IMPLEMENTAÇÃO DE POLITICAS DE SEGURANCA DA INFORMAÇÃO EM UMA EMPRESA DO COMÉRCIO ATACADISTA

Cristhian Gassen[1]
Marilei de Fátima Kovatli[2]

RESUMO

Com o crescente avanço das tecnologias de informação e com a rápida globalização aumentaram também os crimes relacionados a ela, surgindo assim a necessidade de manter as informações das empresas livres de riscos e perigos que possam comprometer sua integridade. Portanto, estudar sobre este assunto significa buscar maior conhecimento para conseguir entender a necessidade de implantar a segurança da informação nas empresas. O objetivo deste trabalho é realizar a análise de uma empresa do comércio varejista e abordar sobre os assuntos de melhoria da segurança da informação, suas formas de gestão e principais finalidades, tendo como objeto de pesquisa as informações contidas em bibliografias e websites. Analisam-se os riscos, tais como: ameaças, ataques e vulnerabilidades, entre outros tópicos. Propõe possíveis soluções à prevenção e conservação da informação, utilizando-se de várias estratégias baseadas na tecnologia da informação, como as barreiras de segurança e principalmente a proposta de implementação de uma política de segurança da informação. Com esta proposta se espera alcançar vários pontos importantes para a segurança da empresa e de seus bens, bem como que ela traga benefícios que devem auxiliar na busca pela vantagem competitiva da empresa e no seu sucesso futuro.

Palavras-chaves: Informação - Segurança da informação – Tecnologia – Riscos.

ABSTRACT

With the growing advancement of information technologies and the fast globalization, related crimes also increased, creating the need to keep the company informations away from risks and threats that could compromise its integrity. Therefore, to study about this subject means to search for better knowledge to understand the need to deploy information security in companies. The objective of this work is to create an analysis of a retail business and talk about the information security improvements, its management models and its main goals, having the research object based on

[1] Acadêmico do Curso de Gestão da Tecnologia da Informação – 6º Semestre. Faculdades Integradas Machado de Assis. cristhiangassen@hotmail.com
[2] Mestre em Ciência da computação. Orientadora. Professora do urso de Gestão da Tecnologia da Informação. Faculdades Integradas Machado de Assis. marilei_gti@fema.com.br

bibliographies and web sites. The risks are analyzed, such as: threats, attacks and vulnerabilities, among others topics. It proposes possible solutions to the prevention and conservation of the information, using several strategies based on information tecnology, as the security barriers and mainly the proposal of an information security policy. With this proposal, it is expected to reach several important points for the security and assets of the company, such as bringing benefits to help in the search for competitive advantage and the future success of the company.

Keywords: Information - Information Security – Technology – Risks.

INTRODUÇÃO

Com o avanço das tecnologias, está cada vez mais difícil acompanhar suas evoluções, e com a crescente valorização das informações, é necessário estar atento para toda e qualquer ameaça gerada pela mesma.

Feito as devidas análises e estudos foi definido o seguinte tema para este projeto: proposta de implementação de políticas de segurança da informação em uma empresa do comércio atacadista.

Assim que foi feita a análise das novas tecnologias, das novas formas de gerir e estudar como a empresa funciona, o tema delimita-se da seguinte forma: implementação de políticas de segurança da informação na empresa do comércio atacadista Topflex Distribuidor de Alimentos Ltda., localizada no município de Santa Rosa, na região noroeste do estado do Rio Grande do Sul, Brasil.

Foi analisado que a empresa não conta com regras básicas de segurança para suas informações, o que influencia para o futuro da organização, possui servidores ao acesso livre de quaisquer funcionários e apenas senhas básicas para o seu ERP[3]. Cabe ressaltar também que a empresa acessa seu sistema ERP na nuvem e a segurança do mesmo é feita por terceiros.

Percebe-se a inexistência do correto gerenciamento da segurança dos dados e de padrões de normas exigidos para o controle de acessos, impedindo a confidencialidade das informações da empresa.

Fazendo a análise das ideias e problemas percebidos, o desenvolvimento do projeto justifica-se desta maneira: ocasionar maior segurança para a empresa em toda a área de TI, construindo junto a empresa uma política de segurança da informação

[3] Enterprise Resource Planning - Planejamento de recursos da empresa.

que se adeque ao seu dia-a-dia, sendo que a empresa é voltada para o comércio e consta com uma vasta área de atendimento.

1 INFORMAÇÃO

Hoje, no mundo informatizado em que vivemos, podemos concordar com Fontes “A informação sempre foi um dos bens mais importantes da organização. A diferença é que há alguns anos a informação mais crítica para a empresa poderia ser guardada e trancada dentro de uma gaveta” (FONTES, 2008, p. 18).

Na era da informação, qualquer mínima informação pode ser crucial para o sucesso ou ruína de uma empresa, podemos ver isto com um argumento de Rayward “o documento é o centro de um processo de comunicação complexo, da acumulação e transmissão do conhecimento, da criação e evolução das instituições” (RAYWARD, 1991, p.137). Sendo assim para Rezende e Abreu:

> A informação tem valor altamente significativo e pode representar grande poder para quem a possui, indivíduos ou instituição. Ela está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos e tecnologia. (REZENDE; ABREU, 2000, p 90)

Assim, é possível ter uma noção básica de como a informação está mudando o rumo do mundo, é, então, nesse ponto que entra a tecnologia na história, ela que está permitindo cada vez mais que resquícios de informação se tornem um bem muito valioso para as organizações.

Rezende e Abreu ainda completam que “a informação e o conhecimento serão os diferenciais das empresas e dos profissionais que pretendem destacar-se no mercado e manter a sua competitividade” (REZENDE; ABREU, 2000, p. 92).

Com a globalização tudo está sofrendo uma constante evolução e esta mudança está mudando o estilo de pensamento dos empresários, ela está modificando o modo em que uma organização cria, filtra, organiza, cuida e utiliza a informação. Um dos principais motivos desta mudança é a tecnologia da informação, que está promovendo a facilidade de compartilhar quaisquer tipos de informações, seja texto, áudio, vídeo ou qualquer outro tipo de mídia digital.

1.1 TECNOLOGIA DA INFORMAÇÃO

A Tecnologia da Informação (TI) vem tomando conta do mundo, a cada dia está mais visível que qualquer empresa necessita dela para sobreviver. Uma organização que não investe em TI é uma organização que aos poucos vai deixando de competir no mercado de trabalho, pois deveria utilizar a tecnologia como aliada para os negócios.

Segundo Laurindo et al., a TI é vista como a fonte de criação de novas estratégias de negócio, de novas estruturas organizacionais e de novas formas de relacionamento entre empresas e entre empresas e seus consumidores (LAURINDO et al., 2012).

Atualmente, o fácil acesso às informações, a chegada da internet e a tecnologia na palma de nossa mão trouxeram grandes mudanças para o mercado e a busca da maleabilidade para acompanhar o ritmo das mudanças. De acordo com Plachta, a aplicação da TI deve possuir os seguintes objetivos:

> Apoiar os processos de negócio, garantindo sua continuidade; auxiliar na tomada de decisões; aumentar a produtividade; otimizar a troca de informações internas e externas; garantir a segurança das informações; buscar novos negócios; e muito mais, ou seja, “maximizar o negócio”. (PLACHTA, 2013, p. 26)

A TI veio para descomplicar o mundo, a facilidade que ela traz proporcionou uma grande alteração nas organizações, fazendo diferença desde o aumento da produtividade até a busca por novos negócios. Neste contexto Mcgee e Prusak enfatizam que:

> Numa economia de informação, a concorrência entre as organizações baseia-se em sua capacidade de adquirir, tratar, interpretar e utilizar a informação de forma eficaz. As organizações que lideram essa competição serão as grandes vencedoras do futuro, enquanto as que não o fizerem serão facilmente vencidas por seus concorrentes. (MCGEE; PRUSAK, 1994, p. 3)

Pensando em avanços tecnológicos, desde os primórdios quem era mais avançado tecnologicamente estava tecnicamente na frente de seus concorrentes, porém, até hoje existem os empresários que não buscam o novo, são contra

mudanças e isso, neste mundo de hoje, traz uma desvantagem considerável, pois o avanço tecnológico é global.

1.2 SEGURANÇA DA INFORMAÇÃO

Com toda a tecnologia envolvida em uma organização, não podemos mais pensar só em cofres para manter documentos a salvo, hoje a informação está em cada computador, celular e equipamentos eletrônicos usados para o trabalho. Sendo assim, a organização deve ficar atenta sobre a segurança de seus ativos para que seus recursos estejam protegidos. Segundo Fontes:

> Segurança da Informação é o 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 sua missão seja alcançada. (FONTES, 2006, p. 130)

Atualmente não podemos mais pensar que dados são apenas dados, hoje toda e qualquer informação é considerada como um ativo e tem um certo valor. As informações devem ser protegidas como se fossem o maior bem da empresa, mantendo-a disponível para o acesso somente às pessoas autorizadas, preservando as informações intactas, sempre sabendo quem está acessando e modificando as mesmas, nunca deixando de garantir a sua integridade. Fontes fala também que:

> A segurança da informação utilizada pela organização é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade, legalidade e auditabilidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado. (FONTES, 2008, p. 248)

Portanto, a tecnologia da informação não é apenas sobre ter dispositivos tecnológicos, para as organizações é considerada uma necessidade dos novos tempos, afinal as informações sempre existiram, mas nunca de uma forma tão volumosa e aproveitável.

> A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplicam-se tanto as informações corporativas quanto as pessoais. Entende-se por

> informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição. (ARAUJO, 2008, p. 55)

Para a CERT.BR (2016), as principais ameaças à segurança da informação para as organizações são mostradas na ilustração 1:

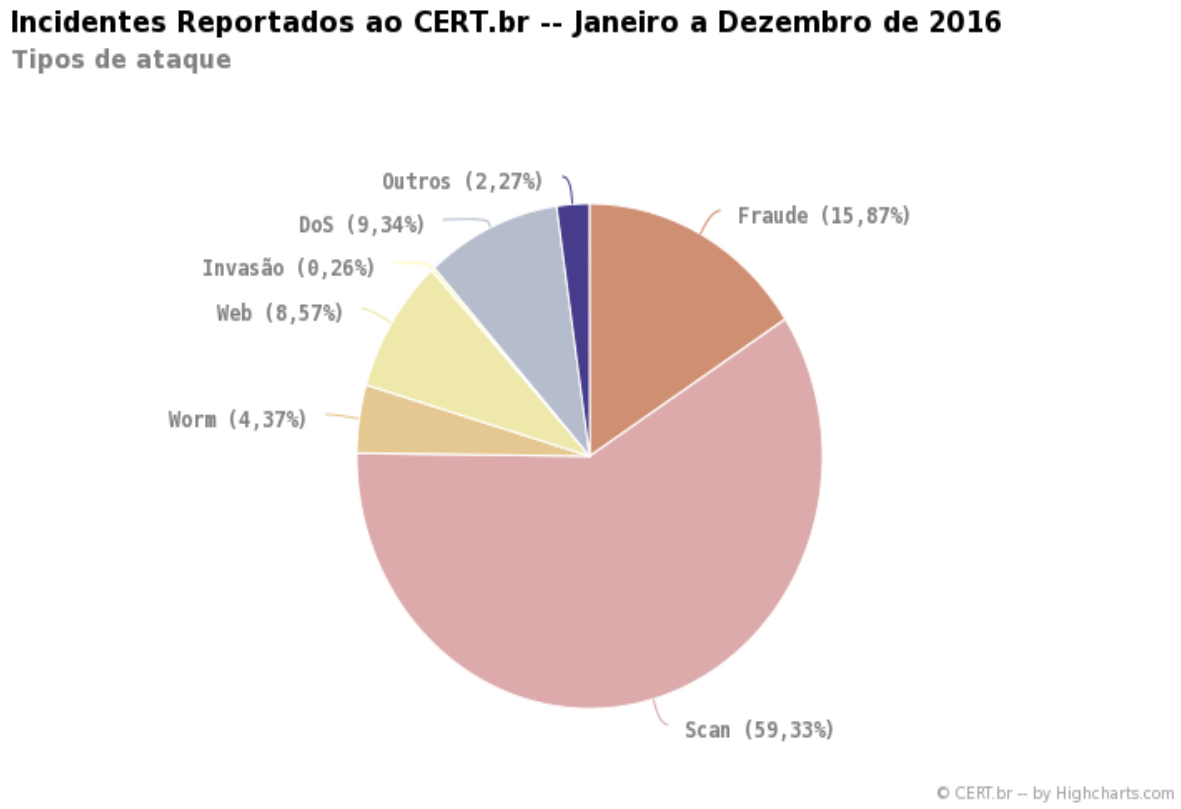

Ilustração 1: Incidentes reportados em 2016
Fonte: https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html (cert.br; 2016.)

Segundo a CERT.BR 2016:

Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

Web: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

Scan: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Fraude: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Outros: notificações de incidentes que não se enquadram nas categorias anteriores. (CERT.BR, 2016)

> A segurança da informação na organização deve ser encarada como um processo que existe com o objetivo de proteger os recursos de informação permitindo que, em relação a esse aspecto, o negócio da organização, seja realizado de forma correta e tenha continuidade ao longo do tempo. (FONTES, 2008, p. 223)

Cuidar da segurança da informação em uma empresa não é algo simples. Apenas ler a norma ISO/IEC 27002 e fazer uma política não significa que estará tudo pronto e as informações estarão seguras. Assim como em outras áreas da organização, a empresa tem que investir na criação e manutenção da área de TI com a infraestrutura necessária, profissionais especializados e incluindo um projeto, planejamento e acompanhamento, mapeando todas as situações que possam ferir os princípios da segurança da informação, sendo esse um fator que pode definir o sucesso ou o fracasso de uma empresa que pretende ter as informações gerenciais necessárias para a tomada de decisão.

Além disso, existem ferramentas de trabalho, normas e práticas que auxiliam na implantação de políticas de segurança, como o ITIL, COBiT e a própria NBR ISO 27002. São eles um suporte a organização que busca se adequar e conseguir uma certificação ou somente melhorar a segurança da sua organização.

1.3 ISO/IEC 27002

A ISO/IEC 27002 (antigo 17799:2005), é a norma internacional que estabelece o código de melhores práticas para apoiar a implementação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.

A ABNT sobre a norma “Esta Norma é projetada para as organizações usarem como uma referência na seleção de controles dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na ABNT NBR ISO/IEC 27001 ou como um documento de orientação para as organizações implementar controles de segurança da informação comumente aceitos. ” (NBR ISO/IEC 27002, 2013, p. 04)

Esta Norma Internacional se aplica a todos os tipos de organização (por exemplo: empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos), que pretendam gerir os riscos que poderiam comprometer a segurança da informação da organização como um todo (ISO/IEC 27005, 2008).

É uma norma formada por um conjunto de boas práticas, criada e mantida pelo Comitê Internacional ISO/IEC. Ela descreve estratégias de controle de segurança, análise e tratamento de riscos, gerenciamento da política de segurança, dos ativos, e da segurança dos recursos humanos, do ambiente e espaço físico, controle de acessos, gestão da infraestrutura tecnológica, conformidade com os requisitos legais e normas técnicas, entre outros.

Segundo Silva, Carvalho e Torres (2003), a proteção tem como objetivo as medidas que visam implantar um sistema de informação, com requisitos de inspecionar e detectar as ameaças para reduzir o impacto causado quando esses princípios se efetivam:

- ➔ Confidencialidade: Para que este princípio seja corretamente aplicado, o acesso às informações deve ser feito somente pelas pessoas explicitamente autorizadas;
- ➔ Integridade: Para garantir esse princípio é necessário ter a segurança que a informação acessada é confiável, estando completa e sem alterações;
- ➔ Disponibilidade: Para garantir esse princípio a informação deve estar disponível (acessível) para as pessoas autorizadas sempre que necessário.

Ferreira e Araujo adicionam dois princípios que são:

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

Pode-se observar a relação entre o ciclo de vida da informação, e suas propriedades, na ilustração 2:

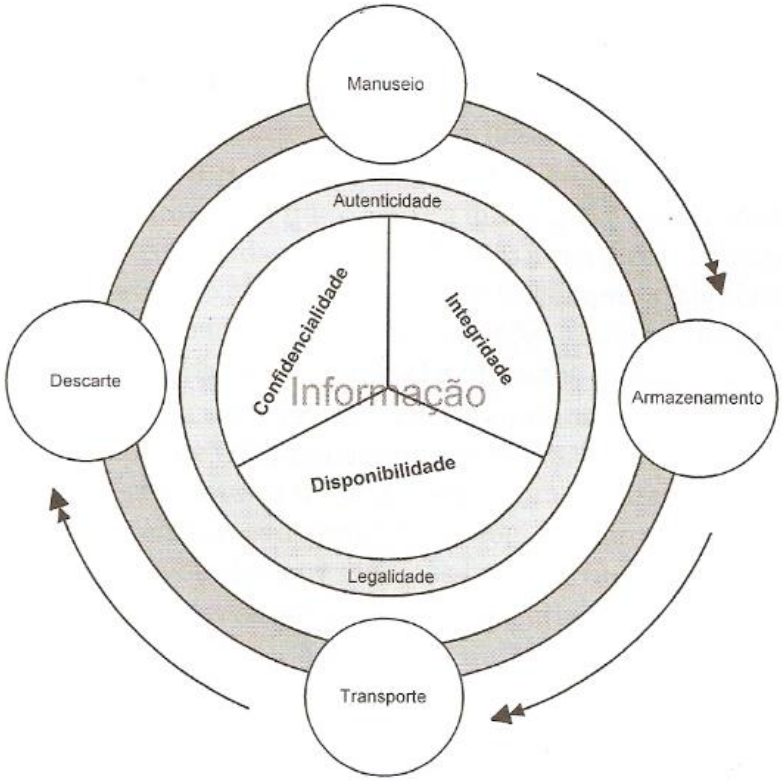

Ilustração 2: Ciclo de vida da informação
Fonte: SÊMOLA (2003)

A Segurança da Informação, para Dantas (2011), abrange ações para proteger informações contra ameaças, com a intuito de garantir a continuação das atividades de uma organização. Esse conceito para a segurança da informação é estabelecido pela norma ISO/IEC 27002:2005, que diz que deve haver preservação da confidencialidade, da integridade e da disponibilidade da informação.

Dividida em 11 seções que correspondem à gestão de segurança da informação, a contagem das seções principais estudadas começam no número 5 que estão descritas a seguir. As demais seções não se aplicam neste estudo.

Seção 5 – Política de segurança da informação

Seção 6 – Organizando a segurança da informação

Seção 7 – Gestão de ativos

Seção 8 – Segurança em recursos humanos

Seção 9 – Segurança física e do ambiente

Seção 10 – Gestão das operações e comunicações

Seção 11 – Controle de acesso

Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas de informação

Seção 13 – Gestão de incidentes de segurança da informação

Seção 14 – Gestão da continuidade do negócio

Seção 15 – Conformidade

Os benefícios proporcionados pela certificação ISO 27002 são significativos para as organizações, especialmente pelo fato de serem reconhecidas mundialmente. Quando aplicada da maneira correta ela melhora a conscientização sobre a segurança da informação, melhora o controle de ativos e informações sensíveis, facilita a implantação de políticas de controles, oportunidade de identificar e corrigir pontos fracos, redução do risco de responsabilidade pela não implementação de um SGSI ou determinação de políticas e procedimentos, torna-se um diferencial competitivo para a conquista de clientes que valorizam a certificação, melhor organização com processos e mecanismos bem desenhados e geridos, promove redução de custos com a prevenção de incidentes de segurança da informação, conformidade com a legislação e outras regulamentações.

1.4 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A política de segurança da informação é um documento que deve conter as normas, métodos e procedimentos que devem ser informados aos funcionários para que sejam cumpridas.

Segundo Ferreira e Araújo “a política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação. ” (FERREIRA; ARAÚJO, 2008, p. 36).

Para que seja funcional, a política de segurança deve ser estabelecida de maneira que controle o acesso de todas as informações sejam elas internamente ou externamente.

Ferreira e Araújo falam que “o assunto Segurança da informação tornou-se um dos temas mais importantes dentro das organizações, devido às fortes necessidades de proteção das informações e grande dependência de TI.” (FERREIRA; ARAÚJO, 2008, p. 43).

Para colocar a segurança da informação em ação deve-se ter em mente que elas mudarão toda a cultura da organização, logo, os funcionários devem estar preparados para as mudanças. Sem contar que as normas devem ter o apoio total da alta direção, sendo fundamental para que a mesma seja efetiva.

Para a criação desta política, Ferreira e Araújo recomendam a criação de um Comitê de Segurança da Informação. Este comitê deve ser formado por profissionais das mais diversas áreas da organização, pelo fato de diversos setores serem contemplados com ele. Inclusive devem-se categorizar as informações, afim de, delegar responsabilidades sobre elas e seus devidos gestores, pois são eles que irão controlar o acesso a elas. (FERREIRA; ARAÚJO, 2008, p. 60).

Já Fontes recomenda também a utilização de uma política principal, que descreva de forma clara como a empresa quer que a informação seja tratada, para que cada usuário tenha em mente suas obrigações para com ela. (FONTES, 2008).

Ferreira e Araújo ainda recomendam caracterizar o negócio como sendo o primeiro passo para desenvolver uma política de segurança, pois cada ramo exige requisitos diferentes. Também é importante definir a estrutura dele, se ele apresenta uma administração centralizada ou não. (FERREIRA; ARAÚJO, 2008).

2 METODOLOGIA

Nesta etapa será apresentado o tipo de pesquisa, o método de abordagem e os métodos de procedimento. Explanar, a categorização do estudo, além da geração de dados, a sua interpretação e a sua análise, no intuito de orientar o leitor no percurso adotado para a investigação.

2.1 CARACTERIZAÇÃO DA PESQUISA

O objetivo desta etapa é mostrar que tipo de pesquisa foi trabalhada e os métodos que foram utilizados ao decorrer da pesquisa

Quanto à natureza da pesquisa, representa uma pesquisa aplicada que, segundo Gil “abrange estudos elaborados com a finalidade de resolver problemas identificados no âmbito das sociedades em que os pesquisadores vivem. ” (GIL, 2010, p. 27). A pesquisa é aplicada porque investiga na empresa as falhas e os problemas e procura através de estudos a solução para eles.

No que se refere à abordagem ao problema, a pesquisa representa um caráter qualitativo. Prodanov afirma que, em uma pesquisa de abordagem qualitativa “o ambiente natural é fonte direta para coleta de dados, interpretação de fenômenos e atribuição de significados. ” (PRODANOV, 2013, p. 128). Desse modo a pesquisa envolveu a aplicação de um questionário aos colaboradores e gestores, com perguntas abertas que possibilitaram fazer uma análise dos dados coletados.

No que se refere aos objetivos, a pesquisa classificou-se como estudo exploratório, que conforme Cervo e Bervian, “é, normalmente, o passo inicial no processo de pesquisa pela experiência e um auxílio que traz a formulação de hipóteses significativas para posteriores pesquisas. ” (CERVO; BERVIAN, 2002, p. 69). A pesquisa é exploratória porque tem como características ouvir os envolvidos com os processos, os responsáveis pela empresa, os colaboradores e também a observação de como se desenvolvem os processos.

Nos procedimentos técnicos, a pesquisa é vista como bibliográfica, pois utilizou-se como fonte de pesquisa livros de autores específicos da área, também análise de documentos, como a norma ISO/IEC 27002 e sites de artigos científicos. Conforme Prodanov, a pesquisa é bibliográfica quando:

> Quando elaborada a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet, com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa. (PRODANOV, 2013, p. 54).

Depois de pronta a classificação dos métodos de pesquisa é possível, então, seguir para a etapa onde ocorrerá a coleta de dados.

2.2 GERAÇÃO DE DADOS

Na geração de dados é quando foram colhidos os dados do funcionamento da empresa ou como Marconi e Lakatos afirmam:

> A coleta de dados é o perfeito entrosamento entre tarefas organizacionais e administrativas com as científicas, obedecendo assim aos prazos estipulados, aos orçamentos previstos e ao preparo do pessoal, trazendo ao projeto uma melhor disposição e organização no seu andamento. (MARCONI; LAKATOS, 2003, p. 165)

Segundo Netto “questionário é uma série ordenada de perguntas que devem ser respondidas por escrito pelo informante” (NETTO, 2008, p. 84). Inicialmente foi aplicado um questionário aos colaboradores da empresa sobre como está o funcionamento da empesa em relação a área de TI e também de que forma a mesma está sendo organizada em relação a segurança da informação.

Diante disso, a técnica utilizada é a de documentação direta, na qual o levantamento das informações é feito através da observação do ambiente interno da empresa, como também através de conversas, em forma de entrevista, com o proprietário e gestor da mesma e em seguida com os colaboradores da empresa.

2.3 ANÁLISE E INTERPRETAÇÃO DE DADOS

Depois de obtidos os dados, chega a hora de transformá-los em informações, fazendo a análise e interpretação dos mesmos.

A análise e interpretação de dados são distintas, onde a análise é representada por evidenciar as relações existentes, com o fenômeno de estudo dividido em interpretação, explicação e especificação (MARCONI; LAKATOS, 2003).

É neste momento que foi colocada em prática a análise e interpretação de dados, esta etapa tem como objetivo observar a possibilidade de realizar o que foi proposto ao longo do projeto.

Segundo Prodanov, “essa fase da pesquisa, analítica e descritiva, prevê a interpretação e a análise dos dados tabulados, a análise e a interpretação desenvolvem-se a partir das evidencias observadas, de acordo com a metodologia”. (PRODANOV, 2013, p. 112).

Segue, a seguir, o questionário utilizado durante a geração dos dados:

1) A empresa consta com quantos funcionários?
2) A empresa conta com algum tipo de sistema de gestão?
3) Quantos e quais funcionários tem acesso ao sistema?
4) A empresa consta com algum tipo de Backup?
5) Onde se localiza e quantos funcionários tem acesso ao Backup?
6) O BKP é realizado de quanto a quanto tempo?
7) A empresa consta com algum tipo de políticas de segurança?
8) Como você considera a segurança da informação da empresa?
9) A empresa usa algum sistema informatizado?
10) Com que frequência você altera a sua senha do sistema da empresa?
11) Qual o principal meio de contato da empresa?
12) Existe alguma norma regulando o uso de redes sociais, E-mail particular e outros tipos de acesso à internet?

O questionário foi aplicado com os funcionários do escritório da empresa TopFlex que utilizam o sistema de soluções para gestão empresarial, gestão ERP, força de vendas e pronta entrega, tudo integrado e em tempo real, emissão de DANFE e boletos na entrega da mesma. Vale ressaltar que o sistema é acessado por conexão remota através da internet em um servidor de uma empresa privada localizada na cidade de Bento Gonçalves.

A empresa Topflex, TopFlex Distribuidor de Alimentos LTDA, se localiza na BR-472 em Santa Rosa, Rio Grande do Sul, Brasil, próxima ao parque de exposições de Santa Rosa, contando com cerca de 176 funcionários. A parte administrativa da empresa consta com os setores de Recursos Humanos, Financeiro, Faturamento, Tecnologia da Informação e setor de Serviços Gerais. Também conta com uma área de merchandising que consta com coordenadores e promotores. Na parte do depósito temos supervisores de logística e do depósito.

A parte de vendas da empresa é complexa, pois consta com duas equipes de vendas, a equipe de vendas varejo, por ser uma equipe maior e com produtos de pronta entrega, conta com um número maior de gerentes e supervisores. Já a equipe de vendas TD (Território do Distribuidor) é uma equipe menor que realiza apenas pedidos para posteriormente serem entregues. Esta apresentada na ilustração 3 o organograma dos setores da empresa.

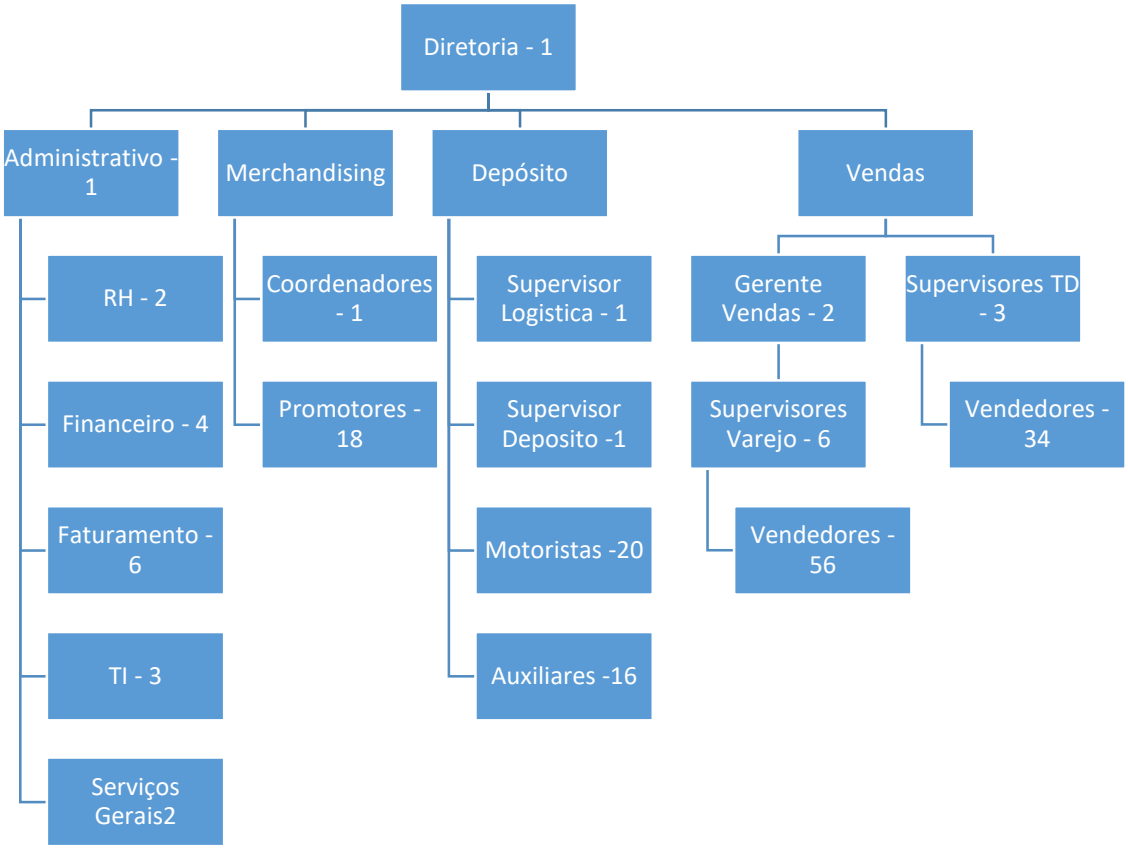

Ilustração 3: Organograma da empresa TopFlex
Fonte: Setor de Recursos Humanos da empresa TopFlex

Analisando o modo em que a empresa se organiza, foi possível visualizar que a empresa tem uma alta rotatividade de funcionários em todos os setores, um dos motivos é a contratação de estagiários para o auxílio em diversos setores da empresa.

Como adverte CHIAVENATO (2010), para operar de forma eficaz o sistema deve ter equilíbrio entre suas entradas e suas saídas. À rotatividade de pessoas é o fenômeno que indica o nível de intercâmbio destes recursos na organização e, portanto, possuem capacidade para influenciar nos processos e nos resultados da organização.

Devido a essa grande troca e novas contratações, mostra-se preocupante o quesito de segurança da informação.

Para os gestores de recursos humanos, conviver com os custos da rotatividade se tornou um constante desafio, pois com a saída de funcionários são inúmeras as obrigações a serem pagas pela empresa, e quanto maior a posição do colaborador, em relação ao nível hierárquico, maior é o impacto causado. (ASSIS, 2005).

Os custos da empresa na saída de um funcionário não é apenas acerto de contas, mas também fazer toda a alteração de cadastro de usuário e mudança de senhas e protocolos conhecidas pelo funcionário.

De acordo com a norma NBR ISO/IEC 27002, “a Segurança da Informação é obtida a partir da implementação de uma série de controles que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software. Esses controles precisam ser estabelecidos para garantir que os objetivos de segurança da organização sejam atendidos” (NBR ISSO/IEC 27002, 2005).

Foi analisado também que a empresa não consta com nenhum controle de armazenamento de segurança de dados (backup), assim qualquer sinistro que aconteça com o servidor de dados da organização, não há maneira de recuperar o que foi perdido.

Sobre o armazenamento e segurança dos dados Lyra esclarece que a norma ISO 17799 recomenda que as mídias de computador sejam controladas e fisicamente protegidas (LYRA, 2008). Analisando a situação da empresa sobre este quesito, justifica-se criar uma política que controle o acesso a fim de proteger esse acesso, evitando assim futuros incidentes e falhas sobre os backups.

Diante desta análise feita sobre a empresa foi elaborada a seguinte proposta de política de segurança da informação:

PROPOSTA DA POLÍTICA DE SEGURANÇA PARA A EMPRESA TOPFLEX

Introdução

Como Fontes afirma “A informação sempre foi um dos bens mais importantes da organização. A diferença é que há alguns anos a informação mais crítica para a empresa poderia ser guardada e trancada dentro de uma gaveta” (FONTES; EDISON, CISM, 2008, p. 110). Nesse documento apresenta-se um conjunto de instruções e procedimentos para normatizar e melhorar a visão e atuação em segurança.

A empresa e a política de segurança

Todas as normas aqui estabelecidas devem ser seguidas por todos os funcionários, parceiros e prestadores de serviços.

Ao receber essa cópia da Política de Segurança, o/a Sr./Sra. comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e

navegação na internet/intranet podem estar sendo monitorados. A equipe de segurança encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

O não cumprimento dessa política

O não comprimento dessas políticas acarretará em sanções administrativas em primeira instância, podendo acarretar no desligamento do funcionário de acordo com a gravidade da ocorrência.

Autenticação

As autenticações nos sistemas de informática serão baseadas em uma senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo. Infelizmente esse meio também é o mais inseguro. Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, brasil), datas (11092001) e outros são extremamente fáceis de descobrir.

Então aprenda a criar senha de forma coerente, observando nossa política de senhas.

Política de senhas

Uma senha segura deverá conter no mínimo 6 caracteres entre eles letras, números, caracteres especiais e com diferentes caixas.

As senhas terão um tempo de vida útil determinado pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas.

Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta-se à vontade para altera-la, mesmo antes do prazo determinado de validade. Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.

Política de e-mail

Não abra anexos com as extensões .**bat**, .**exe**, .**src**, .**lnk** e **.com** se não tiver certeza absoluta de que solicitou esse e-mail. Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. - Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, etc.

Não utilize o e-mail da empresa para assuntos pessoais. Não mande e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc). Evite anexos muito grandes. Utilize sempre sua assinatura criptográfica para troca interna de e-mails e quando necessário para os e-mails externos também

Políticas de acesso à Internet

O uso recreativo da internet não deverá se dar no horário de expediente. Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do supervisor. Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado. É proibido o uso de redes sócias não homologados/autorizados pela equipe de segurança e pelo supervisor imediato.

Lembrando novamente que o uso da internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

Política de uso de estação de trabalho

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretará em responsabilidade sua. Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou o console.

Não instale nenhum tipo de software/hardware sem autorização da equipe técnica ou de segurança.

Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria.

Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

Política Social

Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos. Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha. Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.

Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado. Nunca execute procedimentos técnicos cujas instruções tenham chego por e-mail. Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

Não traga use Pen Drives ou CDs de fora da empresa. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma verificação antes de ser liberado para uso. Reporte atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível. Suspeite de softwares que "você clica e não acontece nada".

Por fim, a política de segurança é finalizada e autenticada com a assinatura do gestor de TI responsável pela mesma.

Implantar um sistema de segurança da informação de alta competência nas organizações não extingue 100% das chances de um ataque, mas é de suma importância para restringir as probabilidades de perdas irreversíveis. O ideal é que gestores e responsáveis pela área de Tecnologia da Informação (TI) nas organizações desenvolvam infraestruturas de TI em parcerias com empresas peritas em soluções de segurança da informação, as quais, são voltadas apenas a análises e soluções sob medida às organizações, podem proporcionar resultados interessantes à organização e aos próprios profissionais de TI das empresas.

A política de segurança foi estruturada baseando-se nas recomendações da ISO 27002, além dos conhecimentos agregados de diversos autores sobre o assunto, e abrangendo todas as áreas que necessitam de atenção neste sentido em conjunto com o responsável pela organização.

Esta proposta apresenta os pontos que devem ser seguidos por todos os colaboradores para garantir que a política atinja seus objetivos.

Segundo Ferreira e Araujo “a política deve possuir a assinatura do principal executivo aprovando-a, a data da última atualização e do início de sua vigência” (FERREIRA; ARAUJO, 2008, p. 43).

Ferreira e Araujo afirmam também que “Após a elaboração da política devemos ter algumas ações para que a política seja de conhecimento e de uso pelos usuários.” (FERREIRA; ARAUJO, 2008, p. 11).

Será realizada uma divulgação ampla, geral e irrestrita para os usuários, o acesso a essa política pelos usuários estará de fácil acesso como em folhetos autoexplicativos, também colocada em murais da empresa, entrega uma cópia física para todos os colaboradores

CONCLUSÃO

Por meio desta pesquisa, e do estudo realizado, foi possível realizar uma avaliação da empresa TopFlex quanto à sua gestão de segurança da informação e métodos de segurança da informação, analisando seus controles e à observação as normas e legislações a que está sujeita.

Foi possível perceber que a gestão da segurança da informação da empresa analisada é um assunto que está em situação problemática, principalmente por não contar com uma política de segurança definida e de acesso a todos os colaboradores.

Por se tratar de uma empresa do comércio varejista e ter a necessidade de competitividade de mercado, a informação é algo considerado como elemento crítico, a ciência da política de segurança da empresa deve ser de conhecimento de todos, porém se faz necessário uma melhor prática para solução deste problema, mesmo diante de toda a complexidade de uma empresa de varejo.

Pode-se se observar também que a alta administração da TopFlex, através de seu planejamento estratégico e políticas orçamentárias, não levam em consideração as questões relacionadas à infraestrutura de tecnologia e o orçamento direcionado aos recursos de TI e a segurança da informação. Existe a falta de uma diretoria para tratar dos assuntos relacionados a TI, para isso, atualmente, a empresa conta com funcionários dotados de conhecimentos relacionados à área para tratar de assuntos como manutenção de dispositivos de tecnologia da informação. A alta direção de negócios da empresa é a mesma que faz a gestão da área de TI, sendo assim um atraso para a área.

Foi possível também a percepção da necessidade de determinadas melhorias em alguns processos tais como a prática de backup e o tratamento dos contratos de prestadores de serviços terceirizados, bem como a necessidade de incentivar uma melhor conscientização dos funcionários no que se refere à utilização de senhas de acesso à rede.

Outra observação importante é a preocupação evidente da administração da TopFlex com questões relativas à segurança de pessoal e do ambiente, existem implantados controles com o objetivo de prover a segurança dos seus clientes e colaboradores, porém existe uma falta de cuidados com os ativos de TI.

Após a análise completa é feita a seguinte conclusão: a empresa necessita de cuidados mais sérios sobre a segurança da informação, o começo ideal é a implementação de políticas de segurança da informação. Estas políticas terão benefícios em curto prazo como a formalização e documentação dos procedimentos de segurança adotados pela empresa, implementação de novos métodos de controles, prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou de desastres, maior segurança nos processos do negócio.

Com isso o estudante tem oportunidade de testar seus conhecimentos no ambiente organizacional, utilizando seus conhecimentos agregados no decorrer do curso, incentivando ele a propor melhorias, a partir da análise do contexto interno de uma empresa real.

Para a instituição de ensino contribui para o desenvolvimento educacional, criando assim material para futuras comparações entre políticas de segurança da informação desenvolvidas pelos acadêmicos, tendo este como suporte ao desenvolvimento de novas políticas ou mesmo para conhecimento especifico, além de, gerar material para pesquisas bibliográficas.

Para a empresa este trabalho tem relevância porque com a atribuição de políticas de segurança ela ganha uma maior confiança no serviço prestado, além de dar maior estabilidade e credibilidade, devido às boas práticas que deverão ser adequadas aos processos atuais. As melhores práticas além de auxiliar na segurança auxiliam na cultura interna da empresa, auxiliando seus funcionários a prestar um serviço de melhor qualidade, gerando satisfação do cliente externo e o interno.

REFERÊNCIAS

RAYWARD, W. B. **The case of Paul Otlet, pioneer of information science, internationalist, visionary**: reflections on biography. Journal of Librarianship and Information Science, London, v. 23, n. 23, p. 135-145, Sep. 1991.

Araujo, Nonata Silva. **Segurança da Informação (TI).** 2008

REZENDE, D.A.; ABREU, A. F. de. **Tecnologia da informação aplicada a sistemas de informações empresariais:** o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000.

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

FONTES, Edison. **Segurança da Informação**: o usuário faz a diferença. 1a edição. São Paulo: Saraiva, 2006.

LAURINDO, Fernando José Barbin; ROTONDARO, Roberto Gilioli. **Gestão Integrada de Processos e da Tecnologia da Informação**. São Paulo: Atlas, 2012.

PLACHTA, C. **A tecnologia no suporte a Gestão da Informação e aos Processos de Negócios Inteligentes. In:** STAREC, C. (org.). Gestão da informação, inovação e inteligência competitiva: como transformar a inovação em vantagem competitiva nas organizações. São Paulo: Saraiva, p. 91- 118, 2013.

MCGEE, J. e PRUSAK, L. **Gerenciamento estratégico da informação:** aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. 5ª ed. Tradução de Astrid Beatriz de Figueiredo. Rio de Janeiro: Campus, 1994.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de**. Política de segurança da informação**. 2ª ed. Rio de Janeiro. Ciência moderna Ltda., 2008.

LAKATOS, Eva Maria; MARCONI, Maria de Andrade. **Fundamentos da metodologia científica**. São Paulo: Atlas. 2010.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar. **Metodologia do trabalho científico:** métodos e técnicas da pesquisa e do trabalho acadêmico. Novo Hamburgo: Feevale, 2013.

VIANNA, Ilca Oliveira de Almeida. **Metodologia do trabalho científico:** um enfoque didático da produção científica. São Paulo: E.P.U., 2001.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. – 5. ed. – São Paulo: Atlas, 2010.

SEMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro, Campus, 2003.

CERT.BR, **Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil, Incidentes Reportados ao Cert**, Disponível em < https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>, acesso em 05 de Out. de 2017.

DANTAS, L.M. **Segurança da Informação - Uma Abordagem Focada em gestão de Riscos. Olinda. Livro Rapido**, 2011.

SILVA T.P; CARVALHO H; TORRES B.C. **Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial**. Portugal. Atlántico, 2003.

CHIAVENATO, Idalberto. **Gestão de Pessoas** 3.ed. Rio de Janeiro: Elsevier, 2010.

ASSIS, Marcelino Tadeu de. I**ndicadores de gestão de recursos humanos: usando indicadores demográficos, financeiros e de processos na gestão do capital humano** – Rio de Janeiro: Qualitymark, 2005.