FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Daniel Sobral do Nascimento

A POLÍTICA DE *BACKUP* NAS ORGANIZAÇÕES

Americana, SP

2015

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Daniel Sobral do Nascimento

A POLÍTICA DE *BACKUP* NAS ORGANIZAÇÕES

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof. Me. Alberto Martins Júnior.

Área de concentração: Segurança da Informação

Americana, SP

2015

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

Nascimento, Daniel Sobral do
N194p A política de *backup* nas organizações. / Daniel Sobral do Nascimento. – Americana: 2015.
79f.

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

Daniel Sobral do Nascimento

A IMPORTÂNCIA DE UMA POLITICA DE *BACKUP* NAS ORGANIZAÇÕES

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de Americana, como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Área de concentração: Segurança da Informação

Americana, 08 de dezembro de 2015.

Banca Examinadora:

Alberto Martins Junior
Mestre
Faculdade de Tecnologia de Americana

José Luiz Zem
Doutor
Faculdade de Tecnologia de Americana

Maria Elizete Luz Saes
Mestre
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus pelo seu infinito amor e graça, por ter me abençoado para a realização deste trabalho, agradeço a minha família por sempre me apoiar e oferecer a base necessária para poder concluir a faculdade, agradeço meus amigos em especial a Juliana Caruso, por sempre me ajudar e incentivar.

Agradeço ao corpo docente em especial ao meu orientador Mestre Alberto Martins Júnior por sempre acreditar em meu potencial e incentivar a realização deste trabalho.

DEDICATÓRIA

Dedico este trabalho a Deus e o presente que ele me deu que é a minha família, dedico aos meus pais e irmã razão da minha existência e vida, dedico também este trabalho a minha querida avó Adalva.

RESUMO

No mundo atual onde a informação é crucial para a organização se manter e crescer no mercado, onde tem-se acesso fácil a vários tipos de informações, tão importante quanto saber armazená-las é saber a maneira correta de armazenamento.

Este trabalho apresenta a importância da informação para as organizações e a importância do *backup* para guardá-las, explicando a gestão na área de TI, trazendo de forma sucinta conceitos de gestão e de como ela é importante na organização. Outro tema abordado é a Tecnologia da informação nas organizações, demonstrando a importância da TI como ferramenta para manter a organização competitiva no mercado. Outro tema trata sobre a Tecnologia da informação e seus recursos, explicando a importância da TI ser bem gerenciada bem como a dependência que as empresas tem dos serviços de TI. Também são abordados os benefícios da TI e seus recursos.

No terceiro capítulo é abordada a necessidade da governança corporativa e de TI e, também, o trabalho aborda o uso de políticas de segurança da informação e continuidade do negócio, demonstrando a importância de uma política de segurança e seu objetivo para com a informação. É tratado o plano de continuidade do negócio e seu objetivo de minimizar o impacto em desastres e incidentes de segurança e, por fim, no capítulo sobre cópias de segurança e *restore,* são abordados tópicos importantes, de como deve-se armazenar e tratar um *backup*, bem como ferramentas automatizadas para realizar *backups* de segurança.

Palavras-chave: Backup; Informação; Tecnologia da Informação;

ABSTRACT

In today's world where the information is crucial for the organization to remain and grow in the market, which has easy access to many kinds of information, it is so important to know how to store them, and to know the right way to store it.

This work shows the importance of information for organizations and the importance of backup to store, explaining the management in the IT area, brining succinctly management concepts and how it is important in the organization. Another theme developed is the information technology in organizations, which demonstrates the IT importance as a tool to keep the organization competitive in the market. Another issue deals with the information technology and its resources, explaining the importance of IT being well managed and the dependence that organization have of IT services. The benefits of IT and its resources are also discussed.

In the third chapter is discussed the need for corporate and IT governance and also the study shows the use of information security policy and business continuity polices, demonstrating the importance of a security policy and its objective to minimize the impact on safety disaster and incidents, and finally, in the chapter regarding backup and restore are addressed important topics of how should store and handle a backup, and automatic tools to make security backups.

Keywords: *Backup; Information; Information Technology;*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BIA: *Business Impact Analysis*

CEO: *Chief Executive Officer*

CIO: *Chief Information Officer*

COBIT: *Control Objectives for Information and related Technology*

E-COMMERCE: *Eletronic Commerce*

FTP: *File Transfer Protocol*

GTI: Governança da Tecnologia da Informação

HD: *Hard Disk*

IBGC: Instituto Brasileiro de Governança Corporativa

ISACA: *Information Systems Audit na Control Association*

ITGI: *IT Governance Institute*

ITIL: *Information Technology Infrastructure Library*

OLA: *Operation Level Agreement*

PSI: Política de Segurança da Informação

SEFAZ: Secretaria da Fazenda

SI: Sistemas de Informação

SLA: *Service Level Agreement*

TCU: Tribunal de Contas da União

TI: Tecnologia da Informação

USB: *Universal Serial Bus*

SUMÁRIO

1 INTRODUÇÃO

Hoje em dia o bem mais importante de qualquer organização são as informações. As informações são de tal importância que uma empresa pode vir à falência caso ocorra perda de informação valiosa, como por exemplo, um banco que armazena milhares de contas de usuários e por algum motivo houve uma falha catastrófica no sistema e o banco perdeu todas as contas dos clientes e os valores depositados em cada uma. Outro exemplo é, quando se está fazendo um trabalho de conclusão de curso e por alguma razão o computador utilizado corrompeu o arquivo do trabalho de conclusão de curso e para piorar, isso aconteceu no dia da apresentação e aquela era a única cópia que tinha, como explicar para a banca que você não realizou o *backup* do trabalho de conclusão de curso e justo no dia da apresentação o computador corrompeu o arquivo? Isso seria um grande problema. Tomando estes exemplos como base, podemos observar quão importantes são as informações e uma política de *backup* para qualquer empresa, negócio, vida pessoal e acadêmica, Sêmola (2003, p. 47), afirma que:

> Todas as empresas, independente de seu segmento de mercado, em todas as fases de existência, sempre usufruem da informação como apoio à tomada de decisão para suas ações e seus planos.

Na grande maioria dos casos é praticamente impossível quantificar quanto custa uma informação em relação a uma quantia em dinheiro, pois a informação é tratada como um ativo intangível (ABREU, 2006).

A informação é fundamental para a empresa moderna. É por meio dela que se consegue ter uma situação de vantagem diante da concorrência (MAÑAS, 2007).

Conforme Dias (2000)

> Na sociedade da informação, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isto, a segurança de informações tornou-se um ponto crucial para a sobrevivência das instituições.

Por mais que se tenha o melhor *hardware* e s*oftware* do mercado não deve-se confiar que nunca ocorrerá uma falha no sistema ou no *hardware*, as falhas podem variar, desde uma falha no sistema a um acidente físico derrubando o *Hard Disk* (HD) no chão e perdendo as informações nele contidas ou até mesmo desastres naturais como incêndio, enchente, furacão entre outros desastres. Apesar de saber a importância do *backup* muitas empresas ainda deixam o *backup* em segundo plano, investindo seu dinheiro em *firewalls*, *hardware* de ponta, *software* entre outros sistemas de proteção, mas se esquecem que não são imunes a uma invasão hacker, ou desastres naturais, são poucas as empresas que dão realmente a importância necessária para o *backup*, algumas elaboram uma política de *backup* onde são salvas cópias de dados em diferentes lugares e lugares distantes um do outro para se protegerem de possíveis catástrofes ambientais ou até mesmo um atentado terrorista como aconteceu em 2001 o atentado que destruiu as torres gêmeas em Nova York levando consigo varias informações valiosas.

> Muitas pessoas, infelizmente, só percebem a importância de ter *backups* quando já é tarde demais, ou seja, quando os dados já foram perdidos e não se pode fazer mais nada para recuperá-los. *Backups* são extremamente importantes, pois permitem:
>
> Proteção de dados: você pode preservar seus dados para que sejam recuperados em situações como falhas de disco rígido, atualização mal sucedida do sistema operacional, exclusão ou substituição acidental de arquivos, ação de códigos maliciosos/atacantes e furto/perda de dispositivos.
>
> Recuperação de versões: você pode recuperar uma versão antiga de um arquivo alterado, como uma parte excluída de um texto editado ou a imagem original de uma foto manipulada.
>
> Arquivamento: você pode copiar ou mover dados que deseja ou que precisa guardar, mas que não são necessários no seu dia a dia e que raramente são alterados (CERT.br, 2012, p. 51-52).

O trabalho **justifica-se** pela importância do uso das informações pelas organizações, bem como a necessidade de ter um plano de continuidade de negócios, uma vez que problemas com perda de dados podem levar as organizações terem sérios problemas.

A política de *backup* em uma organização **justifica-se** pela importância que apresenta, se tratando de salvar informações de extrema importância nas organizações, evitando a perda de informações devido a possíveis desastres ambientais, falha de *software/hardware*, intervenções humanas com intenções de uso inapropriado das informações ou destruição destas informações, evitando assim possíveis desvantagens competitivas, perda do lucro ou a falência da organização.

O **problema** encontrado foi que muitas organizações principalmente as de pequeno porte e grande parte dos usuários de sistemas não dão a devida importância para o processo de *backup* das informações e com isto não estão preparados para se recuperarem de uma perda de informação ou incidentes de segurança. A **pergunta** que este trabalho busca responder é: Qual o grau de importância que as organizações estão dando para o *backup* e se estas organizações estão preparadas para continuarem seus serviços ou recuperarem as informações após um incidente.

As **hipóteses** encontradas foram que mesmo que as organizações e usuários saibam a importância do *backup,* e que confiem em seus equipamentos de *hardware* e *software,* eles não pensam que estes equipamentos e recursos podem falhar, sendo assim também não estão preparados para se recuperarem de um incidente de segurança ou perda de informação.

Este trabalho tem como **objetivo geral** alertar e conscientizar sobre a importância de *backup* e consequentemente sobre boas políticas de *backup* nas organizações, evitando perda de informações valiosas, mantendo estas informações armazenadas de forma segura.

Os **objetivos específicos** desta monografia são:

- Explicar a importância de uma gestão de TI dentro da organização, abordar alguns recursos tecnológicos e falar um pouco sobre governança de TI.
- Elaborar um questionário com o objetivo de coletar informações de como as empresas lidam com a importância de uma política de *backup*.
- Realizar um estudo de caso onde serão coletados os resultados do questionário aplicado e com base nestes dados coletados verificar se as organizações estão dando a devida importância para o *backup* e se estão preparadas para se recuperar de um incidente ou perda de informação.

No presente trabalho foram utilizados **métodos** de pesquisa e de análise qualitativa utilizando-se de um estudo de caso.

Para Godoy (1995, p.22), se tratando de pesquisa qualitativa existem três tipos, pesquisa documental, o estudo de caso e a etnografia.

Segundo Sampaio (2000, p.21), a pesquisa qualitativa “Envolve coletar, analisar e interpretar dados que não podem se significativamente quantificados, isto é, sumarizados em forma de números”.

Godoy afirma que em um documento deve conter materiais escritos como jornais, revistas, diários, obras literárias, científicas e técnicas, cartas, memorandos e relatórios.

Segundo Godoy (1995, p.26), um estudo de caso refere-se a:

> Técnicas fundamentais de pesquisa a observação e a entrevista.
> Produz relatórios que apresentam um estilo mais informal, narrativo, ilustrado com

> citações, exemplos e descrições fornecidas pelos sujeitos, podendo ainda utilizar fotos, desenhos, colagens ou qualquer outro tipo de material que o auxilie na transmissão do caso.

Foi elaborado um questionário utilizando-se da metodologia de análise gráfica/descritiva com base na escala de Likert de cinco pontos conforme Pereira (1999, p.77-83). Esta escala é representada pelos valores 1 considerado totalmente insatisfatório, 2 insatisfatório, 3 regularmente satisfatório, 4 satisfatório e 5 totalmente satisfatório.

Foram utilizados também a analise exploratória que por sua vez tem como suporte a estatística descritiva. Conforme Triviños (1987, p.109) os estudos exploratórios:

> Permitem ao investigador aumentar sua experiência em torno de determinado problema.
>
> O pesquisador parte de uma hipótese e aprofunda seu estudo nos limites de uma realidade específica, buscando antecedentes, maior conhecimento para, em seguida, planejar uma pesquisa descritiva ou de tipo experimental.

Para Levine *et al.* (2000, p.5) entende-se que a estatística descritiva pode ser descrita “Como os métodos que envolvem a coleta, a apresentação e a caracterização de um conjunto de dados de modo a descrever as várias características deste”.

2 REVISÃO DE LITERATURA

No presente capítulo aborda-se uma sistematização do referencial teórico que será utilizado neste trabalho. Dividido em 4 partes serão abordados os assuntos: Gestão na área de TI, Tecnologia da Informação, Governança de TI e Política de Segurança da Informação / Continuidade do negócio, procurando sempre colocar em foco o relacionamento entre os temas e destacar os aspectos relevantes para o desenvolvimento do estudo.

2.1 Gestão na área de TI

2.1.1 Conceito de Gestão

Nos dias de hoje o nível de complexidade dos negócios tem aumentado muito devido a globalização da economia, segundo Cordeiro José e Ribeiro Renato (2002)

> A partir da década de 1990 o ambiente de negócios se tornou mais complexo. Fenômenos econômicos e sociais de alcance mundial estão reestruturando o ambiente empresarial. A globalização da economia, alavancada pela tecnologia da informação e da comunicação, é uma realidade inescapável. As chamadas novas tecnologias, bem como as novas formas de organização do trabalho, têm colocado os métodos tradicionais de gestão no banco dos réus.

Nota-se que devido a tecnologia da informação e da comunicação a gestão passou por mudanças consideráveis no método de gerir as organizações, esta influência exercida pela tecnologia da informação (TI) e a tecnologia da comunicação tem afetado a realidade do negócio com o surgimento de novos concorrentes e um mercado cada vez mais competitivo com uma margem de erro cada vez menor. Portanto, a gestão se mostra cada vez mais importante no mercado atual pois sem ela uma organização não seria competitiva e organizada o suficiente para se manter em um ambiente de negócios tão competitivo.

Segundo Cordeiro José e Ribeiro (2002) o grande desafio da gestão desta década:

> Vem sendo a capacidade e a competência diária que as organizações enfrentam para se adaptarem e levarem a todos os seus níveis hierárquicos e funcionais, da alta gerência ao piso de fábrica, a incorporação de novos modelos, métodos, técnicas, instrumentos, atitudes e comportamentos necessários a mudanças, inovações e à sobrevivência sadia e competitiva no mercado.

Gerir é uma atividade muito mais complexa do que no passado, sendo assim um gestor tem que estar apto a se adequar as varias mudanças que o mercado impõe e então perceber o ambiente, refletir, decidir e agir, segundo Cordeiro José e Ribeiro Renato (2002) o dia a dia de um gestor envolve atualmente diferentes entradas em uma realidade uma realidade complexa, essas entradas são:

- Interdisciplinaridade – os processos de negócio envolvem equipes de diferentes áreas, perfis profissionais e linguagens;
- Complexidade – as situações carregam cada vez mais um número maior de variáveis;
- Exiguidade – o processo decisório está cada vez mais espremido em janelas curtas de tempo, e os prazos de ação/reação são cada vez mais exíguos;
- Multiculturalidade – o gestor está exposto a situações de trabalho com elementos externos ao seu ambiente nativo, e, por conseguinte com outras culturas, clientes, fornecedores, parceiros, terceiros, equipes de outras unidades organizacionais, inclusive do estrangeiro;
- Inovação – tanto as formas de gestão, quanto a tecnologia da informação e da comunicação, estão a oferecer constantemente novas oportunidades e ameaças;
- Competitividade – o ambiente de mercado é cada vez mais competitivo, não só em relação aos competidores tradicionais, mas principalmente pelos novos entrantes e produtos substitutos.

Segundo Mañas (2007)

> O gerenciamento de qualquer atividade empresarial inclui de fato a incumbência de um indivíduo, como pessoa, de gerenciar processos, cujos grandes objetivos são atingidos quando as necessidades de desempenho são atendidas.

Resumindo, hoje em dia a gestão de qualquer negócio exige muito mais do gestor por envolver uma velocidade muito maior na tomada de decisão e rápida adaptação ao mercado, com a chegada da tecnologia o gestor tem que estar sempre atento a novas estratégias para manter a organização competitiva no mercado, observando sempre seus concorrentes.

2.1.2 Gestão estratégica

A gestão estratégica é um modelo de gestão que tem por objetivo a analise organizacional com o mercado de atuação da organização, esta abordagem de gestão visa identificar oportunidades no mercado, ameaças, forças da organização bem como suas fraquezas, após esta análise autocrítica a organização em questão elabora uma estratégia com foco sobre a visão do futuro organizacional, missão da organização, desafios que o mercado irá impor ao sucesso organizacional e os planos de curto, médio e longo prazo.

Segundo Cordeiro José e Ribeiro Renato (2002)

> A utilização do modelo de gestão estratégica leva a empresa a realizar um diagnóstico situacional, destacando oportunidades e ameaças, bem como forças e fraquezas, a fim de cruzar estas realidades e descobrir suas inter-relações.

Lobato *et al* também cita que a gestão estratégica deve apresentar as seguintes características:

> Visão estratégica, alinhamento com a missão da empresa, adaptação à tendência de globalização, domínio da tecnologia de informação e compreensão das mudanças como fator de oportunidade.

A adoção da gestão estratégica ajuda a organização compreender o mercado atual, as oportunidades e diminuir o risco de fracasso em algum investimento, obtendo assim a competitividade estratégica e vantagem competitiva.

Obtém-se competitividade estratégica quando uma empresa consegue formular e implantar com sucesso uma estratégia de criação de valor. Uma estratégia é um conjunto integrado e coordenado de compromissos e ações definido para explorar competências essenciais e obter vantagem competitiva. (IRELAND MICHAEL; HOSKISSON ROBERT, 2008).

Segundo Ireland Michael e Hoskisson Robert (2008)

> Uma empresa só tem vantagem competitiva quando é implementada uma estratégia que os concorrentes não conseguem copiar ou acham custosa demais para imitar e nenhuma vantagem competitiva é permanente, pois o que determina quanto tempo durará a vantagem competitiva é a velocidade com que os concorrentes conseguem adquirir habilidade para duplicar os benefícios de uma estratégia de criação de valor.

Em suma a gestão estratégica deve ser trabalhada de forma cuidadosa, pois ela norteia o futuro da organização, analisando os pontos fortes, fracos, oportunidades no mercado e o futuro da organização com os planos de curto, médio e longo prazo.

2.1.3 Tecnologia da Informação nas Organizações

Na era da informação onde vivemos dentro de um mundo globalizado a Tecnologia da Informação (TI) vem sendo uma ferramenta indispensável para qualquer organização que visa se manter competitiva no mercado atual.

A relação da TI com a organização pode ser notada pela influência que a organização exerce sobre a TI moldando-a de acordo com suas estratégias organizacionais. Nota-se a contribuição da TI para os processos organizacionais da empresa.

Conforme Chiavenato (2003)

> Agora no mundo do e-business, tecnologia tem outro significado: ela é o próprio ambiente de negócio em que vão aparecer as oportunidades e no qual serão realizadas as transações.

Segundo Hatch (1997) as organizações são frequentemente conceituadas como tecnologias, culturas e estruturas sociais e físicas que exercem influência entre si dentro do contexto de ambiente.

Conforme citado por Hatch observa-se que se tratando de organização nenhum conceito ou teoria é completo por si próprio e que a combinação de alguns conceitos traria uma visão mais enriquecedora para uma organização.

Com o passar do tempo observando este conceito de organização alguns pesquisadores desenvolveram modelos de TI que tinha como objetivo medir a influência da TI nas organizações. A ação humana é o aspecto central desses modelos, em particular as ações associadas com as estruturas embutidas dentro de uma tecnologia durante seu desenvolvimento, além das ações associadas com a aprovação dessas estruturas durante o isso da tecnologia (ORLIKOWSKI, 2000).

Segundo Albertin & Albertin (2010)

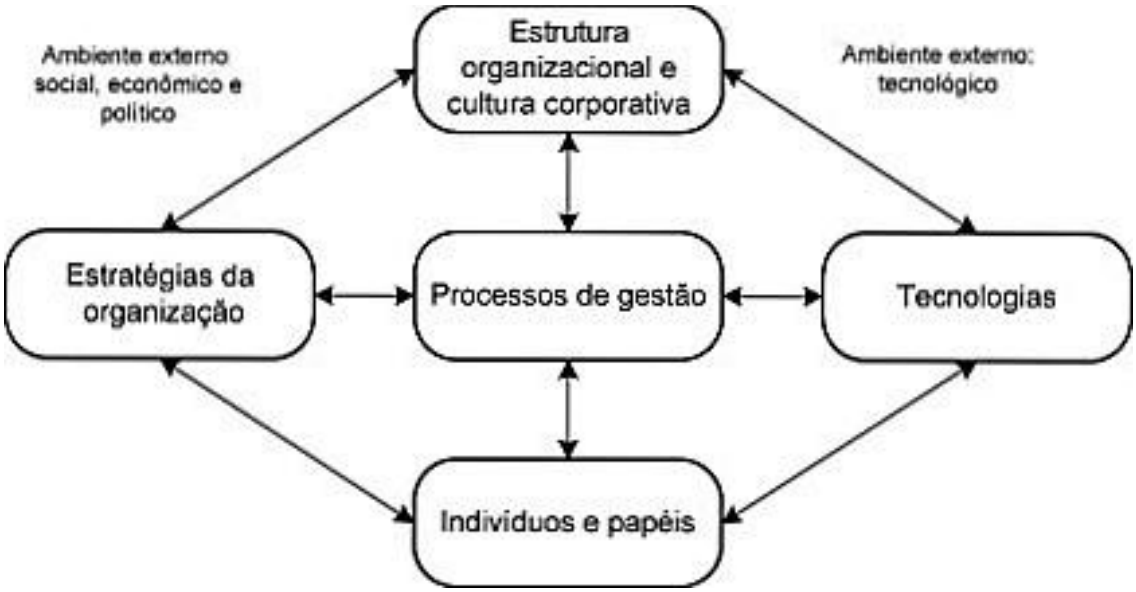
> Num cenário cada vez mais competitivo e de exigências para agilidade e inovação, a informação toma-se em aliado decisivo nas estratégias das organizações, com isso, o papel da TI tornou-se imprescindível para os objetivos e as aplicações de uma organização e, consequentemente, como forma de atuação e vantagem competitiva.

Percebendo quão importante é a TI para os negócios, as organizações adotaram o alinhamento estratégico organizacional com a TI buscando vantagens como tomada de decisão e custo benefício otimizados.

Os três principais elementos de um ambiente organizacional em que a TI atua são: a rede interorganizacional, o ambiente em geral e o ambiente global e internacional (ALBERTIN; ALBERTIN, 2010).

O modelo de Rockart e Scott Morton ajuda a entender um pouco sobre estes elementos.

Figura 1 - Modelo de alinhamento de Rockart e Scott Morton (1984)



Fonte: Rockart e Morton

Uma organização é influenciada pelo seu ambiente externo que é composto por clientes, fornecedores, parceiros, estruturas diversas entre outros elementos, já que este ambiente é responsável diretamente pelo sucesso da organização.

Os ambientes interno e externos definem a estratégia, objetivo e metas da organização. Estas estratégias serão elaboradas pela estrutura organizacional, que formará a cultura corporativa. Os processos de gestão devem verificar se os processos e indivíduos estão de acordo com a estrutura organizacional.

McFarlan, McKenney e Pyburn (1983) apontam a importância de identificar o ambiente onde se encontra a organização para se ter uma ideia da complexidade e tamanho das aplicações de Sistemas de Informação (SI), permitindo assim uma melhor administração e desempenho. Após definir a complexidade da organização e do mercado onde a empresa se encontra é possível encontrar vários ambientes em uma mesma organização, os autores definiram quatro ambientes:

- **Estratégico:** intensa dependência da perfeita funcionalidade das atividades de SI e aplicações em desenvolvimento vitais para a sua competitividade;
- **Reviravolta:** pouca dependência das funcionalidades de SI, porém altamente dependente das aplicações em desenvolvimentos que são estratégicas para a organização;

- **Fábrica:** alta dependência das funcionalidades de SI, porém baixa dependência das aplicações em desenvolvimento;
- **Suporte:** baixa dependência das funcionalidades de SI e das aplicações em desenvolvimento, o que denota pouco peso estratégico ou operacional na carteira completa de SI.

Segundo Albertin & Albertin (2010), estes ambientes precisam ser considerados tanto no papel da TI no negócio quanto nas definições estratégicas e priorização da carteira de TI.

Rockart, Earl e Ross (1996), em artigo sobre organização de TI, desenvolveram oito imperativos que devem ser praticados para alcançar a excelência da TI e sua efetividade nas organizações, são eles:

- Realização do alinhamento estratégico entre negócios e TI, para garantir que as iniciativas estejam alinhadas;
- Desenvolvimento de relacionamento eficaz entre os gestores do negócio e o CIO, pois essa comunicação irá garantir a integração das capacidades dessas áreas;
- Entrega e implementação de novos sistemas abordando a integração e compras de soluções;
- Criação e gerenciamento da infraestrutura, estabelecendo-se padrões e comunicando-se o valor desta infraestrutura para operá-la de forma eficiente;
- Redução dos profissionais de TI, visando a competências voltadas para o negócio;
- Gerenciamento de parcerias com fornecedores, nas quais os CIOs sejam negociadores informados;
- Criação e manutenção de TI com alto desempenho, procurando-se superar os objetivos de desempenho definidos;
- Redesenho e gerenciamento de TI através de políticas, padrões, critérios e normas bem definidos e comunicados para toda a organização, definindo-se o processo de decisão e distribuição de responsabilidades.

Segundo Albertin & Albertin (2010), estes imperativos estão diretamente ligados aos aspectos de sustentação de objetivos, tomada de decisão e definições de responsabilidades.

Resumidamente o uso da tecnologia da informação nas organizações é influenciado por fatores sociais, culturais, econômicos e técnicos, esses fatores determinaram a relação da organização com a TI. Alguns modelos definem a influência da TI na organização, sendo que todos estes modelos tem como centro a ação humana. Sabendo da importância da TI para o sucesso da organização, os responsáveis por gerir a empresa procuram alinhar seus objetivos na TI no contexto interno e externo, tendo ciência que a usabilidade de TI exige diferentes considerações, pois trabalha com características e ambientes distintos. A excelência na área de TI deve ser almejada por meio de imperativos de sua administração e governança.

2.2 Tecnologia da Informação e seus recursos

A Tecnologia da informação se mostra essencial não apenas para manter a empresa competitiva, mas também para não prejudicar a organização em sua área financeira, pois uma TI mal gerenciada seria capaz de gerar grandes perdas financeiras para a organização, sendo assim nota-se que as empresas nos dias atuais criaram uma grande dependência dos serviços de TI.

Segundo Albertin & Albertin (2010)

> As organizações usam a TI para gerenciar, desenvolver e comunicar ativos intangíveis, principalmente numa economia voltada para o conhecimento. Esse uso gera um aumento significativo na dependência da TI e também amplia a vulnerabilidade que é inerente a ambientes de TI complexos.

Um exemplo de dependência das organizações dos serviços de TI é uma organização que utiliza do *eletronic commerce* (E-commerce), que em português significa comércio eletrônico, este tipo de comércio utiliza-se de meios tecnológicos como lojas virtuais para realizar suas transações de vendas. Supondo-se que uma organização que dependa deste tipo de serviço fique com o servidor fora do ar por algumas horas, isso acarretaria em perdas financeiras grandes para esta organização. Outro exemplo é se as informações de transações fossem perdidas por falha em uma política de *backup*, a organização não saberia mais sobre seus títulos de contas a pagar e a receber, isso traria danos incalculáveis para a organização, trazendo em muitos casos a falência da empresa.

Magalhães e Pinheiro (2007),citam uma pesquisa realizada pelo *Gartner Group, Inc*., apresentada por Donna Scott em sua palestra *Operation Zero Downtime*, em maio de 2002, que afirma que 80% das causas de paralisação de serviços de TI são:

- Aplicações não testadas.
- Má gerência de mudanças.

- Sobrecarga de processamento.
- Falhas em procedimento.
- Falhas no cumprimento de requisitos.
- Erros relacionados à segurança ou às rotinas de *backup*.

Para ilustrar melhor esta dependência das organizações, Magalhães e Pinheiro (2007) cita alguns exemplos de prejuízos causados pela falha dos serviços de TI bem como o valor por hora de interrupção dos serviços de TI.

Tabela 1 - Organizações prejudicadas por falhas em serviços de TI

AT&T	Abril de 1998	A atualização da versão do sistema prevista para ser realizada em 6 horas, levou 26 horas, custo de US$ 40 milhões em desconto nas faturas de serviço devido ao não-cumprimento de acordos de nível de serviço celebrados com os seus clientes finais.
eBay	Junho de 1999	Indisponibilidade durante 22 horas devido à falha no sistema. Custo estimado entre US$ 3 e 5 milhões em receitas e declínio de 26% no valor de ações.
Hershey's	Setembro de 1999	Falhas no sistema devido à estratégia de implementação de nova versão. Custo não-estimado com o atraso no envio de encomendas, 12% de redução nas vendas do trimestre e diminuição de 19% no lucro líquido do trimestre em relação ao mesmo período do ano anterior.

Magalhães; Pinheiro, 2007

Tabela 2 - Valor por hora de interrupção dos serviços de TI

Indústria	Serviços	Custo médio por hora de interrupção do serviço (US$)
Financeira	Operação de corretagem	7.840.000
Financeira	Vendas por cartão de crédito	3.160.000
Mídia	Venda por *pay-per-view*	183.000
Varejo	Vendas pela TV	137.000
Varejo	Vendas por catálogo	109.000
Transportes	Reservas aéreas	108.000
Entretenimento	Venda de ingressos por telefone	83.000
Entregas rápidas	Entrega de encomendas	34.000
Financeira	Pagamento de taxas via ATM (*Automatic Teller Machine*)	18.000

Magalhães; Pinheiro, 2007

Pode se notar que é preciso não só ter a TI em uma organização, mas também saber gerencia-la para aumentar a qualidade dos serviços prestados, evitando-se a ocorrência de erros e paralisação de serviços.

2.2.1 Benefícios da TI

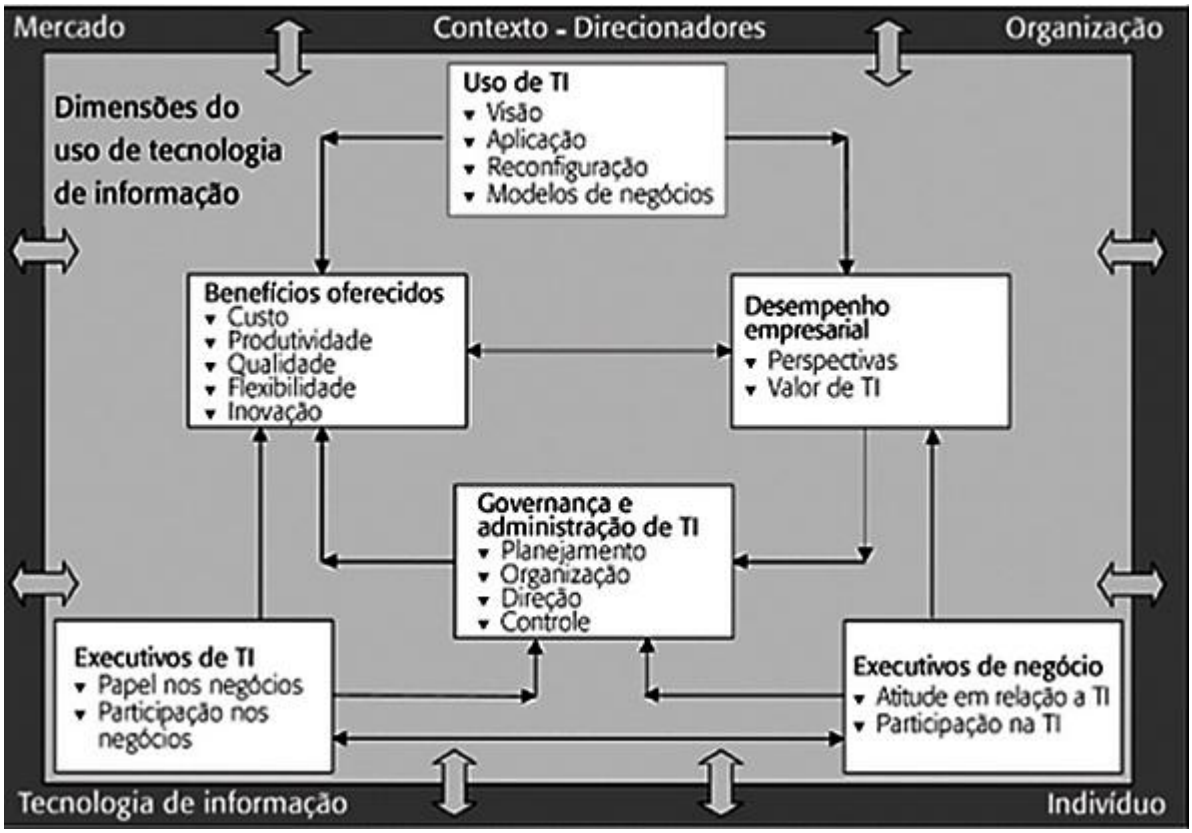
No mundo atual, onde a informação é o bem mais valioso de uma organização conforme já falado no primeiro capítulo por autores citados, a tecnologia da informação não deixa de ser de extrema importância para os objetivos estratégicos organizacionais. Se bem alinhada com as estratégias organizacionais e bem gerenciada, a TI pode maximizar o lucro da organização, otimizar tarefas e mantendo a organização competitiva sempre mostrando novas oportunidades de mercado.

Segundo Albertin (2003, *apud* ALBERTIN; ALBERTIN, 2010, p.4):

> O uso da TI deve ser entendido por meio de suas dimensões, que incluem o contexto com seus direcionadores, os tipos de uso da TI, o desempenho empresarial, a Governança de TI e os executivos de negócio e de TI, bem como a relação que existe entre elas.

Essas dimensões são representadas a seguir no modelo das dimensões do uso da TI em benefício dos negócios.

Figura 2 - Modelo de dimensões do uso da TI em benefício dos negócios



Fonte: Albertin & Albertin, 2009, p.95

O modelo apresentado mostra a influência da governança da tecnologia da informação (GTI) na organização em termos de desempenho e benefícios, a GTI oferece não só apenas um acompanhamento e medição do desempenho, como também alinha a TI com as estratégias de negócio organizacional, definindo papéis e entregas de valor internas e externas.

Murphy (2002, *apud* ALBERTIN; ALBERTIN, 2010, p.5), afirma que as medidas financeiras nem sempre são o suficiente para analisar o desempenho organizacional e justificar um investimento em TI. O autor afirma que a empresa precisa de uma análise minuciosa, levando em consideração várias direcionadores que contribuem para um maior desempenho e alcance das metas estratégicas. Embasado nesta necessidade o autor define cinco pilares para realização de benefícios da TI, este pilares são:

- **Alinhamento estratégico:** o alinhamento estratégico de investimento em Ti, como o atingimento de metas e objetivos do negócio da empresa;
- **Impacto nos processos de negócio:** impacto nos requisitos para desenho de processos de negócio, mas especificamente na integração de cadeia de valor;
- **Arquitetura:** integração, escalabilidade e elasticidade de aplicações, sistemas operacionais, banco de dados e redes que a organização tem ou planeja implementar;
- **Retorno direto:** o entendimento dos benefícios que um projeto de TI pode oferecer;
- **Risco:** identificação dos investimentos propostos que podem apresentar falhas ou um desempenho abaixo do desejado.

2.2.2 Recursos de TI

As organizações hoje em dia costumam utilizar cada vez mais os recursos de TI, ou para se promover através de redes sociais ou para atingir metas estratégicas. Um recurso de TI pode ser tomado como aplicativos que são utilizados como ferramentas para automatizar uma tarefa, informação que provem de um processamento de dados de um sistema de informação, infra-estrutura como *hardware*, sistemas operacionais mídias utilizadas para realizar *backup* entre outras coisas e as pessoas que são contratadas para manter os serviços de TI em condições de atender a organização estrategicamente.

Segundo Magalhães e Pinheiro (2007), uma possível definição de TI é:

> Um conjunto de recursos, TI e não-TI, mantidos por um provedor de TI, cujo objetivo é satisfazer uma ou mais necessidades de um cliente (áreas de

> negócio) e suportar os objetivos estratégicos do negócio de cliente, sendo percebido pelo cliente como um todo coerente.

Com base na definição de Magalhães e Pinheiro (2007) sobre TI, pode-se dizer que recursos da TI vão de hardware, software à serviços da TI bem como normas de gerenciamento da TI.

A *Information Technology Infrastructure Library* (ITIL) define um serviço de TI como “um ou mais sistemas de TI que habilitam um processo de negócio”. Deve-se levar em consideração que um sistema de TI envolve *hardware*, *software*, processo e pessoas.

2.2.2.1 Serviços

Hoje em dia a maioria das organizações que trabalham com a TI, se não todas, prestam algum tipo de serviço seja para o cliente (serviço externo) ou para a própria organização (serviço interno). Como exemplo de serviço externo pode-se citar uma organização que desenvolve um sistema para atender o usuário em emissão de notas fiscais para a SEFAZ (Secretaria da Fazenda) e oferece suporte para os clientes para manter este sistema em funcionamento caso ocorra alguma inconsistência no sistema. Como exemplo de serviço interno pode-se citar o suporte que a área responsável pelo funcionamento dos computadores oferece quando alguma maquina apresenta algum tipo de problema. Estes são apenas alguns exemplos de serviços, tais serviços são muito importantes para organização manter-se no mercado, os serviços podem ser caracterizados como algo intangível.

Conforme Magalhães e Pinheiro (2007) pode-se entender que:

> Um serviço é uma ação executada por alguém ou por alguma coisa, caracterizando-se por ser uma experiência intangível, produzido ao mesmo tempo em que é consumido, não podendo ser armazenado, e apresentando sérias dificuldades para ser produzido em massa ou atender mercados de massa.

A intangibilidade de um serviço significa que os serviços não podem ser apalpados, provados, cheirados ou observados. Um exemplo de serviço seria um simples corte de cabelo, você não consegue ver os resultados antes do serviço ser realizado.

Se tratando de serviços de TI e seu ciclo de vida os autores Magalhães e Pinheiro (2007) afirmam que em cada uma das fases do ciclo de vida de um serviço

devem ser feitas e respondidas varias perguntas de modo a acompanhar o ciclo da vida do serviço, tais perguntas são:

Fase de requisição

- Qual é o serviço necessário?
- Por que ele é necessário?
- Qual a quantidade demandada?

Fase de aquisição

- Onde o serviço será solicitado?
- Onde o serviço será provido?
- Quando será pago pelo serviço?

Fase de atualização

- Como o serviço será usado?
- Como validar o serviço provido?
- Como o serviço será restabelecido em caso de falha?

Fase de desativação

- Quanto esta sendo gasto para manter o serviço?
- Qual o retorno que o serviço proporcionou?
- Há uma nova opção?

2.2.2.2 Definição do valor de um serviço de TI

Para definir o valor de um serviço de TI deve-se levar em conta alguns fatores como a disponibilidade, alinhamento, estratégico e habilidade para se moldar conforme o ambiente de atuação. A seguir tem-se alguns parâmetros utilizados para definir o valor de um serviço de TI.

Conforme Magalhães e Pinheiro (2007) o serviço de TI pode ser medido por quatro parâmetros.

- Alinhamento estratégico com o negócio – Grau em que o serviço de TI está alinhado com as atuais e as futuras necessidades do negócio.
- Custo – Valor monetário desembolsado pela disponibilização do serviço de TI e em cada interação.
- Qualidade – Nível de atendimento do serviço de TI em relação aos acordos de nível de serviço, *Service Level Agreement* (SLA), e acordos de nível operacional, *Operational Level Agreement* (OLA), estabelecidos externa e internamente à área de TI, respectivamente.
- Independência em relação ao tempo – Capacidade da área de TI em reagir à demandas de suporte e em atender às mudanças planejadas em relação ao serviço de TI disponibilizado.

O autor enfatiza que para a maximização dos valores dos serviços de TI deve envolver a integração dos diferentes componentes de um serviço de TI (pessoas, processos e tecnologia) bem como os objetivos estratégicos fixados pela organização, conforme ilustração.

Figura 3 - Integração entre os componentes de um serviço de TI

Fonte: Magalhães e Pinheiro, 2007

2.2.3 Alinhamento estratégico

O alinhamento da TI com a estratégia da organização é importante para o sucesso da organização no mercado com alguns exemplos citados nos tópicos anteriores, sem esse alinhamento a TI será apenas uma fornecedora de tecnologia não interferindo na estratégia da empresa.

Conforme Albertin & Albertin (2010), o alinhamento estratégico entre o negócio e TI deve ser aplicado como uma ferramenta de gestão, buscando uma ligação entre estas áreas através de uma integração de seus planos estratégicos. O autor ainda afirma que o sucesso do desenvolvimento e da implementação dos sistemas de informação deve-se ao relacionamento de TI e negócios.

O alinhamento estratégico é um dos cinco pilares da GTI como apresentado na figura abaixo:

Figura 4 - Domínios da Governança de TI

Fonte: *IT Governance Institute*

Segundo Saccol e Brodbeck (2004, *apud* ALBERTIN; ALBERTIN, 2010 p.23), o alinhamento estratégico está fortemente ligado à estrutura, estratégia, cultura e aos níveis organizacionais. Além desses elementos, tem-se um cenário no qual a necessidade do mercado exige que as organizações tenham maior flexibilidade, e os executivos de TI e negócios precisam adequar capacidades, habilidades e competências.

Resumidamente, o papel da TI em uma organização é otimizar as atividades econômicas, através do alinhamento de negócios em prol da vantagem competitiva. Para ajudar no alinhamento de negócios existem algumas normas ditas como melhores praticas que auxiliam em todo o processo. Um dos principais objetivos da TI nos negócios é maximizar o retorno investido.

Neste novo cenário onde a informação e a tomada de decisão podem fazer toda a diferença no futuro organizacional, a TI entra com seus recursos para otimizar as tomadas de decisões, diminuindo chances de erros estratégicos e mantendo a organização competitiva.

2.3 Governança Corporativa

A governança corporativa surgiu do aumento da complexidade dos negócios e da necessidade de transparência nos negócios para atrair investidores.

A governança corporativa é composta por um conjunto de práticas. A adoção da governança corporativa teve aumento significativo em 2001 após um escândalo financeiro da empresa norte americana Enron que fraudava suas demonstrações financeiras para encobrir os prejuízos obtidos, causando assim a perda de investimentos dos acionistas. Após este escândalo muitas empresas adotaram a governança corporativa como meio de transparência para atrair acionistas e, consequentemente, investimentos para a organização.

Segundo o Instituto Brasileiro de Governança Corporativa (IBGC), a governança corporativa é definida como:

> O sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle.
>
> As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.

O IBGC também cita os princípios da governança corporativa, que são:

- **Transparência:** que é a disponibilidade das informações para as partes interessadas. Esse princípio resulta em um clima de confiança, tanto internamente quanto para terceiros.

- **Equidade:** que caracteriza-se pelo tratamento justo de todas as partes envolvidas no negócio.
- **Prestação de contas:** que associados, conselheiros, executivos, fiscais e auditores devem prestar contas de sua atuação se responsabilizando pelos seus atos.
- **Responsabilidade:** que é o zelo pela sustentabilidade das organizações, buscando sua perenidade.

2.4 Governança de Tecnologia da Informação

O papel da GTI dentro de uma organização é basicamente receber os requisitos necessários dados pela organização para atender os objetivos de negócio, alinhar a TI com os objetivos da organização, ampliando seus lucros, buscando sempre os melhores resultados, visando oportunidades no mercado e mantendo a organização competitiva.

Nos dias de hoje onde a informação é um bem cada vez mais importante dentro da corporação, gerenciá-la é muito importante para manter a organização competitiva. Com este objetivo nasceu a GTI para governar de forma estratégica a TI.

O *IT Governance Institute* (2005) define a GTI como “responsabilidade da alta administração, na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização”.

Conforme Weill e Ross (2004), a GTI é “Modelo que define direitos e responsabilidades pelas decisões que encorajam comportamentos desejáveis no uso de TI”

Outra definição da GTI é: processos pelo qual decisões são tomadas sobre os investimentos em TI, o que envolve: como decisões são tomadas quem toma as decisões, que é responsabilizado e como os resultados são medidos e monitorados (FORRESTER RESEARCH, 2006).

Van Grembergen (2004), afirma que a GTI é “Capacidade organizacional exercida pela alta direção, gerência de negócios e gerência de TI para controlar a

formulação e implementação da estratégia de TI e, com isso. Assegurar o alinhamento entre negócios e TI".

Os resultados da TI precisam também ser medidos e avaliados de forma que a organização possa verificar o retorno de seus investimentos e tomar decisões sobre novas oportunidades de negócio e estratégias de mudanças (WEILL; WOODHAM, 2002). O aspecto crítico para que se garantam esses resultados é a participação da alta gerência em todo o processo, principalmente na identificação de indicadores necessários para essas avaliações (ALBERTIN, 2003).

Segundo Albertin e Albertin (2010)

> A GTI apresenta dentro da organização uma forma de tratar a TI de forma colegiada em que a área de negócio participa das principais definições estratégicas e é responsável pela tomada de decisão. Dessa forma, pode-se garantir uma maior efetividade da TI e principalmente um reflexo no desempenho empresarial através de entrega de valor adequada aos requerimentos organizacionais.

Os autores Fernandes e Abreu (2012) apresentam o ciclo da governança de TI que composto por quatro etapas.

Figura 5 - Ciclo da Governança de TI

Fonte: Fernandes e Abreu, 2012

Estas etapas são:

O alinhamento estratégico e *compliance* referem-se ao planejamento estratégico da tecnologia da informação que leva em consideração as estratégias da empresa para seus vários produtos e segmentos de atuação, assim como os requisitos de *compliance* externos.

A etapa de decisão, compromisso, priorização e alocação de recursos refere-se às responsabilidades pelas decisões relativas à TI em termos de: arquitetura de TI, serviços de infraestrutura, investimentos, necessidades de aplicações, etc., assim como a definição dos mecanismos de decisão, ou seja, em que fóruns da empresa são tomadas essas decisões.

Adicionalmente, trata da obtenção do envolvimento dos tomadores de decisão chaves da organização, assim como da definição de prioridade de projetos e serviços e da alocação efetividade recursos monetários no contexto de um portfólio de TI.

A etapa de estrutura, processos, operação e gestão refere-se à estrutura organizacional e funcional de TI, aos processos de gestão e operação dos produtos e serviços de TI, alinhados com as necessidades estratégicas e operacionais da empresa. Nesta fase são definidas ou redefinidas as operações de sistemas, infraestrutura, suporte técnico, segurança da informação, governança de TI e outras funções auxiliares ao CIO, etc.

A etapa de gestão do valor e do desempenho refere-se à determinada, coleta e geração de indicadores de resultados dos processos, produtos e serviços de TI, à sua contribuição para as estratégias e objetivos do negócio e à demonstração do valor de TI para o negócio.

2.4.1 Diferença entre Gestão de TI e Governança de TI

Quando se trata de governança de TI e gestão de TI, as características que definem a diferença entre elas é que a governança de TI se trata de algo mais abrangente com foco em responder a pergunta de “O que fazer?”. Ela é responsável por atender as demandas atuais e futuras da organização e seus clientes, implantando políticas de uso, estratégias e monitoramento da TI. Quando se trata de gestão da TI o foco é responder a pergunta de “Como fazer?”. A gestão de TI é mais focada no gerenciamento das operações atuais da organização e em ofertas de

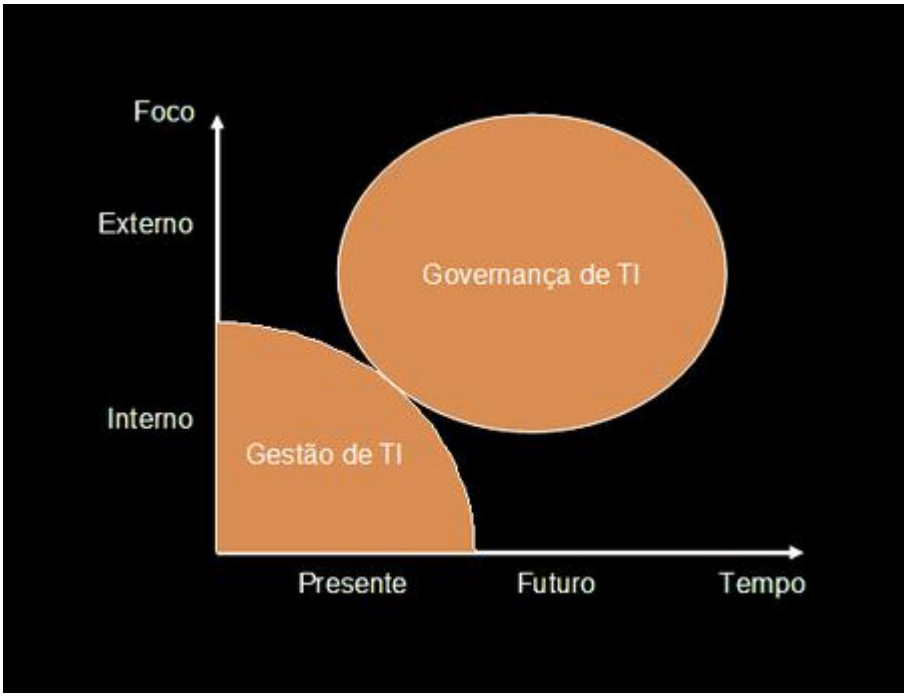
produtos e serviços, focando em gerenciar os serviços operacionais, bem como atuar no planejamento e construção destas atividades.

As ações da gestão de TI são baseadas na estratégia organizacional formal e estável, sendo que a responsabilidade da implementação e desenvolvimento destas estratégias são da direção corporativa. Por outro lado, a direção deve entender e gerenciar os riscos operacionais ou estratégicos, associados aos investimentos de TI, considerando o custo e abrangência do negócio (JORDAN; MUSSON, 2004).

Os autores Albertin & Albertin (2010), definem a gestão de TI com o foco em suprir internamente e de forma efetiva os serviços e produtos de TI e em gerenciar as operações atuais de TI.

Peterson R. (2004) define a GTI como algo mais abrangente que se concentra em desenvolver e transformar a TI para atender às demandas de negócios não só atuais como futuras com (foco interno) e dos clientes do negócio (foco externo).

Figura 6 - Governança de TI e Gestão de TI



Fonte: Van Grembergen, 2004

De acordo com o Tribunal de Contas da União (TCU):

> Pode-se pensar, erroneamente, que a Governança Corporativa não tem relação com a Governança e TI e que esta não tem relação com a Gestão/Gerenciamento de TI. Entretanto, o que de fato ocorre é uma dependência entre elas. O gerenciamento de serviços de TI é, de fato, em

> *enabler* (facilitador) da governança de TI e esta é um facilitador da governança corporativa.

A figura abaixo ilustra esta dependência:

Figura 7 - Dependências da Governança Organizacional

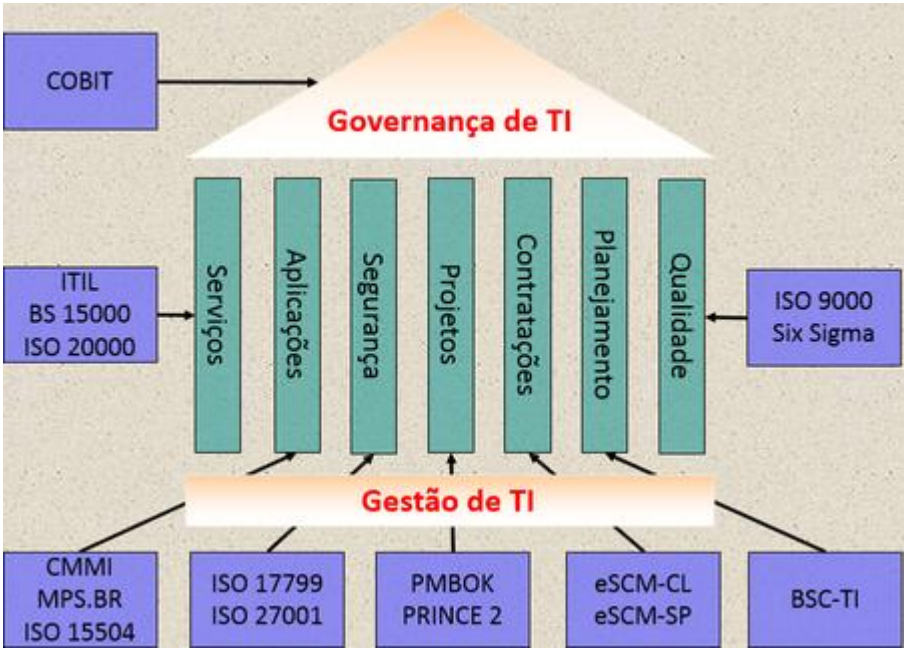
Fonte: Celta Informática. Disponível em:< www.celtainformatica.com.br>

Com base nas referencias abordadas nota-se que não é possível ter uma boa governança corporativa sem uma governança de TI, bem como não é possível ter uma governança de TI sem um gerenciamento de TI adequado.

2.4.2 Modelos de administração da GTI

A governança de TI é implementada na organização como um facilitador da governança corporativa, a GTI utiliza-se de modelos de administração para implementar e monitorar o ambiente de TI. Entre estes métodos, os mais comuns são os *Control Objectives for Information and related Technology* (COBIT) e o *Information Technology Infraestructure Libery* (ITIL).

Figura 8 - Modelos para Gestão e Governança de TI



Fonte: Pink Elephant, 2005

2.4.2.1 COBIT

O COBIT é um *framework* desenvolvido pela *Information System Audit na Control Association* (ISACA) uma organização sem fins lucrativos que é utilizada na governança da TI para otimizá-la, diminuindo os riscos, garantindo entrega de serviço de qualidade e a constante monitoração das atividades de TI.

Segundo o documento do COBIT 5 disponibilizado pela ISAC (2012) o COBIT se baseia em 5 princípios para governança e gestão de TI da organização.

Primeiro princípio: Atender às necessidades das partes interessadas – Organizações existem para criar valor para suas partes interessadas mantendo o equilíbrio entre a realização de benefícios e a otimização do risco e uso dos recursos. O COBIT 5 fornece todos os processos necessários e demais habilitadores para apoiar a criação de valor para a organização com o uso de TI. Como cada organização tem objetivos diferentes, o COBIT 5 pode ser personalizado de forma a adequá-lo ao seu próprio contexto por meio da cascata de objetivos, ou seja, traduzindo os objetivos corporativos em alto nível em objetivos de TI específicos e gerenciáveis, mapeando-os em práticas e processos específicos.

Segundo princípio: Cobrir a Organização de ponta a ponta – O COBIT 5 integra a governança corporativa de TI organização à governança corporativa: Cobre

todas as funções e processos corporativos; O COBIT 5 não se concentra somente na função de TI, mas considera a tecnologia da informação e tecnologias relacionadas como ativos que devem se tratados como qualquer outro ativo por todos na organização. Considera todos os habilitadores de governança e gestão de TI aplicáveis em toda a organização, de ponta a ponta, ou seja, incluindo tudo e todos – interna e externamente que forem considerados relevantes para a governança e gestão das informações e de TI da organização.

Terceiro princípio: Aplicar um modelo único integrado – Há muitas normas e boas práticas relacionadas a TI, cada qual provê orientações para um conjunto específico de atividade de TI. O COBIT 5 se alinha a outros padrões e modelos importantes em um alto nível e, portanto, pode servir como um modelo unificado para a governança e gestão de TI da organização.

Quarto princípio: Permitir uma abordagem holística – Governança e gestão eficiente e eficaz de TI da organização requer uma abordagem holística, levando em conta seus diversos componentes interligados. O COBIT 5 define um conjunto de habilitadores para apoiar a implementação de um sistema abrangente de gestão e governança de TI da organização. Habilitadores são geralmente definidos como qualquer coisa que possa ajudar a atingir os objetivos corporativos. O modelo do COBIT 5 define sete categorias de habilitadores:

- Princípios, Políticas e Modelos
- Processos
- Estruturas Organizacionais
- Cultura, Ética e Comportamento
- Informação
- Serviços, Infraestrutura e Aplicativos
- Pessoas, Habilidades e Competências

Quinto princípio: Distinguir a Governança da Gestão – O modelo do COBIT 5 faz uma clara distinção entre governança e gestão. Essas duas disciplinas compreendem diferentes tipos de atividades, exigem modelos organizacionais diferenciadas e servem a propósitos diferentes. A visão do COBIT 5 sobre esta importante distinção entre governança e gestão é:

- **Governança**

A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos.

Na maioria das organizações, a governança geral é de responsabilidade do conselho de administração sob a liderança do presidente. Responsabilidades de governança específicas podem ser delegadas a modelos organizacionais especiais no nível adequado, especialmente em organizações complexas de grande porte.

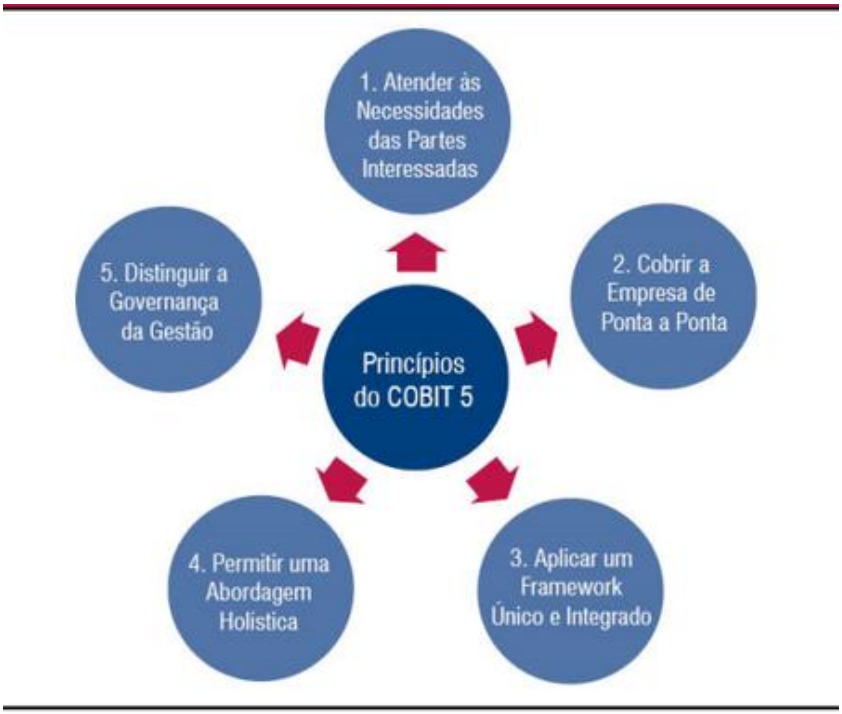
- **Gestão**

A gestão é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades em consonância com a direção definida pelo órgão de governança a fim de atingir os objetivos corporativos.

Na maioria das organizações, a gestão é de responsabilidade da diretoria executiva sob a liderança do diretor executivo (CEO).

Juntos, esses cinco princípios permitem que a organização crie um modelo eficiente de governança e gestão otimizando os investimentos em tecnologia da informação e seu uso para o benefício das partes interessadas.

Figura 9 - Princípios do COBIT 5



Fonte: COBIT 5, 2012

Nota-se que o COBIT pode ser personalizado para se adequar a necessidade da organização, não necessariamente ao utilizar o *framework* COBIT tende-se utilizar todas as suas normas de boas praticas. Esta norma de boas práticas atenta-se em atender as partes interessadas, criando valores, otimizando riscos e uso dos recursos, bem como trazer benefícios para organização. O COBIT trata a organização de uma forma abrangente cobrindo-a de ponta a ponta como citado em seu segundo princípio e distinguindo a Gestão da Governança.

2.4.2.2 ITIL

A *Information Technology Infrastructure Library* (ITIL) constitui-se de boas praticas com foco em gerenciamento de serviços de TI, este modelo é utilizado para ajudar a entrega de serviços de alta qualidade e diminuir os custos de TI, focando a maturidade da organização no uso eficaz e eficiente das ferramentas e ativos de TI.

Segundo Fernandes e Abreu (2012) a ITIL é definida como

> Agrupamento de melhores práticas utilizadas para o gerenciamento de serviços de tecnologia de informação de alta qualidade, obtidas em consenso após décadas de observação prática, pesquisa e trabalho de profissionais de TI e processamento de dados em todo o mundo.

Magalhães e Pinheiro (2007) afirmam que a ITIL é:

> Composta por um conjunto de melhores práticas para a definição dos processos necessários para o funcionamento de uma área de TI, com o objetivo de permitir o máximo de alinhamento entre a área de TI e as demais áreas do negócio, de modo a garantir a geração de valor à organização.

Albertin & Albertin (2010) afirma que a ITIL

> Provê uma estrutura de melhores práticas de diretrizes para o gerenciamento de serviços de TI, considerando que os desafios dos executivos de TI são coordenar e trabalhar em parceria com as áreas de negócio para entregar serviços de alta qualidade de TI.

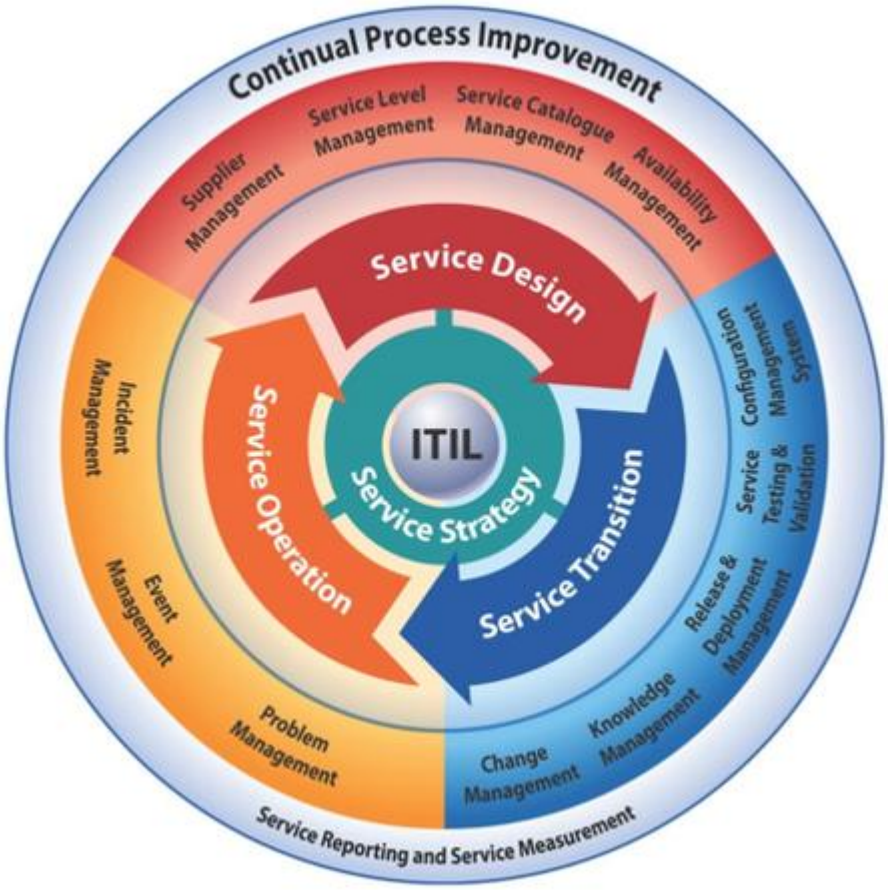
Tomando como base estas citações pode-se considerar que a ITIL é um conjunto de boas praticas que, se adotadas pela organização, podem estabelecer e melhorar a capacidade de gerenciamento de serviços de TI.

Os autores Fernandes e Abreu (2012), citam que a ITIL é composta por cinco publicações, e que cada uma delas ligada a um estágio do ciclo de vida do serviço, contendo uma abordagem integrada de gerenciamento de serviços, tais publicações são:

- **Estratégia do serviço:** orienta sobre como as políticas e processo de gerenciamento de serviço podem ser desenhadas, desenvolvidas e implementadas como ativos estratégicos ao longo do ciclo de vida de serviço. Entre os tópicos abordados nesta publicação, estão os ativos de serviço, o catálogo de serviços, gerenciamento financeiro, gerenciamento do portfólio de serviços, desenvolvimento organizacional, riscos estratégicos etc.
- **Desenho do Serviço:** fornece orientação para o desenho e desenvolvimento dos serviços e dos processos de gerenciamento de serviços, detalhando aspectos do gerenciamento do catálogo de serviços, do nível de serviço, da capacidade, da disponibilidade, da continuidade, da segurança da informação e dos fornecedores, além de mudanças e melhorias necessárias para manter ou agregar valor aos clientes ao longo do ciclo de vida de serviço.
- **Transição do Serviço:** orienta sobre como efetivar a transição de serviços novos e modificados para operações implementadas, detalhando os processos de planejamento e suporte à transição, gerenciamento de mudanças, gerenciamento da configuração e dos ativos de serviço, gerenciamento da liberação e da distribuição, teste e validação de serviço, avaliação e gerenciamento do conhecimento.
- **Operação do Serviço:** descreve a fase do ciclo de vida do gerenciamento de serviços que é responsável pelas atividades do dia a dia, orientando sobre como garantir a entrega e o suporte a serviços de forma eficiente e eficaz e detalhando os processos de gerenciamento de eventos, incidentes, problemas, acesso e de execução de requisições.

- **Melhoria Continua do Serviço:** orienta, através de princípios, práticas e métodos de gerenciamento de qualidade, sobre como fazer sistematicamente melhorias incrementais e de larga escala na qualidade do serviço, nas metas de eficiência operacional, na continuidade do serviço etc., com base no modelo PDCA preconizado pela ISSO/IEC 20000.

Figura 10 - Publicações ITIL



Fonte: BLOG TSG: ITIL Disponível em: <tsg-ufam.blogspot.com>

Resumindo de forma sucinta o ITIL foca na gestão da TI onde se foca em gerenciar os serviços de TI bem como planejá-los, desenvolve-los, executá-los e monitorá-los a fim de atingir os objetivos e metas estabelecidas pela organização.

2.5 Política de Segurança da Informação e Continuidade do Negócio

Como já mencionado neste trabalho, a informação é um bem muito valioso para a corporação e também para a vida pessoal. A primeira informação recebida dos seres humanos é o tapa no bumbum quando uma criança saí do útero de sua

mãe, a criança retribui esta informação com o choro demonstrando que foi recebido esta informação e que ela está viva.

Fontes (2006), afirma que a informação é um recurso que move o mundo e que nos dá conhecimento de como o mundo esta caminhando, o autor afirma também que, do ponto de vista profissional, a informação pode ser comparada ao sangue no corpo do ser humano, sem ela nada existe.

Deve-se também discriminar a diferença entre dados e informação, pois a informação em seu estado bruto, mais conhecida como dado, de nada é valida.

Para Rosini e Palmisano (2003), um dado é um:

> Elemento que representa eventos ocorridos na empresa ou circunstâncias físicas, antes que tenham sido organizados ou arranjados de maneira que as pessoas possam entender e usar.

Da mesma forma citada pelos autores Rosini e Palmisano os autores Laudon e Laudon (2007) afirmam que os dados são correntes de fatos brutos.

Percebe-se que o dado é um elemento que não transmite nenhum conhecimento se não trabalhado. Economia, oportunidade e celular são dados, porém, se trabalhados, podem oferecer uma informação valiosa, exemplo: Com a economia atual as oportunidades de vendas utilizando aparelhos celulares representam uma grande oportunidade de negócio. Com base nas citações acima, pode-se ter como ideia, baseando-se no ponto de vista da tecnologia da informação, que o dado nada mais é que a informação em seu estado bruto, pelo qual não pode ser transmitido nenhum conhecimento para uso organizacional.

Rosini e Palmisano (2003) definem a informação como “Dado configurado de forma adequada ao entendimento e à utilização pelo ser humano”.

Conforme Laudon e Laudon todas as informações seja sobre pessoas, locais e coisas com significado para a organização ou para o ambiente, são contidas em um sistema de informação, portanto as informações são dados apresentados de forma significativa e útil aos seres humanos.

A informação tem um ciclo de vida onde neste ciclo são representados possíveis riscos que a informação pode sofrer, estes riscos são vivenciados quando um ativo seja ele físico tecnológico ou humano faz uso desta informação.

Sêmola (2003) cita quatro momentos do ciclo de vida que merecem atenção são eles:

- **Manuseio:** Momento em que a informação é criada e manipulada, ao folhear um maço de papéis, ao digitar informações em uma aplicação de internet ou, ainda, ao utilizar a senha de acesso para autenticação, por exemplo.
- **Armazenamento:** Momento em que a informação é armazenada, seja em um banco de dados compartilhado, seja em uma anotação de papel posteriormente postada em um arquivo de ferro ou, ainda, em um CD-ROM, DVD-ROM ou *pendrive* depositado na gaveta da mesa de trabalho, por exemplo.
- **Transporte:** Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (e-mail), seja ao postar em um sistema na internet ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
- **Descarte:** Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico do seu contador ou, ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

Após assinalar as diferenças entre dado e informação notando a importância da informação para a corporação, é essencial preocupar-se com a segurança da informação, visto que a informação pode ser comparado com o sangue no corpo humano, sendo de vital importância para a sobrevivência.

2.5.1 Segurança da Informação

A segurança da informação é adotada pela corporação para proteger suas informações de furtos, alterações indevida, e indisponibilidade, a segurança da informação envolve não somente o uso de tecnologias de alta performance para proteger a informação mas também envolve o elo mais fraco da informação que são os seres humanos. De nada adianta obter a mais alta tecnologia para proteção da informação lógica e fisicamente se os funcionários da organização não receberem um treinamento adequado que alerte sobre possíveis ataques de engenharia social.

Segundo Mitnick e Simon (2003)

> Com frequência, a segurança é apenas uma ilusão, que às vezes fica pior ainda quando entram em jogo a credulidade, a inocência ou a ignorância. O cientista mais respeitado do mundo no século XX, Albert Einstein, disse: “Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro”. No final, os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas ou, em geral, apenas desconhecem as boas práticas da segurança.

Conforme Sêmola (2003) a segurança da informação pode ser definida como:

> Uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Fontes (2006), define a segurança da informação como:

> Conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

A segurança da informação tem como objetivo diminuir os riscos na utilização dos recursos de informação, para o bom funcionamento corporativo, para ajudar a proteger a informação a segurança da informação se norteia por alguns princípios que são: disponibilidade, integridade, confidencialidade, legalidade, auditabilidade e não repúdio, o autor Fontes, (2006) descreve estes princípios como:

- **Disponibilidade:** a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.
- **Integridade:** a informação deve estar correta, ser verdadeira e não estar corrompida.
- **Confidencialidade:** a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia.
- **Legalidade:** o uso da informação deve estar de acordo com as leis

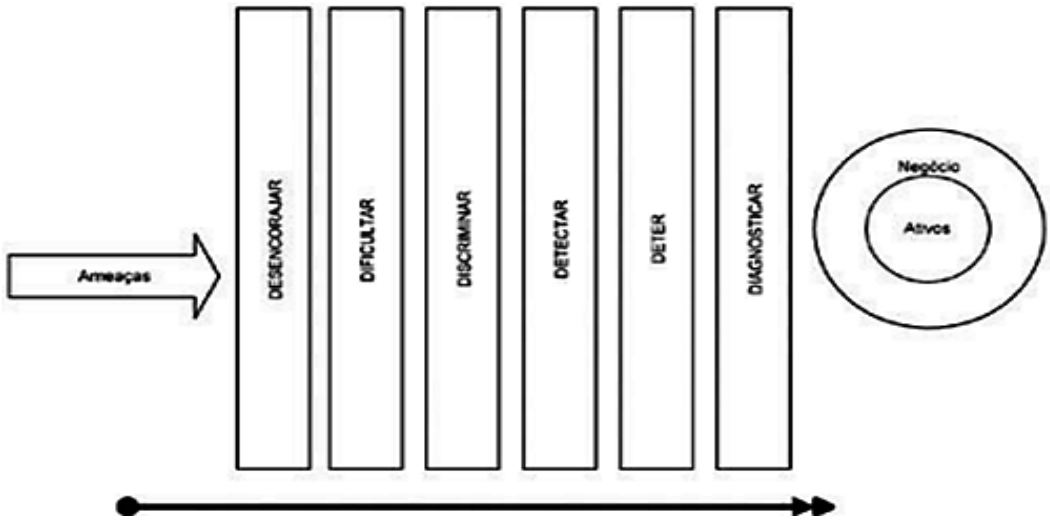
aplicáveis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.

- **Auditabilidade:** o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.
- **Não repúdio de auditoria:** o usuário que gerou ou alterou a informação (arquivo texto ou mensagem de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua auditoria.

2.5.2 Barreiras de Segurança

Diante do papel complexo e amplo que a segurança da informação desempenha existem barreiras da segurança que ajudam a particionar todo o trabalho tornando-o mais claro. Cada uma dessas barreiras é de fundamental importância para o objetivo maior de redução dos riscos, portanto, estas barreiras devem ser implementadas de forma que haja uma interação entre elas se encaixando como se fosse um quebra cabeça, essas barreiras são: Desencorajar, Dificultar, Discriminar, Detectar, Deter e Diagnosticar.

Figura 11 - Diagrama representativo das barreiras de segurança



Fonte: Sêmola, 2003

Barreira 1: desencorajar

Essa é a primeira das seis barreiras de segurança, e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou perder o interesse e o estimulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas já são efetivos nessa fase.

Barreira 2: dificultar

O papel dessa barreira é complementar a anterior através da adoção efetiva dos controles que dificultarão o acesso indevido. Como exemplo, pode-se citar os dispositivos de controle de acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, biométricos, de senhas, de *smartcards* e de certificados digitais, além do *firewall* etc.

Barreira 3: discriminar

Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e banco de dados. Os processos de avaliação e gestão do volume de uso dos recursos, como e-mail, impressora ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades dessa barreira.

Barreira 4: detectar

Agindo de forma complementar às suas antecessoras, essa barreira deve munir a solução de segurança de dispositivos que sinalizem, alerte e instrumente os gestores da segurança na detecção de situações de risco, seja em uma tentativa de invasão, seja em uma possível contaminação por vírus, o descumprimento da política de segurança da empresa ou a cópia e o envio de informação sigilosas de forma inadequada.

Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intruso, que reduziram o tempo de resposta a incidentes.

Barreira 5: deter

Essa quinta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento dessa barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Nesse momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.

Barreira 6: diagnosticar

Apesar de representar a ultima barreira no diagrama, essa fase tem o sentido especial de representar a continuidade do processo de gestão de segurança da informação. Pode parecer o fim, mas é o elo com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores, essa é a barreira de maior importância. Deve ser conduzida por atividades de análise de risco que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados às características e às necessidades específicas dos processos de negócio da empresa (SÊMOLA, 2003).

2.5.3 Política de Segurança da Informação

A política de segurança da informação (PSI) pode-se dizer que é composta por regras e padrões a serem seguido a fim de garantir a integridade, disponibilidade e confidencialidade da informação.

Conforme Nicolau e Ferreira (2008)

> A política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.

Segundo Sêmola (2003) a política da segurança da informação

> Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa.

A política de segurança deve ser criada antes de um incidente de segurança ou depois para evitar uma nova falha de segurança, ela serve tanto para prevenir problemas de segurança quanto para documentar a adesão do processo de qualidade.

As organizações costumam customizar a política de segurança da informação conforme seu ambiente já que cada empresa tem sua particularidade dos ativos que deve proteger, a segurança abrange não só o *hardware* e *software* que compõe os sistemas ela abrange pessoas e processos de negócio.

Nicolau e Ferreira (2008) afirma que em uma política de segurança deve:

> Considerar o *hardware*, *software*, dados e documentação, identificando de quem estes elementos devem ser protegidos. Nesta análise aspectos sobre segurança de dados, *backup*, propriedade intelectual e respostas a incidentes devem ser levados em consideração.

Os autores também recomendam que exista um comitê de segurança da informação que se constituem por profissionais de vários departamentos como jurídico, informática, auditoria, infraestrutura entre outros que forem necessários, e ressaltam que as políticas, normas e procedimentos de segurança da informação devem ser:

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

Um dos fatores mais importantes dentro da política de segurança é o apoio da alta gerência para implementação e validação, pois sem este apoio nenhuma norma seria seguida pelos funcionários.

Os autores Nicolau e Ferreira (2008) sustentam que o desenvolvimento e a implementação de uma política pode ser dividida em 4 partes.

Tabela 3 - Fase 1 do desenvolvimento de uma política

FASES	DESCRIÇÃO
Fase I	**Levantamento de Informações**
1.1	Obtenção dos padrões, normas e procedimentos de segurança já existentes para análise.
1.2	Entendimento das necessidades e uso dos recursos da tecnologia da informação (sistemas, equipamentos e dados) nos processos do negócio.
1.3	Obtenção de informações sobre os ambientes de negócios: • Processos de negócios; • Tendências de mercado; • Controles e áreas de risco.
1.4	Obtenção de informações sobre o ambiente tenológico: • *Workflow* entre ambientes; • Redes de aplicações; • Plataformas computacionais.

Fonte: Nicolau e Ferreira, 2008

Tabela 4 - Fase 2 do desenvolvimento de uma política

FASES	DESCRIÇÃO
Fase II	**Desenvolvimento do Conteúdo da Política e Normas de Segurança**
2.1	Gerenciamento da política de segurança: • Definição da segurança da informação; • Objetivo do gerenciamento; • Fatores críticos de sucesso; • Gerenciamento da versão e manutenção da política; • Referência para outras políticas, padrões e procedimentos.
2.2	Atribuição de regras e responsabilidades: • Comitê de segurança da informação; • Proprietário das informações; • Área de Segurança da Informação; • Usuários de informações; • Recursos humanos; • Auditoria interna.
2.3	Critérios para classificação das informações: • Introdução; • Classificando a informação; • Níveis de classificação; • Reclassificação; • Armazenamento e descarte; • Armazenamento e saídas.
2.4	Procedimentos de segurança de informações: • Classificação e tratamento da informação; • Notificação e gerenciamento de incidentes de segurança da informação; • Processo disciplinar; • Aquisição e uso de *hardware* e *software*; • Proteção contra *software* malicioso; • Segurança e tratamento de mídias; • Uso de Internet; • Uso de correio eletrônico; • Utilização dos recursos de TI; • *Backup;* • Manutenção de teste e equipamentos; • Coleta e registro de falhas; • Gerenciamento de controle da rede; • Monitoração do uso e acesso aos sistemas; • Uso de controle de criptografia e gerenciamento de chaves; • Controle de mudanças operacionais; • Inventário dos ativos de informação; • Controle de acesso físico às áreas sensíveis; • Segurança física; • Supervisão de visitantes e prestadores de serviço.

Fonte: Nicolau e Ferreira, 2008

Tabela 5 - Fase 3 do desenvolvimento de uma política

FASES	DESCRIÇÃO
Fase III	**Elaboração dos procedimentos de Segurança da Informação**
3.1	Pesquisas sobre as melhores práticas em segurança da informação utilizadas no mercado.
3.2	Desenvolvimento de procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização.
3.3	Formalização dos procedimentos para integrá-los às politicas corporativas.

Fonte: Nicolau e Ferreira, 2008

Tabela 6 - Fase 4 de um desenvolvimento de uma política

FASES	DESCRIÇÃO
Fase IV	**Revisão, Aprovação e Implementação das Políticas, Normas e Procedimentos de Segurança da Informação**
4.1	Revisão e aprovação das políticas, normas e procedimentos de segurança da informação.
4.2	Efetiva implantação das políticas, normas e procedimentos de segurança da informação por meio das seguintes iniciativas: • Atuação junto à área responsável pla comunicação, ou área correspondente, na orientação para a preparação do material promocional, de divulgação e de consulta; • Divulgação das responsabilidades dos colaboradores, bem como da importância das políticas, normas e procedimentos de segurança da informação; • Realização de palestras executivas referentes às políticas, normas e procedimentos de segurança da informação desenvolvidas, tendo por público-alvo a Presidência, Diretorias e Gerências; • Realização de palestras referentes às políticas, normas e procedimentos de segurança, tendo por público-alvo outros colaboradores da organização.

Fonte: Nicolau e Ferreira, 2008

Tabela 7 - Cronograma sugerido para o desenvolvimento de uma Política

CRONOGRAMA SUGERIDO								
Atividades	**Semanas**							
	1	2	3	4	5	6	7	8
Fase 1 Levantamento de Informações								
Fase 2 Desenvolvimento do conteúdo da política e normas de segurança								
Fase 3 Elaboração dos procedimentos de segurança da informação								
Fase 4 Revisão, aprovação e implantação das políticas de segurança da informação e palestras.								

Fonte: Nicolau e Ferreira, 2008

Os autores Nicolau e Ferreira (2008) também citam os benefícios alcançados a curto, médio e longo prazo com a adoção de uma política de segurança da informação.

Curto prazo

- Formalização e documentação de segurança adotados pela organização.
- Implementação de novos procedimentos e controles.
- Prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de galhas ou desastres.
- Maior segurança nos processos do negócio.

Médio prazo

- Padronização dos procedimentos de segurança incorporados na rotina da empresa.
- Adaptação segura de novos processos do negócio.
- Qualificação e quantificação dos sistemas de resposta a incidentes.

- Conformidade com padrões de segurança, como a NBR ISSO/IEC 27002 (antiga NBR ISSO/IEC 17799).

Longo prazo

- Retorno sobre o investimento realizado, por meio da redução dos problemas e incidentes de segurança da informação.
- Consolidação da imagem corporativa associada à segurança da informação.

Nos dias atuais em que as organizações se tornam cada vez mais dependentes da tecnologia e da informação, é de muita importância a adoção de uma política de segurança da informação, onde se tem como objetivo proteger estas informações de possíveis perdas, furtos ou acessos indevidos. Hoje em dia as empresas vem notando cada vez mais a importância de elaborar uma política de segurança da informação para proteger seu bem mais valioso, que é a informação, tendo em vista que ao adotar uma PSI a organização vai se beneficiar com os benefícios de curto, médio e longo prazo alcançando assim um maior grau de excelência.

2.5.4 Plano de Continuidade do Negócio

O plano de continuidade do negócio visa garantir um menor impacto em desastres e incidentes de segurança que não puderam ser evitados, como o objetivo de continuidade de processos vitais para a sobrevivência da corporação. Analogicamente o plano de continuidade de negócios funciona como um paraquedas reserva que garante a vida do paraquedista quando o primeiro paraquedas falha.

Para Sêmola (2003) “O plano de continuidade de negócios deve ser elaborado com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados”.

Nicolau e Ferreira (2008) informa que:

> Uma política deve assegurar a existência de uma plano de continuidade capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, incluindo também as atividades de teste e manutenção do plano.

Um dos riscos que podem ser minimizados com o plano de continuidade de negócio são a perda receita, multas e sanções legais por indisponibilidade de serviço, comprometendo assim a qualidade do serviço e credibilidade organizacional.

Nicolau e Ferreira (2008) asseguram que o processo de gestão da continuidade deve prover pelo manos as seguintes atividades de controle:

- Assegurar que um plano formal (escrito) esteja desenvolvido, testado e amplamente divulgado (incluindo treinamento);
- Procedimento de urgência/emergência descritos e testados;
- Procedimentos corretivos e de recuperação desenhados para trazer os negócios de volta à posição em que se encontravam antes do incidente ou desastre;
- Ações para salvaguardar e reconstruir o site original;
- Procedimentos para interação com as autoridades públicas;
- Comunicação com funcionários, clientes, fornecedores, acionistas, alta administração, autoridades públicas e imprensa.

Para se elaborar um plano de continuidade de negócio primeiramente deve-se analisar o impacto da paralisação de cada ativo, o BIA – *Business Imapact Analysis* é muito utilizado para dimensionar a criticidade de cada ativo dentro da organização e este é um passo muito importante para projetar as demais fases do plano de continuidade de negócio, o BIA se resumiria em dimensionar os impactos e selecionar as ameaças a serem consideradas no plano de continuidade.

Sêmola cita algumas estratégias e planos de contingência para minimizar o impacto da ocorrência de uma situação de risco, são elas:

Estratégias de contingência

Hot-site

Recebe esse nome por ser uma estratégia “quente” ou pronta para entrar em operação assim que uma situação de risco ocorrer. Mais uma vez, o tempo de operacionalização dessa estratégia está diretamente ligado ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamento tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milissegundos de tolerância para garantir a disponibilidade do serviço mantido pelo equipamento.

Warm-site

Seguindo a nomenclatura da primeira estratégia, esta se aplica a objetos com maior tolerância à paralisação, podendo se sujeitar a indisponibilidade por mais tempo, até o retorno operacional da atividade. Tomemos, como exemplo, o serviço de e-mail dependente de uma conexão de comunicação. Vemos que o processo de envio e recebimento de mensagens é mais tolerante que o exemplo usado na primeira estratégia, pois poderia ficar indisponível por minutos sem, no entanto, comprometer o serviço ou gerar impactos significativos.

Realocação de operação

Como o próprio nome denuncia, essa estratégia objetiva desviar a atividade atingida pelo evento que provocou a quebra de segurança para outro ambiente físico, equipamento ou link, pertencentes à mesma empresa. Essa estratégia só é possível com a existência de “folgas” de recursos que podem ser alocados em situações de crise.

Muito comum, essa estratégia pode ser entendida pelo exemplo em que se redireciona o tráfego de dados de um roteador ou servidor com problemas para outro que possua folga de processamento e suporte ao acúmulo de tarefas.

Bureau de serviços

Essa estratégia considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado; portanto, fora dos domínios da empresa. Por sua própria natureza, que quer um tempo de tolerância maior em função do tempo de reativação operacional da atividade, torna-se restrita a poucas situações.

O fato de ter suas informações manuseadas por terceiros e em um ambiente fora de seu controle requer atenção na adoção de procedimentos, critérios e mecanismos de controlem que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.

Acordo de reciprocidade

Muito conveniente para atividades que demandariam investimentos de contingência inviáveis ou incompatíveis com a importância da mesma, essa estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes às suas e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional. Estabelecem em conjunto as situações de contingência e definem os procedimentos de compartilhamento de recursos para alocar a atividade atingida no ambiente da

outra empresa. Dessa forma, ambas obtêm redução significativa dos investimentos. Apesar do notório benefício, todas as empresas envolvidas precisam adotar procedimentos personalizados e mecanismos que reduzam a exposição das informações que, temporariamente, estarão circulando e ambiente de terceiros. Esse risco se agrava quando a reciprocidade ocorre entre empresas pseudoconcorrentes que se unem exclusivamente com propósito de reduzir investimentos, precisando fazê-lo pela especificidade de suas atividades, como, por exemplo, no processo de impressão de jornais.

Cold-site

Dentro do modelo de classificação adotado nas duas primeiras estratégias, esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto, é aplicável a situação com tolerância de indisponibilidade ainda maior.

Autossuficiência

Aparentemente uma estratégia impensada, a autossuficiência é, muitas vezes, a melhor ou a única estratégia possível para determinada atividade. Isso ocorre quando nenhuma outra estratégia é aplicável, quando os impactos possíveis não são significativos ou quando são inviáveis, seja financeiramente, seja técnica ou estrategicamente. A escolha de qualquer uma das estratégias estudadas até o momento depende diretamente do nível de tolerância que a empresa pode suportar e do nível de risco que seu executivo esta disposto a correr. Essa decisão pressupõe a orientação obtida por uma análise de riscos e impactos que gere subsídios para apoiar a escolha mais acertada.

Plano de contingência

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

Plano de administração de crise

Esse documento tem o propósito de definir passo a passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem de definir os procedimentos a serem

executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à empresa é um exemplo típico de tratamento dado pelo plano.

Plano de continuidade operacional

Esse documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à internet exemplifica os desafios organizados pelo plano.

Plano de recuperação de desastres

Esse documento tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação. É fator critico de sucesso estabelecer adequadamente os gatilhos de acionamento para cada plano de contingência. Esses gatilhos são parâmetros de tolerância usados para sinalizar o inicio da operacionalização da contingência, evitando acionamentos prematuros ou tardios. Dependendo das características do objeto da contingência, os parâmetros podem ser: percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros etc. A notória complexidade do plano de continuidade operacional - em função da diversidade de objetos, suas características personalizadas, abrangência das ameaças possíveis consideradas e a necessária integração dos planos de administração de crises, planos de continuidade operacional e planos de recuperação de desastres – torna imprescindível a construção de um modelo dinâmico de manutenção dos documentos e de testes. Por se tratar de uma peça importante na gestão corporativa de segurança da informação, principalmente por ser o ultimo recurso depois que todos os demais falharam, os três planos precisam passar por baterias severas de teste e homologação, a fim de garantir sua eficiência e permitir ajustes diante de previsíveis mudanças físicas, tecnológicas e humanas que ocorrem frequentemente no ambiente corporativo. Outros planos podem ser mencionados em outras literaturas ou modelos, como o plano de resposta a incidentes ou o plano de retorno à normalidade, entre outros, mas os mesmos podem ser avaliados como subprodutos dos três planos aqui detalhados (SÊMOLA, 2003).

2.5.5 Backup, Cópias de Segurança e *Restore*

Como já citado diversas vezes neste trabalho, a informação é um bem muito valioso não só no meio corporativo como também na vida pessoas, como fotos guardadas para recordação, cartas escritas, e-mail enviados, vídeos, trabalhos de graduação, músicas, entre outras coisas. Já no mundo corporativo, tem-se informações sobre a estratégia organizacional, informações sobre clientes e fornecedores, títulos a receber e a pagar, XML de uma nota fiscal, que, por sua vez, se não for armazenada ou realizado um *backup*, a falta destes arquivos XML pode gerar multas para organização em caso de auditoria do fisco. Fontes (2006), afirma que a informação tem uma forte característica que é, se um dia destruída e esta informação não tiver nenhuma cópia, ela nunca mais será recuperada.

Tendo como base que a informação é um ativo essencial para a organização pode-se dizer que realizar *backup* é essencial para a continuidade de negócio, porem deve-se levar em conta o que armazenar no *backup*, ou seja, a importância da informação o nível de classificação entre outros fatores.

Nicolau e Ferreira (2008) afirma que as organizações devem elaborar os procedimentos de *backup* nas seguintes premissas:

- Realizar *backups* visando diminuir os riscos da continuidade;
- Manter os *backups* em local físico distante da localidade de armazenamento dos dados originais;
- Realizar testes nas mídias que armazenam os *backups* para assegurar que os mantidos em ambiente interno e/ou externo estejam seguros e em perfeito estado para serem utilizados;
- Desenvolver e manter a documentação dos procedimentos de *backup* e *restore* sempre atualizada;
- Assegurar que seja mantido um inventário sobre as mídias que armazenam os *backups*;

Em relação a frequência de realização da rotina de *backup,* deve-se levar em consideração dois parâmetros muito importantes; a velocidade da informação onde se leva em conta a velocidade na qual a informação é atualizada e a volatilidade da informação, que é o tempo em que informação permanece atual e atualizada. Estes

dois parâmetros devem auxiliar na frequência da realização de uma rotina de *backup*.

Os autores Nicolau e Ferreira (2008) também citam que, para toda cópia de *backup,* devem existir registros da operação envolvidas na ação de realizar a cópia.

E por ultimo, porem não menos importante, deve-se sempre realizar o *restore* ou seja, o teste de restauração para garantir a qualidade do *backup*, para verificar a integridade da informação armazenada, verificar a funcionalidade do procedimento adotado para realização dos *backups*, a identificação de defeitos ou possíveis falhas e a identificação de procedimentos falhos ou não necessários, buscando assim otimizar o processo de backup.

2.5.6 Ferramentas automatizadas de *backup*

Existem ferramentas que tem como objetivo facilitar e automatizar rotinas de *backup,* poupando assim muito tempo de um profissional de TI ou um usuário comum em relação as cópias que devem ser feitas e aos testes de qualidade do *backup* que devem ser feitos algumas destas ferramentas são:

- ***Cobian Backup:*** ferramenta gratuita utilizada no sistema operacional Windows, esta ferramenta cria cópias de segurança que podem ser salvas em mídias físicas como HD ou CD, alem de criar estas cópias esta ferramenta da a opção de criar senhas nestas cópias, para que ninguém além do usuário que realizou as cópias tenha acesso aos arquivos salvos, esta ferramenta pode ser programada para realizar *backup* automaticamente em outros computadores que utiliza-se da mesma rede utilizando o protocolo *File Transfer Protocol* (FTP).
- **Yadis *Backup***: ferramenta gratuita utilizada na plataforma Windows também disponibiliza a opção de cópias através do protocolo FTP além de monitorar os arquivos que o usuário escolhe para realiza *backup,* qualquer alteração que estes arquivos sofrer a ferramenta imediatamente realiza uma cópia automática da nova versão deste arquivo, esta ferramenta roda em segundo plano possibilitando esta monitoração de arquivos, se no momento do *backup* a destino não estiver disponível a ferramenta armazena este *backup* e assim que o

destino estiver disponível novamente a ferramenta realiza o *backup* automaticamente.

- **Redo *Backup and Recovery:*** aplicativo profissional com o uso gratuito limitado, esta ferramenta além de disponibilizar o serviço de *backup* ela também tem a opção *recovery* que se encarrega de recuperar arquivos apagados ou danificados em seu HD, lixeira ou *pendrive,* esta ferramenta é inicializada a partir de um CD ou dispositivo *Universal Serial Bus* (USB) apesar desta ferramenta não oferecer a opção de um *backup* automático no sentido de agendamento de rotinas de *backup* esta ferramenta oferece a vantagem de não precisa instalar diretamente na maquina pois ela é iniciada através de CD ou dispositivo USB sendo perfeita para recuperar informações de dispositivos que não funcionam mais como por exemplo um computador que não funciona mais porque o HD queimou, pode-se utilizar esta ferramenta para fazer um backup deste HD.
- ***Free File Sync:*** ferramenta gratuita suportado nas plataformas Windows, Mac e Linux esta ferramenta oferece a opção de agendamento de tarefas de backup e comparação de arquivos através da opção sincronizar onde a ferramenta realiza uma comparação entre os dados e se necessário atualiza o dado que já foi feito o *backup*, mantendo as cópias sempre atualizadas.
- ***Nimbus Backup:*** Esta ferramenta é uma ferramenta gratuita *open sourse* (código aberto) que suporta as plataformas Windows, Linux e MacOS, ferramenta corporativa desenvolvida para empresas e governos, segue boas praticas, verificando a integridade dos dados, utilizando-se de criptografia à nível militar e backups incrementais, ferramenta desenvolvida para *backup* em rede.
- **Bacula:** ferramenta gratuita corporativa e governamental *open source* (código aberto) utilizada para realizar *backups* em rede compatíveis com os sistemas operacionais Linux, Solaris, FreeBSD, NetBSD, OpenBSD, HP-UX, Tru64, AIX, IRIX, Mac OS X e Windows, ferramenta de backup multi banco de dados envios de mensagens de logs para o

administrador, disponibiliza interface de gerenciamento web entre outros facilitadores.

- **Tivoli *Storage Manager:*** ferramenta paga de propriedade da empresa IBM feita também para uso corporativo e governamental, compatíveis com servidores Linux, Windows, IBM, Sun Solaris e HP/UX, esta ferramenta monitora as atividades desde procedimentos do próprio servidor a recebimento de dados, disponibiliza de um gerenciamento centralizado a partir de uma interface Web, disponibiliza relatórios gerenciais, disponibiliza também o procedimento de *backup* incremental, verifica a qualidade do backup realizado e cuida da segurança utilizando-se de criptografia.

Com estes exemplos de ferramentas citados observa-se que tem-se varias soluções de *backups* automatizados tanto para usuários comuns quanto para organizações, e ambas soluções possuem ferramentas gratuitas e pagas, lembrando que estas são apenas algumas soluções, porem ainda existe inúmeras opções como DropBox, Google Drive, One Drive entre outras ferramentas, se tratando da informação que é importante não só para a organização mas também para usuários comuns, é de grande valia avaliar quais informações são realmente importantes e dedicar-se para elaborar uma estratégia de backup que atenda o nível de necessidade de cada individuo ou organização.

Muitas vezes o fato do *backup* ser um procedimento que demanda um certo tempo para fazer, pessoas e organizações não se preocupam em realizar cópias de segurança, porem com o uso de ferramentas automatizadas e conhecimento para configura-las este problema é solucionado.

3 ESTUDO DE CASO

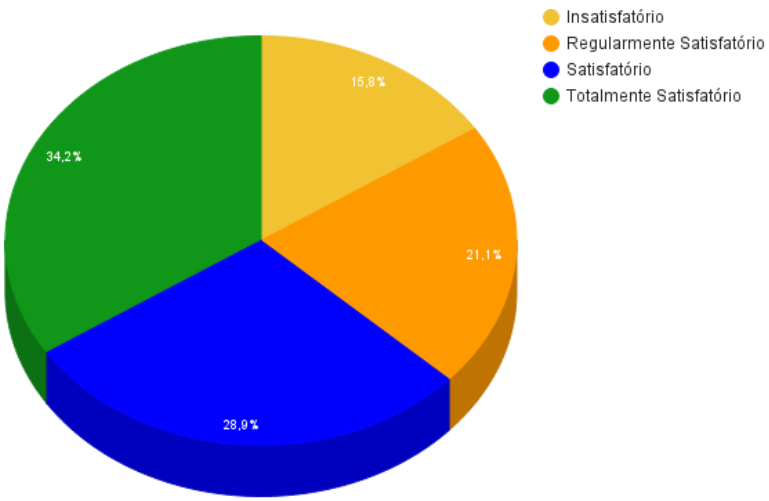
Este estudo de caso tem como objetivo analisar como as organizações em geral estão lidando com o processo de *backup*, se estão preparadas para se recuperarem de incidentes de segurança e perdas de informação e verificar se a TI está alinhada com os negócios da empresa e seus objetivos de mercado, para tanto foi aplicado um questionário contendo 10 questões, seguindo a escala de Likert.

O questionário foi difundido via internet utilizando-se da ferramenta Google *docs*, os dados foram coletados através da mesma ferramenta, o questionário foi distribuído para 30 profissionais de TI de Americana e região, de pequenas, médias e grandes empresas.

Após a aplicação do questionário foram coletados os dados de cada resposta dada pelos entrevistados e foi elaborado um gráfico para cada pergunta.

Questão 1: A organização em que atua dá a devida importância para a informação adotando boas práticas, utilizando-se de políticas de *backup* e políticas de segurança da informação?

Figura 12 - Resultado da primeira questão

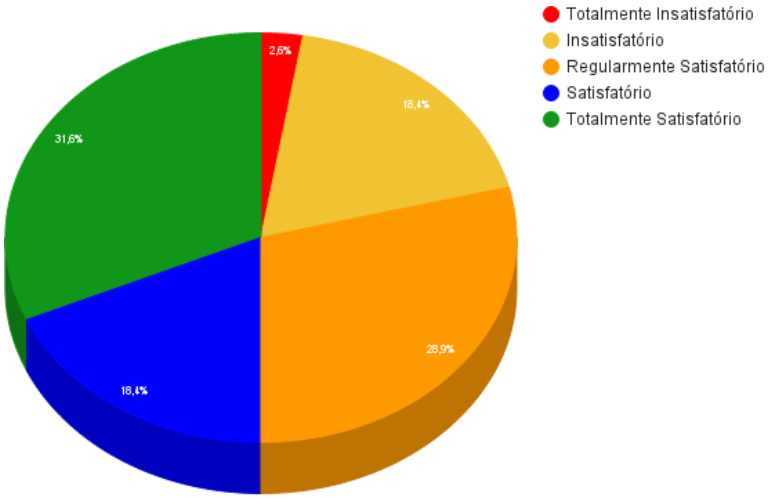


Fonte: elaboração própria

Nesta questão a maior parte dos entrevistados informou que o nível de importância dada para a informação nas organizações em que atuam é totalmente satisfatório com 34,2%, seguido pelo nível satisfatório com 28,9%, regularmente satisfatório com 21,1% insatisfatório com 15,8% e totalmente insatisfatório com 0%.

Questão 2: Em caso de algum acidente que cause perda de informação ou paralisação de serviços qual o nível de preparação para diminuir os danos causados e dar continuidade no negócio que a organização se encontra?

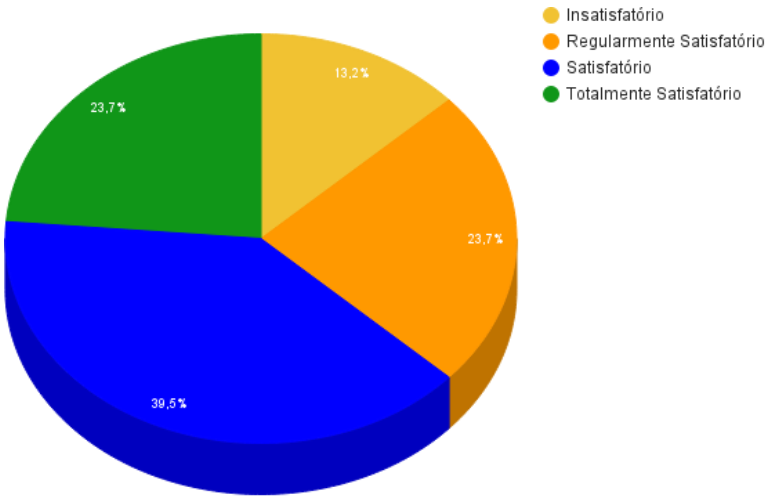
Figura 13 - Resultado da segunda questão



Fonte: elaboração própria

Em caso de algum incidente a maior parte dos entrevistados com 31,5% informou que o nível de preparação para diminuir os danos causados e dar continuidade no negócio da organização é totalmente satisfatório, seguido de 28,9% regularmente satisfatório, em seguida com a mesma porcentagem os níveis satisfatório e insatisfatório com 18,4% e por ultimo totalmente insatisfatório com 2,6%.

Figura 14 - Resultado da terceira questão



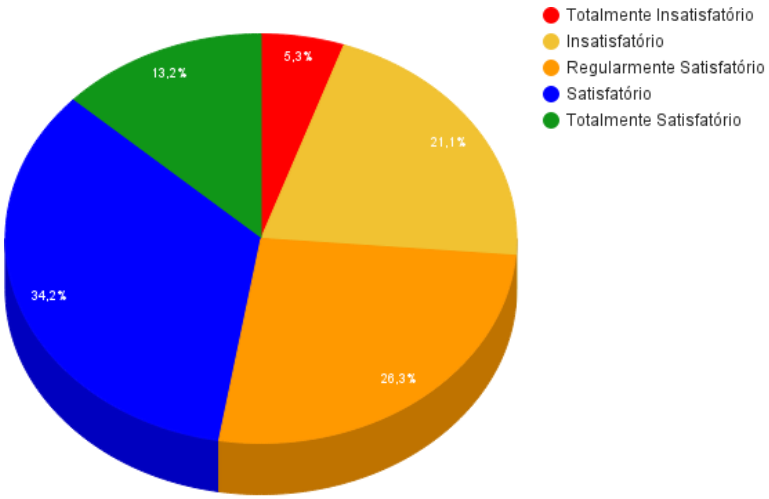
Fonte: elaboração própria

Questão 3: Qual o nível do alinhamento da Tecnologia da Informação (TI) com os negócios da empresa e seus objetivos de mercado?

A maior parte dos entrevistados com 39,5% informou que o alinhamento da TI com os negócios são de nível satisfatório, seguido de totalmente satisfatório e regularmente satisfatório com 23, 7%, insatisfatório com 13,2% e totalmente insatisfatório com 0%.

Questão 4: Qual é o nível de envolvimento da alta gerencia na adoção/aprovação de novas políticas de segurança da informação?

Figura 15 - Resultado da quarta questão



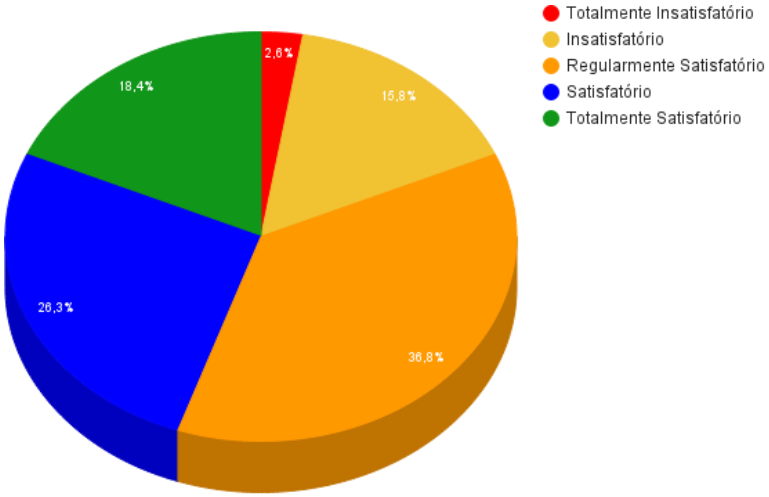
Fonte: elaboração própria

Nesta questão 34,2% dos entrevistados disseram que o nível de envolvimento é satisfatório, 26,3% regularmente satisfatório, 21,1% insatisfatório, 13,2% totalmente satisfatório e 5,3 totalmente insatisfatório.

Questão 5: O grau de disseminação sobre as boas praticas de segurança e a importância do *backup* na organização são satisfatórios?

A maior parte dos entrevistados informou que o grau de disseminação é regularmente satisfatório com 36,8%, seguido de 26,3% satisfatório, 18,4% totalmente satisfatório, 15,8% insatisfatório e 2,6% totalmente insatisfatório.

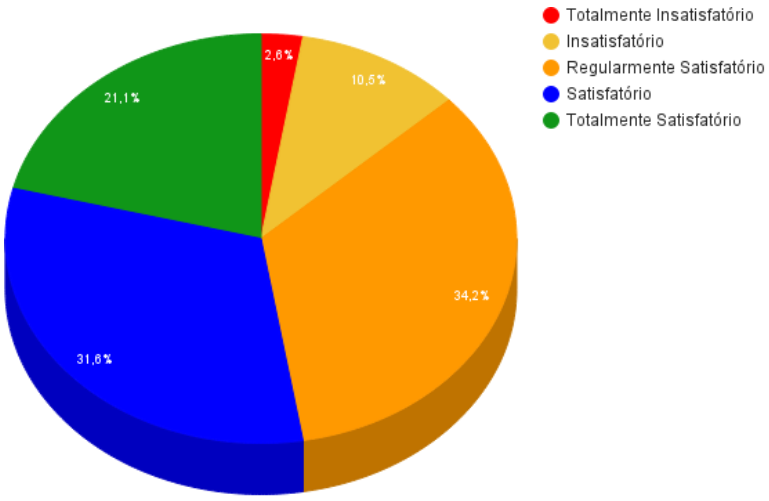
Figura 16 - Resultado da quinta questão



Fonte: elaboração própria

Questão 6: Em relação aos princípios da segurança da informação que são:Disponibilidade, Integridade, Confidencialidade, Legalidade, Auditabilidade e Não repúdio qual o nível de cumprimento destes princípios na corporação?

Figura 17 - Resultado da sexta questão

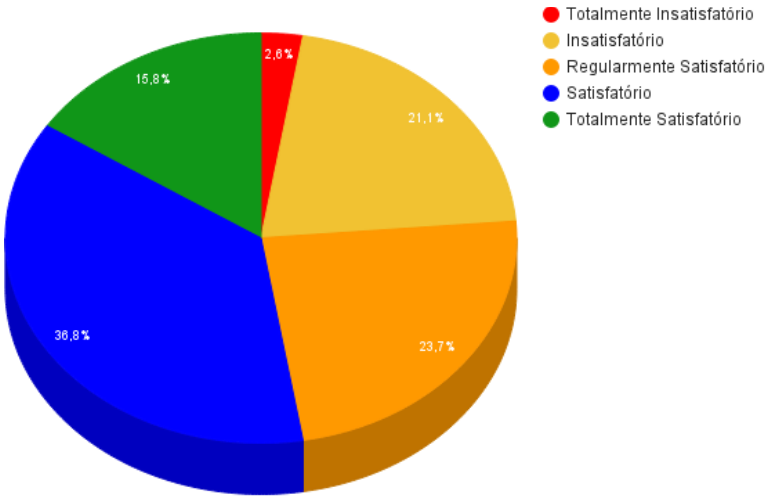


Fonte elaboração própria

Na sexta questão a maior parte dos entrevistados com 34,2% informou que o nível de cumprimento é regularmente satisfatório, seguido de 31,6% satisfatório, 21,1% totalmente satisfatório, 10,5% insatisfatório e 2,6% totalmente insatisfatório.

Questão 7: Ao realizar um *backup* deve-se atestar a sua qualidade através da restauração, para usá-lo em caso de perda de informação, qual o nível de qualidade dos *backups* em sua organização?

Figura 18 - Resultado da sétima questão

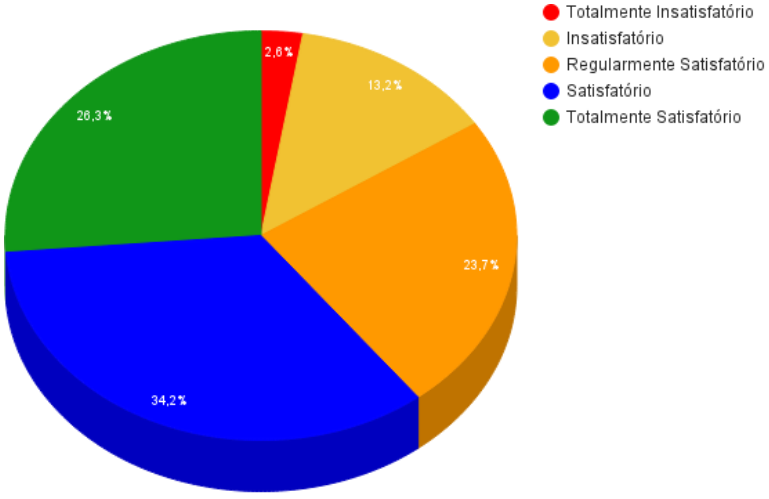


Fonte: elaboração própria

Os entrevistados na sétima questão disseram que o nível de qualidade dos *backups* são de 36,8% satisfatório, 23,7% regularmente satisfatório, 21,1% insatisfatório, 15,8% totalmente satisfatório e 2,6% totalmente insatisfatório.

Questão 8: A política de *backup* adotada em sua organização garante o armazenamento seguro e a qualidade dos *backups* realizados?

Figura 19 - Resultado da oitava questão

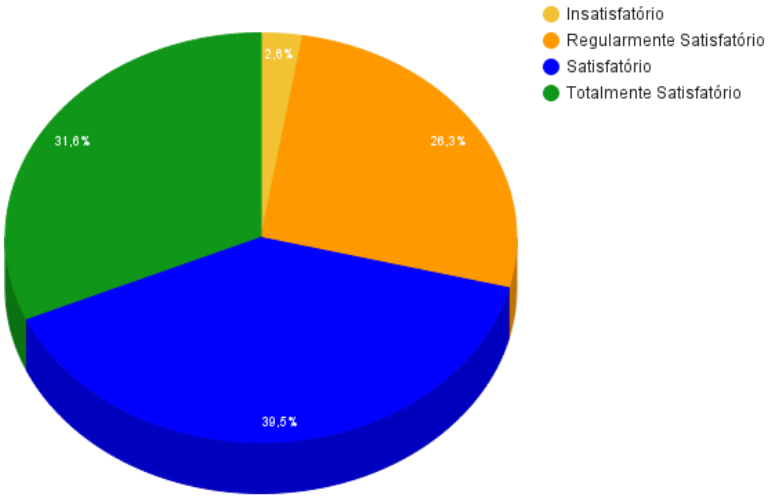


Fonte: elaboração própria

Nesta questão os entrevistados informaram que o nível de qualidade dos *backups* e a garantia de armazenamento seguro são satisfatório com 34,2%, em seguida 26,3% totalmente satisfatório, 23,7% regularmente satisfatório, 13,2% insatisfatório e 2,6% totalmente insatisfatório.

Questão 9: As mídias onde são armazenadas os *backups* são de qualidade?

Figura 20 - Resultado da nona questão



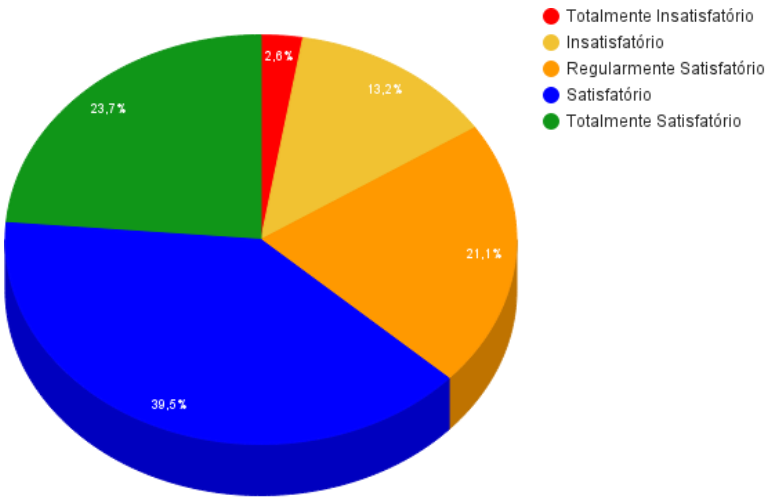
Fonte: elaboração própria

39,5% dos entrevistados disseram que a qualidade das mídias e *backup* são de qualidade satisfatório, seguido de 31,6% totalmente satisfatório, 26,3% regularmente satisfatório, 2,6% insatisfatório e 0% totalmente insatisfatório.

Questão 10: A atual política de backup garante a recuperação da informação em caso de incidente e perda de informação?

39,5% dos entrevistados responderam a questão dez de forma satisfatória, 23,7% totalmente satisfatório, 21,1% regularmente satisfatório, 13,2% insatisfatório e 2,6% totalmente insatisfatório.

Figura 21 - Resultado da décima questão



Fonte: elaboração própria

Os resultado da questão 1 informa que a maioria dos entrevistados com 34,2% acham que sua organização da a devida importância para a informação adotando boas praticas no tratamento da informação, porem por mais que o resultado seja positivo nesta questão, a maioria das organizações tem em sua lista de prioridades a segurança da informação, porem nem sempre estas organizações colocam em pratica o que são ditas como boas praticas de segurança e de *backup*, muitas vezes por falta de tempo ou conhecimento de como fazer, muitas vezes as organizações podem sim se preocupar com o *backup* porem não sabem a maneira correta de realiza-lo, nesta mesma questão ainda existe uma parcela de entrevistados que informam que sua organização tem um nível regularmente satisfatório ou insatisfatório, estas organizações correm um sério risco de fracassar diante de um mercado tão competitivo e com margem de erro tão pequena.

A questão numero 2 visa verificar se a organização onde os entrevistados trabalham estão prontas para minimizar um impacto de segurança e dar continuidade no negócio, a maioria dos entrevistados acham que sua organização esta pronta para se recuperar de um incidente de segurança e dar continuidade no negócio com 31,5%, porem pode-se observar que em segundo lugar vem o nível regularmente satisfatório com 28,9%, pode-se observar neste resultado que uma parcela dos entrevistados que responderam totalmente satisfatório e satisfatório na questão numero 1, responderam regularmente satisfatório ou outros níveis mais baixos de insatisfação, isso mostra que, nem sempre uma organização que acha que da a devida importância para a informação esta pronta para se recuperar de um

incidente, pois uma organização que se preocupa com a informação não adotar e seguir uma política completa de *backup* ou segurança, não esta pronta para se recuperar de um incidente, portanto nem sempre adotar uma boa pratica para proteger a informação é o suficiente, esta boa pratica tem que ser seguida de maneira correta para se alcançar o objetivo proposto de proteger a informação.

O objetivo da questão 3 foi verificar se a TI da organização estava alinhada com as estratégias organizacionais, nesta questão a maior parte dos entrevistados responderam que o nível de satisfação era satisfatório com 39,5%, tendo a TI alinhada com os negócios organizacionais da empresa entende-se que a TI é utilizada para ajudar a organização alcançar seus objetivos, portanto há um grande fluxo de informações gerenciadas por banco de dados que utilizam sistemas de informação, observa-se neste resultado que a informação torna-se importante para a maioria das organizações que os entrevistados atuam portanto é de grande prudência estas organizações terem um nível elevado de satisfação nas questões anteriores dando a devida importância para a informação e estando preparada para se recuperar de um possível incidente.

A questão numero 4 é uma questão muito importante pois o objetivo é saber se alta gerencia da o apoio necessário para adoção/aprovação de novas políticas de segurança da informação, a maioria dos entrevistados responderam que o nível de satisfação é satisfatório com 34,2%, seguido de regularmente satisfatório com 26,3%, o apoio da alta gerencia é de extrema importância para o cumprimento das boas praticas, pois sem a divulgação, treinamento e medidas corretivas em caso de descumprimento de alguma norma, esta pratica adotada não será cumprida de maneira correta na organização levando assim a anulação dos benefícios que uma política de segurança pode trazer para uma organização, em comparação a questão 1 a maioria dos entrevistados que responderam que a organização da a devida importância para a informação também informaram que a alta gerencia da organização da o apoio devido e esta envolvida na adoção/aprovação de novas políticas.

Em relação a questão numero 5 onde o objetivo é saber se o grau de disseminação das boas praticas de segurança e de *backup* são satisfatórios a maioria dos entrevistados com 36,8% responderam regularmente satisfatório e apenas 26,3% satisfatório em comparação com a questão numero 4 onde o apoio da alta gerencia também visa disseminar as boas praticas adotadas pode-se observar

que este apoio da alta gerencia não é tão satisfatório como deveria pois a maioria dos entrevistados responderam como regularmente satisfatório e observa-se que na questão numero 4 a maioria respondeu como satisfatório o nível de apoio da alta gerencia, isso pode ser uma das causas que podem afetar o despreparo das organizações em dar continuidade no negócio e de estarem vulneráveis a perda de informações.

A questão numero 6 visa verificar se a organização atende os princípios da segurança da informação que são Disponibilidade, Integridade, Confidencialidade, Legalidade, Auditabilidade e Não repúdio, a maioria dos entrevistados reponderam que a organização atende de forma regularmente satisfatória com 34,2% seguido de 31,6% satisfatório, uma política de segurança da informação que não segue os princípios de segurança da informação de forma satisfatória corre sérios riscos de vulnerabilidade, portanto uma boa parte dos entrevistados que responderam a questão 1 e 2 de forma satisfatória, mesmo respondendo que adotam um política de segurança da informação e estão preparados para dar continuidade no negócio não estão adotando uma política de segurança de nível satisfatório portanto também não estão preparados de forma satisfatória para dar continuidade no negócio.

Os resultados da questão numero 7 onde o objetivo é verificar o nível de qualidade dos backups, a maioria dos entrevistados responderam de forma satisfatória com 36,8%, seguido de regularmente satisfatório com 23,7% e 21,1% insatisfatório, em comparação com a questão numero 2 onde a maioria dos entrevistados 31,5% responderam de forma totalmente satisfatória, pode-se notar que uma boa parte dos entrevistados que responderam de forma satisfatória a questão numero 2 não estão realmente preparados para se recuperar de um incidente de informação pois um *backup* sem qualidade é inútil para recuperar informações perdidas, nota-se também que o nível regularmente satisfatório e insatisfatório tem uma boa parte das respostas, isso mostra que muitas empresas não estão dando a devida importância para a informação, pois não basta realizar *backup* sem este *backup* não cumprir o objetivo de restaurar os dados.

A questão numero 8 visa verificar se a política de *backup* adotada na organização garante o armazenamento seguro e a qualidade dos *backups* realizados, a grande maioria dos entrevistados reponderam que este nível é satisfatório com 34,2% e totalmente satisfatório com 26,3%, pode-se observar que nesta questão os entrevistados acham que a política de backup adotada atende a

qualidade dos *backups* e o armazenamento seguro, porem em comparação com a questão numero 7 uma parte dos entrevistados deve se atentar a qualidade dos *backups* pois o resultado da sétima questão impacta diretamente na oitava e na questão 7 os resultados não foram tão positivos quanto na oitava questão, pode-se dizer que uma política de backup que não se preocupa com a qualidade de um *backup* não é uma política que atende de forma satisfatória uma organização.

Na questão numero 9 foi analisado o nível de qualidade das mídias onde se armazena os *backups,* grande parte dos usuários responderam que a qualidade das mídias são satisfatória com 39,5% seguido de 31,6% totalmente satisfatório, comparando a questão 9 e 8 nota-se que ao menos neste quesito as organizações estão atentas, pois se preocupam com a mídia onde é armazenado o *backup* melhorando a qualidade do *backup* e diminuindo possíveis problemas ao realizarem o *restore* dos dados.

A ultima questão, a numero 10, tem o objetivo de verificar se a política de *backup* adotada pela organização dos entrevistados garante a recuperação de informação em caso de incidentes e perdas de informação, grande parte dos entrevistados responderam que a política adotada atende garante a recuperação dos dados de forma satisfatória com 39,5% em seguida totalmente satisfatório com 23,7%, comparando a questão 10 com a numero 9 e 8 a maior parte dos entrevistados tem noção sobre a qualidade que um backup tem que ter e o objetivo de uma política de backup que é a recuperação de dados, estas 3 questões tiveram em sua maioria, respostas positivas porem se comparadas com a questão numero 7 pode-se notar que nem todas as organizações realmente realizam procedimentos que testam a qualidade do *backup* de forma satisfatória, portanto é de muito valia se atentar á todos os processos de uma política de *backup* ou de segurança da informação pois se um procedimento for esquecido ou não cumprido pode acarretar em resultados insatisfatórios, de forma geral nota-se que os entrevistados tem noção sobre a importância da informação e de uma política de backup, porem muitas vezes deixam de fazer tais procedimentos por falta de tempo e consequentemente por falta de conhecer ferramentas automatizadas que se encarregam de fazer o *backup* e testar sua qualidade.

4 CONCLUSÃO

A partir dos dados colhidos através do questionário é possível concluir que ao menos na região de Americana-SP, as organizações tem ciência da importância da informação para uma organização. Ainda há uma parcela que ainda não dá a devida atenção, como pode-se observar na questão numero 1 onde 15,8% dos entrevistados informam que a organização não dá a devida importância para a informação, por este motivo as organizações correm sérios riscos pois, o bem mais valioso de uma organização é a informação, como já citado por vários autores neste trabalho. Pode-se notar que, na segunda pergunta do questionário, apesar da maioria dos entrevistados disserem que a organização esta preparada para minimizar o impacto de um desastre, também há uma parte com 18,4% informando que o nível de preparação é insatisfatório, empatando com o nível satisfatório, deixando a desejar pois não é totalmente satisfatório.

Outro resultado curioso da pesquisa elaborada é questão 3, onde se mede o alinhamento da TI com as estratégias de negócio. A maior parte dos entrevistados informou que este alinhamento é satisfatório, porém pode melhorar para totalmente satisfatório. Este alinhamento é extremamente importante para o sucesso da organização, mas uma organização que não da a devida importância para a informação também não pode perceber o valor desta se bem utilizada através da TI. 13,2% dos entrevistados informaram que o nível de alinhamento é insatisfatório. A questão numero 4 é uma das mais importantes, se não a mais importante, pois sem o apoio da alta gerência para executar qualquer tarefa dentro de uma organização esta tarefa tem um curto prazo de duração ou não é executada de forma correta, como por exemplo uma política de segurança da informação sem o apoio necessário da alta gerência para penalizar o descumprimento de uma política, esta política não terá os resultados desejados pois não será cumprida de forma adequada e no resultado colhido. Esta questão é a que tem menos entrevistados que escolheram a opção ‘Totalmente satisfatório’, com 5,3%. Logo pode-se observar que neste quesito as organizações ainda tem muito a melhorar para alcançar um resultado mais consistente em seus objetivos.

De forma geral, a maioria das organizações apresentam um resultado positivo diferente até do esperado, porém ainda existem organizações que não se

preocupam com a informação, com processos de *backup* e armazenamento, e tampouco estão preparadas para minimizar os impactos que um incidente pode causa, e também para recuperar informações por falta de elaborar uma boa estratégia de backup; e se elaborada uma estratégia, esta estratégia não é cumprida de forma correta por falta de apoio total da alta gerência, consequentemente isso influencia no desempenho de uma organização por estar vulnerável a vários tipos de desastres. No mundo onde a informação é essencial para o sucesso organizacional, pode-se dizer que a perda da informação ou a falta de tratamento dela com políticas de backup, políticas de segurança e sistemas de gerenciamento, pode levar a organização ao fracasso em termos de competitividade, bem como sua lucratividade, causando muitas vezes a falência.

O levantamento bibliográfico feito neste trabalho contribuiu para o melhor entendimento de como a informação é importante para os negócios, pode-se notar como a informação afeta o jeito de gerir de uma organização, pois hoje em dia a maneira de gerir uma organização foi muito afetada pela era da informação devido a TI e a tecnologia de comunicação, nota-se que através da informação as organizações se tornam cada vez mais competitivas no mercado e a margem de erro se torna cada vez menor, pode-se notar também que muitos autores ressaltam a importância do papel da TI no objetivo estratégico pois uma TI bem alinhada com os objetivos estratégicos organizacionais podem trazer lucros para a empresa através de seus recursos, benefícios e serviços, além de manter a empresa no mercado competitivo e torna-la cada vez mais competitiva, para ajudar neste alinhamento nota-se também a importância da adoção de modelos de boas praticas como o ITIL e o COBIT onde através destes modelos pode-se monitorar as atividades de TI, diminuindo os riscos e entregando serviços de qualidade, após perceber a importância da informação na organização, como ela afeta o sucesso organizacional e como afeta a estratégia de gestão, foi também estudado através de obras literárias de vários autores como proteger esta informação e dar continuidade no negócio caso ocorra algum incidente de segurança da informação, através da adoção de políticas de segurança da informação, onde o foco é proteger esta informação de incidentes, furtos ou mal uso, políticas de *backup* onde o foco é a adoção de boas praticas de *backup* para tornar possível a recuperação da informação caso ocorra perdas e o plano de continuidade do negócio onde o objetivo é minimizar incidentes que não puderam ser evitados através de adoção de

estratégias de contingência e restaurar totalmente ou parcialmente o ambiente atingindo.

O levantamento bibliográfico ajudou na compreensão da importância da informação, como ela afeta os negócios e o perigo que uma organização corre quando não da a devida importância para a informação, não adotando políticas de segurança da informação, políticas de backup e plano de continuidade do negócio.

REFERÊNCIAS

ABREU, Aline França. **Tecnologia da informação aplicada a sistemas de informação empresariais:** o papel estratégico da informação e dos sistemas de informação nas empresas. 4. ed. São Paulo: Atlas, 2006.

ALBERTIN, A. L. **Enfoque gerencial dos benefícios e desafios da tecnologia da informação para o desempenho empresarial.** São Paulo: FGV-EASP, 2003. (Relatório de Pesquisa FGV/EASP/NPP, 20).

_____; ALBERTIN, R. M. M. **Tecnologia da informação e desempenho empresarial:** as dimensões de seu uso e sua relação com os benefícios de negócio. 2. ed. São Paulo: Atlas, 2009.

ALBERTIN, Rosa Maria de Moura; ALBERTIN, Alberto Luiz. **Estratégias de governança de tecnologia da informação:** Estruturas e Práticas. Rio de Janeiro: Elsevier, 2010.

_____. BLOG TSG: **ITIL**. Disponível em:< tsg-ufam.blogspot.com>. Acesso em: 18 out. 2015.

_____. Cartilha de segurança para a internet. **7. Mecanismos de segurança.** 2012. Disponível em: <http://cartilha.cert.br/mecanismos/>. Acesso em: 07 out. 2015.

_____. Celta Informática Tecnologia que agrega valor. **Governança de tecnologia da informação.** Disponível em:< http://www.celtainformatica.com.br/servicos/governanca-de-tecnologia-da-informacao>. Acesso em: 17 out. 2015.

CORDEIRO, José Vicente B. de Mello; RIBEIRO Renato Vieira. **Gestão da empresa.** Coleção Gestão Empresarial / FAE / Gazeta do Povo, fascículo 2. Curitiba: Associação Franciscana de Ensino Senhor Bom Jesus, 2002.

CHIAVENATO, Idalberto. **Introdução a teoria geral da administração.** 7. ed. Rio de Janeiro: Elsevier, 2003.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel Books, 2000.

FERREIRA, Fernando Nicolau Freitas.; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação:** Guia Prático para elaboração e Implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FERNANDES, Aguinaldo Aragon. ABREU, Vladimir Ferraz de. **Implantando a governança de ti:** da estratégia à Gestão dos Processos e Serviços. 3. ed. Rio de Janeiro: Brasport, 2012.

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

FORREST. **Forrester measuring the business value of it,** 2006. Disponível em:< https://www.forrester.com/search?N=20242+10001&sort=3&everything=true&source=browse>. Acesso em: 12/10/2015.

GODOY, Arilda Schmidt. **Pesquisa qualitativa tipos fundamentais.** São Paulo: Revista de Administração de Empresas - RAE Fundação Getúlio Vargas, v. 35, n 3, maio/junho 1995.

GREMBERGEN, W. **The balanced scorecard and it governance,** 2004. Information System Control Journal.

HATCH, M. J. **Organization theory:** modern, symbolic and postmodern perspectives. Nova York: Oxford University Press, 1997.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Guia de melhores práticas de governança para fundações e institutos empresariais.** Disponível em:< http://www.ibgc.org.br/index.php>. Acesso em: 17 out. 2015.

IRELAND, Michael A. Hitt R. Duane; HOSKISSON, Robert E. **Administração estratégica.** 2. ed. São Paulo: Cengage Learning, 2011.

ISACA. **COBIT®.** Disponível em:< https://cobitonline.isaca.org/>. Acesso em: 18 out. 2015.

IT GOVERNANCE INSTITUTE. COBIT M**anagement guidelines.** 2000. Disponível em:< http://www.isaca.org/Journal/archives/2000/Volume-6/Pages/Management-Guidelines-for-COBIT.aspx>. Acesso em: 11 out. 2015

ITIL official, 2007. Disponível em:< https://www.axelos.com/best-practice-solutions/itil/what-is-itil>. Acesso em 18 out. 2015.

JORDAN, E.; MUSSON, D. **Corporate governance and it governance:** exploring the board's perspective. 2004. Disponível em:< http://papers.ssrn.com/sol3/papers.cfm?abstract_id=787346>. Acesso em: 12 out. 2015.

LAUDON, Kennetch C; LAUDON, Jane P.**Sistemas de informação gerenciais.** 7. ed. São Paulo: Pearson Prentice Hall, 2007.

LEVINE, David M; BERENSON, Mark L; STEPHAN, David. **Estatística:** teoria e aplicações. Rio de Janeiro: LTC, 2000.

LOBATO, D. M. et al. **Estratégia de empresas.** Rio de Janeiro: FGV, 2003.

MAGALHÃES, Ivan Luizio.; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de ti na prática:** Uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

MAÑAS, Antonio Vico. **Administração de sistemas de informação:** Como otimizar a empresa por meio dos sistemas de informação. 7. ed. São Paulo: Érica, 2007.

MCFARLAN, E. W.; MCKENNEY, J. L.; PYBURN, P. **"The information archipelago: plotting a course."** Harvard Business Review, Boston, v. 6, n.1, p. 145-156, jan. 1983.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson, 2003.

MURPHY, T. **Achieving business value from technology:** a pratical guide for today's executive. Nova Jersey: John Wiley & Sons, 2002.

ORLIKOWSKI, W. J. **"Using technology and constituting structures:** a practice lens for studying technology in organizations." Oraganization Science, v. 11, n. 4, p. 404-428 jul.-aug. 2000.

PEREIRA, Júlio Cesar. R. **Análise dados qualitativos:** Estratégias Metodológicas para as Ciências da Saúde, Humanas e Sociais. São Paulo: Editora da Universidade de São Paulo, 2001.

PETERSON, R. R. **"Crafting information technology governance."** Information Systems Management Journal, Londres, v. 21, n. 4, p. 7-22, outono de 2004b.

Pink elephant: knowledge translated into results. Disponível em: < http://www.pinkelephant.com/ResourceCenter >. Acesso em: 17 out. 2015.

ROCKART, J. F.; EARL, M. J.; ROSS, J. W. **"Eight imperatives for the new it organization."** Sloan Management Review, Massachusetts, v. 38, n. 1, p. 43-55, Fall 1996.

ROCKART, J. F.; MORTON, M. S. **Implications of changes in information thechnology for corporate strategy.** Interfaces, v.14, n.1, Jan./Fev. 1984, p. 84-95.

ROSINI, Alessandro Marco; PALMISANO, Ângelo. **Administração de sistemas de informação e a gestão do conhecimento.** São Paulo: Pioneira Thomson Learning, 2003.

SAMPAIO, Járder dos Reis. **Metodologia de pesquisa científica** - A pesquisa qualitativa entre a fenomenologia e o empirismo formal. São Paulo: Revista de Administração de Empresas RAE - FEA/USP, v. 36, n. 2, abril/junho 2001.

SCOTT, G. M. **"Still not solved: the present problem of it strategic planing."** Communications of the Association for information Systems, Atlanta, v. 16, p 2-62, dez. 2005.

SÊMOLA, Marcos. **Gestão da segurança da informação**: Uma visão Executiva. Rio de Janeiro: Campus, 2003.

STITUTE®.**Board briefing on it governance.** 2nd Ed.,United States of America: ITGI, 2003.

_____. STRATEGIA Gestão Empresarial. **Governança corporativa.** Disponível em:< http://www.strategia.srv.br/novo/sucessao-familiar/ >. Acesso em: 17 out. 2015.

_____. **Tribunal de contas da união. fiscalização a serviço da sociedade.** Disponível em:< http://portal.tcu.gov.br/comunidades/fiscalizacao-de-desestatizacao-e-regulacao/home/home.htm >. Acesso em: 17 out. 2015.

TRIVIÑOS, Augusto N. S. **Introdução à pesquisa em ciências sociais** - A Pesquisa Qualitativa em Educação. São Paulo: Atlas, 1987.

TURBAN, Efraim.; VOLONINO, Linda. **Tecnologia da informação para gestão**: Em busca do melhor desempenho estratégico e operacional**.** 8. ed. Porto Alegre: Bookman, 2013.

WEILL, Peter; ROSS W. Jeanne. **Governança de tecnologia da informação.** Editora M.Books do Brasil. São Paulo, 2006.

WEILL, P.; ROSS, J. W. **IT governances: how topo performers manage it decisions rights for superior results.** Boston: Harvard Business School Press, 2004.

.

APÊNDICE A – MODELO DO QUESTIONÁRIO APLICADO

Por favor, selecione os números de 1 à 5 correspondentes à sua percepção sobre as perguntas abaixo, sendo 1 = totalmente insatisfatório, 2 = insatisfatório, 3 = regularmente satisfatório, 4 = satisfatório e 5 = totalmente satisfatório.

A importância de uma política de backup nas organizações

1. A organização em que atua da a devida importância para a informação adotando boas práticas, utilizando-se de políticas de backup e políticas de segurança da informação?

1	2	3	4	5

2. Em caso de algum acidente que cause perda de informações ou paralisação de serviços qual o nível de preparação para diminuir os danos causados e dar continuidade no negócio que a organização se encontra?

1	2	3	4	5

3. Qual o nível do alinhamento da Tecnologia da Informação (TI) com os negócios da empresa e seus objetivos de mercado?

1	2	3	4	5

4. Qual é o nível de envolvimento da alta gerencia na adoção/aprovação de novas políticas de segurança da informação?

1	2	3	4	5

5. O grau de disseminação sobre as boas praticas de segurança e a importância do backup na organização são satisfatórios?

1	2	3	4	5

6. Em relação aos princípios da segurança da informação que são: Disponibilidade, Integridade, Confidencialidade, Legalidade, Auditabilidade e Não repúdio qual o nível de cumprimento destes princípios na corporação?

1	2	3	4	5

7. Ao realizar um backup deve-se atestar a sua qualidade através da restauração, para usa-lo em caso de perda de informação, qual o nível de qualidade dos backups em sua organização?

1	2	3	4	5

8. A política de backup adotada em sua organização garante o armazenamento seguro e a qualidade dos backups realizados?

1	2	3	4	5

9. As mídias onde são armazenado os backups são de qualidade?

1	2	3	4	5

10. A atual política de backup garante a recuperação da informação em caso de incidentes e perda de informação?

1	2	3	4	5