FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO

ALCINDO FACIOLI

PLANO DE CONTINUIDADE DE NEGÓCIOS APLICADO À EMPRESAS DE PEQUENO PORTE

Americana, SP
2016

FACULDADE DE TECNOLOGIA DE AMERICANA
SEGURANÇA DA INFORMAÇÃO

ALCINDO FACIOLI

PLANO DE CONTINUIDADE DE NEGÓCIOS APLICADO À EMPRESAS DE PEQUENO PORTE

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior em Segurança da Informação, sob a orientação do Prof. MSc Alberto Martins Junior.
Área de concentração: Segurança da Informação.

Americana, S. P.
2016

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

F123p FACIOLI, Alcindo

Plano de continuidade de negócios aplicado à empresas de pequeno porte. / Alcindo Facioli. – Americana: 2016.

51f.

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Ms. Alberto Martins Junior

1. Segurança em sistemas de informação I. MARTINS JUNIOR, Alberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU 681.518.5:

ALCINDO FACIOLI

PLANO DE CONTINUIDADE DE NEGÓCIOS APLICADO Á EMPRESAS DE PEQUENO PORTE

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

Área de concentração: Segurança da Informação.

Americana, 06 de dezembro de 2016.

Banca Examinadora:

Alberto Martins Junior
Mestre
Faculdade de Tecnologia de Americana - FATEC/Americana

Eduardo Antonio Vicentini
Mestre
Faculdade de Tecnologia de Americana - FATEC/Americana

Kleber de Oliveira Andrade
Mestre

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus por ter me dado saúde e paciência nos momentos difíceis.

Gostaria de agradecer aos meus professores pelo empenho, dedicação e paciência com que conduziram os trabalhos.

Ao meu amigo João Flavio Diniz, que me ajudou de forma incondicional em todos os momentos, principalmente nas horas de desânimo em que fomos expostos.

Ao meu professor e orientador MSc Alberto Martins Junior, que de forma extremamente eficiente e competente me auxiliou na elaboração deste trabalho.

DEDICATÓRIA

A minha família (esposa e filha) pelo apoio dado durante esta longa jornada, sendo paciente nos momentos em que estive ausente, me encorajando de forma incondicional nas horas de maior dificuldade.

RESUMO

Independente do ramo da organização, é de fundamental importância que as informações sejam protegidas, e garantir que, no caso de um desastre esses ativos possam ser recuperados, uma vez que as informações passaram a ser ativos de maior valor de uma empresa. Este trabalho mostra de forma simples, a importância de uma empresa em desenvolver um plano de continuidade de negócios, visando a recuperação das informações relevantes à missão do negócio, no menor tempo possível. O plano de continuidade de negócios, traça diretrizes capazes de orientar os administradores de como agir nos momentos de parada do sistema e consequentemente a perda das informações.

Palavras Chave: Plano de Continuidade de Negócios; Segurança da Informação; Recuperação de Desastres Aplicados a Ti.

ABSTRACT

Regardless of the organization branch, it is of fundamental importance that your information is protected and ensure that in the event of a disaster such assets can be recovered, since the information started to be active higher value of a company. This work aims to show in a simplified manner, the importance of an organization to draw a business continuity plan applied to the area of T.I., seeking the recovery of relevant information business continuity in the shortest time possible. The business continuity plan sets out guidelines able to guide administrators of the system to act in the system stop times and consequently the loss of information.

***Keywords*:** Business Continuity Plan; Information security; IT Disaster recovery.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O número de informações e a velocidade com que elas trafegam nas redes de computadores aumentam exponencialmente, estas por sua vez, passaram a ser ativos de alto valor agregado ao negócio e sua proteção de extrema importância para a sobrevivência de uma organização.

Conforme definição de Padoveze (2000), “informação é o dado que foi processado e armazenado de tal forma que seja compreensível, acessível e que tenha valor (real ou percebido) para seu receptor. A informação é um produto dos dados organizados para análise e suporte à tomada de decisão”.

Na mesma linha, Oliveira (1998) indica que “a informação é o produto dos dados, devidamente registrados, classificados, organizados e interpretados”. Este contexto abarca não só a qualidade da informação, mas também os aspectos relativos à integridade, confiabilidade e veracidade da mesma.

A informação apenas se mostra importante quando ela gera conhecimento e ajuda na tomada de decisões, assim ela passa a agregar valor e a ser reconhecida como um ativo segundo especifica a NBR ISO/IEC 27002:2005 (ABNT, 2005):

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é essencialmente importante no ambiente dos negócios, cada vez mais interconectado.

A empresa deve estar preparada para situações em que as informações possam apresentar riscos de perdas, ocasionadas por roubos cibernéticos, paralisações dos serviços por quebra ou falha de equipamentos, desastres naturais como enchentes, tornados, etc.

Diante de inúmeros fatores de risco na qual esses ativos estão expostos, as organizações passaram a ter uma atenção especial no manuseio e armazenamento destes, mediante a todos os cuidados que possam ser tomados, tais informações não apresentam uma garantia total de sua preservação.

Traçar diretrizes, capaz de orientar os administradores de como agir e como recuperar as informações em casos de incidentes, passou a ser de extrema importância, pois garante a recuperação desses ativos em menor tempo possível,

diminuindo perdas de credibilidade envolvendo a organização e consequentemente diminuindo as perdas financeiras, foco de toda empresa.

A imensa quantidade de informações que circulam a todo o momento e a uma velocidade cada vez maior, surge a necessidade de que estas sejam controladas e armazenadas de forma segura, garantido sua confiabilidade, integridade e disponibilidade quando requisitada.

Com o decorrer do desenvolvimento da área de informática, toda a informação de uma organização passou a se tornar disponível com maior facilidade, as informações de uma organização passaram a ser o seu bem mais precioso.

Junto com o desenvolvimento e facilidade de se obter informações, surge também um grande número de ameaças capazes de interromper ou dificultar o andamento de um negócio, esses riscos passam a ser uma constante preocupação de uma organização, uma vez que, o vazamento ou a perda dessas informações pode ocasionar prejuízos imensuráveis e até mesmo a interrupção do andamento do negócio.

A segurança da informação passa a ser uma peça chave no desenvolvimento de uma empresa, e as informações um bem precioso que deve ser protegido a todo custo. Garantir que elas estejam armazenadas em local apropriado e que possam ser recuperadas quando na ocasião de algum desastre ou ataque é o objetivo de um **plano de continuidade de negócios.**

Este trabalho tem por objetivo geral o de mostrar a importância da implementação de um plano de continuidade de negócios bem como o de apresentar um documento formal às empresas aqui referenciadas, definindo diretrizes capazes de garantir a continuidade de seus negócios em caso de acidentes envolvendo suas informações.

Para atingir o objetivo geral deste trabalho, foram desenvolvidos alguns objetivos específicos:

- Analisar o conhecimento dos administradores de empresas de pequeno porte quanto a segurança das informações.
- Identificar as diretrizes de um plano de continuidade de negócios, analisando as normas regulamentadoras.
- Definir política de segurança e as fases necessárias para sua implantação.

- Definir plano de continuidade de negócios e as fases para sua implantação.
- Propor um plano de continuidade de negócios, que possibilite às empresas de pequeno porte a recuperação de suas informações quando na presença de um desastre, através da implantação de políticas de Backups e Restore, sistemas alternativos de energia elétrica, sistemas alternativos de Links de Internet, serviços redundantes de servidores e o treinamento da equipe de recuperação de desastre.

Para a confecção deste trabalho, foi utilizado a metodologia da pesquisa em livros, teses de doutorado e normas da ABNT, ITIL, COBIT, ISO 17799, ISO 27001, ISO 27002.

Segundo o SEBRAE (Serviço Brasileiro de Apoio às Micro e Pequenas Empresas) uma empresa de pequeno porte é um empreendimento com faturamento bruto anual entre R$ 360 mil e R$ 3,6 milhões.

Para justificar os estudos apresentado, foi desenvolvido uma pesquisa entre pequenas empresas de vários seguimentos, aplicando um questionário contendo dez questões envolvendo a garantia da informação e a recuperação destas em casos de desastres.

O resultado deste questionário deixa claro a falta de conhecimentos e o despreparo por grande parte das organizações quando na ocorrência de acidentes que ocasionam a parada dos negócios.

Através dos resultados obtidos foi possível verificar a ineficiência das empresas pesquisadas, os riscos envolvidos e o número de empresas que se preocupam com um plano de continuidade de negócios, apesar de algumas organizações se preocuparem com a segurança das informações, muitas não sabem ao certo como proceder em situações de emergência.

Este trabalho foi estruturado da seguinte forma, o capítulo 2 é apresentado uma definição de Tecnologia da Informação mostrando sua importância para as organizações. O capitulo 3 é feito uma definição da Segurança da Informação juntamente com os pilares da segurança. O capitulo 4 é definido um plano de continuidade de negócios mostrando as fases para sua implantação. O capitulo 5 define as normas regulamentadoras utilizadas no traballho, mostrando o histórico de cada norma. O capitulo 6 apresenta um estudo de caso e apresenta uma proposta de

um plano de continuidade de negócios e finalmente no capitulo 7 são feitas as considerações finais.

2 TECNOLOGIA DA INFORMAÇÃO

Estamos vivendo a era da informação, o ativo principal de uma organização passa a ser os dados que caracterizam vantagens competitivas e retorno financeiro, através da inovação tecnológica é possível manter os recursos da organização em dados e a transformação destes em informações relevantes, segundo Albertin (2001) “A era do computador predominou até o final da década de 70 e a era da informação começou a partir dos primeiros anos da década de 80, sendo que no Brasil muitas empresas estão ainda passando por essa transformação”.

Em um mundo globalizado economicamente falando, é necessário que as organizações invistam constantemente em Tecnologia da Informação (TI), permitindo assim uma melhoria na qualidade dos seus serviços de forma a garantir vantagens estratégicas e competitivas, garantindo o aumento da competitividade e do lucro, Albertin (2001) afirma que a “TI é vista como uma das maiores e mais poderosas influências no planejamento das organizações”.

O termo Tecnologia da Informação ainda assusta algumas pessoas, uma vez que, ainda não estão familiarizados e, portanto, não utilizam com plenitude tais recursos em suas empresas. É importante frisar que a Tecnologia da Informação não é mais reconhecida apenas como um suporte da administração e passou a ser uma estratégia usada pela área administrativa.

> O desconhecimento elementar da Tecnologia da Informação e de seus recursos tem causado muitos problemas e dificuldades dentro das empresas, principalmente para as atividades ligadas a Planejamento Estratégico, Sistemas de Informação e Gestão de Tecnologia da Informação (REZENDE; ABREU, 2001).

Atualmente, toda a sociedade está passando por uma transformação ainda em fase de reconhecimento de suas características principais e, as organizações passando por turbulentas mudanças, enfrentando um mercado cada vez mais competitivo e globalizado, necessitando assim de informações e conhecimentos personalizados de forma a auxiliar a gestão de forma inteligente. Nesse contexto, a Tecnologia da Informação passou a estar mais próxima do cotidiano das organizações e das pessoas que nelas trabalham, segundo Castells (1999) a

tecnologia é “o uso de conhecimentos científicos para especificar as vias de se fazer as coisas de uma maneira reproduzível”

Ainda segundo Castells (1999):

> A tecnologia não determina a sociedade, nem a sociedade escreve o curso da transformação tecnológica, uma vez que muitos fatores, inclusive criatividade e iniciativa empreendedora, intervém no processo de descoberta científica, inovação tecnológica e aplicações sociais, de forma que o resultado final depende de um complexo padrão interativo.

Castells (1999) define a T.I “como sendo um conjunto de dispositivos individuais, como hardware, software, telecomunicações ou qualquer outra tecnologia que, faça parte ou gere tratamento da informação ou, ainda, que a contenha”.

A administração da Tecnologia da Informação apresenta diversos desafios e, para acompanhar a situação da nova realidade é necessário atentar-se a alguns quesitos como; a evolução crescente da tecnologia, tornando obsoleto produtos e serviços; a busca de soluções prontas oferecidos por terceiros, necessitando alterações e adaptações internas; alteração do perfil das pessoas envolvidas com a tecnologia, incluindo usuários; alterações das características dos produtos relacionados a TI como; complexidade, tipos, retorno esperado etc.

A TI é sem dúvida a força de transformação da economia e da sociedade em geral, ela vem mudando de forma radical e rápida o mundo, fronteiras já não são instransponíveis e o mundo está inundado em informações, conhecimento, ideias, notícias, modismos, críticas, contestações ou apelos de qualquer natureza.

Segundo o próprio Castells (1999) “A tecnologia da informação tornou-se ferramenta indispensável na implantação efetiva dos processos de reestruturação socioeconômica. ”

Ressalta Castells (1999):

> As novas tecnologias da informação desempenham papel decisivo ao facilitarem a flexibilidade, proporcionando ferramentas para a formação de redes, comunicação a distância, armazenamento/processamento de informação no processo decisório.

O grande desafio que as organizações enfrentam na exploração de todo o potencial da TI é sem dúvida a necessidade de um alinhamento entre as estratégias de negócio da empresa e a TI, portanto esta deve ascender ao nível dos demais

recursos, que constituem o conjunto de variáveis a ser analisado no processo de desenvolvimento da estratégia corporativa.

Segundo Rezende (2002):

> O alinhamento entre as estratégias de negócio e a TI vem sendo fortemente discutido nestas últimas duas décadas no mundo acadêmico e empresarial. Apesar de a literatura apresentar diversos modelos de alinhamento estratégico de negócios com a TI, na prática empresarial não são relatados e claramente ás organizações os recursos sustentadores desse alinhamento.

A Tecnologia da informação traz sem nenhuma dúvida, inúmeros benefícios para as organizações garantindo vantagens competitivas. A TI é vista como uma estratégia para as organizações colaborando com as decisões e ações de seus gestores de forma dinâmica e flexível.

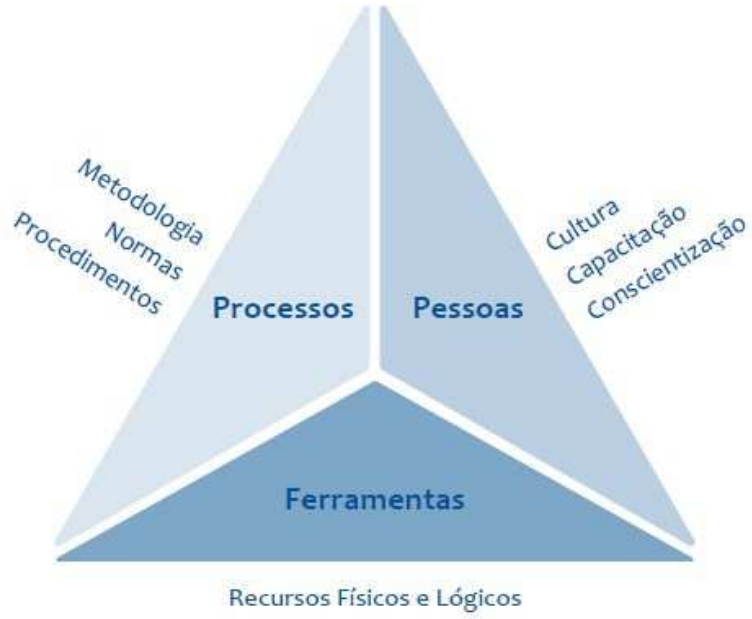
3 SEGURANÇA DA INFORMAÇÃO

Segundo a ABNT NBR ISO/IEC 17799:2005 (ABNT, 2005), “a informação é um ativo de uma organização e como todo ativo é de extrema importância para o negócio, portanto deve ser protegido de forma adequada, garantindo sua recuperação em situações de incidentes”.

Segundo Cerutti (2012) “o programa de segurança da informação deve iniciar pelas pessoas, pois segurança não envolve apenas tecnologia”.

Pode-se observar na Figura 1, um diagrama que mostra o inter-relacionamento entre os componentes envolvidos nos planejamentos relacionados com segurança da informação.

Figura 1: Diagrama de inter-relacionamento entre componentes da segurança da informação.



Fonte: Cerutti (2012)

Conforme observa-se na Figura 1, Cerutti (2012) afirma que o inter-relacionamento ocorre entre pessoas, processos e ferramentas, assim definidas por ele:

Pessoas: São os elementos mais importantes na gestão da segurança, pois são elas que executam e dão suporte aos processos de uma organização. Deve-se

tratar com as pessoas os assuntos relacionados a esta área e estabelecer seus papéis e responsabilidades na organização.

Processos: São os elementos que se bem definidos, tornam a segurança da informação uma responsabilidade de todos e não apenas da equipe de segurança. Essa gestão determina, por meio de diretrizes, as maneiras corretas de se agir nos processos da organização para que a segurança seja a mínima afetada.

Ferramentas: São os recursos físicos e lógicos da segurança, utilizados para dar suporte aos processos na organização. Tem como objetivo facilitar a aplicação das políticas de segurança da informação. Agregam várias funcionalidades, começando pela identificação dos usuários, defesa contra ameaças, criptografia dos dados e gestão da segurança.

Observa-se que independentemente da forma como a informação é armazenada ou transmitida (impressa, escrita em papel, armazenada por meio eletrônico, transmitida por correio, apresentada em filmes, etc.) a segurança desses ativos é fundamental. A garantia da proteção da informação às diversas ameaças, são executadas através da segurança da informação, que trata de garantir a continuidade do negócio, minimizar os riscos envolvidos, aumentar o retorno sobre os investimentos e aumentar as oportunidades relativas ao negócio.

A segurança dos dados depende tanto de *software* como de *hardware* e somente será possível através da implementação de um conjunto de controles que inclui políticas, processos, procedimentos e uma estrutura organizacional. Esse processo é um ciclo continuo e deve ser adequado e melhorado a cada fase.

Estabelecer, implementar, monitorar, analisar e melhorar são as etapas que devem ser seguidas para que a segurança seja alcançada, novas ameaças surgem a todo momento por isso a preocupação com o monitoramento constante.

Assegurar a informação é garantir a competitividade, o vazamento de informações pode ser o diferencial para que o concorrente saia na frente, além do que, a segurança dos dados permite à organização sua lucratividade, o atendimento aos requisitos legais e uma boa imagem da empresa frente ao mercado.

A segurança da informação é limitada tecnicamente, portanto deve ser apoiada por uma gestão e procedimentos corretos, e deve contar com o apoio de todos os funcionários de uma organização, seus acionistas, fornecedores, clientes e outras partes externas envolvidas no processo.

O intuito da Segurança da Informação não se restringe apenas em manter a disponibilidade da informação, mas também suas características essenciais: integridade, disponibilidade e confidencialidade. Segundo a NBR ISO/IEC 27002:2005 (ABNT, 2005)

> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio.

3.1 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

Segundo a ABNT NBR ISO/IEC 17799:2005 (ABNT, 2005) é necessário que a organização identifique corretamente os seus requisitos de segurança da informação, para isso são necessários três tipos de fontes principais para o levantamento desses requisitos.

3.1.1 Análise e avaliação de riscos para a organização

Através de uma análise e de uma avaliação de riscos, são identificadas as ameaças aos ativos da organização e consequentemente as vulnerabilidades, em cima dos dados obtidos é realizado uma estimativa da probabilidade de ocorrência dessas ameaças e qual será o impacto ao negócio da organização.

3.1.2 Legislação

Outra fonte de extrema importância está relacionada a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

3.1.3 Princípios e objetivos

A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

3.2 PILARES DA SEGURANÇA DA INFORMAÇÃO

Podem ser estabelecidos meios para a definição do nível de segurança existente e, com isto, serem estabelecidos padrões para análise e consequentemente traçar métodos para a melhoria da segurança existente.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A segurança da informação é baseada em três pilares fundamentais, que de forma geral garantem o processo, sem a presença desses pilares uma organização apresenta uma maior dificuldade em crescer, lucrar e manter-se no mercado, os três pilares são conhecidos como “CID”, Confidencialidade, Integridade e Disponibilidade.

3.2.1 Disponibilidade

É a garantia de que a informação possa ser obtida sempre que necessário, a informação deve estar disponível no momento de sua requisição.

A disponibilidade da informação também está ligada a parte operacional de uma organização, mas de maneira bem mais direta que a integridade. No mundo em que vivemos praticamente todos os processos de trabalho de uma empresa dependem da informação em tempo real. Segundo Sêmola (2003) a disponibilidade é definida da seguinte forma, “Toda informação deve estar disponível aos seus usuários no momento em que os mesmos dela necessitem para qualquer finalidade”.

Quando a informação fica indisponível, os processos que dela dependem simplesmente ficam paralisados. Caso haja a indisponibilidade de um conjunto grande de informações, ou informação extremamente crítica, a empresa pode parar e o lucro ser reduzido ou mesmo ser levado a níveis através da qual a empresa passa a ter prejuízos.

Vivendo em uma sociedade do conhecimento, cujo as informações passam a ser ativo valioso, sem a disponibilidade a empresa perde a capacidade de operar.

3.2.2 Integridade

É a garantia de que a informação armazenada ou transferida está correta e é apresentada ao seu proprietário de maneira integra. Segundo Sêmola (2003) a integridade é definida da seguinte forma, “O objetivo de se manter a informação da forma que seu autor a criou, protegendo de qualquer alteração por pessoas não autorizadas, seja a alteração intencional ou acidental. ”

Existem basicamente dois pontos durante o processo de transmissão no qual a integridade pode ser comprometida, durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados.

A integridade é absolutamente crítica do ponto de vista operacional, pois valida todo o processo de comunicação em uma empresa ou comunidade.

As comunicações tanto internas como externas, transmitem inúmeros resultados, projeções, estratégias, regras, procedimentos e dados que apenas são efetivas quando o emissor e o receptor podem contar com as mesmas informações.

O grande número de informações geradas nos dias atuais já é uma tarefa extremamente complexa de se fazer o entendimento das mesmas, torna-se ainda mais difícil, lenta e trabalhosa quando as informações sofrem algum tipo de alteração ou são corrompidas no meio do caminho entre o emissor e o receptor.

Essas divergências de informações podem provocar o desperdício de energia, empregadas nas correções e retrabalho durante o processo de verificações, a falta de integridade gera ineficiência e isto se traduz em custos e consequentemente perda de competitividade.

3.2.3 Confidencialidade

É garantia de que a informação não será conhecida por pessoas que não estejam autorizadas ao acesso de tais informações.

O conceito de confidencialidade é um dos pilares mais interessantes, pois está relacionado à curiosidade humana, o que aguça e incentiva diversas invasões. Quando a confidencialidade é quebrada, todo o capital intelectual da empresa é

exposto e em contrapartida a empresa perde as vantagens competitivas, pois todos os esforços e investimentos em novas tecnologias e pesquisas passam a estar disponível aos concorrentes, e com um agravante, o detentor dessas informações passam a ter o bônus dessas descobertas, sem os ônus dos investimentos que foram aplicados em pesquisas de quem as construiu.

Segundo Sêmola (2003), “Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas”.

Quando o vazamento acontece, ocorre uma corrida de forma injusta, através da qual, a empresa que investiu nos conhecimentos dá aos concorrentes aquilo que demandou tempo e dinheiro, assim sendo, é melhor e sai mais barato investir para preservar a confidencialidade das informações.

A confidencialidade é hoje alvo de uma engenharia social, capaz de obter informações importantíssimas das pessoas que as detêm, e que através de estratégias meticulosamente calculadas, conseguem ludibriar os usuários que acabam repassando essas informações aos chamados engenheiros sociais.

3.3 POLÍTICA DE SEGURANÇA

Segundo Ferreira e Araújo (2008), a Política de Segurança “é um conjunto de regras e padrões, de forma a assegurar que a informação e os serviços importantes para a empresa recebam a proteção adequada, garantindo a Confidencialidade, Integridade e Disponibilidade”.

Sendo um conjunto de normas, métodos e procedimentos utilizados assegurando a manutenção da segurança da informação, a política deve ser formalizada e divulgada a todos os usuários que de alguma forma utilizam os ativos da informação. A política de segurança deve atender as expectativas e desejos dos proprietários e ou acionistas da organização, que são os maiores responsáveis pela informação.

Para que uma política de segurança tenha sua eficácia garantida, alguns fatores devem ser considerados:

- ✓ A informação é um ativo importante, (se não o mais importante) de uma organização;

- ✓ A alta administração deve estar totalmente envolvida com relação a segurança da informação;
- ✓ Todos os colaboradores devem assumir formalmente a responsabilidade sobre a salvaguarda dos recursos da informação;
- ✓ Estabelecer padrões para a manutenção da segurança da informação.

A política de segurança é sem dúvida a base de sustentação de uma gestão envolvendo a segurança, ela deve ser elaborada antes do problema ocorrer e modificada após a ocorrência de um problema, evitando sua reincidência.

No momento da elaboração de uma política de segurança, o levantamento daquilo que deverá ser protegido deve ir além dos mecanismos físicos *(hardware*) e lógicos (*softwares*), ela deverá abranger também as pessoas e os processos de negócio. É interessante a formação de um comitê, contendo vários profissionais de várias áreas distintas como; informática, engenharia, recursos humanos, etc., estejam diretamente envolvidos no processo de segurança dos ativos da informação.

A política de segurança da informação, por ser um conjunto de normas e procedimentos visando a segurança, estas devem ser:

- ✓ Simples;
- ✓ Compreensíveis (escrita de forma clara, garantindo sua interpretação e compreensão);
- ✓ Homologadas e assinadas pela alta Administração (A direção da empresa deve conhecer e estar envolvida no processo);
- ✓ Estruturada de forma a permitir que a sua implementação seja executada por fases;
- ✓ Deve estar alinhada com as estratégias de negócio da empresa (a política deve ser elaborada de forma a atender aos propósitos do negócio);
- ✓ Flexíveis (moldadas e alteradas conforme as necessidades atuais);
- ✓ Priorizar os ativos da informação (verificar o que é mais importante).

3.3.1 Etapas para a implantação de uma política de segurança

O processo de desenvolvimento e implantação de uma política de segurança passa por quatro fases, sendo elas: O levantamento das informações; Desenvolvimento do Conteúdo da Política e Normas; Elaboração dos Procedimentos de Segurança; Revisão, aprovação e no fim a implementação da política.

3.3.2 Levantamento das Informações

Nesta fase são levantados as normas e procedimentos de segurança já existentes, entendimento das necessidades e o uso dos recursos da tecnologia da informação, obtenção das informações envolvendo o ambiente de negócio e a obtenção de informações sobre o ambiente tecnológico.

3.3.3 Desenvolvimento do conteúdo da Política e Normas

Nesta etapa, após os levantamentos executados na fase anterior, são elaboradas as políticas e normas, atribuindo regras e responsabilidades a todos os envolvidos no processo, é durante a elaboração da política que as mesmas são classificadas segundo seu nível de importância, e finalmente são fixados os procedimentos de segurança da informação como*: Backups*, utilização dos recursos de TI, segurança física, etc.

3.3.4 Elaboração dos procedimentos de Segurança da Informação

Etapa na qual são elaboradas pesquisas sobre as melhores práticas em segurança, e que são atualmente utilizadas no mercado, o desenvolvimento de procedimentos e padrões para que possa ser discutido com a alta direção da organização, e finalmente, a formalização dos procedimentos para integrá-los ás políticas corporativas.

3.3.5 Revisão, Aprovação e Implantação das Políticas, Normas e Procedimentos de Segurança da Informação

Nessa fase é executada a revisão das políticas e normas a serem implantadas, após o crivo de todos os envolvidos a política é aceita e aprovada para a sua posterior implementação. É executado um plano de divulgação das políticas a todos os colaboradores da organização, bem como todo o material de apoio.

3.3.6 Treinamento e divulgação da política de segurança

A política de segurança define regras estruturais (como o código de ética) e controles básicos para o acesso e uso da informação, desse modo a cultura da empresa em relação a segurança da informação deve ser mudada, para isso os funcionários devem estar preparados e o caminho é o treinamento.

A divulgação de uma política de segurança de forma a ser incorporada na cultura dos colaboradores passa por várias etapas: avisos, palestras de conscientização e sensibilização, material para consulta rápida e treinamento direcionado. Uma organização somente terá sucesso na implantação de uma política de segurança através da conscientização e da sensibilização de todos os envolvidos.

4 PLANO DE CONTINUIDADE DE NEGÓCIOS

O **plano de continuidade de negócio** (PCN) tem por objetivo garantir o funcionamento de uma organização a níveis aceitáveis, quando houver a indisponibilidade dos recursos da informação, a impossibilidade ou a demora na recuperação das informações traz sérios danos à instituição, que vão desde prejuízos financeiros, paradas operacionais e o rebaixamento da imagem da empresa.

O PCN apresenta ações para a continuidade das operações de uma organização quando na presença de um desastre. Durante o projeto de desenvolvimento de um PCN, são identificadas as ameaças e os impactos destas para a organização, como sua própria reputação, marca e atividades de criação de valor Smith (2008) *apud* Ludescher (2011).

O plano deve ser desenvolvido e implementado levando em consideração a análise do impacto no negócio, especificando os riscos e as ameaças. Todos os envolvidos direta ou indiretamente no plano de continuidade de negócios, devem estar cientes e conhecer todas as fases do desenvolvimento desse plano.

O treinamento e principalmente a conscientização de todos os colaboradores é fundamental para que o plano de continuidade de negócio tenha sucesso.

Alguns fatores devem ser levados em consideração quando na elaboração de um plano de continuidade de negócios, estes devem ser tratados para que o mesmo possa ter sua eficiência garantida, esses fatores são: Riscos, Incidentes, Problemas e Plano de Recuperação de Desastre.

Riscos: É definido como sendo o conjunto de probabilidades de um determinado evento ocorrer, esses riscos têm sua potencialidade elevada quando na presença de ameaças e vulnerabilidades.

Incidentes: É definido como sendo um evento que não faz parte do cotidiano, ocasionando a interrupção ou a perda da qualidade de um serviço.

Problemas: É definido como sendo o resultado desconhecido provocado por um incidente.

Desastre: Pode ser definido genericamente como sendo um evento que causa sofrimentos e prejuízos, sejam de ordem física, moral, material ou emocional Houaiss, (2008) *apud* Ludescher (2011).

Pode-se, portanto, relacionar desastre a um acontecimento catastrófico como por exemplo; um terremoto ou a simples falha de um disco rígido de um computador, que contém dados essenciais para o funcionamento da organização.

Plano de Recuperação de Desastre: Trata-se de um conjunto de ações que são necessárias para efetuar a recuperação de uma organização no caso da ocorrência de um desastre. Essas ações, além das que são tomadas pela própria organização, podem incluir diretrizes relacionadas a ações de agentes externos como os clientes e fornecedores, pois estes em geral têm grande influência para a continuidade das operações de uma organização.

Deve-se levar em consideração que essa recuperação será realizada em meio a uma crise e, portanto, deverá ser executada no menor tempo possível, essas ações deverão ser muito precisas e claras, de forma a facilitar as execuções por parte dos profissionais que estarão à frente do processo de recuperação.

Foi durante as décadas de 50 e 60 que as primeiras empresas norte-americanas começaram a se preocupar e a efetuar o armazenamento de informações que eram relativamente críticas. A princípio essas informações eram feitas em papéis, em seguida passaram a ser efetuadas em fitas magnéticas ou até mesmo guardadas em outras localidades que não dentro da própria empresa, não importando o meio na qual se utilizavam.

Nos anos 70 essas técnicas de armazenagem de dados foram aperfeiçoadas e surgiram empresas especializadas em executar tais operações, esses pontos ou locais de armazenamento ficaram conhecidos como locais quentes ou *hot sites* segundo The History (2009) *apud* Ludescher (2011).

Nessa época, especificamente em instituições financeiras, que tinham como base de funcionamento a sua estrutura computacional, foi criada uma norma no ano de 1983, monitorado pelo Escritório de Controle Monetário dos EUA, para que essas organizações passassem a elaborar planos de recuperação de desastre de forma documentada.

Anos mais tarde essa norma foi reforçada pelo Conselho Federal de Exames de Instituições Financeiras, que passou a exigir uma documentação mais bem elaborada, manutenção e a elaboração de testes desses planos de recuperação de desastres.

Durante a década de 90 e na primeira década deste século, várias outras normas foram implementadas, ainda em instituições financeiras e que foram

disseminadas para outras áreas como a saúde. Essas normas voltadas à área médica, direcionavam essas empresas a estabelecer processos de forma segura durante o armazenamento das informações médicas de seus pacientes, principalmente que elaborassem planos para a continuidade de suas instalações (hospitais).

4.1 DESASTRES EM SISTEMAS COMPUTACIONAIS

Um desastre pode causar sofrimento e dor, além de perdas de ordem física, moral, material e emocional, mas existe uma definição própria em se tratando da área computacional.

> Um desastre é a interrupção não planejada de processos de negócios em uma empresa, resultante da inoperância de um sistema crítico que suporta os processos de negócios da empresa devido à falha de componentes da infraestrutura de tecnologia da informação (TOIGO, 2003).

Quando a organização apresentar um alto grau de dependência dos processos ligados a sistemas computacionais, a interrupção do processo pode afetar a empresa como um todo, resultando em vários tipos de perdas que podem ser de ordem financeiras, informações, tempo e em determinadas situações podem ocasionar até mesmo a morte de pessoas.

Diversos tipos de desastres podem afetar uma organização, esses desastres podem ser fenômenos climáticos como terremotos, maremotos, vendavais, etc., mas existem outros tipos de interrupções que devem ser levados em consideração e consequentemente ser atacado através de um plano de recuperação de desastre.

Falhas em redes de transmissão e distribuição de energia elétrica, falhas nas redes de canais de comunicação, atividades relacionadas a crimes cibernéticos, interrupção dos processos por paralisação dos funcionários em caso de greve ou reinvindicações, devem ter atenções especiais quando na elaboração de um plano de continuidade de negócio.

Mediante o apresentado pode-se dividir os desastres em dois grandes grupos: Desastres Naturais e Desastres Humanos. Os fenômenos naturais por incrível que pareça, podem ser mais previsíveis do que os desastres por natureza humana.

No momento da implantação de uma organização, a empresa pode claramente determinar em qual região demográfica esta deve ser instalada de forma a minimizar

os riscos relacionados a desastres naturais. Se uma empresa optar por fazer suas instalações em um país como o Japão, a probabilidade dessa empresa ser afetada por um terremoto será bem maior do que uma empresa que possui suas instalações em um país como o Brasil.

Em se tratando de desastres de ordem humana, esses podem ocorrer em qualquer lugar a qualquer momento, tornando muito mais difícil sua previsibilidade dificultando os métodos de combate e prevenção.

Os desastres tanto naturais como humanos podem ser divididos em níveis de categoria, que vão desde desastres de nível baixo, médio e alto.

Desastres de níveis baixos são aqueles que ocasionam prejuízos pequenos que podem ser, por exemplo, a perda de uma pequena quantidade de dados devido à falha de um disco rígido de um sistema computacional,

Desastre de nível médio pode ser, por exemplo, um incêndio em um data center de uma organização atingindo e destruindo todo o seu centro de informações.

Quando os desastres tomam proporções maiores, estes são definidos como sendo de **nível alto**, um exemplo bem claro pode ser a interrupção de um sistema de distribuição de energia elétrica, vários são os relatos dessa ordem. Diversos países e aqui incluímos o Brasil, já sofreram paralisações de grandes proporções que ficou conhecido como apagões, quando estes ocorrem, geralmente cidades e até mesmo estados inteiros podem ser afetados.

Os desastres de nível alto ocasionam transtornos e perdas de dimensões muitas vezes imensuráveis e irrecuperáveis, podendo levar sérios riscos à vida, pode-se aqui exemplificar através da paralisação de um hospital e consequentemente toda a área cirúrgica e das unidades de tratamento intensivo, podendo levar a fatalidades se estes não tiverem um plano de continuidade de negócios.

Este trabalho fica restrito a desastres voltados a sistemas computacionais, uma vez que, os sistemas de tecnologia da informação são sem dúvida a grande preocupação das grandes organizações hoje em dia. A maioria das organizações se utiliza de seus sistemas de informação para a condução dos negócios e garantir a segurança dessas informações é garantir a sobrevivência e a lucratividade dessas empresas.

4.2 FASES DE UM PROJETO DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

Quando se pensa em um projeto de plano de continuidade de negócios (PPCN), o desenvolvimento passa por todas as fases de um projeto tradicional, essas fases compreendem desde a definição do projeto, desenvolvimento, implementação, teste, manutenção e treinamento, alguns autores divergem com relação ao número de fases que podem compreender um PCN.

Diferente de um projeto normal, o projeto para o plano de continuidade de negócios é um processo contínuo, desta forma ele deve estar em constante evolução, não necessariamente desenvolver novas ferramentas quando em situações de emergência, mas estar atento e se adequar conforme as necessidades que vão sendo apresentadas.

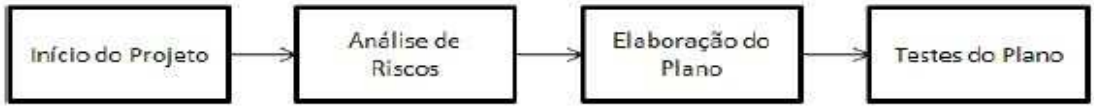
Segundo Varguese (2002) *apud* Ludescher (2011), o PPCN engloba cinco fases principais: Início do projeto, Análise de Riscos, Criação e Implementação do Plano, Testes do Plano e Manutenção do Plano, conforme apresentado na Figura 2.

Figura 2 - Fases da elaboração de um PPCN

Fonte: Varguese (2002) *apud* Ludescher (2011)

Wallace (2004) *apud* Ludescher (2011), afirma que o PPCN apresenta fases de nomenclaturas diferentes, mas no contexto geral as fases abordam os mesmos tópicos, essas fases podem ser divididas em quatro etapas: Início do Projeto, Análise de Riscos, Elaboração do Plano e Testes do Plano, conforme demonstra a Figura 3:

Figura 3 - Fases da elaboração de um PPCN



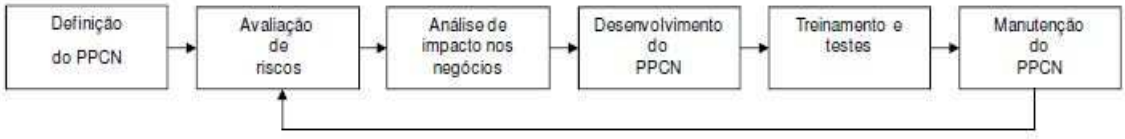
Fonte: Wallace (2004) *apud* Ludescher (2011)

É importante observar que, quanto maior o número de fases envolvidas em um projeto para o desenvolvimento de um plano de continuidade de negócios é permitido um tratamento mais adequado pelos componentes da equipe do projeto. Para cada

fase do projeto são destinados profissionais habilitados e específicos, possibilitando um melhor tratamento dos problemas apresentados em cada fase.

Segundo Snedaker (2007) *apud* Ludescher (2011) o PPCN passa por seis etapas que são: Definição do PPCN, Avaliação de Riscos, Análise de Impactos nos Negócios, Desenvolvimento do PPCN, Treinamento e Testes, Manutenção do PPCN, conforme demonstra figura 4:

Figura 4 - Fases da elaboração de um PPCN



Fonte: Snedaker (2007) *apud* Ludescher (2011)

Ainda segundo Snedaker (2007) *apud* Ludescher (2011) a divisão mais detalhada permite um tratamento de forma mais adequada pelos integrantes da equipe do projeto, visto que, existem profissionais específicos para cada área do projeto, fazendo o tratamento correto para cada fase. Além disso, a divisão com um número maior de fases permite, também, a divisão de tarefas entre os especialistas de cada área da organização, resultando em mais velocidade na finalização de cada etapa, e consequentemente na finalização do projeto.

4.3 ANÁLISE DE IMPACTOS

Dentro de uma organização são vários os sistemas computacionais usados para que a empresa consiga atingir seus objetivos, independente do ramo que a empresa atua, devendo ser levado em consideração os impactos que cada sistema pode ocasionar em caso de um desastre.

Pode-se relacionar alguns sistemas que as empresas dependem atualmente como: sistemas gerenciadores de bancos de dados, sistemas para armazenamento de arquivos, etc. A análise dos impactos passa por várias fases, o primeiro passo é a identificação da relação entre o sistema computacional e os processos que estes controlam dentro do negócio, procurando identificar e relacionar quais os que podem ocasionar a interrupção e o descumprimento da missão da organização em uma eventual parada provocada por um incidente.

Os impactos provocados pela interrupção de tais serviços podem ser, por exemplo: queda no faturamento pela não geração de renda provocada pela paralisação do sistema controlador de vendas, ou ainda a interrupção de serviços hospitalares ocasionados pela interrupção dos serviços de armazenamento de imagens (Raios X), etc.

Uma vez identificado os sistemas e numerados por ordem de criticidade, é necessário determinar o tempo máximo que a empresa pode tolerar sem os serviços estarem sendo executados, bem como o tempo de início e término dos reparos.

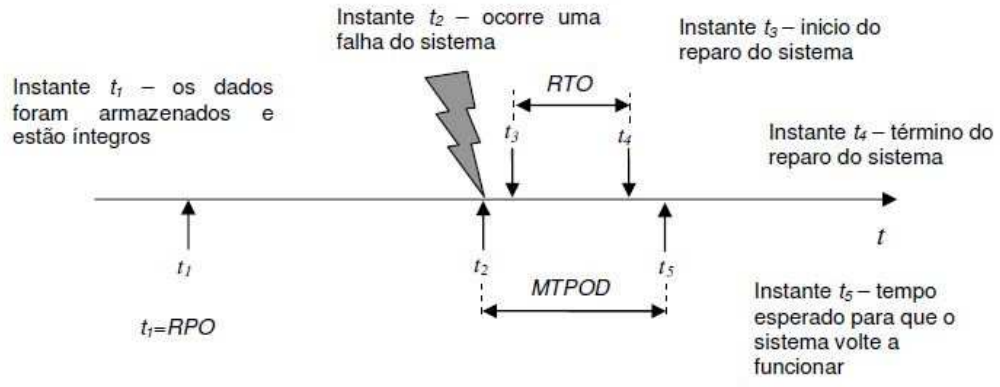
O tempo de paralisação das atividades é conhecido como MTPOD (Maximum Tolerable Period of Disruption), já o tempo de reparo é conhecido como RTO (Recovery Time Objective).

O tempo de paralisação das atividades (MTPO) é sempre maior que o tempo de reparo (RTO), uma vez que, existe um tempo a partir da interrupção do serviço ao início do reparo, o mesmo acontece no final do reparo, existe um tempo entre o fim do conserto e a inicialização do sistema.

Outro dado importante a ser considerado é o RPO, este é o último instante em que o sistema operou e armazenou corretamente as informações, de forma que estes pudessem ser recuperados através de restauração de *backup.*

Essas informações podem ser mais bem interpretadas analisando a figura 5.

Figura 5 - Tempo de recuperação (RTO) e ponto de Recuperação



Fonte: Ludescher, (2006) *apud* Ludescher (2011)

Esses tempos devem ser efetuados de acordo com os requisitos determinados pela organização, ou ainda, para o atendimento dos requisitos da legislação pertinente aos ramos das atividades. É bom ressaltar que, essas informações podem também

ser obtidas através de entrevistas com as diversas áreas da organização, obtendo dessa forma os valores médios por hora da inatividade dos sistemas.

Os sistemas computacionais podem ser divididos em quatro categorias, de acordo com as necessidades da organização, conforme ilustra a Tabela 1, sendo que os objetivos de recuperação (RPO e RTO) apresentados, são os adotados tipicamente pelas organizações e apresentados por institutos de pesquisa, como o desenvolvido por Gartner Group Scott (2002) *apud* Ludescher (2011).

Tabela 1 - Categorias da criticidade de sistemas computacionais

Categoria	Nome	Descrição	Objetivos de Recuperação
1	Missão Crítica	Funções críticas para geração de receita (venda, faturamento, troca de mensagens interbancárias, autorização de cartão de crédito) ou para as atividades em que exista dependência de vidas.	RPO = 0h RTO = 2h
2	Vital	Funções essenciais para a organização (folha de pagamento, sistema de detecção de fraudes).	RPO = 4h RTO = 24h
3	Importante	Funções importantes de apoio (correio eletrônico, acesso à internet).	RPO = 24h RTO = 72h
4	Menor Importância	Funções departamentais de importância reduzida (servidor de impressão, compartilhamento de arquivos).	RPO = 24h RTO = 120h

Fonte: Scott (2002) apud Ludescher (2011)

5 NORMAS REGULAMENTADORAS

5.1 ITIL

Criado no final da década de 80 pela Câmara de Comércio Britânico (OGC – *Office of Government Commerce*), o ITIL (I*nformation Technology Infrastructure Library*) visa disciplinar e permitir a comparação entre as propostas dos diversos proponentes e prestadores de serviços de TI para o governo Britânico. Formado por uma biblioteca com 31 volumes com as melhores práticas para o gerenciamento dos serviços de TI.

Em 2002 essa biblioteca sofreu uma grande revisão sendo reformulada e consolidada em oito volumes distribuídos da seguinte forma:

- ✓ Suporte aos serviços
- ✓ Entrega de serviços
- ✓ Planejamento e Implementação
- ✓ Gerenciamento de aplicações
- ✓ Gerenciamento da segurança
- ✓ Gerenciamento da Infraestrutura de TI e de comunicações
- ✓ Perspectiva do negócio
- ✓ Gerenciamento dos ativos de software

A segunda versão do ITIL tem como principal objetivo a entrega e o suporte dos serviços de TI de forma a torná-lo mais aderentes e apropriados aos requisitos dos processos de negócio. Já a terceira versão do ITIL foi lançada em maio de 2007 e é composta por 5 livros. A 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, no ITIL v3 seu foco é o alinhamento estratégico da TI com o negócio.

Segundo Ludescher (2011), o ITIL v3 é formando por cinco livros:

Estratégia de Serviços: Define os objetivos, conceitos e regras sobre a estratégia de serviços, analisa o impacto dos serviços necessários para as funções principais e vitais do negócio, definição e métodos de gestão do risco.

Desenho de Serviços: Descreve os objetivos, planos e cria um desenho de serviços, detalhando cada um dos processos relativos ao gerenciamento de nível de

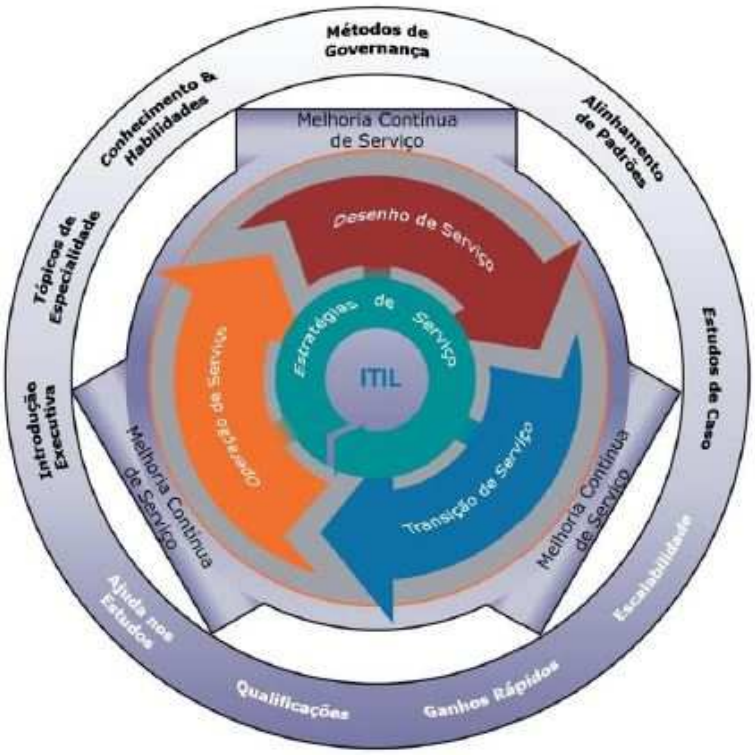
serviço, gerenciamento do catalogo de serviços, gerenciamento da disponibilidade, gerenciamento da capacidade, gerenciamento da segurança da informação, gerenciamento da continuidade dos serviços e o gerenciamento dos fornecedores.

Transição de Serviços: Descreve as formas para garantir o desenho de serviços na forma pretendida, incluindo os processos de gerenciamento de mudanças, gerenciamento da configuração de ativos dos serviços e gerenciamento de liberação e distribuição.

Operação de Serviços: Descreve a gerência 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 também o gerenciamento de eventos, gerenciamento de incidentes, gerenciamento de problemas, gerenciamento de acessos e as requisições de serviços.

Melhoria continua de serviços: Descreve como 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.

Figura 6: Visão Geral do Ciclo de Vida da biblioteca de melhores práticas ITIL v3



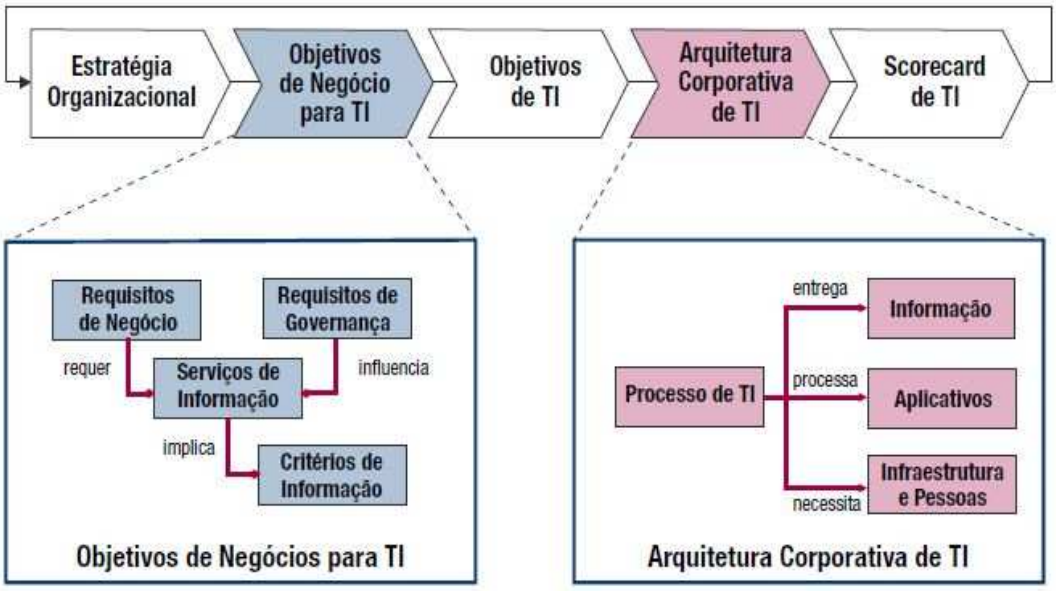
Fonte: Ludescher (2011)

5.2 COBIT

O COBIT é um *framework* de governança de TI que atua no alinhamento dos objetivos da TI com os objetivos do negócio, estabelecendo controles para avaliação da maturidade dos processos.

Conforme a IT GOVERNANCE INSTITUTE (2007), a figura 7 ilustra como a estratégia da empresa deveria ser traduzida pela área de negócios em objetivos relacionados às iniciativas de TI (objetivos de negócios para TI).

Figura 7 - Definindo os objetivos de TI e a Arquitetura da Empresa para TI



Fonte: IT Governance Institute (2007)

O COBIT (*Control Objectives for Information and Related Technology*) fornece as boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. Seu foco é mais nos controles e menos na execução, otimizando os investimentos em Tecnologia da Informação, assegurando a entrega dos serviços e provendo métricas para julgar as coisas quando estas não darem certo.

Para que o departamento da Tecnologia da Informação possa apresentar resultados satisfatórios, entregando os serviços requisitados pelo negócio, os responsáveis devem implementar sistemas de controle ou uma metodologia. Através

dos controles apresentados pelo COBIT é possível atender as necessidades do negócio.

O COBIT é dividido em 4 Domínios e 34 processos alinhado as áreas responsáveis em planejar, implementar, entregar e monitorar, provendo desta forma uma visão geral da área de TI.

Planejamento e Organização (PO): Este domínio é formado por 10 processos e é responsável pelo desenvolvimento dos planos estratégicos de TI e fornece suporte aos objetivos e metas empresariais.

Aquisição e Implementação (AI): Composto por 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 é responsável pela manutenção, teste, certificação e identificação das alterações que posam afetar a disponibilidade das informações.

Entrega e Suporte (DS): 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, o Suporte prevê que os processos sejam executados de forma eficiente e efetiva.

Monitoração e Avaliação (ME): Composto de 4 processos, visando o monitoramento através dos acordos de nível de serviço, verificando se o que foi proposto está sendo realizado.

O COBIT visa suportar a **governança de TI**, provendo uma metodologia capaz de assegurar que a área de TI esteja alinhada ao negócio, que a área de TI habilite o negócio e maximize os benefícios, que os recursos de TI sejam usados de forma responsável e que os riscos de TI sejam gerenciados apropriadamente.

Segundo o *IT Governance Institute (2007)*

> A governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização.

5.3 NBR ISO/IEC 27002 (ANTIGA NBR ISO/IEC 17799)

Criada pela *British Standard Institute* (*BSI*) inicialmente conhecida por BS7799, na qual considerava o mais completo padrão de gerenciamento da Segurança da Informação no mundo, através desta norma era possível implementar um sistema de

gestão da segurança baseado em controles definidos por normas e práticas internacionais.

A partir de 2000, a parte I da BS7799 tornou-se norma oficial da ISO sob o código ISO/IEC17799. Em agosto do próximo ano o Brasil adotou essa norma como seu padrão, através da ABNT, sob o código NBR ISO/IEC 17799

Em junho de 2005, foi publicada uma nova versão da Parte I da ISO/IEC 17799, revisada e com a inclusão de novos capítulos, dentre eles o gerenciamento de riscos e a gestão de incidentes de segurança.

Com foco na prevenção, a norma é de fácil compreensão e implementação, contendo um número substancial de objetivos de controles, sendo alguns de certa complexidade. De forma a reunir diversas normas de segurança da informação, a ISO criou a série 27000. A norma NBR ISO/IEC 27001:2006 é a norma BS7799-2:2002 revisada e aprimorada, na qual abrange o ciclo PDCA (Plan-do-Check-Act) e visão de processos que as normas de sistemas de gestão já possuem (FONTES, 2008).

A norma foi projetada para as organizações usarem como uma referência na seleção de controles dentro de um processo de implementação de um sistema de gestão da segurança. É também usada para o desenvolvimento de organizações e indústrias específicas de gerenciamento de segurança da informação.

5.4 ISO 27001

A ABNT ISO/IEC 27001 (ABNT, 2005) foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01). Esta norma é uma tradução idêntica da ISO/IEC 27001:2005, que foi elaborada pelo *Join Technical Committee Information Technology* (ISO/IEC/JC 1), *subcommittee IT Security Techniques* (SC 27).

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

6 ESTUDO DE CASO

O estudo desenvolveu-se a partir do levantamento de dados de empresas de pequeno porte na qual este trabalho é focado. O processo de levantamento das informações relativos a um plano de continuidade de negócios, partiu da aplicação de um questionário (APÊNDICE I) cujo objetivo era o de verificar o quanto as empresas conhecem e o quanto elas estão preparadas em caso de incidentes e/ou acidentes envolvendo suas informações.

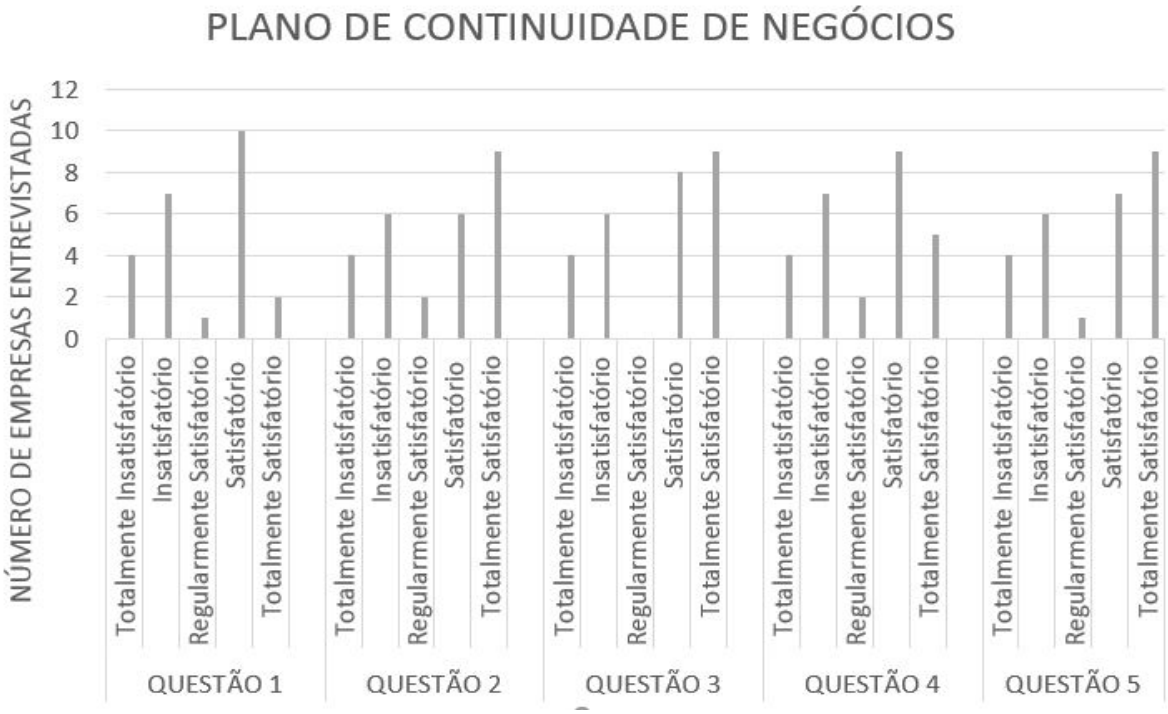
Mediante aos resultados apresentados após as análises das respostas do questionário (APÊNDICE II), foi verificado os pontos mais fracos (vulneráveis) apresentados pelas referidas empresas. Mediante a esses dados, foi desenvolvido o plano de continuidade de negócio, este plano não tem por objetivo o de informar dados técnicos de equipamentos, mas apresentar um documento formal (plano de continuidade) capaz de alertar e orientar da importância de medidas que garantam que suas atividades possam continuar mesmo após um desastre, procurando a restauração das informações no menor tempo possível e com menores consequências.

A informação coletada pelo questionário foi desenvolvida através de metodologia de análise gráfica/descritiva associada à escala de *Likert* de cinco pontos, conforme Pereira (1999). Nessa escala o valor 1 é considerado totalmente insatisfatório, o 2 insatisfatório, o 3 regularmente satisfatório, o 4 satisfatório e o 5 totalmente satisfatório.

O questionário foi aplicado usando uma ferramenta *on-line*, direcionado por e-mail, através da qual as organizações de diversos segmentos de mercado responderam um total de 10 questões relativas à segurança e plano de continuidade de negócio. Diante dos resultados obtidos foi criado um gráfico, que através deste, foi possível identificar o despreparo das empresas e de seus colaboradores quanto a segurança da informação.

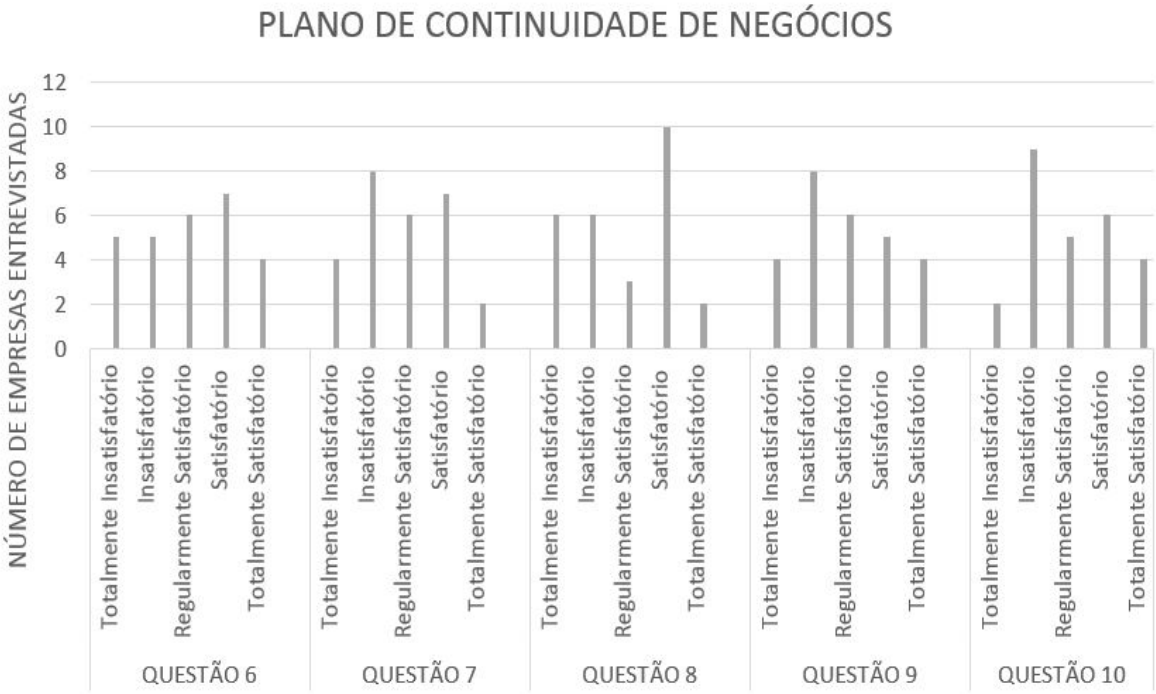
Os gráficos das figuras 8 e 9 mostram os resultados do questionário aplicado em 27 empresas, todas de pequeno porte:

Figura 8: Resultado das questões 1 a 5



Fonte: Próprio do Autor

Figura 9: Resultado das questões 6 a 10



Fonte: Próprio do Autor

Observa-se que, um elevado número de empresas considera que o seu sistema é “totalmente insatisfatório” ou “insatisfatório” do ponto de vista da segurança

da informação, e por consequência não apresentam um plano de continuidade de negócio, ou quando possui, eles consideram que esse plano não é eficaz.

Boa parte das empresas entrevistadas através da aplicação do questionário, existe uma certa preocupação em relação a segurança da informação quando se trata dos colaboradores internos (colaboradores diretos), mas se esquecem, e não se preocupam em aplicar mecanismos de segurança ao tratar de colaboradores indiretos, como por exemplo, os seus fornecedores.

O mesmo ocorre quando o assunto é treinamentos, estes aplicam-se diretamente à funcionários e não para seus colaboradores indiretos (fornecedores), o que torna a empresa extremamente vulnerável, lembrando que, muitas das informações relevantes à continuidade da empresa está nas mãos de seus fornecedores, uma vez interrompido os serviços desses prestadores, a empresa poderá sofrer danos que em proporções seriam iguais a perda de suas próprias informações.

Observa-se ainda, a inexistência na maioria das empresas, de um documento formal capaz de orientar com exatidão o que as pessoas envolvidas na segurança da informação devem fazer em casos de um desastre, tornando o procedimento mais moroso e com grandes probabilidades de falhas.

As empresas em geral não realizam periodicamente testes de avaliação de riscos, o que faz com que os riscos envolvendo a segurança sejam na maioria das vezes desconhecido, o que torna ainda mais difícil o tratamento e uma ação de reação aos desastres.

É claro e totalmente perceptível que as empresas e seus funcionários, de forma geral, estão despreparados para enfrentar uma situação de emergência, a maioria trabalha com armazenamento de informações sem nenhum requisito de segurança, podendo levá-las a perda de suas informações e consequentemente, a perdas financeiras e de credibilidade frente a seus clientes.

Diante da falta de conhecimentos e de como agir mediante a imprevistos, é necessário que essas empresas busquem profissionais capazes de orientá-los, mitigando os riscos de perdas e melhorando a segurança no que diz respeito a proteção de seu ativo mais importante, as suas informações.

Através do plano de continuidade de negócio é possível mitigar ou até mesmo eliminar os riscos da perda das informações vitais a sobrevivência dessas empresas.

6.1 PROPOSTA DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

A proposta a seguir deverá assegurar a existência de um documento formal (Plano de Continuidade) capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, deverá também apresentar atividades envolvendo testes e manutenção do plano, além do devido treinamento de todos os envolvidos.

As orientações a seguir não têm o objetivo de ser uma regra, mas um guia para que as empresas tenham no que se orientar quando na implementação de um sistema que garanta a continuidade do negócio. As empresas devem buscar a confecção de um plano que atenda em específico as suas atividades, identificando o foco principal de sua organização, as informações relevantes ao negócio, ou seja, precisa determinar o sistema de missão crítica que envolve a organização.

6.1.1 Backup e Restore

O *Backup* deve ser apoiado por uma política de segurança fornecendo as diretrizes capaz de orientar o desenvolvimento dos procedimentos de Armazenamento e Restauração (*Backup e Restore*), o *Backup* é sem dúvidas um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisações quando na presença de um sinistro.

A importância da informação deve ser levada em consideração na implementação de um *Backup*, além do nível de qualificação utilizado, a periodicidade de atualização e a volatilidade.

Quando na execução de um *Backup*, algumas premissas deverão ser observadas:

- ✓ Realizar os *Backups* de forma a garantir que sejam mitigados os riscos relacionados a continuidade no negócio.
- ✓ Manter os *Backups* em local físico distante da localidade de armazenamento dos dados originais, além de um *Backup* em nuvem (fora de um ambiente físico)
- ✓ Periodicamente providenciar testes nas mídias que armazenam os *Backups*, assegurando que estejam seguros e em perfeito estado para a realização dos serviços.
- ✓ Determinar a periodicidade dos *Backups*.

- ✓ Desenvolver uma documentação e mantê-la atualizada, quanto aos procedimentos de *Backup e Restore.*
- ✓ Manter um inventário atualizado sobre as mídias que armazenam os *Backups*.

Conforme citado nas premissas a serem seguidas, a frequência (periodicidade) para a realização dos *Backups* deverá ser determinada levando em consideração a velocidade e a volatilidade com que os dados são alterados.

Velocidade da informação: É a periodicidade com que a informação é atualizada.

Volatilidade da informação: Trata-se do período de tempo na qual a informação permanece atualizada.

Os *Backups* a serem realizados podem ser de três tipos conforme necessidade:

***Backup* Completo ou Normal (*Full*):** Procedimento na qual será realizada a cópia de todos os arquivos contidos em um determinado disco, esse procedimento é aconselhável ser executado quando da primeira realização de um *Backup*, trata-se de um procedimento mais demorado e que deverá ser evitado em Backups posteriores.

***Backup* Diferencial:** Nesse sistema apenas os arquivos alterados após o último *Backup* serão copiados. Nesse tipo de *Backup* não são marcados os arquivos como salvos em *Backup* (o atributo de arquivo não é desmarcado), portanto toda vez que realizar um *Backup* Diferencial todos os arquivos que foram alterados serão novamente copiados em relação ao *Backup* Completo

***Backup* Incremental:** Parecido com o *Backup* Diferencial quando realizado pela primeira vez, pois todos os dados alterados desde o último *backup* serão copiados, nos *Backups* posteriores, os arquivos a serem copiados serão apenas os que foram alterados no último *backup*, e não como é feito pelo *Backup* Diferencial que copia os últimos arquivos relacionados ao *Backup* completo.

O armazenamento dos Backups não deverá ser realizado juntamente com os equipamentos cujo os dados originais estão sendo gerados, desastres (incidentes causados pela natureza como incêndios, terremotos e incidentes ocasionados por atos maliciosos) poderão comprometer totalmente o ambiente impossibilitando a restauração das informações.

A contratação de um serviço terceirizado para o armazenamento dos *Backups* também deverá ser levado em consideração (serviço de *Backup* nas nuvens). Os

Backups realizados devem contar com registros das operações executadas, a seguir serão apresentadas algumas sugestões dessas informações:

- ✓ Identificação do Servidor: Identificar corretamente o servidor responsável pela execução dos *Backups*, deve aqui ser listado todos os servidores, sejam eles físico ou virtualizados;
- ✓ Identificação das mídias: Especificar os tipos de mídias utilizadas para os *Backups* (CD, DVD, fita DAT, etc.), bem como a quantidade utilizada;
- ✓ Localização do Servidor: Registrar as localizações dos Servidores;
- ✓ Descrição do conteúdo: Descrever detalhadamente os arquivos, sistemas, etc., contido em cada *Backup*;
- ✓ Período de Retenção: Determinar e especificar o tempo na qual as informações contidas nos *Backups* sejam armazenadas, ou seja, o ciclo de vida da informação;
- ✓ Horário de *Backup*: Estipular o(s) horário(s) na qual será realizado os Backups, preferencialmente em horários na qual o sistema está com menos sobrecarga, exemplo: Se a empresa não trabalha no período noturno, aconselha-se a fazer os *Backups* nesses horários.
- ✓ Instruções de Software: Documentar com o máximo de detalhes possíveis as operações do software de *Backup*, e se possível com o uso de cópias das telas do *software* em questão, facilitando o processo de entendimento das operações.

Assim como o *Backup* requer procedimentos que devem ser seguidos de forma rigorosa, o processo de Recuperação (*Restore*) das informações também devem seguir alguns critérios:

- ✓ Verificar a integridade da informação armazenada;
- ✓ Avaliar a funcionalidade dos procedimentos;
- ✓ Verificar a capacitação e a falta de treinamento da equipe;
- ✓ Verificar a identificação de procedimentos não atualizados ou que não tenham uma boa eficácia;
- ✓ Identificar falhas e possíveis defeitos durante o processo de *restore*.

A organização deve se preocupar em realizar os testes de restauração, buscando detectar possíveis anomalias que impossibilitaria a restauração das informações, os testes passariam pela verificação das mídias utilizadas, o tempo de

recuperação para o levantamento dos serviços, testes de *links* reservas de internet caso necessite para executar o *download* dos *Backups* realizados nas nuvens, além de informar explicitamente quem será responsável por cada procedimento, e ainda estipular prazos para a realização dos testes.

Aconselha-se apresentar um *check-list* do que será testado, o resultado dos testes e possíveis modificações ou adaptações conforme necessidades e ou dificuldades apresentadas durante a realização dos testes.

6.1.2 Energia Elétrica

Para garantir a disponibilidade das informações aconselha-se a aquisição e a instalação de um gerador de energia, buscando a garantia do funcionamento dos equipamentos e serviços em casos de interrupção de energia pela concessionária.

A rede elétrica e o gerador deve ser sempre estabilizada e dimensionada por profissionais gabaritados, considerando no planejamento a carga necessária. A fiação para o CPD (Central de Processamento de Dados) deve ser única e independente evitando a penetração de ruídos que podem interferir no funcionamento do sistema.

Realizar uma análise criteriosa de risco, levando em consideração o grau de exposições da rede elétrica e das instalações do cabeamento de dados, e consequentemente realizar ações de maneira a mitigar a possibilidade de desastres naturais e/ou atos de vandalismo, ações de prevenção como a instalação de eletrodutos metálicos nos cabeamentos de rede de dados e de energia elétrica, assim como a instalação de cadeados em racks dos switches, devem ser levados em consideração.

A rede elétrica deve estar provida de um bom sistema de aterramento, garantindo a equipotencialização da rede e dos equipamentos, a escolha do tipo de aterramento deverá ser feita por um profissional experiente e as medições da eficiência do sistema, deverá ser acompanhado periodicamente através de medições com equipamentos apropriados.

6.1.3 Servidores Redundantes

A empresa deverá sempre contar com servidores físicos redundantes garantindo o espelhamento dos arquivos e dos serviços de rede, os servidores redundantes não devem permanecer no mesmo prédio, pois desastres naturais e atos

maliciosos podem comprometer todo o sistema. A empresa deverá ainda contar com servidores não físicos (servidores em nuvens) aumentando a probabilidade de uma recuperação mais rápida das informações, precisando para isso apenas um *link* com a internet.

6.1.4 *Link* de Internet

A empresa deve contar com um *link* alternativo de Internet, podendo este ser de capacidade inferior ao *link* principal, esse *link* tem a finalidade de garantir a disponibilidade do sinal de internet em caso de interrupção do *link* principal, ou seja, ser uma redundância de serviço, outra exigência é que este *link* não tenha o mesmo trajeto do anterior, ou seja, evitar que os *links* venham pela mesma rede (caminho), pois uma vez esse caminho sendo interrompido impedira o funcionamento de ambos os serviços.

Aconselha-se utilizar um *link* de internet via rádio, por ser diferenciado e mais flexível, não precisando de infraestrutura dentro da empresa. Este *link* redundante será utilizado por alguns setores que não podem de maneira alguma interromper suas atividades (sistema de missão crítica) e também pode ser replicado para a empresa em caso do outro link estar indisponível.

6.1.5 Treinamento

Para que um plano de continuidade de negócios tenha sua funcionalidade assegurada, é de extrema importância que a equipe envolvida no processo tenha treinamentos constantes, visando garantir agilidade durante o processo de recuperação das informações em caso de desastre. O treinamento constante possibilita que a equipe identifique eventuais falhas no plano de continuidade de negócios, revisando e melhorando o processo.

A equipe deve definir antecipadamente (antes do desastre) as tarefas de cada integrante, as atividades devem estar documentadas e, o responsável pelo processo deve cobrar periodicamente da equipe que acompanhem e revisem as suas atividades.

O plano de continuidade de negócios sempre será executado em situações de extrema emergência e pressão de todos os sentidos, não é momento para verificar o

que será feito, mas colocar em prática tudo o que foi anteriormente estipulado, portanto, a equipe não pode apresentar nenhuma dúvida.

7 CONSIDERAÇÕES FINAIS

Os conceitos e as preocupações aqui apresentados, não terão nenhum objetivo se as organizações não adotarem uma cultura voltada para a segurança. Vale ressaltar que a segurança não pode ser encarada de forma isolada, muito menos achar que a competência na solução dos problemas é de algumas pessoas. Todos os funcionários, por mais humilde que seja sua função, devem ser incorporados os conceitos básicos de segurança da informação e, de alguma forma, deve ser exigida a sua participação e sua parcela de colaboração.

A sobrevivência de uma organização não está ligada apenas ao aspecto da rentabilidade (lucratividade) do seu negócio, mas também a manutenção de sua operacionalidade. A perda das informações pode levar uma empresa a ter sua credibilidade rebaixada, ou ainda, impossibilitar a retomada dos serviços, levando à extinção do negócio.

O plano de continuidade de negócios visa a garantia da sobrevivência das organizações, quando submetidas a acidentes de diversas categorias, mostra através de diretrizes o que e como as empresas devem agir, garantindo a restauração das informações e serviços no menor tempo possível.

Um plano de continuidade de negócios não termina na sua implementação, deve estar em constante evolução e adaptação para as ocorrências recentes, requer revisões periódicas e treinamento constante do pessoal envolvido.

De forma geral as empresas de pequeno porte não conhecem ou sabem muito pouco sobre o assunto, o profissional da área de segurança encontra um campo bem vasto para explorar e conseguir introduzir seus conhecimentos nessa fatia de mercado, garantindo a segurança e a continuidade dessas empresas.

Cabe ao profissional da área de segurança, juntamente com os gestores do negócio, implementar uma cultura voltada a segurança, aumentando de forma significativa a capacidade de as organizações atuarem de forma mais segura.

O desenvolvimento de uma empresa, entre outros fatores, depende da imagem que ela transmite ao mercado, garantir a segurança das informações de uma empresa é aumentar sua participação no mercado, garantir a confiança dos clientes, aumentar o retorno dos investimentos e assegurar sua sobrevivência. O papel do profissional da segurança está no acompanhamento de todo esse processo, orientando e desenvolvendo ferramentas capazes de atender a essas necessidades.

REFERÊNCIAS

ABNT, **NBR ISO/ IEC 17799 Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

ABNT. **NBR ISO/ IEC 27001 Tecnologia da informação – Técnicas de segurança – Sistema de Gestão da segurança da informação – Requisitos**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

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

ABREU, Leandro Farias dos Santos. **A segurança da informação nas redes sociais.** Monografia (Graduação Tecnólogo em Processamento de Dados). Faculdade de Tecnologia de São Paulo**.** Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf> Acesso em: 13 mar. 2016

ALBERTIN, Alberto Luiz. Valor estratégico dos projetos de tecnologia de informação. São Paulo: **RAE - Revista Administração de Empresas** – FGV, v. 41, n.3, jul. /Set. 2001.

BROOK, Jon-Michael C. **CIA triad:** CIPP guide. Estados Unidos da América: Ago. 2010. Disponível em: <http://www.cippguide.org/2010/08/03/cia-triad>. Acesso em: 01 mar. 2016.

CASTELLS, Manuel. **Sociedade em rede**. São Paulo: Paz e Terra, 1999.

CERUTTI, Fernando. **Necessidade e componentes gerais da segurança da informação,** 2012. Disponível em: <http://www.diegomacedo.com.br/?s=Necessidade+ e+componentes+gerais+ da+seguran%C3%A7a+da+informa%C3%A7%C3%A3o%2C > Acesso em: 09 Set. 2016

COBIT 4.1. Disponível em: < http://analistati.com/wp-content/uploads/2010/01/cobit41_ portuguese.pdf> Acesso em: 08 Out. 2016.

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Marcio Tadeu de. **Política de segurança da informação – Guia prático para elaboração e implementação.** 2ª Edição – Revisada. Rio de Janeiro, Editora Ciência Moderna Ltda. 2008.

FONTES, Edison Luiz Gonçalvez. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

LUDESCHER, Wagner. **Modelo para avaliação da qualidade de projetos de planos de continuidade de negócios aplicados a sistemas computacionais**, 2011. 257 f. Tese (Doutorado em Engenharia de Computação e Sistemas Digitais) – Escola Politécnica da Universidade de São Paulo. Disponível em: <http://www.teses.usp.br/ teses/disponiveis/3/3141/tde-10082011-142221/pt-br.php>. Acesso em: 20 mar. 2016.

MAGALHÃES, Ivan Luizio. **Gerenciamento de serviços de TI na prática:** Uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

OLIVEIRA, Djalma de Pinho Rebouças. **Sistemas, organização e métodos:** uma abordagem gerencial. 10. ed. São Paulo: Atlas, 1998.

PADOVEZE, Clovis Luiz. **Sistemas de informações contábeis:** fundamentos e análise**.** 2. ed. São Paulo: Atlas, 2000.

REZENDE, Denis Alcides, ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas. 2001.

REZENDE, Denis Alcides. **Tecnologia da informação**: integrada a inteligência empresarial. São Paulo: Atlas, 2002.

SEBRAE. Disponível em: < http://www.sebrae.com.br/sites/PortalSebrae/estudos_pesquisas/empresa-de-pequeno-portedetalhe8,8e5713074c0a3410VgnVCM1000003b74010aRCRD> acesso em: 10 Out. 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação**. 11.ed. Rio de Janeiro: Campus, 2003.

SMITH, D. **Business Continuity Management:** Good Practices Guide lines. Business Continuity Institute. Bershire:2008. Disponível em http://www.thebci.org/gpg.htm Acesso em 14.mai. 2015

TOIGO, J, W. **Disaster recovery planning**: Preparing for the unthinkable, New Jersey: Pearson Eduction, 2003.

VARGUESE, M**. Disaster Recovery Planning**. Boston: Course Techonology, 2002.

APÊNDICE I

QUESTIONÁRIO

1. A empresa e os seus colaboradores diretos e indiretos, sabem o que é Segurança da informação?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

2. Existe um documento formal de política de segurança da informação definindo as diretrizes e filosofia da organização em relação ao uso e proteção da informação?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

3. A empresa conhece a necessidade da proteção de suas informações e os impactos em caso da perda dessas informações?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

4. É realizada periodicamente uma avaliação de risco com foco nas ameaças que podem indisponibilizar recursos de informação e que podem parar ou degradar em muito o desempenho da realização do negócio?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

5. Existem cópias de segurança considerando aspectos de operação, de auditoria, histórico e legal guardados de forma segura, suficientes para uma recuperação da informação?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

6. Existe um manual atualizado que definem os procedimentos a serem feitos quando da ocorrência de uma situação de contingência?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

7. A empresa e os seus colaboradores diretos e indiretos, sabem o que é um Plano de Continuidade de Negócios?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

8. Existe um Plano de Continuidade de Negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

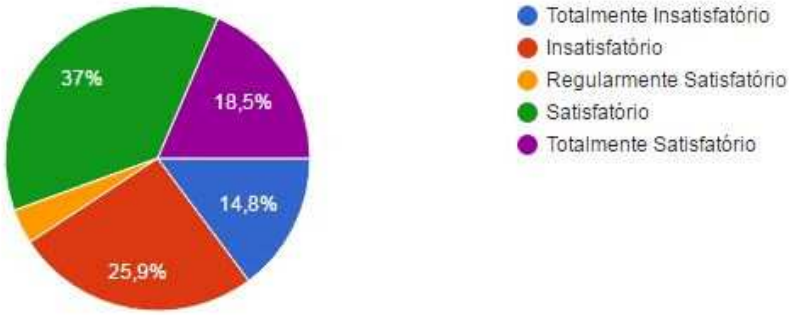
9. A empresa considera que seus funcionários estão totalmente preparados para enfrentar uma situação de emergência envolvendo a perda das informações do negócio?
   ( ) Totalmente Insatisfatório
   ( ) Insatisfatório
   ( ) Regularmente Satisfatório
   ( ) Satisfatório
   ( ) Totalmente Satisfatório

10. A empresa executa treinamentos constantes dos funcionários, possibilitando que estejam preparados para um eventual desastre envolvendo os serviços de informações e a informação propriamente dita?
    ( ) Totalmente Insatisfatório
    ( ) Insatisfatório
    ( ) Regularmente Satisfatório
    ( ) Satisfatório
    ( ) Totalmente Satisfatório

APÊNDICE II

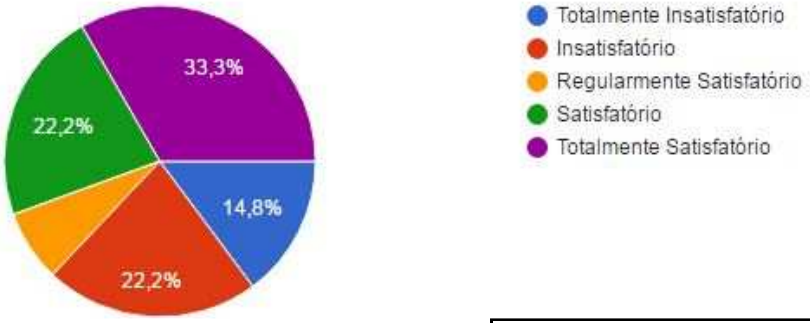
RESPOSTAS DO QUESTIONÁRIO

1- A empresa e os seus colaboradores diretos e indiretos, sabem o que é Segurança da informação?
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	7
Regularmente satisfatório	1
Satisfatório	10
Totalmente satisfatório	2

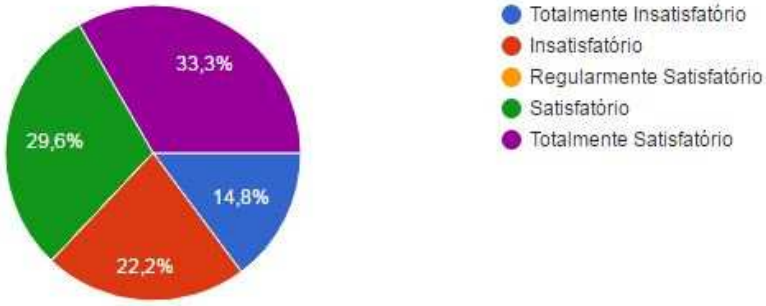
2- Existe um documento formal de política de segurança da informação definindo as diretrizes e filosofia da organização em relação ao uso e proteção da informação?
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	6
Regularmente satisfatório	2
Satisfatório	6
Totalmente satisfatório	9

3- A empresa conhece a necessidade da proteção de suas informações e os impactos em caso da perda dessas informações?

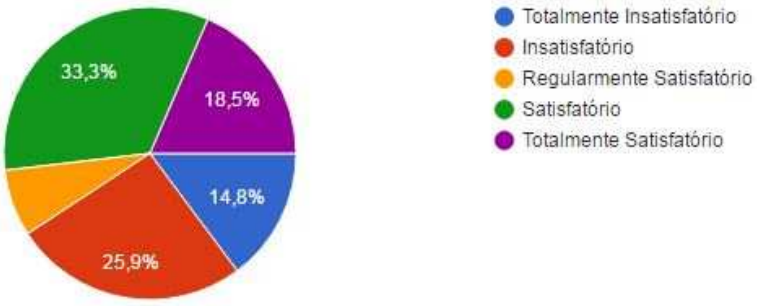
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	6
Regularmente satisfatório	0
Satisfatório	8
Totalmente satisfatório	9

4- È realizada periodicamente uma avaliação de risco com foco nas ameaças que podem indisponibilizar recursos de informação e que podem parar ou degradar em muito o desempenho da realização do negócio?

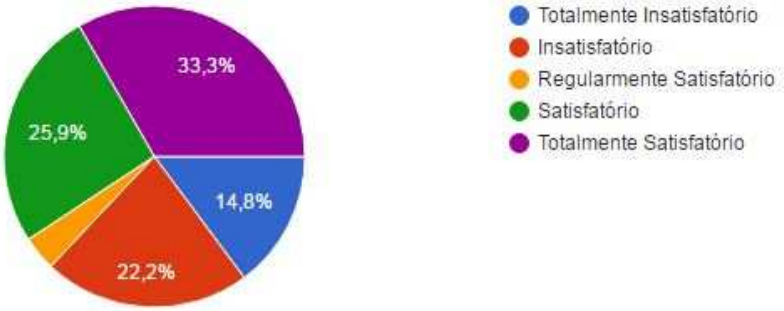
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	7
Regularmente satisfatório	2
Satisfatório	9
Totalmente satisfatório	5

5- Existem cópias de segurança considerando aspectos de operação , de auditoria, histórico e legal guardados de forma segura, suficientes para uma recuperação da informação?

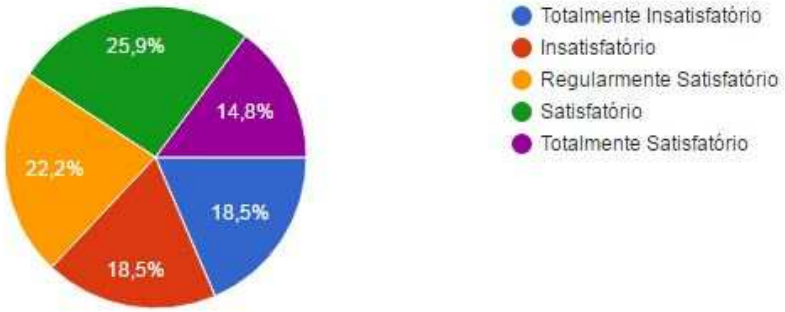
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	6
Regularmente satisfatório	1
Satisfatório	7
Totalmente satisfatório	9

6- Existe um manual atualizado que definem os procedimentos a serem feitos quando da ocorrência de uma situação de contingência, ou seja, quando da necessidade de se recuperar as informações por motivo de um desastre?

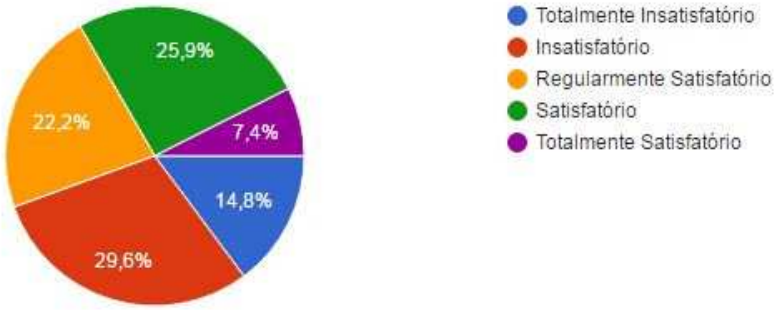
(27 respostas)



Totalmente insatisfatório	5
Insatisfatório	5
Regularmente satisfatório	6
Satisfatório	7
Totalmente satisfatório	4

7- A empresa e os seu colaboradores diretos e indiretos, sabem o que é um Plano de Continuidade de Negócios?

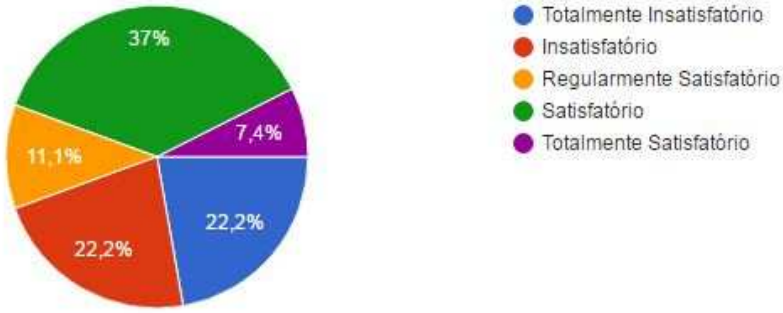
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	8
Regularmente satisfatório	6
Satisfatório	7
Totalmente satisfatório	2

8- Existe um Plano de Continuidade de Negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação?

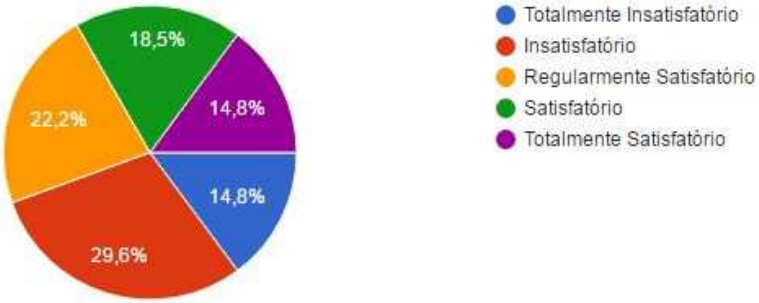
(27 respostas)



Totalmente insatisfatório	6
Insatisfatório	6
Regularmente satisfatório	3
Satisfatório	10
Totalmente satisfatório	2

9- A empresa considera que seus funcionários estão totalmente preparados para enfrentar uma situação de emergência envolvendo a perda das informações do negócio?

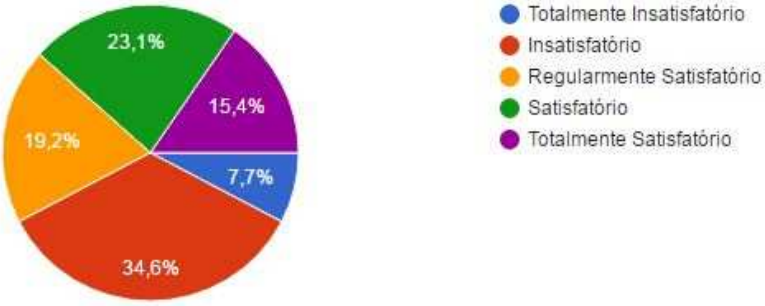
(27 respostas)



Totalmente insatisfatório	4
Insatisfatório	8
Regularmente satisfatório	6
Satisfatório	5
Totalmente satisfatório	4

10- A empresa executa treinamentos constantes dos funcionários, possibilitando que estejam preparados para um eventual desastre envolvendo os serviços de informações e a informação propriamente dita?

(26 respostas)



Totalmente insatisfatório	2
Insatisfatório	9
Regularmente satisfatório	5
Satisfatório	6
Totalmente satisfatório	4