SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO DA GLOBOAVES: unidade de Formiga/MG

INFORMATION SECURITY ADMINISTRATION THE GLOBOAVES: Unit Formiga/MG

Jordana Calixto de Faria*

Nivaldo Oliveira **

RESUMO
Em plena era de comunicação e tecnologias, e seu crescente avanço, a empresa Globoaves, inserida dentro deste contexto, expõe os controles de sua Política de Segurança da Informação dentro da sua administração. Esta empresa utiliza os recursos adequados para garantir a disponibilidade, confidencialidade e a integridade de suas informações? Este trabalho trata sobre a importância desta política aplicada dentro de uma instituição mostrando que pode oferecer diversas vantagens quanto ao seu plano de gerenciamento no que diz respeito a produtos/serviços e seus funcionários. Foi realizada uma entrevista semi-estruturada, tendo como sujeitos de pesquisa funcionários que trabalham diretamente com a política de segurança da informação e o diretor da unidade em Formiga/MG. Foram obtidos resultados de caráter prático perante os controles propostos na NBR ISO/IEC 27002 e seu alto grau de conformidade com a legislação e esta norma. Enfatiza o papel da Segurança da Informação para garantir a imagem da empresa que requer, portanto, a participação de todos os funcionários da organização.

Palavras-chave: Segurança da informação. NBR ISO ISO/IEC 27002. Gestão da informação.

ABSTRACT
In broad age of communication and technologies, and its growing advance, the company Globoaves, inserted into this context, expose the controls of its Politic of Safety of Information inside its administration. This company uses appropriate resources to ensure the availability, confidentiality and integrity of its information? This work treats about the importance of this politic applied inside an institution showing that it can offer several advantages about its plan of management in what it concerns to products/services and their employees. It was made a semi-structured interview, using as subjects of research employees who work directly with the politic of safety of information and the director of the unit in Formiga – Minas Gerais. There were obtained results of practical character for the controls proposed in NBR ISO/IEC 27002 and its high degree of conformity with the legislation and this rule. It emphasizes the role of Safety of Information to ensure the image of the company that requires, so, the participation of all the employees of the organization.

Keywords: Information Security. ISO/IEC 27002. Information management.

_____

1 INTRODUÇÃO

As decisões tomadas por diretores e executivos das grandes organizações podem ter um grande impacto no rendimento de suas empresas conforme as informações são geradas, enviadas e recebidas. A partir delas é que se dará a exploração das oportunidades de investimento e de riscos. Por isso, é necessário atenção a todos os acontecimentos dentro e fora do ambiente de trabalho.

Os dados processados incluem a informação de contato, históricos pessoais, registros financeiros, e identificadores oficiais tais como números de CPF, Título de eleitor, Identidade entre outros. Esta riqueza de informação permite que os negócios e o governo operem-se mais eficientemente. Porém, utilizados indevidamente pode

ocorrer na exposição das pessoas a quem a informação se relaciona a grandes riscos, tais como: roubo de identidade, perdas monetárias, de propriedade intelectual, de privacidade, de reputação, e chantagens.

Devido a essa acelerada gama de informações produzidas no mundo, faz-se necessário que a informação esteja acessível e segura, de um modo confidencial e íntegro, mas não só tecnologicamente. Nesse sentido a segurança da informação tem que ser tratada com seriedade e por uma gestão e técnicas adequadas

Através do estudo de caso em um Centro de Processamento de dados da empresa a Globoaves São Paulo Agroavícola Ltda, instalada em Formiga-MG, esse trabalho aborda a importância de uma Política de Segurança da Informação, e o propósito dessa política quanto à garantia de seus ativos, dando aos seus clientes, funcionários e interessados, o maior grau possível de garantia quanto à informação.

Mediante tais fatores, como a Política de Segurança da Informação é aplicada na empresa Globoaves São Paulo Agroavícola Ltda. - Unidade de Formiga-MG? Essa empresa utiliza os recursos adequados para garantir a Disponibilidade, Confidencialidade e a Integridade de suas informações? Estes são os questionamentos básicos que embasaram esta investigação.

O objetivo principal é descrever a importância da Política de Segurança da Informação para as informações geradas e correntes na Globoaves São Paulo Agroavícola Ltda.- Unidade de Formiga-MG, destacando os aspectos mais relevantes e o impacto para a organização.

Para maior compreensão da segurança da informação é importante conceituar adequadamente alguns termos sobre o tema proposto:

a) Informação: ativo que se fundamenta para gerenciar processos, administrar dados de forma que contribuía para o desenvolvimento do conhecimento (NBR/ISO/IEC17799, 2005);
b) gestão de risco: rotinas que afastam as incertezas dos processos e as medidas que minimizam as possibilidades de uma ameaça explorar uma vulnerabilidade e provocar impactos à confidencialidade, a integridade e a disponibilidade da informação (DAS; TENG, 1998);
c) ameaças: razão espontâneo ou potencial que pode resultar em prejuízo a alguém ou alguma organização (FONSECA, 2008);
d) vulnerabilidades: É uma fraqueza que pode ser disparada acidentalmente ou explorada intencionalmente. Exemplos: contas sem senha; falhas em programas aplicativos ou sistemas operacionais: buffer, overflow em serviços DNS, SMTP, comandos SQL e outros (AGÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO, 2011).

É necessário também, analisar criticamente as certificações usadas na organização, identificar o papel do *Security Officer* (Profissional diretamente responsável pela implementação e verificação da Política de Segurança da Informação na empresa. (HOUGHTON MIFFLIN COMPANY, 2000), e analisar as formas para despertar e gerenciar junto aos funcionários a necessidade de integrar os diferentes dispositivos de segurança, para prover confiança entre os membros e parceiros da organização. Buscar informações para a inovação e agilidade nas atividades da empresa, observar se a informação está de forma ordenada e interagir com a área de Tecnologia da Informação da empresa, tentando diagnosticar os riscos e abranger os resultados obtidos na literatura;

Atualmente, a proteção de dados e informações que possuem um valor exclusivo, tornou-se um aspecto básico de sobrevivência dos ambientes institucionais, sendo eles, empresarial ou corporativo, governamental, educacional, entre outros.

Tendo isso como princípio, avaliando a política de Segurança da Informação e a metodologia utilizada para implementação de controles que minimizem as carências no acesso à informação seja ela restrita ou abrangente, aumentará, a conscientização do quadro funcional da instituição, tornando-os capazes de passar aos seus usuários/clientes a importância da informação íntegra, tornando-os co-autores da segurança da informação.

2 A INFORMAÇÃO, SUA SEGURANÇA E SUA GESTÃO

Hoje, a informação pode ser visto como um produto de base, similar à eletricidade, sem a quais, muitas empresas simplesmente não poderiam operar (CARR, 2003). A informação é resultado da manipulação, processamento e organização de dados de tal forma que represente uma ampliação do conhecimento, existindo em diversas formas e suportes: tácitas, impressa, apresentada em vídeos, simplesmente falada em conversas, armazenada eletronicamente, transmitida pelo correio convencional ou por meios eletrônicos. Seja qual for seu suporte ou apresentação, seja ela compartilhada ou armazenada, é aconselhável que seja sempre adequadamente protegida. De fundamental importância a informação é um ativo é essencial para o sucesso de uma organização. Neste sentido, necessita de proteção adequada contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (SÊMOLA, 2003).

A segurança da informação que pode ser alcançada por meios técnicos é limitada e por isso, é necessário suporte de uma gestão e por métodos adequados. (NBR/ISO/IEC 27002, 2007).

O principal objetivo da gestão da informação é de amparar a política global da empresa, para que se tornem mais eficientes o conhecimento e o tratamento da informação, contribuindo então na evolução organizacional da empresa. Daí sua importância, fazer a informação certa e segura, chegar a(s) pessoa(s) que necessita(m) dela, no momento que se necessita dela, sem causar prejuízo aos lucros e rendimentos da empresa ou a qualquer um de seus funcionários e clientes.

A gestão da segurança da informação requer, portanto, a participação de todos os funcionários da organização. Sendo necessário também, se for o caso, a participação de acionistas, fornecedores, terceiras partes, clientes ou outras partes externas. Como afirmam Maior, Santos e Dal Lacqua (2006), as pessoas envolvidas precisam estar cientes que cada informação obtém a sua classificação e salvaguarda, e também, que cada uma delas tem o seu acesso permitido, isto é, os indivíduos que compõem a organização devem estar atentos em relação aos graus de importância das informações. Tudo isso para garantir a impossibilidade de pessoas não autorizadas obterem informações indevidas durante o acesso, o armazenamento, o transporte e o descarte das mesmas.

Neste contexto, a NBR ISO/IEC 27002 (2007) define segurança da informação como "[...] Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas".

Os três princípios que caracterizam a preservação da informação, de acordo com Sêmola (2003), podem ser definidos da seguinte maneira: confidencialidade: toda informação deve estar segura de que será acessada somente pelas pessoas a quem ela se destina; integridade: toda informação deve estar protegida e isenta de erros, ou seja, na exatidão em que a mesma foi disponibilizada. Visando também a proteção contra eventuais alterações acidentais ou intencionais; disponibilidade: toda informação deverá estar

disponível aos seus usuários autorizados quando eles solicitarem e com a freqüência que necessitarem.

Segundo Baldissera e Nunes (2006, p. 3), "[...] a preservação destes três princípios constitui o paradigma básico da segurança da informação, mas é importante conhecer seus agentes: ameaças, vulnerabilidades, perímetro, riscos, mecanismos de segurança."

E é essencial que a organização identifique os requisitos de segurança que irão melhor adequar à sua política de informação. Primeiro, deve ser feita uma análise/avaliação de riscos, quais são as ameaças aos ativos e as vulnerabilidades destes. Infelizmente, segundo Van Niekerk e Von Solms (2009) no mundo interconectado em que vivemos, a informação é muito mais vulnerável do que outros produtos básicos. Assim, é vital para as organizações garantir o seu contínuo acesso a esta mercadoria, protegendo seus ativos informacionais. É importante verificar a legislação vigente, etc e organizar um conjunto particular de princípios, objetivos e os requisitos do negócio para o gerenciamento da informação que a organização irá processar. Dessa forma, a gestão de riscos, acompanhamento dos níveis de risco e a adoção de controles que eliminem vulnerabilidades, afastando ameaças e reduzindo a probabilidade de uma ameaça explorar uma vulnerabilidade, será uma gestão de alta qualidade para os serviços e produtos da empresa.

A segurança da informação é uma batalha travada dia-a-dia pela empresa, devido aos riscos que a informação sempre fica exposta. Riscos esses passam a existir em tempo real e um pequeno descuido pode gerar contratempos com grandes conseqüências. A todo tempo, criam-se novas formas de invasão, ataque, vírus, funcionários insatisfeitos e, até mesmo os usuários que às vezes não têm a devida ciência da importância das informações, deixando que elas vazem.

3 O FATOR HUMANO

Os recursos humanos podem ser o elo mais crítico da organização no que se diz respeito à segurança da informação, uma vez que não correspondem diretamente a área essencialmente técnica. É imprescindível dentro de uma política de segurança da informação, acolher medidas voltadas para o treinamento, capacitação de funcionários, apresentação de seminários, palestras, e outros, que foquem a seriedade com que deve ser tratada a ação humana, dentro de uma política de Segurança da Informação.

> A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas, atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação (MENEZES, 2004, p. 4).

Os pontos fracos "humanos" podem ser voluntários ou não. Os erros e acidentes que ameaçam a informação, às vezes ocorrem dentro do ambiente de trabalho. A maior vulnerabilidade é o desconhecimento das providências tomadas quanto à segurança que deveria ser adotada por cada elemento do sistema, principalmente aqueles internos da organização, [...] grande parte dos problemas de segurança são originados na rede interna da organização e, muitas vezes, são causados pelo desconhecimento de conceitos e procedimentos básicos de segurança por parte dos usuários (MENEZES, 2004, p. 4).

Neste contexto, a Segurança da Informação necessita de uma pessoa ou grupo responsável pela aplicação ou administração da política de segurança aplicada a todo o sistema, o profissional de segurança ou o *Security Officer* que, juntamente com um comitê de segurança, irá considerar os ativos físicos e tecnológicos da organização, identificando as ameaças e vulnerabilidades, através de observação, inspeções físicas e

presenciais aos ambientes, e pesquisa à documentação. Com os resultados da análise de riscos, poderão ser então aplicados os controles da norma NBR ISO/IEC 27002:2007, dentro do nível de conformidade. Outra responsabilidade é garantir a compatibilidade da empresa em que atua com as melhores e mais atualizadas práticas mundiais.

4 CONFORMIDADE COM AS NORMAS

Com o objetivo de assegurar a continuidade dos negócios e minimizar riscos de incidentes de segurança, por meio da implementação e avaliação de práticas de gestão da segurança da informação, criou-se a versão brasileira da Norma Britânica BS7799-1, pela Associação Brasileira de Normas Técnicas (ABNT), a NBR ISO/IEC 27002 que trata de tecnologia da informação: código de prática para a gestão da segurança da informação.

A norma britânica, criada na Inglaterra, se divide em duas partes:

> A BS7799-1 é a primeira parte da norma que contém uma introdução, definição de extensão e condições principais de uso da norma. A BS7799-2 é a segunda parte da norma e tem por objetivo proporcionar uma base para gerenciar a segurança da informação dos sistemas das empresas. (ARAÚJO, 2005, p. 65).

A norma brasileira contém onze seções de controles, que são as ações que a organização deve tomar para reduzir os riscos avaliados.

> Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais. (NBR/ ISO/IEC 27002, 2007, p. 1).

A ISO/IEC 27002 foi criada com o objetivo de ser um padrão flexível, apenas para orientar quanto a possíveis medidas a serem adotadas na criação de uma política de segurança da informação e nunca guiar seus usuários a seguirem uma solução de segurança específica. As recomendações da norma são neutras com relação à tecnologia e não fornecem nenhum subsídio na avaliação ou julgamento nas medidas de segurança já existentes dentro da organização.

Cabe aos diretores decidirem se aderem ou não às recomendações apresentadas pelas normas, já que, pragmaticamente, cada vez mais empresas buscam a adesão de padrões nacionais ou internacionais, de segurança.

> Com os funcionários bem treinados e conscientes de suas responsabilidades com segurança da informação para a empresa, certamente as tecnologias posteriormente implementadas apresentarão melhores resultados (MAIOR; SANTOS; DAL LACQUA, 2006, p. 109).

Desconhece-se qualquer solução puramente tecnológica ou física para problemas também considerados sociais. Sendo um conceito elevadamente social, já que trata também de pessoas, a segurança da informação necessita de uma visão igualmente de alicerces com conceitos sociais, além dos tecnológicos, para sua correta implantação.

5 MATERIAIS E MÉTODOS

Neste trabalho foi realizado um estudo de caso na empresa Globoaves São Paulo Agroavícola Ltda. – Unidade de Formiga-MG. De acordo com (GIL, 2002, p. 53), "[...] a pesquisa é desenvolvida por meio da observação direta das atividades do grupo estudado e de entrevistas com informantes para capturar suas explicações e interpretações do que ocorre no grupo."

Apresenta características de pesquisa exploratória, ostenta também seus resultados com base em pesquisa bibliográfica. A

pesquisa é de cunho indutivo, pois, segundo Ferreira (2008, p. 4) "[...] parte-se da observação de fatos ou fenômenos cujas causas se deseja conhecer, comparando-os com a finalidade de descobrir as relações existentes entre eles e proceder à generalização [...]"é também de cunho qualitativo, ou seja, que é "[...] possível imprimir significados aos fenômenos humanos com o apoio de exercícios de interpretação e compreensão, pautados na observação participante e na descrição densa [...]", pois, "[...] parte da premissa de que é possível explicar um determinado fenômeno com a exploração intensa/exaustiva de uma única unidade de estudo." (LIMA, 2004, p. 30-31).

A técnica selecionada para coleta de dados foi a entrevista semi-estruturada, ou seja, um conjunto estruturado de perguntas precisas, baseando-se apenas em uma ou poucas questões/guias, quase sempre fechadas. Segundo Tanaka e Melo (2001, p. 27) durante a realização da entrevista pode-se introduzir outras questões que surgem de acordo com o que acontece no processo em relação às informações que se deseja obter [...]. Assim, podem-se obter dados que possibilite a compreensão de um fato ou situação e permite a edificação para argüir em um processo de avaliação.

A entrevista foi aplicada ao Diretor e funcionários da empresa da Globoaves São Paulo Agroavícola Ltda – Unidade de Formiga, que estão diretamente ligados à Segurança da Informação, esta empresa tem como missão, oferecer ao mercado produtos avícolas obtidos das melhores linhagens, promovendo o melhor atendimento, lucratividade, processos de trabalho eficientes e eficazes, satisfação das pessoas e atendimento das necessidades dos clientes. Depois da entrevista, foi feita com base na literatura, a avaliação das informações coletadas.

Neste trabalho, foram tomados todos os cuidados éticos de sigilo e garantiu-se que as informações colhidas em seu desenvolvimento, serão utilizadas apenas com o intuito de produção científica, protegendo a integridade da empresa e dos entrevistados.

6 RESULTADOS E DISCUSSÕES

A Globoaves São Paulo Agroavícola Ltda, Unidade de Formiga-MG, tendo como maior objetivo a qualidade total na produção de seus serviços e produtos, procura conscientizar a importância da preservação do patrimônio informacional, através de métodos e normas técnicas. Nota-se que, com apanhado de visões dentro da administração dessa empresa, a informação é um fator crucial na gestão, por ser um recurso importante e indispensável, tornando-se mais confiável, mais íntegra e, por conseqüente, mais digno será o trabalho na empresa, aumentando sua potencialidade diante das ameaças na árdua e contínua tarefa de administrar a segurança.

Na entrevista semi-estruturada, havia 27 questões, organizadas em 7 grupos de setores e profissionais que trabalham com computador diariamente nos seus ambientes de trabalho e em determinadas áreas. O principal objetivo do questionamento era identificar sobre a ciência dos colaboradores relacionados à segurança da Informação quanto a política, a segurança organizacional, pessoal, físicas e ambiente, o gerenciamento das operações e comunicações, controle de acesso e a conformidade com as normas. Assim, obteve-se um resultado bem expressivo e cerca de mais de 95% dos inquiridos responderam estar cientes dos procedimentos adotados pela empresa no que diz respeito às políticas de desenvolvimento de atividade informacionais e com a segurança da informação.

Portanto, como confirma Sêmola (2003, p. 151) a empresa que atinge este resultado pode ser considerada como exceção e deve estar em destaque em seu segmento de mercado devido à abrangência dos controles

que aplica nos negócios. Apesar de não termos como avaliar a uniformidade das ações, [...], podemos dizer que esta empresa está conscientizada da importância da segurança para a saúde dos negócios.

Como a empresa Globoaves unidade de Formiga-MG tem um sistema rigoroso de segurança vindo diretamente da sua matriz, classificar a informação não é rotina difícil já que essa atividade controla e garante o sigilo das informações. Foi apurado que informações consideradas confidenciais pelos departamentos são enviadas somente pela rede interna e para destinatários específicos que só tem acesso com login e senha. As informações externas são efetuadas diretamente com o receptor, tomando precauções para que não sejam disponibilizadas para terceiros.

Há controles dentro da política que diminui a oportunidade de pessoas não autorizadas a obterem informações sigilosas. Depois de definido o grau de importância dos documentos, estes são armazenados e arquivados pelo pessoal competente do departamento, sendo ele responsável pela sua disseminação e restrições de acesso conforme sua classificação.

Assim, a não classificação dessas informações poderia gerar transtornos em toda a estrutura administrativa causando danos irreversíveis e irreparáveis.

Visando identificar oportunidades de melhoria contínua e colaboração na evolução dos processos de trabalho, os funcionários, assim que dão início ao seu vínculo com a empresa, recebem as orientações e treinamentos necessários para o bom encaminhamento das suas atividades. Em relação aos funcionários que lidam com a gestão da informação, observam-se princípios importantes, como:

a) cada funcionário ou usuário da *intranet* da empresa é responsável pela sua senha;
b) todo funcionário ou usuário deve reportar incidentes de segurança;
c) o funcionário não consegue baixar ou instalar *software* nos computadores da empresa sem intervenção da matriz;
d) o funcionário deve utilizar seu *e-mail* pessoal de domínio da empresa e *intranet* no seu horário de trabalho;
e) as informações da empresa pertencem à empresa, e não são divulgadas sem autorização.

A principal parte da política de segurança da informação da Globoaves São Paulo Agroavícola Ltda, Unidade de Formiga-MG, vem direto da sua matriz em Cascavel-PR.

Tratando-se de uma empresa de grande porte e por ter várias filiais no país inteiro, ela procura estabelecer princípios básicos em sua política e os difunde através das suas redes.

Todas as unidades têm sua própria política, mas todas elas são baseadas na política da matriz, bem como os controles de rede, que são “cuidados” pelo Comitê de Segurança da Informação da Unidade de Cascavel-PR.

Todos os funcionários têm como dever estar conscientes das regras previstas na política de Segurança da Informação e torná-la um documento ativo e constante dentro da empresa. Algumas dessas regras são repassadas aos clientes que também aderem aos controles para um melhor atendimento.

7 CONCLUSÃO

Acreditar que a batalha para garantir efetiva Segurança da Informação, é remota e, como anteriormente falado, praticamente impossível. A tendência atual é cada vez maior, a total falta de privacidade. Informações devem ser tratadas com o princípio básico de elevada importância, para

cada vez mais, serem respeitadas e valorizada por cada funcionário da organização.

Simplesmente afirmar que existe uma forma mais adequada que irá assegurar totalmente qualquer ambiente de trabalho que manipule informação é imprudente e equivocado. Ficam como conceito para dificultar a manipulação destas informações, o comportamento, o exercício, os costumes, e ainda o comprometimento que todos devem ter, ao gerenciar informações, sejam elas de cunho privado ou não.

A Segurança da Informação é um assunto de planejamento e deve ser assumido pela diretoria e/ou gerência da organização. Não deveria ser simplesmente delegada ao nível tecnológico operacional, o qual tem papel acentuado, mas que não toma decisões estratégicas que envolvam a Tecnologia da Informação e a continuidade dos negócios. Igualmente como ocorre na Globoaves São Paulo Agroavícola Ltda Unidade de Formiga-MG, que acontece do nível mais alto da administração e passa para as filiais em seus setores responsáveis.

Essa empresa se preocupa tanto com os aspectos físicos, quanto com os tecnológicos, bem como a segurança de acordo com os padrões e normas e a segregação das atividades dos funcionários responsáveis. Verifica-se que o gerenciamento das informações ali produzidas, é de responsabilidade dos diretores quanto dos funcionários que por serem qualificados e capacitados tem o dever de informar qualquer que seja o risco que alguma informação esteja correndo.

A maioria das organizações direciona as atenções e investimentos em segurança apenas nos seus ativos palpáveis, físicos e financeiros, mas dedicam pouca atenção e investimentos aos ativos de informação, considerados vitais na gestão dos negócios, porém o que torna as organizações diferenciadas são os recursos da informação e do conhecimento, que se bem gerenciados, através de uma gestão eficaz do conhecimento, poderão ser acessados, processados e compartilhados pelos indivíduos em processos recorrentes de geração de conhecimento com propósitos, principalmente de manutenção da inteligência competitiva.

Por fim, é por essas razões que o profissional da informação, um gestor do conhecimento, seria uma resposta para o ambiente competitivo de uma organização, pois busca a contínua atualização das informações, garantindo conseqüentemente a rapidez nas buscas informacionais. Por isso, recomenda-se novos estudos sobre essa temática visando refletir sobre o papel dos bibliotecários nos processos de gerenciamento da organização, para comprovar a eficácia e necessidade do profissional da informação na otimização da gestão informacional.

REFERÊNCIAS

AGENCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO. **Termos e definições**: terminologia. Recife, 2007. Disponível em: http://200.238.107.167/c/portal/layout?p_l_id=PU B.1149.69>. Acesso em: 1 abr. 2011.

ARAUJO, E. E. A **vulnerabilidade humana na segurança da informação**. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Faculdades Uniminas, Uberlândia, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27002**: tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2007.

_____. **NBR ISO/IEC 17799**: tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2005.

BALDISSERA, T. A.; NUNES, R. C. Impacto na implementação da norma NBR ISO/IEC 17799 para a gestão da segurança da informação em colégios: um estudo de caso. In: ENCONTRO NACIONAL DE ENGENHARIA DA PRODUÇÃO, 27., 2006, Foz do

Iguaçu. **Anais...** Foz do Iguacu: Associação Brasileira de Engenharia da Produção, 2007. 1 CD-ROM.

BRASIL. Ministério da Saúde. Resolução 196/96 do Conselho Nacional de Saúde/MS. Sobre diretrizes e normas regulamentadoras de pesquisa envolvendo seres humanos. Diário Oficial da União, Brasília, 10 out. 1996.

CARR, N. G. It doesn't matter. **Harvard Business Review**, Harvard, p. 41-49, May 2003.

CASSA, M. A importância e a implementação da segurança da informação no âmbito das atividades de negócios. **TECHoje**, Belo Horizonte, 2006. Disponível em: < http://www.ietec. com.br/site/techoje/categoria/detalhe_artigo/221 >. Acesso em: 13 jan. 2011.

DAS, T. K.; TENG, B. S. Resource and risk management in the strategic alliance making process. **Journal of Management**, Stillwater, v. 24, n. 1, p. 21-42, Jan. 1998.

FERREIRA, S. M. **Métodos e técnicas de pesquisa**. Formiga: Unifor-MG, 2008. Apostila.

FONSECA, R. **Conceitos básicos de Segurança da Informação**. 2011. Disponível em: <http://cavalcanteti.blogspot.com/2008/08/conceitos-bsicos-de-segurana-da.html>. Acesso em: 21 abr. 2011.

GIL, A. C. Como classificar as pesquisas? In: _____. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002. cap. 4, p. 41-56.

HOUGHTON MIFFLIN COMPANY. **Dictionary of the English Language**. 4. ed. Indianápolis: American Heritage, 2000. Disponivel em: <http://www.thefreedictionary. com/security+ guard>. Acesso em: 21 abr. 2011.

KADAN, A. W. Information security policy: development an implementation. **Information Systems Security**, Boston, v. 16, n. 5, p. 246-256, Sept. 2007.

LESSA, B. M. **Gestão Estratégica da segurança da informação**. Monografia de Final de Curso (Especialista em Gerência de Tecnologia da Informação)-Universidade FUMEC, Belo Horizonte, 2004.

LIMA, M. C. Uma breve reflexão sobre os métodos quantitativos e qualitativos. In: _____. **Monografia**: a engenharia da produção acadêmica. São Paulo: Saraiva, 2004. cap. 2, p. 25-36.

MAIOR, A. O. B.; SANTOS, F. A.; DAL LACQUA, S. C. **Gestão da segurança da informação**. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação)-Faculdade Gennari & Peartree, Pedreiras, 2006.

MARCIANO, J. L. P. **Segurança da informação**: uma abordagem social. Brasília, 2006.

MARCIANO, J. L. P.; LIMA-MARQUES, M. O enfoque social da segurança da informação. **Ciência da Informação**, Brasília, v. 35, n. 3, 89-98, set./dez. 2006.

MENEZES, H. et al. **O fator humano na segurança da informação**. Rio de Janeiro, 2004. Disponível em: < http://www.lyfreitas.com/artigos_mba/fator-humano.pdf>. Acesso em: 14 jan. 2011.

PEIXOTO, M. C. P. **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações**. Monografia (Bacharel em Ciências da Computação)-Centro Universitário do Triângulo, Uberlândia, 2004.

REES, J.; BANDYOPADHYAY, S.; SPAFFORD, E. H. Pfires: a policy framework for information security. **Communications of the ACM**, New York, v. 46, n. 7, p. 101-106, July 2003.

SANTOS, J. C.; NASCIMENTO, H. A. D. do. Implantação de um sistema de gestão de segurança da informação na UFG. In: WORKSHOP DE TECNOLOGIA DA INFORMAÇÃO DAS IFES, 2., 2008, Gramado **Anais...** Gramado: UFRGS, 2005. 1 CD-ROM.

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

SILVA, W. A. **Controle de acesso**: uma abordagem sobre segurança de banco de dados eletrônicos. Monografia (Bacharel em Sistemas de Informação)- Instituto Luterano de Ensino Superior de Itumbiara, Itumbiara, 2004.

TANAKA, O. Y.; MELO, C. **Avaliação de programas de saúde do adolescente**: um modo de fazer. São Paulo: Edusp, 2001.

VAN NIEKERK, J. F.; VON SOLMS, R. Information security culture: a management perspective. **Computers & Security**. Amsterdam, v. 28, n. 7, p. 491-728, Oct. 2009.

ZAPATER, M.; SUZUKI, R. **Segurança da informação**: um diferencial determinante na competitividade das corporações. São Paulo: Promom Business & Technology Review, 2005.

_____

Dados sobre Autoria

*Bacharel em Biblioteconomia pelo Centro Universitário de Formiga – UNIFOR/MG, Especialista pelas Faculdades Integradas de Jacarepaguá (FIJ) e Coordenadora da Biblioteca Pública de São José da Barra-MG. E-mail: jordana.calixto@gmail.com

**Graduado em Biblioteconomia e Especialista em Gestão do Conhecimento e tecnologia da Informação pelo Centro Universitário de Formiga (2002). Atualmente é bibliotecário da Pontifícia Universidade Católica de Minas Gerais e professor do Centro Universitário de Formiga. E-mail: zoopas@gmail.com

Artigo enviado em outubro de 2010 e aceito em fevereiro de 2011.