UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA DE REDES DE COMPUTADORES

JORGE HOSNI PEREIRA DE PEREIRA JUNIOR

Plano de continuidade de negócios aplicado à segurança da informação

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. MSc. Henrique Jorge Brodbeck
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, novembro de 2008.

AGRADECIMENTOS

A minha esposa Vivian Lago

Ao meu tio Valdir Kolosque

Aos meus pais Jorge Hosni e Maria Ivone

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BS	*British Standard*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI	Comitê Gestor da Internet
CobiT	*Control Objectives for Information and related Technology*
COE	Centro de Operacional de Emergência
CPD	Centro de Processamento de Dados
CVSS	*Common Vulnerability Scoring System*
DDoS	*Distribuited Denial of Service*
DMZ	*DeMilitarized Zone*
DoS	*Denial of Service*
GCN	Gestão de Continuidade de Negócios
HIDS	*Host-Based Intrusion Detection System*
HIPS	*Host-Based Intrusion Prevention System*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commision*
IP	*Internet Protocol*
IRC	*Internet Relay Chat*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
KIDS	*Kernel Intrusion Detection System*
LIDS	*Linux Intrusion Detection System*
NBR	Normas Brasileiras
NIC.br	Núcleo de Informação e Coordenação do Ponto br

NIDS	*Network-Based Intrusion Detection System*
NIPS	*Network Intrusion Prevention System*
NIST	*National Institute of Standards and Technology*
OGC	*Office of Government Commerce*
OTP	*One-Time Password*
PCN	Plano de Continuidade de Negócios
PDCA	*Plan-Do-Check-Act*
PIN	*Personal Identification Number*
SEI	*Sotfware Engineering Institute*
SGSI	Sistema de Gestão da Segurança da Informação
SLA	*Service Level Agreement*
SW-CMM	*Capability Maturity Model for Software*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
UCE	*Unsolicited Commercial E-mail*
USENET	*Unix User Network*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Antigamente o ambiente computacional era pequeno e controlado, tornando a informação mais segura. Atualmente, esse ambiente é complexo e a informação tornou-se o ativo mais importante para a sobrevivência e o sucesso de uma organização. Portanto, as organizações precisam estar protegidas contra ameaças e vulnerabilidades e as informações precisam estar disponíveis quando solicitadas. A preocupação com a continuidade do negócio começou a ser levada realmente a sério após os eventos ocorridos no dia 11 de setembro de 2001, levando a uma reformulação de normas e procedimentos relacionados à segurança da informação.

O presente trabalho tem o propósito de apresentar os conceitos, as fases e as melhores práticas utilizadas na implementação de um plano de continuidade de negócios aplicado à segurança da informação. Inicialmente são definidos alguns conceitos sobre gestão de risco e segurança da informação. A seguir, são apresentados o modelo de processo de melhoria contínua, as etapas para realização do gerenciamento de riscos, as normas e as melhores práticas adotadas hoje para auxiliar a organização no mapeamento e tratamento dos seus processos de negócio.

As organizações precisam estar protegidas contra atividades maliciosas que podem tornar indisponíveis os seus ativos de informação. Neste trabalho são apresentadas as principais ameaças, tais como, *spam*, engenharia social e *malwares*, que podem afetar o ambiente de tecnologia e comprometer a continuidade dos negócios. São apresentadas ainda as defesas, como por exemplo, *firewall*, sistema de detecção de intrusão e criptografia, que devem ser implementados para garantir que a informação esteja protegida e disponível quando necessária.

Por fim foi proposto um *checklist* para identificar os riscos e a maturidade da organização quanto aos processos de segurança da informação e implementação de um plano de continuidade de negócios focando a segurança da informação. O *checklist* foi construído baseado nos principais controles propostos na norma ABNT NBR ISO/IEC 27002 e BS 25999-1 e CobiT que são considerados padrões internacionalmente reconhecidos.

Palavras-Chave: gestão de risco, plano de continuidade de negócios, segurança da informação.

Business Continuity Plan applied to information security

ABSTRACT

In the old days, the computer environment was small and controlled, making the information more secure. Nowadays, this environment is complex and the information has become the most important asset for the survival and success of an organization. Therefore, the organizations need to be protected against threats and vulnerabilities as well as the information needs to be available when needed. The preoccupation with the business continuity plan started to be taken seriously after the events happened on September 11th 2001, leading to a reformulation of rules and procedures related to information security.

The current work has the aim of presenting the concepts, the phases and the best practices used in the implementation of a business continuity plan applied to information security. Firstly, some concepts about risk and information security are defined. The model of continuous improvement process, the steps for the risk management, the rules and the best practices adopted nowadays to help the organization in the mapping and treatment of its business processing are also presented.

The organizations need to be protected against the malicious activities that can make the information assets unavailable. In this work, the main threats such as spam, social engineering and malwares, which can affect the technological environment and compromise the business continuity, are presented. The defenses firewall, intrusion detection system and cryptography are also discussed, once they must be implemented to guarantee that the protection and the necessary availability of the information.

Lastly, it was proposed a checklist to identify the risks and the maturity of the organization in relation to the information security processes and the implementation of a business continuity plan focusing on the information security. The checklist was built based on the main controls proposed in the rules ABNT NBR ISO/IEC 27002 and BS 25999-1 and CobiT, which are considered international standardized regulation.

Palavras-Chave: risk management, business continuity plan, information security

1 INTRODUÇÃO

Com a imensa quantidade de informação que circula pelas redes de computadores sem restrição de tempo, distância e velocidade e a comunidade atual exigindo e consumindo cada vez mais informação. Surge a necessidade de que está informação seja entregue de forma segura e eficiente, pois, o sucesso e a sobrevivência de uma organização depende muito de como a informação é controlada, armazenada e manipulada.

No passado, os controles estavam basicamente no departamento financeiro, sendo este o coração da organização. Com o passar dos anos e com o surgimento da computação, tornando a informação disponível com mais facilidade, o departamento de informática passa a ser o centro da organização, e a informação o seu bem mais precioso.

Num mundo atualmente muito competitivo, com constantes e inesperadas mudanças, as organizações necessitam ter agilidade e flexibilidade para estar preparado para as falhas decorrentes de mudanças constantes no ambiente computacional. Surge a necessidade das organizações criarem mecanismos que possam garantir a continuidade dos negócios em momentos de crise. O gerenciamento apropriado do risco interno e externo ajuda as organizações a manter o ambiente de tecnologia da informação alinhado com o planejamento estratégico definido pela direção da organização.

O capítulo 2, trás a definição do que é risco, incidente e problema, descreve as atividades que devem ser realizadas no gerenciamento de riscos, seguindo o modelo de melhoria continua conhecido pela sigla PDCA. Além de abordar as normas e melhores práticas utilizadas em tecnologia da informação, tais como: ABNT NBR ISO/IEC 27002, BS 25999-1, ITIL e CobIT. Por fim é analisada a gestão da continuidade de negócios, a estrutura e os componentes que devem conter um plano de continuidade de negócios.

No capítulo 3, é discutida a segurança da informação segundo os seus principais atributos que são: disponibilidade, confidencialidade, integridade, entre outros. Também são apresentadas as principais ameaças que as organizações estão expostas e os mecanismos e métodos de defesa que devem ser aplicados para proteção ou mitigação do risco no ambiente tecnológico da organização.

No capítulo 4, é apresentada uma proposta de *checklist* para identificar os riscos e avaliar a maturidade de organização no que se refere a elaboração e utilização de um plano de continuidade de negócios. Onde as questões foram formuladas com base nos principais controles propostos nas normas ABNT NBR ISO/IEC 27002 e BS 25999-1.

2 PLANO DE CONTINUIDADE DE NÉGOCIOS

O plano de continuidade de negócios tem como principal objetivo possibilitar o funcionamento da organização em um nível aceitável nas situações de contingência onde há indisponibilidade dos recursos de informação. A impossibilidade de realizar as suas operações traz sérios impactos financeiros, operacionais e de imagem. O plano deve ser elaborado após a realização de uma análise de impacto no negócio e especificar as ameaças e riscos identificados na organização.

A direção e os demais interessados na organização devem conhecer todas as partes e fases do desenvolvimento do plano de continuidade de negócios e aprovar as ameaças e os riscos que podem afetar os ativos de informação, mas que estão de fora do plano. O plano deve ser elaborado inicialmente considerando as situações de maior risco e maior impacto e ir amadurecendo conforme a maturidade da organização frente a proteção dos seus ativos. O treinamento e a conscientização de todos os colaboradores é de grande importância, permitindo que a organização gerencie os riscos, esteja preparada para os momentos de contingência e garanta a continuidade do negócio.

2.1 Risco, incidente e problema

Segundo ABNT ISO/IEC Guia 73:2005, risco é a combinação da probabilidade de um **evento** e de suas conseqüências. Sendo que o evento é uma relação entre as **ameaças**, **vulnerabilidades** e os possíveis **danos** causados, ou seja, as conseqüências.

Probabilidade: é o grau de possibilidade de que um evento ocorra.

Evento: é a ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da segurança da informação, ou uma situação desconhecida, que passa a ser relevante para a segurança dos ativos.

Ativo: qualquer coisa que tenha valor para a organização.

Conseqüência: é o resultado de um evento, podendo ser positivo ou negativo. Pode haver mais de uma conseqüência de um evento.

Ameaças: é uma causa potencial de um incidente indesejado resultar em um dano para o sistema ou organização (ABNT NBR ISO /IEC 27002, 2007).

Vulnerabilidades: são definidas como a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (ABNT NBR ISO /IEC 27002, 2007).

Incidente: qualquer evento que não faz parte da operação normal de um serviço e que pode causar, ou causa, uma interrupção do serviço ou uma redução de sua qualidade.

Gerenciamento do incidente: processo responsável pelo tratamento e pela resolução de todos os incidentes ocorridos na organização, objetivando o restabelecimento dos serviços de Tecnologia da Informação (TI) no menor tempo possível e minimizar os impactos para o negócio.

Problema: causa desconhecida de um ou mais incidentes.

Gerenciamento de problemas: processo responsável pela resolução definitiva de eventos que afetam o funcionamento normal dos serviços de TI, objetivando garantir a correção das falhas e prevenir a recorrência de um incidente.

2.2 Gestão de riscos

Por que devemos estar atentos à gestão de riscos?

A Gestão de Riscos é definida como as atividades coordenadas para direcionar e controlar uma organização no que se refere ao risco (ABNT ISO/IEC Guia 73:2005). A gestão de riscos deve ser um processo que inclui a identificação, análise, avaliação, tratamento, aceitação, comunicação, monitoramento e revisão do risco, onde se deve analisar todos os riscos inerentes às atividades de uma organização.

O processo de melhoria continua conhecido como Plan - Do - Check - Act (PDCA) é um ciclo de análise e melhoria dos processos gerenciais necessários para o sucesso da organização e para a área de segurança da informação. O PDCA deve ser utilizado para estruturar os processos do Sistema de Gestão da Segurança da Informação (SGSI) e alinhar os processos de gestão de risco.

A primeira etapa do processo (Planejar) inicia com a definição das estratégias e a forma como elas vão ser alcançadas, ou seja, a definição de políticas, controles e procedimentos para garantir a segurança das informações. É de extrema importância que a direção da organização esteja de acordo e comprometida com os processos estratégicos definidos. Segundo a norma ISO 27005, na fase de planejamento são tratados os processos de Definição do Contexto, Análise/Avaliação de Riscos, Definição do Plano de Tratamento do Risco e Aceitação do Risco.

Na segunda etapa (Executar), os processos definidos são implementados e executados. Também é necessária a coleta de informações para utilização na próxima etapa. Alinhando com a norma ISO 27005 é implementado o plano de Tratamento do Risco.

Na terceira etapa (Checar) é feita a avaliação dos processos implementados para verificar se o planejado foi realmente executado de forma adequada para alcançar as metas. Nessa fase são identificados os desvios de execução e apresentados os resultados para uma análise crítica da direção. Nessa etapa, segundo a norma ISO 27005, é realizado o Monitoramento Contínuo e Análise Crítica do Risco.

Na quarta etapa (Agir) são realizadas ações corretivas e preventivas baseadas na identificação de desvios de execução e nas considerações apresentadas pela direção da organização. A norma 27005 orienta manter e melhorar o processo de Gestão de Riscos de Segurança da Informação (BRANDÃO 2008; HARUNARI apud GUARAGNA, 1992, p. 79).

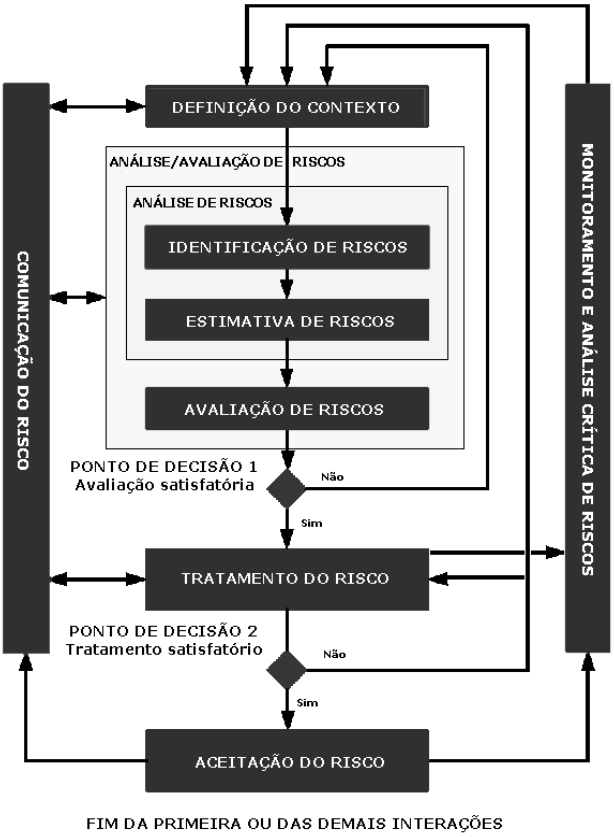

Figura 2.1: Visão geral do processo de gestão de riscos segundo a norma ISO 27005.

2.2.1 Comunicação do risco

Na fase de Comunicação do Risco as partes envolvidas, ou seja, os *stakeholders*, e as partes interessadas, pessoa ou grupo que tem interesse no desempenho ou no sucesso da organização, devem ser identificadas e os seus papéis e responsabilidades devem ser definidos. Um plano de comunicação é criado para conhecimento das partes do andamento do processo de gestão do risco.

2.2.2 Definição do contexto

A Definição do Contexto define o escopo da gestão de riscos que será utilizado para a identificação, avaliação, impacto e aceitação dos riscos. Nessa etapa são coletadas todas as informações relevantes sobre a organização, mas principalmente para a gestão de riscos de segurança.

Os principais resultados da definição do contexto devem ser a descrição dos objetivos da gestão do risco e dos ambientes nos quais eles estão contextualizados. Também são definidos os critérios que serão utilizados na determinação dos riscos, isto é, a determinação das conseqüências de segurança e os métodos usados para a análise e avaliação dos riscos.

2.2.3 Identificação de riscos

O papel da identificação de riscos é identificar junto aos gestores os eventos de cada processo de negócio existente na organização que possam afetar o funcionamento das

atividades essenciais e causar perdas potenciais. São respondidas as perguntas: “O que pode acontecer?”, “Quando e onde?” e “Como e por quê?”.

É necessário identificar as ameaças, os controles existentes, as vulnerabilidades e as conseqüências para cada propriedade da segurança da informação, ou seja, confidencialidade, integridade e disponibilidade.

2.2.4 Estimativa de riscos

A estimativa de riscos analisa a origem dos riscos, suas conseqüências e as probabilidades da ocorrência dos riscos. Os dados devem ser mensurados através de uma metodologia qualitativa ou quantitativa. Como exemplo pode ser adotada a metodologia *Common Vulnerability Scoring System* (CVSS) para cálculo do impacto das vulnerabilidades.

A norma ISO 27005 orienta estimar o risco de duas formas. Qualitativamente, onde é utilizada uma escala com atributos como, por exemplo, baixa, média e alta. Quantitativamente deve ser usada uma escala de valores numéricos para estimar o risco.

2.2.5 Avaliação de riscos

Na fase de avaliação de riscos são definidos como os mesmos serão tratados tomando como base os resultados obtidos nas fases de identificação e estimativa de riscos. Algumas organizações definem que todos os riscos serão tratados e outras focam somente nos riscos que afetam os principais processos de negócio da organização. Os riscos devem ser ordenados por prioridade e associados aos processos de negócio.

2.2.6 Tratamento de riscos

O tratamento de riscos inicia com a priorização entre os riscos encontrados, levando em conta os riscos que têm maior probabilidade de se concretizar, tornando-se um incidente. Os riscos devem relacionados conforme as opções de tratamento, que são: redução, retenção, evitação e transferência.

A redução do risco é definida como as ações tomadas para reduzir a probabilidade, as conseqüências negativas, ou ambas, associadas a um risco. A retenção do risco é a aceitação do ônus da perda associado a um determinado risco. Evitar o risco significa decidir por não se envolver ou agir em uma determinada atividade para evitar a situação de risco. A decisão deve ser tomada conforme o resultado da avaliação de risco.

A transferência do risco é o compartilhamento com outra parte do ônus da perda ou do benefício do ganho associado a um risco. É importante analisar se a transferência do risco não vai gerar novos riscos ou modificar o risco existente. Após o tratamento, o evento que ainda possa produzir um risco é chamado de risco residual. O tratamento deve ser refeito para reduzir o risco a um patamar aceitável.

2.2.7 Aceitação de riscos

Na fase de aceitação, os riscos residuais devem ser formalmente aceitos pela organização levando em conta o escopo elaborado na definição do contexto.

2.2.8 Monitoramento e análise crítica dos riscos

A fase de monitoramento e análise crítica dos riscos é de extrema importância para a gestão de riscos, pois é necessário que os riscos sejam monitorados e os processos revisados para identificar oportunidade de melhoria no tratamento dos riscos. Tendo em vista que o ambiente computacional é dinâmico, revisões e auditorias periódicas devem ser realizadas para identificar modificações internas e externas que possam alterar o contexto do processo de negócio da organização.

2.3 Normas e melhores práticas em tecnologia da informação

Cada vez mais as organizações necessitam manter forte e atualizado o seu departamento de Tecnologia da Informação, para manipular os dados operacionais e prover informações gerenciais a direção da organização de uma forma mais rápida, dinâmica e com custos cada vez mais baixos. No intuito de auxiliar na melhoria dos processos de negócio e garantir o retorno de investimento foi criado um movimento chamado Governança de TI (MANSUR, 2007).

Governança de TI é definida como uma estrutura de relações e processos que dirige e controla uma organização a fim de atingir seu objetivo, que é de adicionar valor ao negócio através do gerenciamento balanceado do risco com o retorno do investimento de TI (FAGUNDES, 2004). Como forma de compreender e controlar os riscos inerentes do uso das tecnologias, foram criadas algumas normas e guias para auxiliar no processo de gerenciamento dos processos de TI. A seguir são apresentadas as principais normas e guias utilizadas atualmente para gerenciamento de risco e processos de TI.

2.3.1 BS 25999-1

A norma BS 25999-1, criada em 2007, tem o propósito de fornecer as melhores práticas para que as pessoas responsáveis pelos negócios da organização possam entender, desenvolver e implementar ações e procedimentos para a continuidade dos negócios. A norma descreve diversos termos relacionados à continuidade dos negócios, os fundamentos e os elementos chaves que devem existir na Gestão da Continuidade de Negócios (GCN) (BS 25999-1, 2006).

Os fundamentos da GCN são:

- Melhorar proativamente a resiliência da organização frente a possíveis perturbações ou interrupções de sua capacidade de entregar seus produtos e serviços e atingir seus principais objetivos.
- Prover métodos para restabelecer a capacidade de uma organização fornecer seus produtos e serviços em um nível previamente acordado.
- Obter uma comprovada capacidade de gerenciar uma interrupção no negócio e proteger a reputação e a marca da organização.

A norma descreve alguns elementos chaves que o GCN deve conter. São eles:

- Entender o contexto de todos os processos operacionais da organização;
- Entender os produtos e processos críticos que a organização entrega;
- Entender quais são as barreiras ou interrupções que a organização pode se deparar ao tentar entregar esses produtos ou processo críticos;

- Entender como a organização pode continuar a atingir seu objetivo no caso de uma interrupção ocorrer;
- Entender os critérios para implementar uma resposta de emergência e os procedimentos de recuperação do negócio;
- Assegurar que todos os envolvidos compreendam suas funções e responsabilidades quando um incidente ocorrer;
- Construir em consenso e compromisso a implementação, execução e o exercício da continuidade nos negócios;
- Integrar a continuidade dos negócios na rotina diária da organização.

A GCN deve ser definida dentro da organização e estar relacionada com a finalidade estratégica organizacional e com a gestão de risco. A elaboração do GCN irá resultar na criação de um ou mais Planos de Continuidade de Negócios (PCN).

2.3.1.1 Ciclo de vida da GCN

O ciclo de vida é composto pelas seis etapas necessárias para o entendimento, desenvolvimento e implementação do GCN.

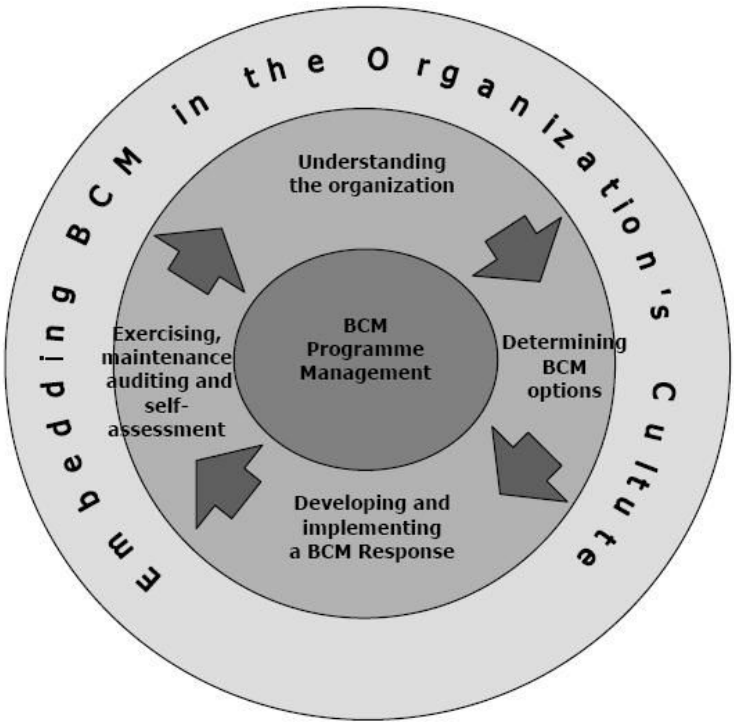

Figura 2.2: Ciclo de vida da gestão da continuidade de negócios.

Gestão do programa de GCN

São definidas as responsabilidades pela implementação do GCN. Deve ser nomeada uma pessoa como responsável por todo o processo de implementação. Na política de gestão da continuidade de negócios devem existir diretrizes básicas definindo seu

escopo e como serão alocados os recursos. A implementação deve ser planejada e ter uma manutenção continua.

Entendendo a organização

Deve ser realizada uma análise de impacto no negócio para realizar um mapeamento dos produtos e serviços fundamentais. Identificar as atividades que suportam a entrega desses produtos e serviços, estimar o tempo necessário para recuperação no caso de falha, identificar e avaliar as ameaças mais significativas e como a organização vai tratar os riscos.

Determinando a estratégia da continuidade de negócios

A organização deve definir uma estratégia para a GCN. É necessário analisar as estratégias possíveis e escolher a mais adequada considerando tempo e custo de implementação da estratégia e os recursos necessários, tais como: pessoas, instalações, tecnologia, informação e suprimentos.

Desenvolvendo e implementando uma resposta de GCN

Definida a estratégia, a organização deve criar um plano de resposta para os incidentes que atenda às expectativas dos *stakeholders* e esteja de acordo com o que foi apurado na análise de impacto do negócio. O plano deve conter o seu objetivo, responsabilidade das pessoas, como será ativado e mantido o plano, definir um responsável por manter, alterar e atualizar o plano regularmente e a forma de comunicação dos fatos com a mídia e *stakeholders* da organização.

Testando, mantendo e analisando os preparativos de GCN

A organização deve implantar um programa de teste do GCN contendo a definição do que cada envolvido deve fazer e do nível de complexidade do teste. Também deve ser realizada uma análise crítica dos resultados, manutenção do programa de testes e definição de como serão realizadas as auditorias para verificar as conformidades do GCN com a legislação, padrões, *frameworks* e guias de melhores práticas.

Incluindo a GCN na cultura da organização

O desenvolvimento, promoção e incorporação da cultura de GCN na organização garantem que os processos de continuidade de negócio se tornem parte dos valores básicos e da gestão da organização. Esse processo pode ser longo e difícil caso exista certo nível de resistência por parte dos usuários, atividades de conscientização e treinamento de todos os usuários devem ser realizadas para que os mesmos possam compreender que a GCN é muito importante para a organização.

2.3.2 COBIT

O *Control Objectives for Information and Related Technology* (CobiT) é um guia de melhores práticas criado pela *Information Systems Audit and Control Association* (ISACA) para prover um modelo para o gerenciamento da Governança de TI. O CobiT possue 210 objetivos de controle divididos em 34 processos agrupados em 4 domínios (COBIT 4.1, 2005; LAHTI; 2006). São eles:

Planejamento e Organização (PO)

Aquisição e Implementação (AI)

Entrega e Suporte (DS)

Monitoração e Avaliação (ME)

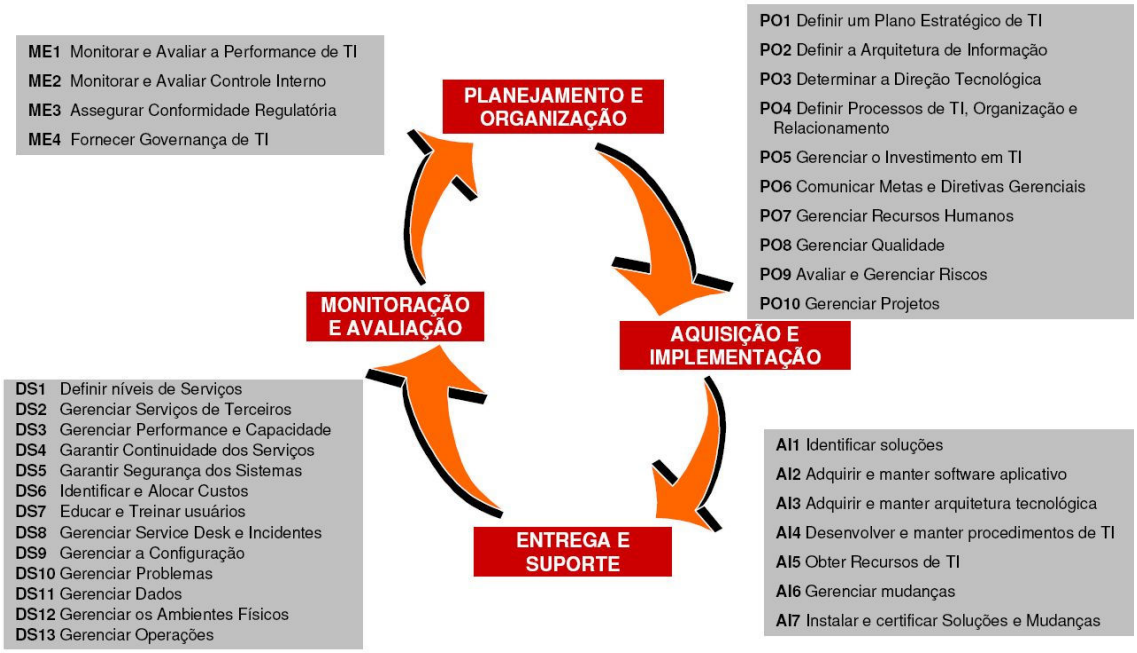

Figura 2.3: Visão geral dos 34 processos e os 4 domínios do CobiT.

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 7 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 13 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 4 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.

2.3.3 ITIL

O *Information Technology Infrastructure Library* (ITIL) foi criado no final da década de 80 pela Câmara de Comércio Britânico (OGC - *Office of Government Commerce*) com o intuito de disciplinar e permitir a comparação entre as propostas dos diversos proponentes a prestadores de serviços de TI para o governo britânico. Era composto por uma biblioteca com 31 volumes com as melhores práticas para o Gerenciamento dos Serviços de TI.

Em 2002 a biblioteca sofreu uma grande revisão e foi reformulada e consolidada em 8 volumes, sendo eles:

Suporte aos Serviços (*Service Support*)

Entrega de Serviços (*Service Delivery*)

Planejamento e Implementação (*Planning and Implemention*)

Gerenciamento de Aplicações (*Applications Management*)

Gerenciamento da Segurança (*Security Management*)

Gerenciamento da Infra-Estrutura de TI e de Comunicações (*Information and Communication Technology Infrastructure Management*)

Perspectiva do Negócio (*Business Perspective*)

Gerenciamento dos Ativos de Software (*Software Asset Management*)

A versão 2 do ITIL foca principalmente na entrega e no suporte dos serviços de TI, para torná-los mais aderentes e apropriados aos requisitos dos processos de negócio.

Figura 2.4: Visão geral da biblioteca de melhores práticas ITIL v2.

Os processos de Suporte aos Serviços focam nas tarefas diárias e necessárias para a manutenção dos serviços de TI. São eles: Gerenciamento de Configuração, Gerenciamento de Incidente, Gerenciamento de Problema, Gerenciamento de Mudança e Gerenciamento de Liberação.

Os processos de Entrega de Serviço concentram-se nas atividades de planejamento a longo prazo e na melhoria dos serviços entregues e atualmente utilizados pela organização. Os processos são: Gerenciamento do Nível de Serviço, Gerenciamento de Capacidade, Gerenciamento da Disponibilidade, Gerenciamento da Continuidade dos Serviços de TI e Gerenciamento Financeiro (MAGALHÃES, 2007).

A terceira versão do framework ITIL foi lançada em maio de 2007 e é composta por cinco livros. Sua principal mudança foi a introdução do ciclo de vida para o Gerenciamento de Serviços de TI. O ITIL v2 era baseado em processos com uma visão linear do serviço, e agora, o ITIL v3 está focado no alinhamento estratégico da TI com o negócio.

Os cinco livros do ITIL v3 são:

Estratégia de serviços – definição de objetivos, conceitos e regras sobre a estratégia de serviços, análise do impacto dos serviços necessários para as funções vitais do negócio, definição e métodos de gestão do risco. Orientações para os processos de gerenciamento financeiro, gerenciamento de demanda e gerenciamento de portfólio de serviços.

Desenho de serviços – descreve os objetivos, planos e cria um desenho de serviços, detalhando cada um dos processos relativos ao gerenciamento de nível de serviço, gerenciamento do catálogo de serviços, gerenciamento da disponibilidade, gerenciamento da capacidade, gerenciamento da segurança da informação, gerenciamento da continuidade dos serviços e o gerenciamento dos fornecedores.

Transição de serviços – descreve as formas para garantir o desenho de serviços na forma pretendida. Inclui os processos de gerenciamento de mudanças, gerenciamento da configuração e ativos dos serviços e gerenciamento de liberação e distribuição.

Operação de serviços – descreve a gerencia do serviço através do ciclo de vida de produção, é discutida a classificação e priorização de chamados, o modelo de comunicação e o gerenciamento de conflitos. Inclui o gerenciamento de evento, gerenciamento de incidentes, gerenciamento de problemas, gerenciamento de acesso e as requisições de serviços.

Melhoria continua de serviços – descreve formas para garantir a entrega dos serviços de forma eficaz e eficiente, são realizadas análises para identificar, compreender e medir os pontos fracos e fortes e orientar na implantação de melhoria dos serviços através, por exemplo, de indicadores chaves de desempenho. No livro melhoria continua de serviços é tratado o gerenciamento de nível de serviço.

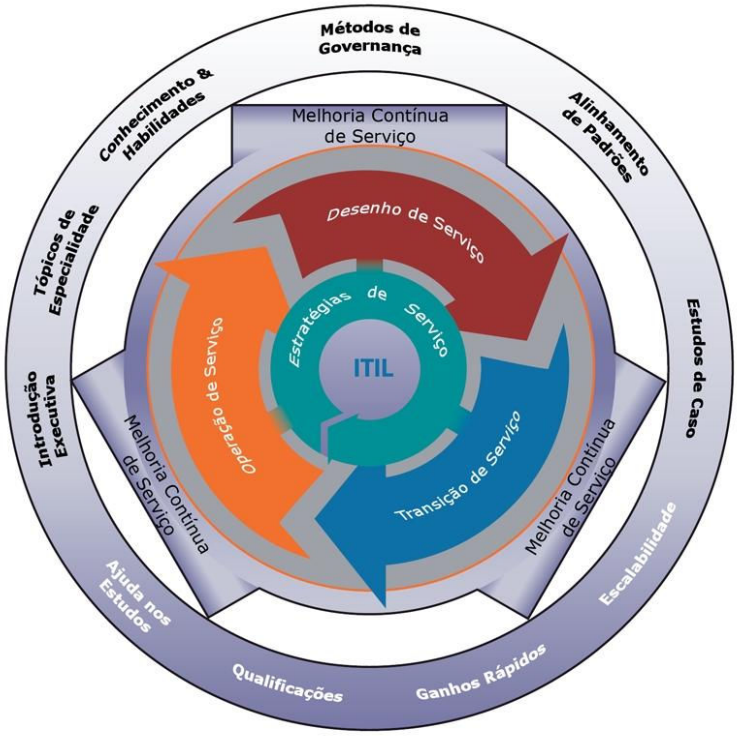

Figura 2.5: Visão geral do ciclo de vida da biblioteca de melhores práticas ITIL v3.

2.3.4 ABNT NBR ISO/IEC 27002

Criada pela *Brisith Standard* (BS) em 1999, a norma foi definida como BS 7799 - *Code of Practice for Information Security Management* e era composta por um guia contendo 36 objetivos de controle e decomposta em 127 medidas de controle. No ano 2000 foi homologada pela *International Organization for Standardization/International Electrotechnical Commision* (ISO/IEC) tornando-se um padrão internacional denominada ISO/IEC 17799. No Brasil a norma foi traduzida e definida como ABNT NBR ISO/IEC 17799 no ano 2000 e passou por uma revisão e atualização no ano de 2005. Em 2007 a norma é novamente submetida a revisão e atualização e passa a chamar-se ABNT NBR ISO/IEC 27002.

A norma ABNT NBR ISO/IEC 27002 foi criada com a intenção de estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (ABNT NBR ISO/IEC 27002, 2007). A norma deve ser utilizada como um guia para elaboração de uma política de segurança e

não tem o propósito de ser o único material na sua elaboração, a definição dos controles que serão avaliados e monitorados depende da necessidade e dos processos de negócios utilizados em cada organização.

A norma é dividida em 11 seções onde são descritos os objetivos de controles e as formas de implementação para alcançar o objetivo de negócio da organização, a seguir é apresentada cada seção:

Política de segurança da informação - orienta a direção na criação de uma política de segurança da informação, alinhada com os objetivos do negócio e apoiada pela direção da organização.

Organizando a segurança da informação - orienta a direção da organização no gerenciamento da segurança da informação, devem ser definidas as atribuições e responsabilidades de todos os envolvidos na política de segurança.

Gestão de ativos - orienta a direção na identificação dos ativos, definição dos seus proprietários e regras de uso. Deve ser realizada a classificação da informação e a definição dos procedimentos de rotulação e tratamento da informação.

Segurança em recursos humanos - a direção deve assegurar que os colaboradores, fornecedores e terceiros compreendam suas responsabilidades e estejam conscientes, através de treinamento, quanto às ameaças relativas à segurança da informação.

Segurança física e do ambiente - orienta a direção na prevenção do acesso físico não autorizado, danos e interferências nas instalações e a mitigação das perdas, danos, roubo ou interrupção das atividades da organização.

Gestão das operações e comunicações - orienta a direção na elaboração de procedimentos e responsabilidades operacionais, tais como, gestão de mudança, segregação de funções, separação dos ambientes de produção, desenvolvimento e testes, gerenciamento dos serviços terceirizados e gerenciamento de segurança em redes.

Controle de acessos - orienta a direção na implementação de controles de acesso à informação e aos recursos de processamento das informações. São propostas diretrizes para gerenciamento de privilégios e controle de acesso à rede.

Aquisição, desenvolvimento e manutenção de sistemas de informação - orienta a direção na definição dos requisitos necessários à segurança de sistemas de informação, tais como, uso de criptografia e diretrizes para a segurança dos arquivos de sistemas.

Gestão de incidentes de segurança da informação - orienta a direção na definição de responsabilidades na gestão de eventos de segurança da informação, além da coleta de evidências e mecanismos de análise de incidentes e seus impactos para a organização.

Gestão da continuidade do negócio - orienta a direção na definição de medidas para prevenir a interrupção do negócio da organização. Deve ser realizada a análise e avaliação de riscos para o desenvolvimento de um plano de continuidade dos ativos.

Conformidade - orienta a direção para garantir a conformidade dos processos quanto às leis, estatutos, regulamentações ou obrigações contratuais.

2.3.5 ABNT NBR ISO/IEC 27005

Criada em julho de 2008, a norma ABNT NBR ISO/IEC 27005, fornece as diretrizes para o processo de gestão de riscos em segurança da informação, a mesma foi criada para dar suporte às especificações e conceitos estabelecidos na norma ABNT NBR ISO/IEC 27001:2006. Define os requisitos para a criação de um sistema de gestão da segurança da informação (SGSI) (ABNT NBR ISO/IEC 27001, 2006).

A norma ABNT NBR ISO/IEC 27005 define de forma objetiva e estruturada as atividades de gestão de riscos, identificando as entradas no SGSI bem como as informações necessárias para o desempenho da atividade. Também orienta na elaboração de ações que descrevem a atividade, as diretrizes para implementação fornecendo as diretrizes para a execução da ação e as saídas que são as informações resultantes da execução da atividade (MÓDULO, 2008).

2.4 Modelo de maturidade

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.

O modelo de maturidade descrito pelo CobiT é baseado no modelo de maturidade para desenvolvimento de software, conhecido como *Capability Maturity Model for Software* (SW-CMM) proposto pela *Sotfware Engineering Institute* (SEI). CobiT desenvolveu um roteiro para cada um dos seus 34 processos baseado em uma classificação de maturidade, objetivando responder as seguintes perguntas (FONTES, 2008):

Qual o status atual da organização?

Qual o atual estágio de desenvolvimento da outras organizações?

Qual o atual estágio dos padrões internacionais?

Aonde a organização quer chegar e como ela planeja isso?

As organizações devem realizar uma avaliação honesta da sua capacidade para enfrentar as situações de contingência. A organização e, principalmente a direção, devem conhecer os pontos fortes e os pontos fracos em relação à continuidade do negócio.

A seguir são descritos os níveis do modelo de maturidade:

Nível zero (Inexistente) - Completa inexistência de quaisquer processos reconhecíveis. 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 a autorização para execução das responsabilidades é limitada. São implementadas soluções de contorno para resposta aos incidentes utilizando diversas abordagens reativas e inapropriadas.

Nível dois (Repetitivo) - Existe um reconhecimento da direção da necessidade de se ter um Plano de Continuidade de Negócios, mas as abordagens para garantir a continuidade do negócio são fragmentadas. Não existe um Plano de Continuidade de Negócios documentado apesar dos princípios serem conhecidos. Não há treinamento ou divulgação formal de procedimentos padronizados e as responsabilidades são deixadas a cargo das pessoas, existindo um alto grau de dependência em relação ao conhecimento individual, conseqüentemente, os erros são prováveis.

Nível três (Definido) - Os processos e procedimentos estão padronizados, documentados e divulgados através de treinamento, objetivando proativamente identificar, minimizar ou eliminar situações de indisponibilidade. 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.

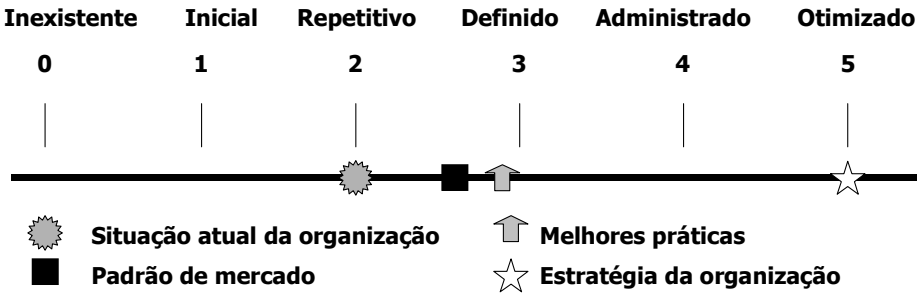

Figura 2.6: Gráfico representando o modelo de maturidade.

2.5 Gestão da continuidade de negócios

As organizações devem estar preparadas para enfrentar as situações de contingências que tornam indisponíveis os ativos de informação. É necessário que a organização tenha certa maturidade no processo de GCN, possuindo indicadores que permitam medir e gerenciar os processos do PCN. O objetivo do Plano de Continuidade de Negócios é determinar os pontos críticos das áreas de TI e do negócio da organização (MAGALHÃES, 2007). O processo de GCN deve obter e analisar as informações que vão resultar numa estratégia integrada e com um plano de ação correspondente para reagir a um incidente não-programado nas atividades relativas ao negócio.

A organização deve identificar os processos de negócios que compreendem um conjunto de atividades realizadas na organização, associadas às informações que

manipula, utilizando os recursos e a estrutura da organização. A Tabela 2.1 apresenta os pontos mais críticos para a organização, dividido em seus respectivos domínios.

Tabela 2.1: Pontos mais críticos para o negócio

Visão do Negócio	Atendimento aos clientes
	Atendimento a leis e regulamentações
Processos de Negócio	Processos de negócio de missão-crítica
	Plano de continuidade de negócios
Aplicações	Aplicações e bases de dados de missão-crítica
	Processamento de dados
	Procedimentos de recuperação de desastre
Infra-Estrutura	Segurança física e lógica
	Comunicações confiáveis
	Informações protegidas
	Hardware/*Software* – redundância

Fonte: MAGALHÃES, 2007. p. 667.

Muitas organizações começaram a compreender a importância da continuidade do negócio após os ataques terroristas ao *World Trade Center*, ocorrido em 11 de setembro de 2001 em Nova Iorque, onde algumas organizações deixaram de existir com a tragédia ou, por não possuírem um plano de continuidade de negócios ou, por terem um plano se utilizando dos recursos da torre ao lado. Após esse evento pergunta deixou de ser, "Qual a probabilidade disso acontecer?" e passou a ser, "E se isso acontecer?" (FONTES, 2008).

2.6 Estrutura de um plano de continuidade de negócios

O PCN deve apontar quais os processos críticos de TI que suportam o negócio da organização e os procedimentos necessários para evitar ou mitigar a indisponibilidade dos serviços de TI, de forma que os processos possam ser recuperados no menor intervalo de tempo possível e de acordo com as prioridades do negócio, após a ocorrência de um desastre.

2.6.1 Definição do escopo e do cenário

A organização deve definir o escopo e descrever o cenário atual levando em conta o nível de maturidade que se encontra. Deve ser pensado em um plano completo, onde vão existir diversas etapas e versões cada uma melhor do que a anterior. A administração como patrocinadora do plano, deve ter conhecimento da abrangência e das limitações do plano que está sendo criado.

2.6.2 Avaliação de ameaças e riscos

A organização deve realizar uma análise das ameaças e riscos considerando o escopo e cenário definidos anteriormente. A avaliação deve ser medida com valores qualitativos (alto, médio, baixo) e a avaliação deve contar com a avaliação de mais de uma pessoa.

2.6.3 Análise de impacto no negócio

É necessário que as conseqüências de desastres, falhas de segurança, perda de serviços e disponibilidade de serviços, passem pelo processo de análise de impacto nos negócios.

A análise de impacto nos negócios deve mapear os seguintes itens:

- Quantificar impactos financeiros, de imagem e operacionais;
- Processos de negócio críticos e suas prioridades;
- Dependências internas e externas;
- Recursos críticos;
- Prazos para impacto severo.

A análise de impacto vai trazer respostas para as questões, tais como, qual o tempo de indisponibilidade que o negócio suporta?

2.6.4 Identificação de soluções

Baseado nas informações obtidas nas etapas anteriores devem ser avaliadas as diversas soluções para processamento da informação. A opção mais adequada deve ser utilizada na implementação.

2.6.5 Elaboração do plano de continuidade de negócios

Deve ser criado um conjunto de documentos e manuais que permitam as pessoas, no caso de uma situação de contingência, seguir as instruções para solucionar o incidente.

O PCN é o conjunto de documentos normativos que devem descrever de forma clara, concisa e completa os riscos, as pessoas e suas responsabilidades.

Segundo MAGALHÃES 2007, o PCN deve ser elaborado com pelo menos os seguintes tópicos:

1. **Sumário executivo**, contendo, o propósito do plano, autoridade e responsabilidades das pessoas-chaves, tipos de emergências que podem ocorrer e o local de gerenciamento da operação.
2. **Gerenciamento dos elementos de emergência**, descrevendo os processos de direção e controle, comunicação, recuperação e restauração, administração e logística.
3. **Procedimento de resposta à emergência**, a organização deve elaborar *checklists* para orientar as ações que devem ser tomadas para proteção das pessoas e manutenção dos equipamentos, os procedimentos devem conter:

alertas para avisos de catástrofes naturais, condução de evacuação, desligamento das operações, proteção dos dados vitais e restauração das operações.

4. **Documentos de suporte**, a organização deve anexar ao PCN alguns documentos, tais como: lista de telefones das pessoas envolvidas no processo, planta das instalações físicas, guias com o desenho da infra-estrutura de TI e procedimentos para recuperação dos serviços de TI.
5. **Identificar desafios e priorizar atividades**, o PCN deve conter uma lista de tarefas para ser executada definindo Quem e Quando e determinar como devem ser tratados os problemas identificados na fase de levantamento.

2.6.6 Plano de teste e de manutenção

O PCN deve ser testado constantemente, não deve ser tratado com um processo estático, que uma vez elaborado, não vai necessitar de manutenção. Os testes também podem identificar situações até então não previstas no plano e que devem ser incorporadas (FONTES, 2008).

A etapa de manutenção vai permitir que o PCN seja cada vez mais completo, aumente o seu escopo e os cenários. Cabe salientar que as necessidades da organização se modificam e o PCN deve acompanhar as mudanças, os processos descritos num determinado momento podem não representar mais a real necessidade da organização (MAGALHÃES, 2007).

O sucesso do PCN vai ser obtido se todos os colaboradores, terceiros e prestadores de serviço tenham conhecimento do plano e, portanto, os mesmos precisam ser treinados para executar as atividades necessárias para minimizar a indisponibilidade do negócio. A conscientização e o treinamento devem ser realizados para todos, inclusive para a direção, considerando o papel de cada pessoa na operacionalização do plano.

2.7 Componentes de um plano de continuidade de negócios

O objetivo do PCN é a documentação de um planejamento de ações que deveram ser executadas na ocorrência de uma situação de crise, possibilitando a organização de continuar suas atividades de negócio em um nível aceitável definido pela área de negócio e pela direção.

O PCN deve ser construído para atingir uma determinada área ou solução considerando o cenário dos recursos, do escopo organizacional e das ameaças consideradas e que serão tratadas. Diversas organizações incorrem no erro de elaborar da primeira vez um plano que considere todas as situações. A orientação é começar por situações de maior risco e maior impacto (FONTES, 2008).

A organização deve elaborar o PCN contendo três itens sendo eles: o primeiro é o plano de administração/gerenciamento de crise, onde são nomeados os coordenadores que realizaram a busca por respostas às crises a fim de minimizar o impacto nos negócios; em seguida é criado o plano de resposta/continuidade empresarial, contendo os processos necessários para manter as funções essenciais da organização mesmo numa situação de crise e, por último a construção do plano de recuperação de desastre, elaborado para cobrir as situações onde a perda de recursos e a respectiva recuperação

demandam um esforço significativo e maior. A seguir são descritos os três itens que compõe o PCN (IMONIANA, 2008; FONTES, 2008).

2.7.1 Plano de administração/gerenciamento de crise

O plano de administração/gerenciamento de crise é um documento disponibilizado para os diretores da organização, objetiva reduzir os riscos e as incertezas do gerenciamento da situação sem controle e permitir que os executivos tenham maior controle sobre a organização durante a crise. Esse plano deve conter as informações dinâmicas necessárias, tais como, listas de contatos, relação e atividades das equipes envolvidas.

A organização deve criar uma equipe de administração/gerenciamento de crise, composta pelos seguintes diretores, diretor chefe, diretor financeiro, diretor de operações, diretor de tecnologia, diretor jurídico, gerente de continuidade dos negócios e o diretor de relações públicas. A equipe reunida vai atuar de forma rápida e decisivamente durante uma crise (MAGALHÃES, 2007).

O time de administração/gerenciamento de crise é responsável pela criação de políticas e é o responsável por fornecer proteção para os empregados e ativos da organização. Também é responsável por manter o controle sobre a continuidade no negócio, assegurar a comunicação entre a direção e as outras áreas e gerenciar a imagem pública da organização.

2.7.2 Plano de continuidade/resposta empresarial

No plano de continuidade/resposta empresarial são definidos os procedimentos de resposta para estabilizar a situação na ocorrência de um incidente ou evento indesejado. O plano também define normas que devem seguidas pelo Centro Operacional de Emergência (COE) que é o centro de comando de uma crise.

O plano objetiva identificar os tipos potenciais de emergências e as respectivas respostas necessárias, verificar a existência de procedimentos de respostas apropriados às emergências, recomendar o desenvolvimento de procedimentos de emergência que ainda não existem, identificar os requisitos de comando e controle para o gerenciamento de emergência. Também objetiva integrar os procedimentos de resposta com os procedimentos de recuperação de desastres e continuidade de negócios, sugerir a elaboração de procedimentos definindo o papel dos envolvidos e os processos para comunicação entre a equipe do COE e os demais envolvidos no evento ou incidente de crise.

Na elaboração do plano de continuidade/resposta empresarial algumas etapas devem ser seguidas. São elas: realizar uma análise da situação, elaborando as hipóteses e os possíveis cenários de crise; definir objetivos e metas, analisando a viabilidade e a prioridade com que os danos serão tratados; organizar a equipe, elaborando a estrutura organizacional que vai dar suporte ao plano, definindo procedimentos para ativação do plano, níveis de autoridade, papéis e as responsabilidades.

2.7.3 Plano de recuperação de desastre

As diretrizes de recuperação definem os procedimentos para restaurar, no menos tempo possível, as operações de tecnologia da informação em caso de interrupção não-

programada. Também devem prever os impactos da paralisação e o tempo máximo necessário para a recuperação as atividades da organização.

As principais estratégias para recuperação são: recuperação gradual ou *cold site*, onde é realizada a reconstrução da infra-estrutura começando do zero em outro local físico. Recuperação intermediaria ou *warm site*, quando a organização possui um contrato de locação com um fornecedor que possibilite o uso de processamento, armazenamento e conectividade para permitir a execução dos serviços de TI no local do fornecedor. Recuperação imediata ou *hot site*, a organização possui outro local próprio que possa executar o suporte aos serviços de TI. São conhecidos como Centro de Processamento de Dados (CPD) backup ou site de *Disaster Recovery* onde é possível transferir em pouco tempo os sistemas para outro local.

3 SEGURANÇA DA INFORMAÇÃO

A informação é o bem mais importante para as pessoas e para as organizações, antigamente essa informação ficava armazenada em um ambiente pequeno e controlado, hoje as informações são processadas e armazenadas em um complexo ambiente tecnológico e os dados estão disponíveis para todos os colaboradores da organização, precisando ser protegida e gerenciada adequadamente (BRASIL, 2007). Os principais atributos relacionados à segurança da informação são:

Disponibilidade – atributo que define que a informação deve estar disponível e integra quando solicitada pelas pessoas autorizadas pelo proprietário da informação. Mantendo a disponibilidade é garantida a prestação contínua do serviço, ou seja, sem interrupções no fornecimento de informações para os que têm direito a ela.

Confidencialidade – atributo que define que a informação deve ser acessada somente pelas pessoas autorizadas pelo proprietário da informação.

Integridade – atributo que define que a informação quando acessada esteja completa e com suas características originais definidas pelo proprietário da informação.

Autenticidade – atributo que garante que a informação foi enviada pelo proprietário da informação.

Não-repúdio – atributo que previne que a pessoa negue ser o emitente ou recebedor de determinada informação.

A proteção dos ativos é de extrema importância para a sobrevivência da organização e muitas vezes essa proteção não é realizada de forma adequada ou com o investimento necessário. As organizações devem tratar a segurança da informação para prevenção e não somente após ocorrer algum desastre. A seguir são apresentadas as principais ameaças que os ativos estão expostos e os mecanismos de defesas que devem ser aplicadas no ambiente computacional da organização (ABNT NBR ISO/IEC 27002).

3.1 Ameaças

A ameaça é causa potencial de um incidente indesejado, que pode resultar em dano a um sistema ou para a organização. Podendo ser caracterizado como ameaça natural, onde condições climáticas tais como, incêndios e inundações, podem causar danos nos ativos. Já a ameaça intencional, é causada de forma dolosa, ou seja, com a intenção de provocar um prejuízo, como por exemplo, fraudes eletrônicas e sabotagem. Por fim, a ameaça involuntária pode ser causa por ações inconscientes ou ingênuas do usuário, um exemplo é a engenharia social.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um grupo de resposta a incidentes de segurança para a Internet brasileira e é responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet brasileira. O grupo é mantido NIC.br (Núcleo de Informação e Coordenação do Ponto br) que faz parte do Comitê Gestor da Internet (CGI) e também atua na conscientização sobre os problemas de segurança (CERT.br, 2008).

O CERT.br mantém estatística de incidentes a ele reportados pelos administradores de rede, analistas de rede e outros profissionais que cuidam das telecomunicações no Brasil e exterior. A tabela abaixo mostra o total de 33.909 incidentes que foram reportados voluntariamente para a equipe de profissionais do CERT.br entre os meses de julho e setembro de 2008, desse total 45,89% são referente a fraude e pouco mais de 33,5% relacionados a scan de porta.

Tabela 3.1: Totais mensais e trimestral - Classificados por tipo de ataque.

Mês	Total	worm(%)		dos(%)		invasão(%)		aw(%)		scan(%)		fraude(%)		outros(%)	
Jul	13735	1806	13	2	0	20	0	232	1	4041	29	7463	54	171	1
Ago	11488	1859	16	0	0	19	0	530	4	3383	29	5505	47	192	1
Set	8686	1619	18	5	0	36	0	262	3	3986	4	2593	29	185	2
Total	33909	5284	15	7	0	75	0	1024	3	11410	33	15561	45	548	1

Fonte: CERT.br, 2008.

Legenda:

dos - denial of service;
aw: ataque a servidor web.

O gráfico abaixo mostra os incidentes divididos por tipo de ataque, onde se pode notar que quase 46% estão relacionados a fraude, onde a conscientização dos usuários quanto a importância da segurança da informação pode minimizar os ataques conhecidos como engenharia social. Os próximos itens descrevem as principais ameaças relacionadas à segurança da informação.

Figura 3.1: Gráfico dos incidentes reportados ao CERT.br – Julho a Setembro de 2008.

3.1.1 Usuário

Usuários desatentos e sem o treinamento adequado para utilização de sistemas, são considerados uma das principais ameaças à segurança da informação das organizações. O usuário é a pessoa que inicia qualquer procedimento ou processo e, portanto, tem o poder de decisão para clicar, autorizar, aceitar, executar ou simplesmente ignorar o que, em uma fração de segundo, pode representar um risco (SÊMOLA, 2008).

A organização deve cuidar do seu recurso humano através de programas de conscientização e treinamento de todos os usuários em segurança da informação. O usuário deve ser considerado um fator crítico para o sucesso no processo de proteção da informação. É importante que os usuários mais antigos orientem os mais novos quanto à segurança da informação, pelo exemplo dos colegas, chefia e principalmente da direção é que o novo colaborador vai considerar e se comportar quanto às regras da organização no processo de segurança da informação (FONTES, 2008).

O acesso à informação deve ser restrito e somente os usuários que necessitam aquela informação deve ter acesso à mesma, não adianta a organização possuir a melhor solução de controle de acesso lógico, se o usuário emprestar a sua senha para outro que não tinha acesso àquela informação. A facilidade de uso pelo usuário deve ser levada em conta, os controles necessários devem ser implementados, mas não podem engessar o processo de negócio.

Os usuários devem estar atentos para não proteger somente o computador, mas devem ter cuidado para não deixar informações confidenciais impressas, por exemplo, em salas após as reuniões. Os usuários costumam por desatenção comentar informações confidenciais em locais, tais como, elevador, táxi e *happy hour*, e sem perceber que podem prejudicar os negócios da organização. Sendo que o objetivo estratégico da organização é a realização do negócio, é necessária a conscientização do usuário para que o bem mais importante, a informação, seja protegida de forma adequada (FONTES, 2008).

3.1.2 Intrusos

Uma das ameaças à segurança é a do intruso, são pessoas de dentro ou fora da organização com a intenção de promover ataques aos sistemas de forma benigna, somente para explorar a rede e ver o que tem dentro dela, ou de forma maligna, para realizar modificações não autorizadas nos dados ou interromper os sistemas.

Existem três tipos de intrusos:

Mascarado: Uma pessoa que não tem autorização para usar os recursos, mas que penetra nos controles de acesso de um sistema para explorar a conta de um usuário legítimo, geralmente é alguém externo da organização.

Infrator: Um usuário legítimo da organização, mas que acessa dados, sistemas ou recursos dos quais não tem autorização ou tendo autorização, faz mau uso de seus privilégios.

Usuário clandestino: Uma pessoa que se apropria do controle de administrador do sistema e utiliza tal controle para escapar de auditorias e controles de acesso, pode ser de dentro ou de fora da organização (STALLINGS, 2008).

Os ataques de intrusão podem ser considerados desde não perigosos até sérios, existem atacantes de alto nível com conhecimento profundo da tecnologia e, os de baixo nível com pouco conhecimento e que utilizam programas prontos nos seus ataques.

3.1.3 *Spam* e Engenharia Social

Spam são mensagens indesejadas, geralmente enviadas para um grande número de pessoas sem a sua solicitação ou autorização. São também chamadas de UCE (*Unsolicited Commercial E-mail*) quando o conteúdo é exclusivamente comercial.

Historicamente o primeiro *spam* foi enviado por dois advogados, Canter e Siegel, a mensagem era sobre uma loteria de *Green Cards* americanos e foi enviada para um grupo de discussão da *Unix User Network* (USENET). Posteriormente a mesma mensagem foi enviada para diversos grupos de discussão da USENET causando espanto e revolta em muitos assinantes do grupo.

Os usuários são afetados de diversas formas, tais como (CERT.br, 2006):

Não recebimento de e-mails - No caso do provedor de internet limitar o tamanho da caixa postal dos usuários, o recebimento de muitos *spam* pode exceder o limite de armazenamento, fazendo com que os e-mails sejam descartados, uma solução é o uso de regras anti-*spam*.

Gasto desnecessário de tempo - O usuário tem que gastar um tempo para ler e identificar o e-mail como *spam*.

Aumento de custos - Quem paga a conta pelo envio do *spam* é quem o recebe. No *download* da mensagem *spam* consome a franquia mensal ou a ligação, no caso de conexão discada.

Prejuízos financeiros causados por fraude - O *spam* tem sido usado para induzir o usuário a acessar páginas clonadas de instituições financeiras ou para instalar programas maliciosos para furtar dados pessoas e financeiros.

Os provedores de acesso, *backbones* e organizações são afetados por causas, tais como (CERT.br, 2006):

Impacto na banda - O tráfego gerado pelos *spams* tem obrigado às organizações e provedores aumentarem seus *links* de conexão.

Má utilização dos servidores - Os servidores de e-*mail* são obrigados a gastar tempo e espaço em disco para tratar as mensagens indesejadas.

Inclusão em listas de bloqueio - O provedor ou servidor de e-*mail* da organização podem ser incluídos em listas de bloqueio, chamadas de *blacklist*. A inclusão prejudica o recebimento de e-mails legítimos e autorizados.

Investimento em pessoal e equipamentos - Os provedores e as organizações necessitam contratar profissionais especializados, comprar mais equipamentos e sistemas de filtragem de *spam*.

Engenharia social é um termo utilizado para descrever um método de ataque, onde alguém faz uso de persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações (CERT.br, 2006).

As mensagens mais enviadas estão relacionadas a supostos problemas no serviço de *Internet Banking* e pedem para o usuário acessar um *link* contendo o aplicativo que vai realizar a correção do problema. Esse método é conhecido como *phishing scam*, onde são enviados e-*mails* em massa, semelhante ao *spam* com o intuito de, na execução, furtar a senha de acesso da conta bancária do usuário e enviar para o atacante (TREVENZOLI, 2006; CERT.br, 2006).

Outro método é um ataque por telefone, onde o atacante liga para a vítima dizendo ser do suporte técnico do provedor de acesso. O atacante informa que existe um problema na conexão com a internet e solicita a senha da vítima para realizar a correção do problema. A senha é utilizada para atividades maliciosas e, as ações, ficam relacionadas ao login do usuário atacado.

A seguir algumas recomendações que dever ser seguidas para evitar ataques de engenharia social (CERT.br, 2006).

- Não fornecer dados pessoais, números de cartões e senhas através de contato telefônico;
- Ficar atento a e-mails ou telefonemas solicitando informações pessoais;
- Não acessar sites ou seguir *links* recebidos por e-mail ou presentes em páginas sobre as quais não se saiba a procedência;
- Sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contato com a instituição, provedor ou empresa para verificar a veracidade dos fatos.

3.1.4 Ataques físicos

Roubos de informações importantes da organização são realizados através de ataques físicos, onde equipamentos, fitas magnéticas, CDs, DVDs e *pendrives* são retirados da organização ou roubados de funcionários para posterior análise. A norma ABNT NBR ISO/IEC 27002 trata da segurança física e do ambiente com o objetivo de propor diretrizes para prevenção do acesso físico não autorizado, danos e interferências nas instalações e informações (CARVALHO, 2005).

Devem ser tomadas medidas para impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização. O acesso físico deve ser protegido com a criação de um perímetro de segurança física, incluindo controles de entrada física, segurança nos escritórios, salas e instalações, proteção contra ameaças externas e do meio ambiente e acesso do publico, área de entrega e carregamento (ABNT NBR ISO/IEC 27002, 2007).

Com relação à segurança do ambiente e equipamentos, atenção deve ser dada para instalação e proteção dos equipamentos, interrupções por falta de energia, segurança do cabeamento, manutenção e segurança dos equipamentos fora da organização, reutilização e descarte seguro dos equipamentos. Para proteção relacionada à segurança física são utilizados dispositivos de autenticação (ver 3.2.2) e criptografia (ver 3.2.5).

3.1.5 *Malwares*

Código malicioso ou *Malware* (***Mal****icious Soft****ware***) é um termo utilizado que caracteriza os programas desenvolvidos para executar ações maliciosas, com o intuito

de danificar ou roubar informações de um computador. Um software legal que contenha falha de programação (intencional ou não) e execute ações ilícitas também é considerado como *malware*. A seguir são apresentados os diversos tipos de *malwares*.

O vírus é um programa de computador que contém comandos maliciosos, para simplesmente perturbar o usuário até causar sérios dados, alterando ou destruindo programas ou arquivos do disco. O vírus se propaga inserindo cópias de si mesmo ao se deslocar. Depende da ação do usuário, ou seja, a execução do programa ou arquivo hospedeiro na disseminação do vírus é realizada pelo usuário. Alguns tipos de vírus são: vírus de boot, vírus de executável, vírus de macro, vírus de *e-mail* e vírus de telefone celular que se propagam através da tecnologia *bluetooth* (TANEMBAUM, 2003; CERT.br, 2006).

O *worm* (verme) é um programa ou fragmento de programa que propagam cópias de si mesmo a outros computadores através de conexões de rede e não precisam da ação do usuário. Um *worm* busca outras estações para infectar e cada computador infectado vai servir de base de lançamento para automaticamente atacar outras máquinas. Na replicação o *worm* utiliza, por exemplo, recursos de *e-mail*, enviando cópias de si mesmo para outros usuários ou sistemas. Também tem a capacidade de execução remota e de login remoto, podendo realizar acesso remoto a um sistema e depois executar comandos para se propagar (STALLINGS, 2008).

O *bot* é um programa capaz de se propagar automaticamente pela rede, explorando as vulnerabilidades ou falhas de configuração dos sistemas, diferentemente do *worm*, o *bot* é capaz de se comunicar remotamente com o atacante. O *bot* e o atacante se conectam a um servidor *Internet Relay Chat* (IRC) e entram numa determinada sala, onde são enviadas mensagens contendo uma seqüência especial de caracteres que é interpretada e executada pelo *bot* residente no computador invadido. Um conjunto de computadores infectados com bots cria uma rede chamada de *botnets*, utilizadas para o envio de milhares de *phishing scam* e disparar ataques de negação de serviço (WEBER, 2008; CERT.br, 2006).

Cavalo de tróia (*trojan horse*) é um programa ou procedimento de comando aparentemente útil, que executa as funções as quais foi criado, mas contém código oculto que realiza funções maliciosas, indesejadas e sem o consentimento do usuário. São utilizados, por exemplo, para disseminação de *backdoor*, instalação de *keyloggers* ou *screenlogers* e a destruição de dados (CERT.br, 2006).

Um *backdoor* (porta dos fundos) ou *trapdoor* (alçapão) é um programa instalado indevidamente e que deixam a porta aberta para futuros acessos remotos do atacante. Inicialmente os programadores utilizavam os *backdoors* para disparar e testar seus programas, mas se tornou uma ameaça quando *hackers* começaram a utilizá-lo para invadir os sistemas. Geralmente o computador recebe o *backdoor* através de um cavalo de tróia e é disparado quando reconhece um seqüência especial de entrada ou é executado por um determinado ID de usuário (STALLINGS, 2008).

Keyloggers são programas que realizam a captura e armazenamento das teclas digitadas pelo usuário em um sistema. Na maioria dos casos, a ativação do *keyloggers* acontece com a ativação do usuário e esse tipo de *malware* possui mecanismos que enviam automaticamente as informações colhidas para o atacante. Com o aperfeiçoamento desse *malware* surgiram os *screenloggers*, que são programas que capturam e armazenam a posição do cursor e a tela apresentada no monitor e a região que circunda a posição onde o *mouse* é clicado (CERT.br, 2006).

O *adware* (*Advertising software*) é um software com a função exclusiva de apresentar propaganda, sendo através do navegador do usuário ou de outros softwares, tais como o *MSN Messenger*. Muitas organizações têm utilizado o *adware* de forma licita para patrocínio, principalmente em projetos ou serviços gratuitos. A utilização de forma ilícita acontece quando o *adware* tem a função de monitoração dos hábitos de navegação do usuário para envio de propagandas mais especificas (WEBER, 2008).

O *spyware* é um programa utilizado para realizar o monitoramento das atividades realizadas pelo sistema e enviar as informações coletadas para o atacante. Da mesma forma que o *adware*, existem os *spywares* que são utilizados de forma licita, como por exemplo, para a monitoração das atividades dos usuários de uma determinada organização. Por outro lado, o *spyware* é muito utilizado para ativar o *keyloggers ou screenloggers* quando identifica que o usuário está acessando um site de banco.

Os *rootkits* são programas instalados no computador da vítima e projetados para ficarem ocultos dentro do sistema para esconder as atividades e informações do invasor. Os *rootkits* podem ter as mais variadas funcionalidades, tais como: *backdoors*, *sniffers* que são programas que capturam informações que trafegam pela rede, *keyloogers* entre outros.

3.1.6 Ataques de negação de serviço (DoS e DDoS)

Um ataque de negação de serviço ou DoS (*Denial of Service*) consiste em um *host* ou nó de rede enviar um número indiscriminado de requisições ao *host*, através de programas maliciosos chamados de *flood* (inundação). Como resultado o *host* é estressado ao limite e resulta na indisponibilidade do sistema ou serviços impedindo o acesso ao mesmo. Ataque de *buffer overflow* (estouro de memória), onde o tamanho de um *buffer* ultrapassa a capacidade máxima de armazenamento, corrompendo ou travando o sistema, causando o ataque de negação de serviço.

O ataque conhecido como SYN *Flooding*, tem a intenção de esgotar o link de dados, onde são enviados vários pacotes SYN para encher a fila de conexões do servidor e causa a negação de serviço. No ataque de IP *Spoofing* o programa faz a falsificação do endereço IP de origem, técnica utiliza em ataque de DoS, onde vários *hosts* podem enviar pacotes como se fossem um determinado endereço de origem, derrubando servidores que realizam a autenticação via endereço IP.

Nos ataques de DDoS (*Distribuited Denial of Service*), são utilizados milhares de computadores para realizar ataques de negação de serviço, onde o atacante consegue instalar software malicioso em estações comuns, depois de infectadas chamadas de zombis que realizam requisições ao *host* alvo, tornando os sistemas indisponíveis (CARVALHO, 2005; STALLINGS, 2008).

3.1.7 *Packet Sniffing*

O ataque de *packet sniffing* realiza o monitoramento passivo do tráfego da rede e captura os pacotes que possam conter informações importantes, tais como, senhas e realiza a cópia de arquivos que circulam pela rede. Faz o monitoramento passivo do tráfego da rede (CARVALHO, 2005).

3.1.8 *Port Scanning* e *Scanning* de vulnerabilidades

No ataque conhecido como *port scanning* ou varredura de porta é realizado o mapeamento das portas abertas e dos serviços que estão ativos no *host*. Existem outros tipos de varreduras, como por exemplo, a varredura de *firewall* onde são verificas as portas filtradas pelo *firewall* e a varredura ICMP (*Internet Control Message Protocol*) – protocolo que realiza o intercâmbio de pacotes de controle entre um roteador e um *host* ou entre *hosts* e objetiva detectar se o *host* está ativo. O CERT.br divulgou recentemente o número de incidentes reportados relacionados a scans de porta. No total do terceiro trimestre de 2008 foram 11.410 incidentes reportados sendo que praticamente a metade dos incidentes foi referente a porta 22, utilizada para realizar acesso remoto a *hosts*.

Incidentes reportados ao CERT.br - Julho a Setembro de 2008

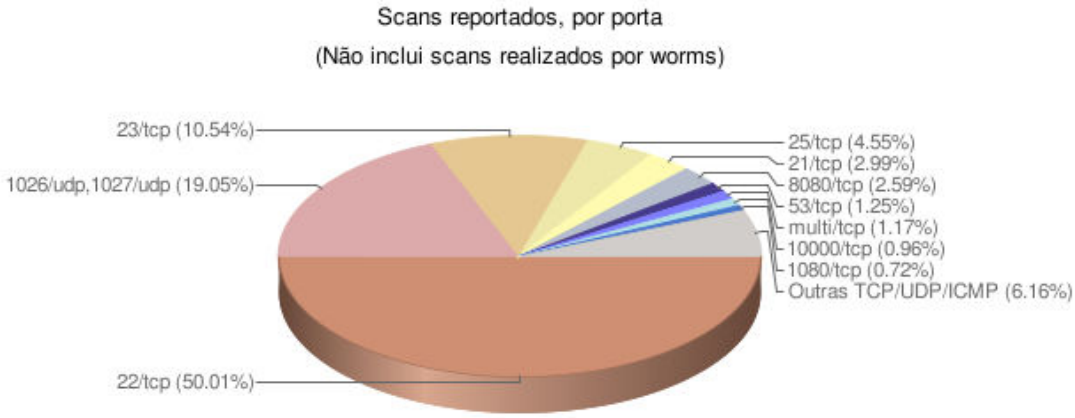

Figura 3.2: Gráfico dos incidentes de scans por porta reportados ao CERT.br

3.2 Defesas

As organizações precisam implementar mecanismos para a proteção das ameaças e mitigação dos riscos que podem afetar a continuidade do negócio. A seguir são apresentados os principais mecanismos para proteção dos ativos.

3.2.1 Educar o usuário

Principal responsável para manutenção da segurança da informação, a organização deve cuidar de forma adequada do seu recursos humanos, a conscientização e o treinamento dos usuários que um fator importante para disseminar a cultura de proteção da informação.

Conscientização do usuário quando ao uso e definição da senha devem ser realizadas, a seguir são apresentados alguns cuidados devem ser tomados (STALLINGS, 2008; FONTES, 2008; FONTES, 2006):

1. Trocar imediatamente a senha padrão fornecida pelo administrador na criação do login de acesso;
2. Não utilizar senhas curtas, recomenda-se a utilização de no mínimo oito caracteres, contendo letras, números e caracteres especiais;
3. Não utilizar senhas com palavras que possam ser encontradas em dicionários.

4. Não utilizar datas de nascimento, nomes de pessoas, nomes de times ou outras informações que estejam ligadas a você ou à organização;
5. Não utilizar números de telefones, números de documentos ou letras e números de placas de automóveis.

3.2.2 Autenticação

A autenticação tem o propósito de validar a identificação dos usuários nos sistemas ou recursos, é a garantia de que uma comunicação é autêntica e que o solicitante da comunicação é realmente aquele que afirma ser. Os métodos de autenticação podem ser divididos em três tipos: utilizando algo que você é, algo que você sabe e algo que você possui (CARVALHO, 2005).

A autenticação utilizando algo que você É, realiza a autenticação utilizando informações referentes as características físicas e comportamentais do usuário, é conhecida como biometria. São exemplos de identificação biométrica as impressões digitais, a leitura da retina e da íris, geometria das mãos e reconhecimento de voz. A implementação do controle de acesso e autenticação através de biometria é considerada de alto custo para as organizações, passível de ocorrência de falsos positivos ou falsos negativos e a autenticação pode ser afetada no caso de acidente ou estado de saúde do usuário.

A autenticação utilizando algo que você SABE, é a forma mais utilizada nas organizações e com o custo financeiro mais baixo. As senhas são seqüências de caracteres utilizadas para verificar a identidade de um usuário frente ao sistema que o mesmo deseja acessar, considerada a forma mais comum de autenticação e também a menos segura já que a segurança do sistema fica dependente do segredo da senha. Outra forma de autenticação é com o uso de PIN (*Personal Identification Number*) que é uma seqüência de números e/ou letras usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, sendo somente para pessoas autorizadas (ICP Brasil, 2006).

A autenticação utilizando algo que você POSSUI, está sendo utilizada cada vez mais nas organizações e geralmente são utilizados dispositivos físicos para realizar a identificação do usuário. Os certificados digitais são arquivos eletrônicos que contém dados de um usuário ou organização e são armazenados em um *smart card* (cartão inteligente), onde um *microchip* inserido num cartão plástico armazena e processa os dados, são muito utilizados para armazenar certificados digitais (ICP Brasil, 2006).

A técnica de autenticação conhecida como OTP (*One-Time Password*), em português senha descartável, é implementada geralmente em *token*, dispositivo de *hardware* que armazena um programa que gera uma nova senha periodicamente ou a cada autenticação do usuário. Uma vantagem na utilização da OTP é a proteção contra *phishing* de senha.

3.2.3 *Firewall*

Firewall é um dispositivo baseado em *software* e/ou *hardware* utilizado para segmentar e controlar o acesso entre redes distintas, analisando todos os pacotes que passam pela rede, aceitando, descartando ou rejeitando os pacotes com base em um conjunto de regras especificadas. O *firewall* é inserido entre a rede local e a internet, protegendo um perímetro contra ataques e para garantir um único ponto de controle

onde são inseridas as implementações de segurança e auditoria. Atualmente os *firewalls* são implementados utilizando técnicas de controle de serviço, controle de direção, controle de usuário e controle de comportamento que são utilizadas para controlar o acesso e impor a política de segurança da organização. A seguir são apresentadas as técnicas, os tipos e as arquiteturas para implementação de um *firewall* na organização.

3.2.3.1 Tipos de firewall

O *firewall* de filtragem de pacotes, realiza a análise do cabeçalho de cada pacote, permite a entrada do pacote na rede interna validando o endereço de origem baseado num conjunto de endereços previamente configurado no *firewall*. A análise do pacote é realizada na camada de rede e transporte do modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*). Esse tipo de *firewall* é vulnerável a ataques conhecidos como *IP Spoofing*, onde pacotes inválidos são inseridos na conexão através da falsificação do IP de origem.

O *firewall* de inspeção com estados (*stateful inspection firewalls*) realiza a validação do pacote através das regras de filtragem e adicionalmente utiliza tabelas de estado de conexão para controlar toda sessão aberta entre a origem e o destino. Com isso é garantida uma conexão segura e mais rápida entre os dois pontos. A informação do estado anterior das comunicações é guardada e verificada na tomada de decisão para novas conexões (STALLINGS, 2008).

O *gateway* em nível de circuito, *application gateways* ou *proxy* realiza a intermediação entre o *host* cliente e o *host* externo, não permitindo uma conexão ponta a ponta. São realizadas duas conexões no *gateway*, uma entre o *host* cliente e ele mesmo e outra entre ele e o *host* externo, com isso o conteúdo da conexão é analisando e só depois é repassado para a outra ponta.

3.2.3.2 Arquiteturas de firewall

A arquitetura de *firewall* se preocupa com a disposição dos equipamentos em relação a localização do *firewall*. A DMZ (*DeMilitarized Zone*) ou zona desmilitarizada pertence ao perímetro de segurança e é uma área entre a rede interna e a rede externa, onde são mantidos todos os serviços que possuem acesso externo e, por questões de segurança, necessitam ficar fora da rede local. Chamados de *bastion hosts*, são *hosts* que fornecem serviços para outros *host* que estão fora da rede interna da organização.

Existem três tipos de arquitetura de *firewall*, são elas: Arquitetura *dual-homed host*, consiste na separação entre a rede interna e a rede externa, utilizando um *host* contendo duas interfaces de rede, onde a conexão do *host* de origem é realizada primeiramente com o *firewall* e o mesmo realiza a conexão com o *host* de destino. Na arquitetura *screened host*, é utilizado um *firewall* de filtragem de pacotes e um *bastion host* que funciona como um *proxy*, onde todos os *hosts* internos devem se conectar a ele para acessar a rede externa. Por fim, a arquitetura *screened subnet*, é utilizado um *bastion host* localizado na DMZ que fará a intermediação entre o *firewall* interno e o externo. No caso de um ataque vai ser necessário que o invasor passe por dois *firewalls* para acessar a rede interna da organização (STALLINGS, 2008).

3.2.4 Detecção e prevenção de intrusão

Os sistemas de detecção e os de prevenção de intrusão são dispositivos de monitoramento capazes de perceber a ocorrência de atividades suspeitas, impróprias,

incorretas ou anômalas. A detecção de intrusão é baseada na suposição de que o comportamento do intruso difere daquele de um usuário legítimo.

Mesmo que o comportamento de um intruso seja diferente a do usuário legítimo, existe uma sobreposição desses comportamentos. Assim uma interpretação em relação ao comportamento de um intruso, também levará a falsos positivos ou usuários autorizados identificados como intrusos. Por outro lado no caso de tentar eliminar falsos positivos com a implementação rígida do sistema de detecção levará ao aumento de falsos negativos, ou seja, intrusão não identificada como intrusão. A seguir são descritos os tipos de *Intrusion Detection System* (IDS) e *Intrusion Prevention System* (IPS) e a metodologia de detecção.

3.2.4.1 Tipos de sistemas de detecção de intrusão

O sistema de detecção baseado em *host*, em inglês *Host-Based Intrusion Detection System* (HIDS), monitora e detecta alterações no sistema de arquivos checando a integridade dos arquivos. O HIDS calcula o valor de função de prova (*hash*) para os arquivos críticos no momento da instalação, periodicamente é recalculado o valor de *hash* dos arquivos, havendo diferença nos valores originais e nos novos, o arquivo foi alterado e é gerado um alerta. Também são utilizados registros de eventos de auditoria e arquivos de *log* na detecção baseada em *host*. Os HIDS realizam também o monitoramento de processo e atividades nos sistemas, uso da CPU, modificação nos privilégios dos usuários, detecção de *port scanning* e programas que estão sendo executados.

As principais vantagens do HIDS são: ataques criptografados podem ser detectados, não necessita de *hardware* adicional, gera poucos falsos positivos, são independentes da topologia de rede, ataques físicos no sistema podem ser detectados e detecta o sucesso ou falha de um ataque ao sistema com base no registro do sistema. Por outro lado, as desvantagens na utilização do HIDS são: dependência do sistema operacional, não detecta ataques de rede, o *host* monitorado apresenta perda de desempenho, informações podem ser perdidas em uma invasão ao HIDS e são pouco eficientes em sistemas com poucas informações de auditoria.

O sistema de detecção baseado em rede, em inglês *Network-Based Intrusion Detection System* (NIDS), monitora o tráfego de rede utilizando algoritmos estatísticos e baseado em assinatura, semelhante ao antivírus. Esta abordagem gera menos falsos positivos do que as técnicas estatísticas. No monitoramento estatístico são criados perfis de tráfego “normal” da rede, que são utilizados para identificar atividade não usual.

As principais vantagens do uso de NIDS são: ataques são detectados em tempo real, monitoramento pode ser realizado em ambiente multiplataforma, detecção em nível de rede, monitoramento estatístico não necessita de atualização de assinatura, sem impacto na rede e monitoramento de atividades em portas conhecidas. As desvantagens na utilização do NIDS são: atualização das assinaturas deve ser freqüente, não é realizado o monitoramento de tráfego cifrado, dificuldade de utilização em redes segmentadas e de implementação em redes rápidas. O ideal é a utilização a combinação das duas abordagens.

Uma nova ferramenta de detecção de intrusos que começa a ser utilizada pelos administradores de redes é o sistema de detecção no *Kernel*, em inglês *Kernel Intrusion Detection System* (KIDS), permitindo a captura de pacotes no módulo do *kernel* do Linux. Podemos citar o projeto *Linux Intrusion Detection System* (LIDS) que é um

patch de melhorias para o *kernel* do Linux onde foram adicionadas esquemas de segurança que não são possíveis nas funções nativas da *kernel* (TAMBORIM, 2008). Por último existem os sistema híbridos de detecção de intrusão, em inglês *Hybrid Intrusion Detection System* (Hybrid IDS), são sistemas que agregam os pontos positivos dos HIDS e NIDS, atuando na análise somente do tráfego destinado a si próprio.

3.2.4.2 Metodologias de detecção de intrusão

A metodologia de detecção por assinaturas, em inglês *Knowledge-Based Instrusion Detection*, utiliza uma base de dados com padrões de ataques (assinaturas) para comparação com o possível ataque em andamento. Um vantagem é que esse tipo de sistema, por possuir uma base de ataques conhecidos, realiza a detecção de forma mais rápida e gera menos falsos positivos. Um desvantagem é que ataques novos podem não ser detectados caso não estejam na base de assinaturas, ou seja, depende de constante atualização para ser um método eficiente.

O método de detecção estatística de anomalia, em inglês *Behavior -Based Instrusion Detection*, é composta por duas categorias: detecção de limiar e sistemas baseados em perfil. Na detecção de limiar, o evento é considerado uma intrusão quando um número de ocorrências de um tipo de evento pré-definido é realizado. No caso dos sistemas baseados em perfil, são definidos perfis de usuários partindo da caracterização do comportamento passado dos usuários, qualquer desvio significativo no comportamento é considerado como violação e é gerado um alerta. Uma vantagem é que as decisões podem ser tomadas por meio de análise estatísticas ou heurísticas, sem a necessidade de conhecimento prévio das falhas de segurança, onde o sistema vai aprendendo o que é o comportamento "normal" e depois procura os desvios. Um desvantagem é o grande número de falsos positivos e falsos negativos gerados pelo sistema.

3.2.4.3 Tipos de Sistemas de Prevenção de Intrusão

O sistema de prevenção baseado em *host*, em inglês *Host-Based Intrusion Prevention System* (HIPS) utiliza assinaturas e padrões para identificar atividade não usual, as ações executadas são no sentido de encerrar processos e bloquear o tráfego de rede de ou para um dispositivo comprometido. Já o sistema de prevenção baseada em rede, em inglês *Network Intrusion Prevention System* (NIPS) realizam a análise completa dos pacotes e identifica os pacotes suspeitos, encontrando um pacote malicioso, o mesmo e seus subseqüentes são descartados. A identificação incorreta de pacotes válidos pode impedir o tráfego e funcionamento dos sistemas.

3.2.5 Criptografia

A criptologia é o estudo das técnicas para garantir o sigilo e/ou a autenticidade da informação e se divide em dois ramos principais, a criptografia que é definida com a arte ou ciência que trata do projeto dessas técnicas, tornando a mensagem confusa, incompreensível para qualquer pessoa que não seja o destinatário da mesma; e a criptoanálise, que trata dos mecanismos para reverter essas técnicas, recuperar a informação ou forjar informações tidas como autênticas (STALLINGS, 2008; WEBER, 2008). A seguir são apresentadas as duas formas de implementação de criptografia, sendo elas, simétrica e assimétrica.

Criptografia simétrica, também conhecida como criptografia convencional, onde com uma única chave é realizada a cifragem e decifragem da informação. O texto claro,

com a mensagem ou dados originais é cifrado com a utilização de um algoritmo de criptografia que realiza diversas substituições e transformações embaralhando o texto original.

Uma vantagem na utilização de criptografia simétrica é a rapidez no processo de cifragem e decifragem. Em contra partida as desvantagens consistem na necessidade de que para cada par de usuários tenhamos uma chave diferente, a chave precisa ser transmitida pelo menos uma vez do emissor para o receptor, com isso a transmissão pode ser interceptada comprometendo a integridade da informação e a autenticidade e o não-repudio. Exemplos de algoritmos: DES, 3DES, IDEA e o AES (CARVALHO, 2005).

Existem duas técnicas de ataque associados a criptografia convencional, a criptoanálise onde o atacante tenta descobrir o texto claro explorando características do algoritmo. Outra técnica é o ataque por força bruta onde o atacante experimenta cada chave possível, utilizando um dicionário de dados, até obter o texto claro. Geralmente, o ataque é bem sucedido testando metade de todas as chaves possíveis (STALLINGS, 2008).

Na criptografia assimétrica ou de chave pública, criptagem e decriptagem são realizadas utilizado um par de chaves, sendo uma pública, de conhecimento de todos e a outra privada mantida em sigilo pelas partes. O algoritmo de chave pública utilizam funções matemáticas para realizar varias transformações no texto original (SILVA, 2005).

Uma vantagem na utilização da criptografia assimétrica é a segurança, pois é computacionalmente inviável determinar a chave de decriptografia tendo o conhecimento apenas da chave de criptografia e com isso é garantida a confidencialidade. A desvantagem reside no tempo gasto para se criptografar ou decriptografar a informação, sendo muito superior ao da cifragem simétrica. Exemplos de algoritmos: RSA e Diffie-Hellman (STALLINGS, 2008; WEBER, 2008).

4 CHECKLIST DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

O *checklist* a seguir visa avaliar e orientar a organização quanto a sua maturidade na gestão de riscos e a conformidade com as melhores práticas utilizadas atualmente no que se refere a segurança da informação e gerenciamento de risco. As questões foram elaboradas seguindo a maioria dos controles propostos nas normas ABNT NBR ISO /IEC 27002 e BS 27999-1. É recomendado que a organização utilize as respostas do *checklist* para mapear os principais riscos e ameaças que os ativos podem estar sujeitos.

As respostas possíveis da legenda abaixo foram elaboradas seguindo o modelo de maturidade discutido no item 2.4 e nas sugestões propostas por FONTES, 2008. Quanto mais próximo do sim for a resposta, mais adequada com as normas o controle está e maior é o nível de maturidade frente aos processos de segurança da informação. O *checklist* pode ser aplicado em toda a organização ou somente em um departamento.

LEGENDA:

	Resposta	
AV – Avaliação	0 - Solução em planejamento inicial. 1 - Está planejada a implantação da solução. 2 - Parcialmente implementada. Instável. Ainda não confiável. 3 - Possui o mínimo de atendimento aos requisitos. Prestes a ser melhorada. 4- Quase totalmente implementada. Satisfatório para situações normais. 5 - Totalmente implementada. Solução implementada é referência de mercado.	
NA - Não Aplicável	S - Sim	N - Não
NV - Não Verificado	S - Sim	N - Não

CHECKLIST - PLANO DE CONTINUIDADE DE NEGÓCIOS							
OBJETIVO:							
DATA:			**ÁREA DE ABRANGÊNCIA:**				
Nº	ADEQUAÇÃO		CONTROLE/PROCEDIMENTO				
	NORMA	ITEM	QUESTÃO	AV	NV	NA	OBS
G01			**Fatores críticos de sucesso**				
C01			Envolve a área de segurança da informação no planejamento das ações de negócio da organização.				
C02			Define os objetivos do negócio e a forma de atuação da organização.				
C03			Define recursos financeiros para o processo de segurança da informação.				
C04			Avalia periodicamente o desempenho da gestão da segurança da informação.				
C05			Avalia as prioridades da implementação dos controles de segurança da informação.				
G02			**Política de segurança da informação**				
C01			Possue um documento de política de segurança da informação, contendo uma definição, seus objetivos e a importância da segurança no uso e proteção da informação.				
C02			Declara o comprometimento e aprovação da direção, apoiando os objetivos e princípios da segurança da informação.				
C03			Publica e comunica a todos os colaboradores e partes externas o documento da política de segurança da informação.				
C04			Relata as políticas, princípios e padrões de segurança, abordando às obrigações legais e contratuais, necessidade de treinamento, prevenção, gerenciamento da continuidade do negócio e as conseqüências em caso de violação da política de segurança.				
C05			Define as responsabilidades gerais e específicas na gestão da segurança da informação.				
C06			Faz referências a outras literaturas sobre segurança que possam ajudar a elaboração da política de segurança da informação.				
C07			Define um responsável definido para revisão e manutenção da política de segurança.				
C08			Garante que a política de segurança da informação esteja de acordo com o código de				

			ética e demais políticas organizacionais.				
C09			Assegura que a política de segurança da informação esteja coerente com a legislação do seu país.				
G03			**Organizando a segurança da informação**				
C01			Possue uma estrutura gerencial para iniciar e coordenar a implementação do processo de segurança da informação.				
C02			Define claramente todas as responsabilidades pela segurança da informação.				
C03			Existe um fórum gerencial responsável pela aprovação da política de segurança da informação e monitoração da implementação desta política de segurança.				
C04			Identifica e define as responsabilidades pelos ativos e processos de segurança da informação.				
C05			Define níveis de autorização para os responsáveis pelos ativos de segurança.				
C06			Define um processo de gestão de autorização para aquisição de novos recursos computacionais.				
C07			Autoriza a utilização de meios pessoais de processamento de informações no ambiente de trabalho.				
C08			Realiza contato com autoridade policiais, órgãos regulamentadores, provedores de serviços e operadoras de telecomunicações para obter apoio no caso de incidentes de segurança.				
C09			Existe a independência da área responsável pelo processo de segurança da informação na definição dos requisitos de segurança da informação.				
C10			Realiza uma avaliação de riscos determinando formas de garantir a segurança, onde houver necessidade de acesso de terceiros.				
C11			Possue contrato definindo a permissão do acesso de terceiros.				
C12			Diferencia os riscos de acesso físico dos riscos de acesso lógico.				
C13			Monitora e define o tipo de acesso utilizado, o valor das informações, os controles utilizados pela terceira parte e as implicações deste acesso para segurança das informações da organização.				

C14			Existe acordo permitindo auditoria para verificar responsabilidades contratuais e o direito de realizar auditorias por meio de terceira parte.				
G04			**Gestão de ativos**				
C01			Possue inventário de todos os ativos.				
C02			Identifica os ativos quanto a propriedade e o classifica quanto à segurança.				
C03			Define níveis de proteção em relação ao valor e a importância dos ativos.				
C04			Os ativos de informação possuem um grau de confidencialidade, sendo classificados quanto à necessidade, a prioridade e o grau de proteção.				
C05			Define para o usuário o gestor da informação apresentada.				
C06			Define procedimento de manuseio das informações no formato físico e eletrônico.				
C07			Define procedimento para o descarte da informação.				
G05			**Segurança em recursos humanos**				
C01			Verifica a veracidade as informações apresentadas pelo candidato a emprego, fornecedores e terceiros.				
C02			Define os papéis e responsabilidades pela segurança da informação de colaboradores, fornecedores e terceiros.				
C03			Formaliza através de termos e condições de emprego a responsabilidade dos colaboradores, fornecedores e terceiros em relação à segurança da informação, estendendo-se por um período definido após o término do vínculo com a organização.				
C04			Realiza, antes do início das atividades, treinamento e conscientização dos colaboradores, fornecedores e terceiros em relação à segurança da informação.				
C05			Estabelece a abertura de processo disciplinar para colaboradores, fornecedores e terceiros que cometem quebras de segurança.				
C06			Define as responsabilidades para realizar o encerramento ou a mudança de um trabalho.				
C07			Define um processo formalizado para devolução de todos os ativos da organização que estejam de posse dos colaboradores, fornecedores e terceiros, após o encerramento				

			do seu contrato.				
C08			Define procedimento para retirada de todos os direitos de acesso dos colaboradores, fornecedores e terceiros, após o encerramento do seu contrato.				
G06			**Segurança física e do ambiente**				
C01			Define um perímetro de segurança para área onde estão localizadas as instalações físicas da organização.				
C02			Existe área de recepção com atendentes ou outro meio de controlar o acesso físico.				
C03			Existem barreiras físicas impedindo entrada não autorizada e contaminação ambiental como, por exemplo, causadas por incêndio ou inundação.				
C04			Existem portas corta-fogo no perímetro de segurança.				
C05			Supervisiona os visitantes e registra o horário de entrada e saída.				
C06			Informa aos visitantes os procedimentos de segurança e de emergência.				
C07			Obriga o visitante a utilizar alguma forma de identificação visível.				
C08			Avalia, na construção da área, à possibilidade de danos causados por incêndio, inundação ou outras formas de desastres naturais ou provocados.				
C09			Existe monitoramento e a gravação de imagens na área de segurança.				
C10			Define um período de armazenamento das imagens para necessidade de recuperação.				
C11			Realiza o controle da entrada e saída de material.				
C12			Dispõe os equipamentos para evitar acesso desnecessário entre áreas de trabalho.				
C13			Adota controles para diminuir riscos de ameaças tais como roubo, incêndio, fumaça, poeira etc.				
C14			Protege os equipamentos contra falta de energia e outras interrupções.				
C15			A fonte de energia está de acordo com as especificações do fabricante do equipamento.				
C16			Possue saída de emergência e iluminação de emergência.				
C17			Protege o cabeamento de energia e telecomunicações contra interceptação ou				

			danos.				
C18			Realiza manutenção periódica dos equipamentos e segue as especificações do fabricante.				
C19			Realiza o registro de entrada e saída dos equipamentos e informações da organização.				
C20			Realiza a análise das mídias de armazenamento de dados antes do descarte.				
G07			**Gerenciamento das operações e comunicações**				
C01			Possue documentação atualizada dos procedimentos operacionais que estão descridos na política de segurança da informação.				
C02			Possue documentação detalhada contendo informações suficientes para outro profissional com o mesmo conhecimento técnico execute as atividades do profissional original.				
C03			Realiza controle de todas as alterações em equipamentos, *softwares* ou procedimentos.				
C04			Mantém *logs* registrando as alterações realizadas nos *softwares*.				
C05			Realiza a segregação de tarefas, diminuindo responsabilidades, reduzindo o risco de má utilização do sistema e a oportunidade de alterações não autorizadas.				
C06			Define, controla e documenta as regras para transferência de *software* do processo de desenvolvimento para o status operacional.				
C07			Divide as atividades de desenvolvimento e homologação.				
C08			Controla a troca de informações com parceiros terceirizados, garantindo controles de segurança da informação.				
C09			Realiza o monitoramento e gerenciamento dos serviços prestados por terceiros, permitindo a realização de auditorias.				
C10			Gerencia os processos de mudança nos serviços terceirizados.				
C11			Monitora a capacidade dos sistemas, identificando atividades novas ou em andamento para garantir e melhoria da disponibilidade e eficiência dos sistemas.				
C12			Define, documenta e testa os requisitos e critérios para aceitação de novos sistemas.				

C13			Conscientiza os colaboradores, fornecedores e terceiros sobre o risco na utilização de software malicioso ou não autorizado.				
C14			Possue cópia de segurança das informações e dos *softwares*.				
C15			Possue documentação sobre os procedimentos de restauração das informações e dos *softwares*.				
C16			Armazena a cópia de segurança a uma distância segura do local principal.				
C17			Garante a proteção física e ambiental da cópia de segurança.				
C18			Realiza testes nas mídias utilizadas para o armazenamento da cópia de segurança.				
C19			Define controles para segurança dos dados nas redes e a proteção de serviços que se utilizam das redes.				
C20			Define procedimentos para gerenciar as mídias removíveis, tais como, *pendrive*.				
C21			Apaga os dados existentes nas mídias removíveis quando estes não são mais necessários.				
C22			Estabelece procedimentos para manuseio e armazenamento de informações.				
C23			Documenta os procedimentos e níveis de autorização para manuseio e armazenamento das mídias.				
C24			Possue restrições de acesso para pessoal não autorizado.				
C25			Existe procedimento e controle estabelecido para troca de informações e *softwares* internamente à organização e com quaisquer entidades externas.				
C26			Possue controles para proteção das mídias durante o transporte físico.				
C27			Existe uma política sobre uso do correio eletrônico.				
C28			Implementa o mecanismo de assinatura digital nas transações on-line.				
C29			Utiliza controles especiais, por exemplo, chaves de criptografia, para proteger itens sensíveis.				
C30			Protege a integridade das informações disponibilizadas publicamente.				
C31			Possue processo formal de autorização antes de disponibilizar publicamente as informações.				

C32			Armazena por um determinado período o registro de auditoria das atividades dos colaboradores, fornecedores e terceiros para futuras investigações.				
C33			Realiza o monitoramento do uso de recursos do sistema.				
C34			Garante a autenticidade, acesso não autorizado e falsificação dos registros de auditoria.				
C35			Armazena os registros de auditoria das atividades realizadas pelos administradores e operadores do sistema.				
C36			Registra e analisa o registro de falhas ocorridas nos sistemas.				
C37			Garante a sincronização dos relógios com uma hora oficial de todos os sistemas.				
G08			**Controle de acessos**				
C01			Define e documenta os requisitos de controle de acesso as informações.				
C02			Define regras e direitos de controle de acesso para cada usuário e/ou grupo de usuários.				
C03			Existe procedimento formal para cadastramento e descadastramento de usuários.				
C04			Armazena o registro de todos os colaboradores, fornecedores e terceiros que utilizam determinado sistema.				
C05			Remove imediatamente os direitos de acesso aos usuários que trocam de função ou deixam a organização.				
C06			Identifica os privilégios de acesso de cada sistema ou serviço.				
C07			Exige dos colaboradores, fornecedores e terceiros a assinatura em declaração que iram manter confidenciais suas senhas.				
C08			Possue outras formas de autenticação de usuários tais como biométrica, verificação de assinaturas ou cartões com *chip*.				
C09			Revisa os direitos de acesso dos usuários periodicamente e após alguma alteração.				
C10			Existe processo de conscientização para o uso de senhas seguindo as boas práticas de segurança da informação.				
C11			Orienta os colaboradores, fornecedores e terceiros dos requisitos e procedimentos de segurança para proteção dos equipamentos				

			desacompanhados.				
C12			Utiliza métodos de autenticação para permitir conexões externas.				
C13			Realiza uma avaliação de risco para determinar o nível de proteção necessária para as conexões externas.				
C14			Permite suporte técnico através de conexões remotas.				
C15			Divide a rede em domínios lógicos evitando acesso não autorizado aos sistemas.				
C16			Possue controle de roteamento assegurando uma conexão segura entre a origem e o destino.				
C17			Registra acessos bem-sucedidos e fracassados ao sistema operacional.				
C18			Restringe o tempo de conexão ao sistema operacional.				
C19			Implementa identificador único de uso pessoal e exclusivo para a autenticação nos sistemas.				
C20			Fornece mensagens de ajuda durante o processo de *logon*.				
C21			Valida as informações de *logon* somente após o término da entrada de dados.				
C22			Limita a quantidade de tentativas fracassadas de *logon*.				
C23			Administradores, programadores e operadores possuem identificador exclusivo para uso pessoal proporcionando responsabilidade individual.				
C24			Possue um sistema de gerenciamento de senhas.				
C25			Altera a senha padrão dos fornecedores logo após a instalação do *software* e outros equipamentos.				
C26			Prevê que os terminais inativos sejam desconectados após um tempo definido de inatividade.				
C27			Limita o horário de conexão as aplicações definidas de alto risco.				
C28			Controla os direitos de acesso dos usuários à informação e às funções de sistemas, restringindo leitura, gravação e exclusão da informação.				
C29			Os sistemas considerados sensíveis e de alto risco possuem um ambiente computacional isolado.				
C30			Realiza uma avaliação de risco para				

			definir o nível de monitoramento quanto ao uso do sistema.				
C31			Analisa periodicamente o resultado do monitoramento das atividades.				
C32			Possue uma política formal descrevendo os riscos do uso das facilidades da computação móvel.				
C33			Possue uma política, procedimentos ou padrões para controlar as atividades de trabalho remoto.				
G09			**Aquisição, desenvolvimento e manutenção de sistemas de informação**				
C01			Possue uma metodologia de desenvolvimento de sistemas contendo os requisitos de segurança.				
C02			Divulga a metodologia de desenvolvimento de sistemas a todos os desenvolvedores (colaboradores e terceiros)				
C03			Treina novos desenvolvedores sobre os padrões e forma de trabalho na organização.				
C04			Existe três ambientes computacionais bem definidos, sendo eles: desenvolvimento, teste e produção.				
C05			Identifica todos os requisitos de segurança na fase de requisitos de um projeto e os mesmos são justificados, acordados e documentados para um sistema de informação.				
C06			Define controles para validação dos dados de entrada.				
C07			Valida os dados gerados pelo sistema, podendo identificar possível corrupção de informações, erros ou ações maliciosas.				
C08			Define controles para validação dos dados de saída.				
C09			Existe uma política para uso de controles criptográficos para a proteção da informação.				
C10			Existe um processo para controlar a instalação de *software* em sistemas operacionais.				
C11			Utiliza dados criados especialmente para testes na realização de testes de sistema.				
C12			Mantém um controle sobre o acesso ao código-fonte de *softwares*.				
C13			Existe controle para implementação de alterações.				

C14			Documenta e testa as alterações permitindo serem reaplicadas quando necessário.				
C15			Realiza uma análise para verificar a continuidade do fornecedor frente ao mercado de tecnologia				
C16			Existe controle para prevenir o vazamento de informações.				
C17			Monitora e supervisiona o desenvolvimento terceirizado de *software*.				
C18			Existe gestão de vulnerabilidades técnicas dos sistemas de informação.				
G10			**Gestão de incidentes de segurança da informação e melhorias**				
C01			Existe um procedimento estruturado para o tratamento de incidentes de segurança da informação.				
C02			Estabelece a segregação de responsabilidade na gestão de incidentes de segurança da informação.				
C03			Existe procedimento para gestão dos diferentes tipos de incidentes de segurança da informação.				
C04			Existe uma integração da gestão de incidentes de segurança da informação com um processo de gestão de incidentes da organização.				
C05			Planeja e implementa ação corretiva para prevenir a reincidência de um incidente de segurança da informação.				
C06			Documenta em detalhes todas as ações de emergência para recuperação de correção de falhas do sistema.				
C07			Possue um canal de comunicação possibilitando ao colaborador, fornecedor ou terceiro registrar a ocorrência de um incidente.				
C08			O canal de comunicação auxilia na análise de incidente de segurança da informação indicando necessidade de melhoria ou controles adicionais.				
C09			Existe procedimento para coleta de evidências, armazenamento e apresentação em conformidade com as normas aplicáveis.				
G11			**Gerenciamento da continuidade**				

			do negócio				
C01			Existe um plano de continuidade de negócios que deve ser aplicado na ocorrência de um desastre que indisponibilize recursos computacionais.				
C02			Contempla no plano de continuidade de negócios os requisitos de segurança da informação.				
C03			Identifica todos os ativos envolvidos em processos críticos do negócio.				
C04			Identifica os eventos que podem causar interrupção nos processos de negócio.				
C05			Identifica os eventos levando em conta a probabilidade e o impacto de tais interrupções e as conseqüências para a segurança da informação.				
C06			Realiza periodicamente uma avaliação de risco focando as ameaças que podem indisponibilizar recursos de informação.				
C07			Existe uma estratégia para suportar uma situação de contingência que atenda os requisitos de recuperação do negócio.				
C08			Implementa uma estratégia validada pela direção da organização.				
C09			Existe conscientização e treinamento adequado para as pessoas nos procedimentos e processos do plano de continuidade de negócios.				
C10			Possue um roteiro atualizado definindo os procedimento a serem tomados quando da ocorrência de uma situação de contingência.				
C11			Possue processo formal garantindo a atualização do plano de continuidade de negócios.				
C12			Realiza testes periódicos para a utilização correta do plano de continuidade de negócios.				
G12			**Conformidade**				
C01			Tem conhecimento do conjunto de legislação, regulamentos, estatutos e obrigações contratuais que a organização deve cumprir.				
C02			Existe conscientização de que todos os usuários devem conhecer os requisitos para tratar a informação no desenvolvimento de sistemas.				
C03			Existe a interação do departamento jurídico com o departamento de tecnologia da informação para garantir a conformidade da				

			organização com a legislação e outros regulamentos.				
C04			Existe um processo que garanta a atualização constante da organização quanto à legislação e demais regulamentos.				
C05			Garante a proteção dos dados e a privacidade de informações pessoas conforme exigido na legislação e demais regulamentos.				
C06			Guarda as cópias de segurança num local com o mesmo nível de segurança do local original.				
C07			Transporta fisicamente as cópias de segurança em embalagens específicas.				
C08			Monitora seguindo a legislação e demais regulamentos o mau uso dos recursos computacionais.				
C09			Utiliza controles de criptografia em conformidade com as leis e demais regulamentos.				
C10			Garante a conformidade dos procedimentos de segurança da informação de acordo com as normas e políticas de segurança da informação.				
C11			Existe um processo que defina os procedimentos de auditoria e de desempenho computacional.				
C12			Realiza as auditorias com pessoas que sejam independentes das atividades auditadas.				

5 CONCLUSÃO

Atualmente, a proteção dos ativos de informação tornou-se de vital importância para o gerenciamento do negócio, mas a tecnologia ao mesmo tempo que agiliza os processos também torna a informação mais vulnerável, necessitando com isso de maior segurança para que está não cair em mãos erradas.

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

É importante salientar que a segurança da informação não deve ser tratada somente como um processo de tecnologia. Todos os departamentos da organização devem estar comprometidos com a proteção da informação, pois a impossibilidade de realizar adequadamente suas operações vão resultar em prejuízos financeiros, operacionais e de imagem.

Espero que este trabalho seja mais uma fonte referencial no estudo de gerenciamento de riscos e plano de continuidade de negócios. Lembrando que, a implementação e a manutenção dos processos de gerenciamento de risco e construção do plano de continuidade de negócios devem ser sempre claros e ter o apoio de todos os envolvidos no processo, principalmente a direção da organização. Com trabalho futuro sugiro o aperfeiçoamento do *checklist*, com inclusão, exclusão e aperfeiçoamento dos controles, conforme a característica da organização.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC GUIA 73**: Gestão de riscos - Vocabulário – Recomendações para uso em normas. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2006**: Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Requisitos. Rio de Janeiro, 2006.

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, 2007.

BRANDÃO, J. E. M. S.; FRAGA, J. S., Gestão de Riscos. In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, SBSeg, 8., 2008, Gramado. **Anais...** Porto Alegre: SBC, 2008. p. 1-43.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação / Tribunal de Contas da União.** 2. ed. Brasília: TCU, Secretária de Fiscalização de Tecnologia da Informação, 2007.

BRITISH STANDARDS INSTITUTE. **BS 25999-1**: Code of Practice for Business Continuity Management. London, 2006

CARVALHO, L. G. **Segurança de Redes**. São Paulo: Ciência Moderna, 2005.

CERT.br. **Cartilha de Segurança para Internet.** Versão 3.1. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

FAGUNDES, E. M. **COBIT**: um kit de ferramentas para a excelência de TI**.** São Paulo, 2004. Disponível em: <http://www.efagundes.com/artigos/COBIT.htm>. Acesso em: out. 2008.

FONTES, E. L. G. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FONTES, E. L. G. **Segurança da Informação - O usuário faz a diferença!** São Paulo: Saraiva, 2006.

ICP Brasil. **Glossário ICP-BRASIL - Versão 1.1**. Brasília, 2006. Disponível em: <https://www.icpbrasil.gov.br/duvidas/glossary>. Acesso em: out 2008.

IMONIANA, J. O. **Auditoria de Sistemas de Informação**. 2. ed. São Paulo: Atlas, 2008.

IT GOVERNANCE INSTITUTE. **CobIT 4.1**. Illinois, 2007.

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

MAGALHÃES, I. L.;PINHEIRO W. B. **Gerenciamento de Serviços de TI na prática:** Uma abordagem com base no ITIL. Porto Alegre: Novatec, 2007.

MANSUR, R. **Governança de TI**. São Paulo: Brasport, 2007.

MÓDULO. **Lançamento da Norma ISO/IEC 27005:2008.** São Paulo, 2008. Disponível em: <http://www.modulo.com.br/site?infoid=2506&lng=br&sid=78> Acesso em: out. 2008.

SÊMOLA, M. As principais ameaças à segurança em 2008. **IDG NOW! Tecnologia em primeiro lugar**. São Paulo, 2008. Disponível em: <http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2007-12-20.0767720515/>. Acesso em: ago. 2008.

SILVA, L. S. **Virtual Private Network**. 2. ed. São Paulo: Novatec, 2005.

STALLINGS, W. **Criptografia e Segurança de Redes:** Princípios e Práticas. 4. ed. São Paulo: Prentice-Hall, 2008.

TAMBORIM, A. L. **Segurança extrema com LIDS**. Disponível em: <http://www.vivaolinux.com.br/artigo/Seguraca-extrema-com-LIDS/>. Acesso em: out. 2008.

TANEMBAUM, A. S. **Redes de Computadores**. 4. ed. São Paulo: Campus, 2003.

TANEMBAUM, A. S. **Sistemas Operacionais Modernos**. 2. ed. São Paulo: Prentice-Hall, 2003.

TREVENZOLI, A. C. **Perícia forense computacional – ataques, identificação da autoria, leis e medidas preventivas das ameaças sobre o ambiente operacional.** Sorocaba, 2006.

WEBER, R. Slides de Aula. Disciplina de Segurança em Serviços e Aplicações. Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores. 2008. Instituto de Informática, UFRGS, Porto Alegre.