior capacidade de análise do cenário no qual foi realizado o estudo de caso, sendo possível, desse modo, a elaboração e aplicação de um teste de controle de segurança e nível de riscos a fim despertar a conscientização dos gestores da organização quanto ao nível de maturidade com relação à segurança de suas informações e necessidade de um Plano de Continuidade de Negócio.

A análise de riscos e impactos foi feita através de um *checklist*, onde são apresentadas as principais ameaças e probabilidades de ocorrência que mais impactam nas estratégias do negócio para, a partir daí, poder definir a estratégia de tolerância no tempo de paralização dos seus ativos mais críticos e definição do escopo e recursos.

Com base nas estratégias definidas acima, são traçadas as diretrizes para elaboração de um único plano capaz de atender as três fases que englobam um plano de contingência, que são: administração de crise, continuidade operacional e recuperação de desastre. A dificuldade do processo foi na definição do escopo de cada etapa do plano, que não poderia apresentar tamanha abrangência devido aos recursos disponibilizados pela empresa em estudo.

O modelo adaptado e moldado conforme as necessidades operacionais é composto por formulários contendo vários campos com a descrição das responsabilidades bem definidas, informações para contato de todos os envolvidos na execução do plano, tempo objetivado para recuperação do processo de negócio, comunicação do desastre, ações que deverão ser executadas em caso de interrupção das atividades e análise e sugestões de melhorias.

Buscando dar continuidade a este trabalho, sugere-se que sejam feitos novos estudos com o objetivo de um maior detalhamento dos itens de cada etapa do plano e elaboração de um plano específico para cada etapa, além da aplicação e elaboração de um plano de testes.

REFERÊNCIAS

ALVES, Gustavo Alberto. *Segurança da informação: uma visão inovadora da gestão*. Rio de Janeiro: Ed. Ciência Moderna Ltda., 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *ABNT NBR ISO/IEC 22301:2013*: Segurança da Sociedade: Sistema de gestão de continuidade de negócios. Rio de Janeiro: ABNT, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TECNICAS. *ABNT NBR ISO/IEC 17799:2001*: Tecnologia da informação: Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27002:2007*: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2007.

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

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

BEAL, Adriana. *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas, 2005.

CALDER, A.; WATKINS, S. *IT governance: a manager's guide to data security and ISO 27001/ISO 27002*. 4a. ed. London e Philadelphia: Kogan Page Limite, 2008.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. *Segurança em Informática e de Informações*. São Paulo: SENAC, 1999.

FERREIRA, F. N. F.; ARAÚJO, M. T. *Política da Segurança da Informação: Guia Prático para Elaboração e Implementação.* 1. ed. Rio de Janeiro: Ciência Moderna, 2006.

FISCHER, Urs. Identify, *Govern and Manage IT Risk*. ISACA Journal, vol. 4, 5 e 6, 2009.

FONTES, Edison. *Segurança da Informação: o usuário faz a diferença*. São Paulo: Saraiva, 2006.

FONTES, Edison. *Praticando a Segurança da Informação*. Rio de Janeiro: Brasport, 2008.

FRIEDENHAIN, Vitor. *Um estudo sobre métodos e processos para a implantação da gestão de continuidade de negócios aplicáveis a órgãos da administração pública federal brasileira*. Brasília: Universidade de Brasília, 2008.

KROLL, J. ; FONTOURA, L. M.; WAGNER, R.; DORNELLAS, M. C. *Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008*. Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010, Marabá. Anais do Simpósio Brasileiro de Sistemas de Informação (SBSI), 2010.

LAHTI, C. B.; PETERSON, R. *Sarbanes-Oxley: Conformidade TI Usando CobIT e Ferramentas Open Source*. São Paulo: Alta Books, 2006.

LAWLER, C.M.; SZYGENDA, S.A. *Components of Continuous IT Availability & Disaster Tolerant Computing*. In: 2007 IEEE Conference on Technologies for Infrastructure Dependability. 2007 IEEE Conference on 16-17 May 2007.

LYRA, Maurício Rocha. *Segurança e Auditoria em Sistemas de Informação*. Rio de Janeiro: Ciência Moderna, 2008.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Cláudia Fernandes; ESCRIVÃO FILHO, Edmundo. *A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa* – Revista de Gestão da Tecnologia e Sistemas da Informação, v.1, n.1, 2004.

NERY, Fernando; PARANHOS, Maurício. *COBIT ou ISO 17799?* Módulo Security Magazine. Disponível em: <http://www.modulo.com.br>. Acesso em 10 de set. 2014.

OHTOSHI, Paulo Hideo. *Análise Comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005*. Brasília: Universidade de Brasília, 2008.

OLIVA, Rodrigo Polydoro; OLIVEIRA, Mírian. *Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799*. Rio Grande do Sul: ENANPAD, 2003.

OLIVEIRA, Djalma de Pinho Rebouças. *Sistemas de informações gerenciais*. 11. ed. São Paulo: Atlas, 2007.

OLIVEIRA, M. A. F.; ELLWANGER, C.; VOGT, F. C. & R. C. NUNES. *Framework para gerenciamento de riscos em processos de gestão de segurança da informação baseado no modelo DMAIC*. XXIX Encontro Nacional de Engenharia de Produção (ENEGEP), 2009, Salvador, XXIX Encontro Nacional de Engenharia de Produção. Rio de Janeiro: Abepro, 2009.

PALMA, Fernando. *ISO 27001 e ISO 27002*. 2011. Disponível em: <http://www.portalgsti.com.br/2011/05/iso-27001-e-27002.html>. Acesso em: 10 Set. 2014.

PELTIER, Thomas R. *Information Security Risk Analysis*. 2.ed. EUA: Auerbach Publications: 2005.

PEREIRA JUNIOR, Jorge Hosni. *Plano de Continuidade de Negócios Aplicado à Segurança da Informação*. Rio Grande do Sul: UFRGS, 2008.

PINHEIRO, Rosewelt. *Mapa das Micro e Pequenas Empresas*. Disponível em: <http://www.brasil.gov.br/economia-e-emprego/2012/02/o-mapa-das-micro-e-pequenas-empresas>. Acesso em: 15 fev. 2013.

SCHMIDT, Paulo; SANTOS, José Luiz; ARIMA, Carlos Hideo. *Fundamentos de auditoria de sistemas*. São Paulo: Atlas, 2006.

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

VARGAS, Ricardo. *Manual Prático do Plano de Projeto Utilizando o PMBOK Guide.* 4. ed. Rio de Janeiro: Brasport, 2009.

WESTERMAN, G.; HUNTER, R. *O Risco de TI: Convertendo ameaças aos negócios em vantagem competitiva*. São Paulo: M. Brooks, 2008.

APÊNDICES

APÊNDICE A

Teste de Verificação – Controles de Segurança

TESTE DE VERIFICAÇÃO - CONTROLES DE SEGURANÇA				
		Sim	**Desatualizada**	**Não**
Política de Segurança	Política de Segurança			**X**
	Responsável pela P.S			**X**
Segurança Organizacional	Infraestrutura de S.I para gerenciar ações corporativas			**X**
	Atribuições de resposabilidade associadas à segurança da informação			**X**
	Identificação dos Riscos no acesso de prestadores de serviços			**X**
	Requisitos de segurança dos contratos de terceirização			**X**
Classificação e controle dos ativos de informação	Inventário dos ativos físicos, tecnológicos e humanos			**X**
	Critérios de classificação da informação			**X**
Segurança em pessoas	Critérios de seleção e política de pessoal			**X**
	Acordo de confidencialidade, termos e condições de trabalho			**X**
	Processos para capacitação e treinamento de usuários			**X**
	Estrutura para notificar e responder aos incidentes e falhas de segurança			**X**
Segurança física e de ambiente	Definição de perímetros e controles de acesso físico aos ambientes	**X**		
	Recursos para segurança e manutenção dos equipamentos		**X**	
	Estrutura para fornecimento adequado de energia	**X**		
	Segurança do cabeamento		**X**	

TESTE DE VERIFICAÇÃO - CONTROLES DE SEGURANÇA				
		Sim	**Desatualizada**	**Não**
Gerenciamento das operações e comunicações	Procedimentos e responsabilidades operacionais	**X**		
	Controle de mudanças operacionais			**X**
	Segregação de funções e ambientes	**X**		
	Planejamento e aceitação de sistemas			**X**
	Procedimento para cópias de segurança		**X**	
	Controles e gerenciamento de Rede			**X**
	Mecanismos de segurança e tratamento de mídias			**X**
	Procedimentos para documentação de sistemas			**X**
	Mecanismo de segurança do correio eletrônico			**X**
Controle do acesso	Requisitos do negócio para controle de acesso			**X**
	Gerenciamento de acessos do usuário	**X**		
	Controle de acesso à rede			**X**
	Controle de acesso ao sistema operacional		**X**	
	Controle de acesso às aplicações		**X**	
	Monitoração do uso e acesso ao sistema			**X**
	Critérios para computação móvel e trabalho remoto			**X**
Desenvolvimento e manutenção de sistemas	Requisitos de segurança de sistemas			**X**
	Controles de criptografia			**X**
	Mecanismos de segurança nos processos de desenvolvimento e suporte			**X**
Gestão da continuidade do negócio	Processo de gestão da continuidade do negócio			**X**
Conformidade	Gestão de conformidade técnicas e legais			**X**
	Recursos e critérios para auditoria de sistemas			**X**

Fonte: Próprio autor.

APÊNDICE B

Modelo do Plano de Gestão de Incidentes – Folha de rosto.

Data:	**Plano de Gestão de Incidentes**	Nome da Empresa
Versão:		Folha 1

Identificação do Documento	

Plano de Gestão de Incidentes

Cenário		
Área		
Autor/ Responsável		
Contato	**Fone comercial**	
	Fone residencial	
	Fone móvel	
Objetivo		
Grupos Funcionais		

Modelo do Plano de Gestão de Incidentes - Pré-Contingência.

Data:	Plano de Gestão de Incidentes	Nome da Empresa
Versão:		Folha 2

AÇÕES PRÉ-CONTINGÊNCIA	
Grupo Funcional	
Nome	
Telefone	
E-Mail	
Cargo	
Função	

SISTEMAS CRÍTICOS	
Nome do Sistema	
Local Atual	
Outros Locais	
Sistema de Backup	

RECURSOS NECESSÁRIOS

Modelo do Plano de Gestão de Incidentes – Acionamento e comunicação de crise.

Data:	Plano de Gestão de Incidentes	Nome da Empresa
Versão:		Folha 3

ACIONAMENTO DA CRISE	
Responsável pela Ativação e Comunicação	
Telefone	
E-Mail	
Cargo	
Função	
Tempo objetivado para recuperação	
Ambiente	

COMUNICAÇÃO DO INCIDENTE	
Responsável pela Comunicação	
Telefone	
E-Mail	
Cargo	
Função	

Modelo do Plano de Gestão de Incidentes – Continuidade operacional.

Data:	Plano de Gestão de Incidentes	Nome da Empresa
Versão:		Folha 4

RESPONSÁVEIS PELA EXECUÇÃO	
Grupo Funcional	
Nome	
Telefone	
E-Mail	
Cargo	
Função	
Substituto	

PROCEDIMENTOS	
Incidente	
Grupo funcional	
Responsável	
Tempo Total	

ID	Instrução
1	
2	
3	
4	

FORNECEDORES		
Empresa	Tipo	Dados
		Endereço:
		Telefone:
		E-mail:
		Endereço:
		Telefone:
		E-mail:

Modelo do Plano de Gestão de Incidentes – Recuperação de desastre.

Data:	Plano de Gestão de Incidentes	Nome da Empresa
Versão:		Folha 5

AVALIAÇÃO DE DANOS	
Processo Chave do Negócio	
Descrição do Problema	
Extensão do Dano	

RELATÓRIO DE CONCLUSÃO DE RECUPERAÇÃO		
Nome		
E-Mail		
Cargo		
Comentários		
Assinatura _____		

TESTE DO PLANO

AVALIAÇÃO DAS MEDIDAS

PROPOSTAS E SUGESTÕES DE MELHORIAS

Fonte: Próprio autor.

APÊNDICE C

Exemplo do Plano de Gestão de Incidentes para Interrupção de energia na Empresa X – Folha de rosto.

Data: 14/11/2014	**Plano de Gestão de Incidentes**	**EMPRESA X**
Versão: 1.0		Folha 1

Identificação do Documento	001.2014.70.20

Plano de Gestão de Incidentes

Cenário		Falha no fornecimento de energia elétrica
Área		Filial Centro - Escritórios e Logística
Autor/ Responsável		João da Silva
Contato	**Fone comercial**	(19) 3333-0044
	Fone residencial	(19) 2345-9323
	Fone móvel	(19) 9 9987-3333
Objetivo	Reestabelecer a energia no menor tempo possível.	
Grupos Funcionais	Operação, Direção, Suporte, Comunicação	

Exemplo do Plano de Gestão de Incidentes para Interrupção de energia na Empresa X - Pré-Contingência.

Data: 14/11/2014	Plano de Gestão de Incidentes	EMPRESA X
Versão: 1.0		Folha 2

AÇÕES PRÉ-CONTINGÊNCIA	
Grupo Funcional	Operação
Nome	Manual de Oliveira
Telefone	(19) 3309-0033
E-Mail	manuel.oliveira@empresax.com.br
Cargo	Gerente de Manutenção Geral
Função	# Acompanhar e validar os relatórios de manutenção mensal realizada pela empresa manutenção. # Acompanhar as realizações dos testes dos No-breaks.

SISTEMAS CRÍTICOS	
Nome do Sistema	Energia elétrica para os servidores
Local Atual	Sala 23 - PISO 2
Outros Locais	Não se aplica
Sistema de Backup	NO-BREAK 1 e NO-BREAK 2

RECURSOS NECESSÁRIOS
Manual de operação e chaveamento do No-Break

Exemplo do Plano de Gestão de Incidentes para Interrupção de energia na Empresa X – Acionamento e comunicação de crise.

Data: 14/11/2014	Plano de Gestão de Incidentes	EMPRESA X
Versão: 1.0		Folha 3

ACIONAMENTO DA CRISE	
Responsável pela Ativação e Comunicação	Paulo Mendes
Telefone	(19) 3303-4499
E-Mail	paulo.mendes@empresax.com.br
Cargo	Diretor de TI
Função	Gerenciamento do início e fim da crise
Tempo objetivado para recuperação	30 minutos
Ambiente	Filial Centro - Escritórios e Logística

COMUNICAÇÃO DO INCIDENTE	
Responsável pela Comunicação	Maria Clara Machado
Telefone	(19) 3303-4567
E-Mail	maria.clara@empresax.com.br
Cargo	secretária da diretoria
Função	Comunicação com funcionários, clientes e fornecedores sobre o incidente e possíveis atrasos nos processos

Exemplo do Plano de Gestão de Incidentes para Interrupção de energia na Empresa X – Continuidade operacional.

Data: 14/11/2014	Plano de Gestão de Incidentes	EMPRESA X
Versão: 1.0		Folha 4

RESPONSÁVEIS PELA EXECUÇÃO	
Grupo Funcional	Suporte
Nome	Geraldo Luis Vieira
Telefone	(19) 3303-0800
E-Mail	geraldo.vieira@empresax.com.br
Cargo	Coordenador de Manutenção Geral
Função	Manutenção Geral
Substituto	Ronaldo da Silva (19 - 9 8990-4545)

PROCEDIMENTOS

Incidente	Queda de energia elétrica geral
Grupo funcional	Suporte
Responsável	Geraldo Luis Vieira
Tempo Total	75 minutos

ID	Instrução
1	Se houver queda de energia elétrica no servidor de Banco de Dados, o nobreak nº 1 automaticamente entrará em funcionamento.
2	Verificar quadro elétrico na sala 2. Caso o disjuntor encontra-se na posição "ON" ligado, aguardar o retorno da energia elétrica fornecida pela concessionária. Caso encontra-se na posição "OFF" desligada, contatar o responsável pela manutenção predial.
3	Caso o nobreak 1 não entrar em funcionamento após 8 segundos de parada, acionar o nobreak 2 e aguardar retorno da concessionária.
4	Comunicar aos responsáveis por cada área de negócio

FORNECEDORES

Empresa	Tipo	Dados
CPFL	Conssionária de Energia Elétrica	Endereço: Rua Jasmim, 1234 - Taquaral Telefone: (19) 2456-0090 E-mail: suporte@cpfl.com.br
SMS	Fornecedor de No-break	Endereço: Rua do Horto, 120 - Centro Telefone: (19) 2300-3499 E-mail: atendimento@sms.com.br

Exemplo do Plano de Gestão de Incidentes para Interrupção de energia na Empresa X – Recuperação de desastre.

Data: 14/11/2014	Plano de Gestão de Incidentes	EMPRESA X
Versão: 1.0		Folha 5

AVALIAÇÃO DE DANOS	
Processo Chave do Negócio	Vendas
Descrição do Problema	Interrupção de energia elétrica em todo o sistema
Extensão do Dano	Perda de possíveis vendas e novos clientes, atraso na entrega, entre outros

RELATÓRIO DE CONCLUSÃO DE RECUPERAÇÃO	
Nome	Geraldo Luis Vieira
E-Mail	geraldo.vieira@empresax.com.br
Cargo	Coordenador de Manutenção Geral
Comentários	# Os procedimentos foram realizados conforme especificados no plano. O No-Break 2 teve que ser acionado devido ao aumento do consumo de energia do servidor durante o período de recuperação.
Assinatura _____	Data 30/11/2014

TESTE DO PLANO
O teste do plano foi realizado em 21/11/2014.

AVALIAÇÃO DAS MEDIDAS
As medidas tomadas foram realizadas com sucesso devido a algumas melhorias realizadas no treinamento dos envolvidos.

PROPOSTAS E SUGESTÕES DE MELHORIAS
Aumento da capacidade de fornecimento do No-break 1.

Fonte: Próprio autor.