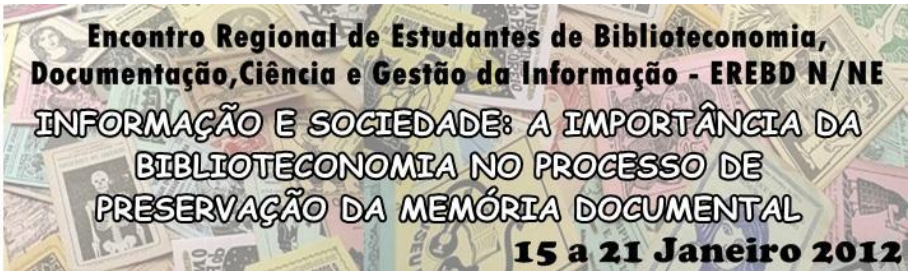

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: perspectivas baseadas na tecnologia da informação (T.I.)[1]

Oliveira, Gabriella Domingos de*

Moura, Rafaela Karoline Galdêncio de **

Araújo, Francisco de Assis Noberto Galdino de ***

Resumo

Objetiva-se, com este trabalho, abordar os conceitos preliminares no que diz respeito à segurança da informação, suas formas de gestão e principais finalidades, tendo como objeto de pesquisa as informações contidas em bibliografias e websites. Apresenta perspectivas aplicáveis no que se refere ao gerenciamento das informações organizacionais de forma detalhada, descrevendo a informação como principal ferramenta na atualidade, caracterizando-a e atribuindo valores ao qual necessita ser preservado, organizado, gerenciado e disseminado. Enfoca o processo de armazenamento e expõe os recursos informacionais consideradas relevantes e estabelece parâmetros, explorando os quatro pilares atrelados a esta, sendo vinculados à tecnologia da informação (TI). Explanam e Analisam-se os riscos, tais como: ameaças, ataques, vulnerabilidades, entre outros. Propõe possíveis soluções à prevenção e conservação da informação, utilizando de várias estratégias baseadas na T.I., como as barreiras de segurança, entre outras. Deste modo, finaliza-se com os aspectos relevantes à informação e suas perspectivas abrangentes, promove a construção de novos conhecimentos, a fim de colocá-los em prática no exercício cotidiano e profissional com um olhar mais acurado.

Palavras-chave: Informação. Segurança da informação. Tecnologia. Gestão organizacional.

---

[1] Comunicação oral apresentada ao GT 05 – Memória, gestão e tecnologia da informação e comunicação.

* Universidade Federal do Rio Grande do Norte (Campus Natal). Graduanda em Biblioteconomia. Email.gabryellaholiveirah@gmail.com

** Universidade Federal do Rio Grande do Norte (Campus Natal). Graduanda em Biblioteconomia. Email. rafaelakarolline@hotmail.com

*** Universidade Federal do Rio Grande do Norte (Campus Natal). Professor Substituto do Departamento de Biblioteconomia. Orientador. . Email. francisco_bibufrn@yahoo.com.br

1 INTRODUÇÃO

O presente artigo tem por finalidade apresentar uma visão clara e objetiva a respeito dos principais conceitos, finalidades e princípios da gestão da segurança da informação, lembrando que a mesma está diretamente ligada com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

A informação é um fator bastante importante em nosso dia-a-dia, pois a todo instante somos bombardeados por dados e informações vastas, que, se soubermos usar, enriqueceremos nossos conhecimentos e fornecemos subsídios para não cairmos em nenhuma armadilha virtual. Deste modo, a informação é obtida e repassada de forma que a mesma seja disseminada corretamente e segura sem danos ou interferências. Com isto, iremos abordar a segurança junto à tecnologia da informação, ou seja, se as duas caminham lado a lado corretamente ou se sofre algum tipo de dificuldade. Sendo assim, o objetivo deste artigo é avaliar estes riscos e trazer conhecimentos a respeito da segurança para que se tenham possíveis soluções.

No mundo atual existe um ambiente repleto de inter-relações que se permeiam em constante estado de mutação, e neste contexto destacamos que informação e conhecimento representam patrimônios cada vez mais valiosos e necessários para se compreenderem e responderem as mudanças de perigos que possam abater os mesmos. Com o crescente aumento das tecnologias de informação e com a rápida disseminação dela, cresceram também os crimes relacionados à mesma, surgindo então, a necessidade de se manterem as informações empresariais e pessoais livres de riscos e perigos que possam danificá-la, para que haja uma informação confiável.

A segurança precisa ser obtida dentro de um nível hierárquico da informação aos quais são: o dado, a informação e conhecimento. Entretanto, é necessário que se tenham noções de segurança da informação, pois os mesmos poderão ter ruídos ou serem danificados até que se cheguem ao destino final. Os conceitos desses três níveis hierárquicos (dado, informação e conhecimento) sofrem variações, mas existem explicações com o mesmo contexto, ou seja, um conjunto de dados não produz necessariamente uma informação, nem um conjunto de informações representa necessariamente um conhecimento. Em síntese, um dado pode ser entendido como registros ou fatos em sua forma primária, não necessariamente física; e quando esses fatos e registros são organizados ou que tenham uma combinação significativa eles se transformam em uma informação. Da mesma forma que a informação é produzida a partir de dados, o conhecimento também tem como origem a informação, quando as mesmas são agregadas com outros elementos. O conhecimento costuma ser classificado como explícito ou tácito; o explícito é aquele que pode ser transformado em documentos, roteiros e treinamentos e o conhecimento tácito é difícil de registrar, documentar e de difícil transmissão.

> Nota-se que normalmente as pessoas são o elo mais frágil quando o assunto é segurança da informação, as soluções técnicas não contemplam totalmente sua segurança, desta forma torna-se necessário que os conceitos pertinentes a segurança sejam compreendidos e seguidos por todos dentro da organização, inclusive sem distinção de níveis hierárquicos. (MOREIRA, 2008).

2 GESTÃO DA SEGURANÇA DA INFORMAÇÃO: CONCEITOS E FINALIDADES

2.1 CONCEITOS

Assim como em toda organização existe gestão, a segurança da informação também possui a sua forma de gerenciar e administrar as informações veiculadas na sociedade atual. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, fazendo com que esta segurança esteja restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

A confidencialidade tem como princípio o acesso das informações apenas pelos usuários autorizados. (Fontes, 2000, pag. 21). Mencionado por Campos (2006, pag. 6), a confidencialidade é respeitada quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação, ou seja, a informação no ambiente organizacional requer essa atenção por parte dos gestores da informação em designar as pessoas certas no que diz respeito à guarda das informações para que não haja quebra da confidencialidade. Quanto à integridade, esse fator é primordial para que a organização tenha destaque e referência no tratamento das informações, ao qual é ressaltado por Campos (2006, pag. 6): o princípio da integridade é respeitado quando a informação acessada está completa, sem alterações e, portanto, confiável. Ou seja, quando a informação é alterada ou chegada de forma incorreta ao seu destino, isto faz com que a integridade se quebre. No que diz respeito à disponibilidade, este fator tem como principal finalidade a garantia de que as informações sejam passadas levando a empresa a atingir o nível de segurança adequado ao seu negócio, de forma correta para os usuários, com a participação dos associados na organização.

É importante salientar que o conceito de segurança propriamente dito se aplica a todos os aspectos de proteção de informações e dados. O conceito denominado *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionada com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si, pois sabemos que os mesmos são os controles físicos,

tecnológicos e humanos personalizados com o objetivo de viabilizar a redução e administração dos riscos.

Segundo Greewood, referido por Cautela e Polioni (1982), "A informação é considerada como o ingrediente básico do qual dependem os processos de decisão". Entretanto, se por um lado, uma empresa não funciona sem informação, por outro, é importante saber usar a informação e apreender novos modos de visualizar o recurso informação para que a empresa funcione melhor, isto é, para que esta se torne mais eficiente.

> 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).

Em suma, segundo Wilson (1989), a gestão da informação é entendida como a gestão eficaz de todos os recursos de informação relevantes para a organização, tanto de recursos gerados internamente como os produzidos externamente e fazendo apelo, sempre que necessário, à tecnologia de informação. No passado a questão segurança da informação era muito mais simples, pois os arquivos contendo inúmeros papéis podiam ser trancados fisicamente; porém, com a chegada das tecnologias da informação e comunicação esse fator ficou bem mais complexo. Atualmente a maioria dos computadores conecta-se a internet e consequentemente a internet conecta-se a eles; além disto, sabemos que dados em formato digital são portáteis, fator este que fez com que estes ativos tornassem atrativos para ladrões. Mas isto não é tudo, pois existem inúmeras situações de insegurança que podem afetar os sistemas de informação tais como: incêndios; alagamentos; problemas elétricos; fraudes; uso inadequado dos sistemas; engenharia social, entre outros.

2.2 FINALIDADES

A informação organizacional possui quatro pilares importantes vinculadas a ela, as quais são denominadas de*: pública, interna, confidencial e secreta*. A informação pública é de uso livre, sem qualquer restrição; já a interna é marcada pela integridade por se tratar da quantidade e qualidade de informações; a confidencial assemelha-se à interna, a única

diferença é que esse tipo de informação é de caráter principalmente empresarial, fazendo com que esta fique restrita ao grupo empresarial; por fim, a **secreta** é mais restrita nas organizações, pois apenas poucas pessoas devem ter conhecimento desta, a fim de garantir a confidencialidade na própria instituição.

2.3 AMEAÇAS

Assim como todo indivíduo vive sujeito a ameaças de todas as formas, as organizações também passam por estes riscos que podem ser combatidos. As ameaças organizacionais podem ser classificadas como: *naturais, involuntárias ou voluntárias*. A ameaça natural acontece através de fenômenos da natureza e outro fator natural como o próprio nome sugere; as ameaças involuntárias ocorrem por meio de acidente, geralmente pela falta de conhecimento em determinado sistema ou problemas de natureza elétrica; entretanto, as ameaças voluntárias acontecem com o propósito de destruir a própria informação, fator este que pode ser causado por pessoas tais como hackers, ladrões, fraudadores, espiões, entre outros. Segundo Campos (2006, p.13) a ameaça é um agente externo ao ativo de informação, se aproveitando das vulnerabilidades da informação suportada ou utilizada por ele.

2.4 ATAQUES

Ataque pode ser considerado como o ato de prejudicar algo ou alguém, fator este que também interfere na própria informação. É importante ressaltar que existem ataques de várias formas, tanto humanas como tecnológicas; porém será dado destaque ao ataque tecnológico, que pode ser por meio de *interceptação*, que se trata do acesso à informação sem autorização organizacional; através de *interrupção*, podendo definir como uma forma de atrapalhar a chegada da mensagem; *modificação*, na qual toda a informação é modificada sem autorização alguma e, por fim, a *personificação*, que trata da entidade que se passa por outra, tendo acesso à informação.

2.5 VULNERABILIDADE

A vulnerabilidade pode ser considerada um ponto crucial na informação, na qual toda a informação armazenada corre o risco de ser alterada de acordo com os fatores tecnológicos e

humanos. É impreterível o cuidado de identificar as vulnerabilidades em determinado sistema, podendo livrar a organização de qualquer desastre.

> Vulnerabilidade são fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade e disponibilidade. (CAMPOS, 2006, pag. 11)

A mesma é relacionada a vários ambientes, como o ambiente tecnológico em que se pode citar, por exemplo, os computadores sem atualização de anti-vírus e rede local, ou seja, rede acessível por senha, padrão ou pública; outro fator que causa a vulnerabilidade e sérios danos empresariais e pessoais deve-se ao fato da ausência de uma política institucional de segurança e pessoas especializadas sobre segurança da informação no trabalho, sem que haja um grupo de especialistas e procedimentos para o tratamento contra a vulnerabilidade e ataques indesejáveis ao sistema organizacional.

2.6 CICLO PDCA

Este ciclo é denominado PDCA devido às palavras inglesas*: plan* (planejar), do (executar), *check* (verificar) e *action* (agir). É importante esse ciclo na informação porque uma depende da outra, ou seja, ao se definir metas, ao mesmo instante deve-se tomar iniciativa ao desenvolver o sistema; vendo então os resultados, deve ser feita uma análise acurada da informação a fim de que estes correspondam aos testes feitos anteriormente, identificando com o fator agir (action), vendo se necessita de alguma melhoria.

2.7 BARREIRAS DE SEGURANÇA

Esta etapa tem por finalidade impedir que algo ruim aconteça na instituição, ou seja, proteger contra ataques. Na gestão da segurança da informação as principais barreiras dividem-se em: *desencorajar*, no qual é vinculado ao fator *dificultar*, tendo por objetivo desmotivar e dificultar qualquer operação tanto humana como tecnológica; *discriminar*, que tem por função primordial a identificação e a gerência de determinado acesso*; detectar*, que é

mais uma barreira de cunho tecnológico por se tratar da segurança propriamente dita; *deter*, fator este que pretende impedir algo desastroso em qualquer lugar; e, por fim, a barreira de *diagnosticar*, que trata justamente da análise de riscos, visando à identificação dos pontos de riscos a que a informação está exposta, identificando, desta maneira, quais os pontos que necessitam de maior empenho em proteção.

3 TECNOLOGIA DA INFORMAÇÃO

A tecnologia da informação *(T.I.)* pode ser definida como todo recurso tecnológico e computacional destinado à coleta, manipulação, armazenamento e processamento de dados ou informações dentro de uma organização. Outra definição sobre a TI é como sendo o uso de recursos computacionais para o desenvolvimento de sistemas de informação. Seus componentes essenciais são hardware e software, e também seus recursos de telecomunicação.

Hardware- Dispositivos físicos digitais, com função de receber, armazenar e processar dados.

Software- programas de computador, que tem como função dirigir, organizar e controlar o hardware, fornecendo-lhe instruções e comandos de funcionamento. (NORTON, 1996).

Telecomunicações- são transmissões eletrônicas de Sinais para comunicações, inclusive meios como telefone, rádios, televisão. A arquitetura é formada por computadores que fazem a recepção e o envio de dados através de meios de comunicação, com fios telefônicos ou ondas de rádio.

> As comunicações de dados são um subconjunto especializado de telecomunicações que se referem à coleta, processamento e distribuição eletrônica de dados, normalmente entre os dispositivos de hardware de computadores (STAIR, 1998).

3.1 A SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

Existem dois tipos de segurança envolvendo a tecnologia da informação, tendo como pré-requisito a necessidade de se conseguir estratégias. Para sair dessas armadilhas, os fatores

para promover boas estratégias de fuga dos perigos são o fator humano e o computacional ou do sistema, que é a segurança física dos equipamentos de informática e a lógica, ao qual se explana um pouco sobre as mesmas a seguir.

Segurança física- São danos que podem ser causados por descuidos, acidentes até mesmo criminais, ou também por fatores naturais, falta de manutenção dos equipamentos ou servidores. Quando existem esses erros de segurança, os prejuízos para uma organização são grandes, prejuízos estes que podem ser a perda de mercado, desgaste na sua imagem e desmotivação de funcionários, aos quais são bastante relevantes a serem estudados, e não somente os prejuízos computacionais que estes são percebidos imediatamente. A responsabilidade do gestor de informática é avaliar e apresentar os riscos, verificar os possíveis danos e sugerir soluções para as situações.

Segurança lógica – Esta segurança é feita por softwares que se constitui de dois níveis: o controle e o nível de acesso à informação.

> O controle de aceso às informações pode ser elaborado por meio de senhas (passwords) específicas para cada cliente e/ou usuário, as quais devem ser alteradas com certa regularidade. Sua principal função é permitir ou não, o acesso a um sistema. (RESENDE, 2000).

Um sistema de segurança seguro dentro de uma organização é o software firewall, pois ele possibilita um ambiente seguro com outros softwares que fazem criptografia. Estes mecanismos de criptografia permitem a transformação reversível da informação de forma a torná-la identificáveis a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados.

> O firewall deve estar adequadamente configurado a fim de bloquear com eficácia as informações que entram e saem da rede, sem que isso represente transtornos de queda de performance a redução de flexibilidade que acarretam na inoperância ou indisponibilidade de informações (SÊMOLA, 2001).

4 DICAS DE SEGURANÇA PARA OS AVANÇOS TECNOLÓGICOS[2]

Há alguns anos, as informações eram acessadas apenas dentro da empresa e o departamento de TI possuía mais controle sobre os dados corporativos. Hoje, as informações podem ser acessadas a partir dos mais diferentes dispositivos e em qualquer lugar. A evolução da tecnologia oferece vantagens como maior agilidade nos negócios e melhor relacionamento entre as empresas e seus públicos. Por outro lado, as organizações precisam ter cuidado e atenção redobrados com seus dados críticos.

Cada vez mais, os funcionários usam seus próprios dispositivos móveis para acessar dados corporativos, uma tendência conhecida como "consumerização da TI". Com base na pesquisa Symantec Consumerization of IT Smartphone End User Survey, realizada recentemente pela Symantec, confira as principais dicas de segurança para serem compartilhadas com funcionários e garantir a segurança das informações corporativas:

1 - Utilize senhas: por norma, todos os funcionários devem proteger seus dispositivos móveis com senha e devem ser instruídos a alterá-la com frequência para dificultar o acesso dos hackers a informações confidenciais.

2 - Criptografe os dados nos dispositivos móveis: informações da empresa e mesmo pessoais armazenadas em dispositivos móveis são, muitas vezes, confidenciais. Criptografar esses dados é uma obrigação. Se o dispositivo for perdido e o cartão SIM roubado, o ladrão não será capaz de acessar os dados se a tecnologia de criptografia apropriada estiver aplicada no dispositivo.

3 - Certifique-se de que o software está atualizado: os dispositivos móveis devem ser tratados como PCs, que sempre usam softwares atualizados, especialmente o de segurança. Isso vai proteger o equipamento contra novas variantes de malware e vírus que ameaçam informações críticas das empresas.

4 - Desenvolva e aplique políticas de segurança fortes para o uso de dispositivos móveis: é importante aplicar políticas de download de aplicações e gerenciamento de senhas para gerentes e funcionários. O uso de senhas fortes ajuda a proteger os dados armazenados no telefone, nos casos em que o aparelho for perdido ou invadido.

---

[2] Informações da Burson-Marsteller/ Symantec

5 - Autenticação: a maioria das redes corporativas exige um nome e uma senha para identificar os usuários, porém os mesmos podem ser violados. Usando uma tecnologia de autenticação dupla, ou de segundo fator, é possível ter maior de segurança quando os funcionários se conectarem à rede corporativa a partir de aparelhos portáteis.

6 - Evite abrir mensagens de texto inesperadas de remetentes desconhecidos: assim como acontece com e-mails, os invasores podem usar mensagens de texto para espalhar malware, golpes de phishing e outras ameaças entre os usuários de dispositivos móveis. O mesmo cuidado que se tem com e-mails deve ser aplicado à abertura de mensagens de texto não solicitadas.

7 - Controle do acesso à rede: soluções de gerenciamento móvel que incluem recursos de controle do acesso à rede podem ajudar a garantir o cumprimento das políticas de segurança de uma empresa e assegurar que apenas dispositivos seguros, compatíveis com as normas, acessem as redes corporativas e os servidores de e-mail.

8 - Clique com cuidado: Os usuários não devem abrir links não identificados em redes sociais, nem bater papo com pessoas estranhas ou visitar sites desconhecidos.

9 - Atenção a quem está em volta ao acessar informações confidenciais: ao digitar senhas ou visualizar dados confidenciais, os usuários devem ter cuidado com quem possa enxergar por cima dos seus ombros.

10 - Saiba o que fazer se o dispositivo for perdido ou roubado: em caso de perda ou roubo, os funcionários e seus gerentes devem saber o que fazer em seguida. Devem ser tomadas medidas para desativar o dispositivo e proteger as informações contra invasão. Há produtos que automatizam essas medidas para que pequenas empresas possam respirar aliviadas se tais incidentes ocorrerem.

5 METODOLOGIA

Com o auxilio de pesquisas bibliográficas, revisões teóricas e informações contidas em websites, o tema que foi exposto no artigo tem por finalidade analisar as características e avaliar suas capacidades e limitações. Percebe-se que as pessoas e organizações não estão preparadas e qualificadas para administrar as ferramentas tecnológicas sem que cause algum dano à segurança informacional, pois com esta dificuldade/barreira o fator humano faz com

que a segurança fique mais vulnerável a ataques quando não se tem conhecimento prévio sobre o assunto. O déficit de informações sobre segurança da informação englobando a tecnologia da informação é pouco discutido nas organizações. Considera-se, então, o artigo como um manual acessível para quem não tem conhecimento sobre a abordagem da segurança pessoal e profissional

6 CONSIDERAÇÕES FINAIS

Podemos inferir que a gestão da segurança da informação é um fator primordial, na qual visa não só a segurança dos dados, mas também a qualidade e preservação das mesmas, principalmente no meio organizacional. Foram propostas formas em que as informações têm seus riscos e vulnerabilidades, apresentando também possíveis soluções para que determinados danos não aconteçam e prejudiquem qualquer instituição, com o uso de softwares seguros e a manutenção que ocorre entre a circulação das informações organizacionais. Assim, espera-se por parte das tecnologias da informação e os seus profissionais, uma circulação de dados que produzam soluções pertinentes às diversas necessidades informacionais seguras e eficientes. Nossa perspectiva é de que todas as informações aqui citadas sejam como um manual, onde encontrará as formas de preservação e conservação de dados e de como as vulnerabilidades surgem ao longo de uma informação computacional ou não.

REFERÊNCIAS

Alecrim, Emerson. **O que é Tecnologia da Informação (TI**)? 2011. Disponível em:<http://www.infowester.com/ti.php>. Acesso em: 11 de dez. de 2011.

Araujo, Nonata Silva. **Segurança da Informação (TI)**. Disponível em:< http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/>. Acesso em 11 de dez. de 2011.

Beal, Adriana. **Introdução à gestão de tecnologia da informação**. 2011. Disponível em:<http://2beal.org/ti/manuais/GTI_INTRO.PDF>. Acesso em: 11 de dez. de 2011.

Burson-Marsteller/Symantec. **10 dicas de segurança para os avanços tecnológicos.** Disponível em:< http://www.added.com.br/noticia/10-dicas-de-seguranca-para-os-avancos-tecnologicos.html>. Acesso em 11 de Nov. de 2011.

Furtado, Vasco. **Tecnologia e gestão da informação na segurança publica**. 2002.

Laureano, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**.2005 Disponível em:< http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 11de dez. de 2011.

Moreira, Ademilson. **A importância da segurança da informação.** 2008. Disponível em:< http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>.

FONTES, Edison. **Vivendo a segurança da informação:** orientações práticas para pessoas e organizações. São Paulo: Sicurezza, 2000.

CAMPOS, André L. N. **Sistema de Segurança da Informação:** Controlando os Riscos. Florianópolis: Visual Books, 2006.