REVISTA CARIBEÑA DE CIENCIAS SOCIALES

Julio 2019 - ISSN: 2254-7630

GESTÃO DE SEGURANÇA DA INFORMAÇÃO: AS PESSOAS – um dos principais ativos das organizações

Adriana Sales Silva De Oliveira[1]
Prof. M. Sc. Rickardo Léo Ramos Gomes[2]

Para citar este artículo puede utilizar el siguiente formato:

Adriana Sales Silva De Oliveira y Rickardo Léo Ramos Gomes (2019): "Gestão de segurança da informação: as pessoas – um dos principais ativos das organizações", Revista Caribeña de Ciencias Sociales (julio 2019). En línea

https://www.eumed.net/rev/caribe/2019/07/gestao-seguranca-informacao.html

RESUMO

O objetivo deste artigo é identificar na literatura e ressaltar aos leitores que a importância de se proteger as informações e os ativos de tecnologia da informação (TI), com relação aos riscos e ameaças, traz para o foco das discussões a influência das pessoas, um dos principais ativos das organizações, na Gestão de Segurança da Informação. Nesse contexto, explicamos "A Importância da Governança de TI na Gestão de Segurança da Informação", depois apresentamos "A Importância do Fator Humano, associada aos Controles e Práticas voltadas para a Conscientização e Educação, como Pilar Fundamental na Gestão de Segurança da Informação" e na sequência, apontamos "As Abordagens Utilizadas na Hora de Sensibilizar as Pessoas sobre Segurança da Informação nas Organizações". Ao final do estudo, conclui-se que ainda existe uma grande lacuna na segurança da informação no que se refere à conscientização das pessoas sobre a importância das informações manipuladas e no papel de cada uma dessas pessoas com a segurança dessas informações.

Palavras Chave: Gestão. Pessoas. Segurança da Informação. Tecnologia da Informação.

RESUMEN

El objetivo de este artículo es identificar en la literatura y resaltar a los lectores que la importancia de proteger las informaciones y los activos de tecnología de la información (TI), con relación a los riesgos y amenazas, trae para el foco de las discusiones la influencia de las personas, de los principales activos de las organizaciones, en la Gestión de Seguridad de la Información. En este contexto, explicamos "La Importancia de la Gobernanza de TI en la Gestión de Seguridad de la

[1] Graduada em Redes de Computadores (FATENE). Graduada em Letras - Português/Inglês (UECE). Pós-graduada em Governança de Tecnologia da Informação com ênfase em ITIL e CobiT (Centro Universitário UniAteneu) e Especialista em Segurança da Informação (Estácio). Chefe da Unidade de Gestão da Informação do Complexo Hospitalar da UFC/Ebserh.

[2] Professor da Disciplina de Metodologia do Trabalho Científico (Orientador) – Centro Universitário UNIATENEU; Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE); Instituto Euvaldo Lodi (IEL). Dr. (Tít. Cult.) em Ciências Biológicas pela FICL; M. Sc. em Fitotecnia pela Universidade Federal do Ceará (UFC); Spec. em Metodologia do Ensino de Ciências pela Universidade Estadual do Ceará (UECE); Spec. (Tít. Cult.) em Paleontologia Internacional pela Faculdade Internacional de Cursos Livres (FICL). Graduado em Agronomia pela Universidade Federal do Ceará (UFC); Licenciado nas disciplinas da Área de Ciências da Natureza, Matemática e suas Tecnologias pela Universidade Estadual Vale do Acaraú (UVA); Consultor Internacional do BIRD para Laboratórios Científicos. Conveniado com a ABNT.

Información", luego presentamos "La Importancia del Factor Humano, asociada a los Controles y Prácticas orientadas a la Concientización y Educación, como Pilar Fundamental en la Gestión de Seguridad de la Información" y en la secuencia, apuntamos "Los Enfoques Utilizados en la Hora de Sensibilizar a las Personas sobre Seguridad de la Información en las Organizaciones". Al final del estudio, se concluye que todavía existe una gran laguna en la seguridad de la información en lo que se refiere a la concientización de las personas sobre la importancia de las informaciones manipuladas y en el papel de cada una de esas personas con la seguridad de esas informaciones.

Palabras clave: Gestión. Personas. Seguridad de la Información. Tecnología de la información.

ABSTRACT

The objective of this article is to identify in the literature and to emphasize to the readers that the importance of protecting the information and the assets of information technology (IT), with respect to the risks and threats, brings to the focus of the discussions the influence of the people, a of the main assets of organizations, in Information Security Management. In this context, we explain "The Importance of IT Governance in Information Security Management", then we present "The Importance of the Human Factor, Associated with Controls and Practices for Awareness and Education, as a Fundamental Pillar in Information Security Management" and in the sequel, "The Approaches Used to Sensitize People on Information Security in Organizations." At the end of the study, it is concluded that there is still a large gap in information security regarding the awareness of the people about the importance of the information manipulated and the role of each of these people with the security of this information.

Descriptors JEL: D08 - Information, Knowledge, and Uncertainty; D83 – Search, Learning, Information and Knowledge, Communication, Belief, Unawareness.

Keywords: Management. People. Information security. Information Technology.

1 INTRODUÇÃO

As organizações estão cada vez mais investindo na área de segurança física e lógica (firewall, controle de acesso, segurança eletrônica, antivírus, softwares de detecção de intrusão, entre outros) para controlar o acesso não autorizado a um dos seus principais ativos: a informação. O intuito é evitar que as vulnerabilidades se tornem ameaças concretas. Contudo, apesar de todos os avanços tecnológicos, o comportamento humano ainda tem interferido significativamente nessa área, por não ter a devida importância na gestão da segurança da informação, trazendo, assim, prejuízos consideráveis para as organizações. Gerir o risco considerando pessoas como o ativo é estar atento a todas as vulnerabilidades humanas, como a falta de conhecimento e/ou comportamento éticos.

Segundo Prestes (2018), tecnologias atuais, tais como: UEBA (*User and Entity Behavior Analytics*), UBA (*User behavior analytics*), e outras ferramentas de análise comportamental de usuários, que visam detectar ameaças presentes, colocam o indivíduo como destaque nas últimas tendências de desenvolvimento da segurança da informação. É necessário investir mais em capacitação técnica para os usuários, considerando o fator comportamental, para que eles possam ser conscientizados sobre seu papel no processo de proteção das informações da organização, de modo que essas informações, consideradas muitas vezes confidenciais, não venham a ser encontradas em e-mails pessoais, anotações de smartphones particulares ou, indevidamente, caiam até nas mãos de terceiros desautorizados.

Colocar o fator humano como pilar base para estudos na área de segurança da informação pode ser considerado uma saída, pois o aspecto humano, não raro, é desvalorizado, contribuindo para a realização de práticas que levam a prejuízos significativos para as organizações. Desta forma, será que podemos considerar a ausência de controles e práticas voltadas para a conscientização e educação das pessoas como responsáveis pelo mal desempenho da Gestão de Segurança da Informação nas Organizações?

Trazer para o foco das discussões a influência das pessoas, consideradas atualmente também como um dos principais ativos das organizações, e mostrar como elas podem vir a impactar diretamente na gestão de segurança da informação; discutir as consequências sobre a ausência de controles e práticas voltadas para a conscientização e educação das pessoas na segurança da informação têm reflexos diretos na implementação de uma boa gestão de segurança da informação, pode trazer bons resultados nessa área. Por outro lado, negar a importância das pessoas nesse contexto e deixar as empresas pensarem que estão fazendo a abordagem certa, colocando as pessoas em último plano e investindo somente em tecnologias, pode levar ao agravamento de situações de insegurança e roubo de informações que podem comprometer o funcionamento das organizações.

O presente trabalho visa mostrar a importância das pessoas, através de pesquisa bibliográfica, básica e qualitativa, e de caráter exploratório, levando em conta que os usuários são os principais conhecedores e manipuladores das informações, destacando como o aspecto comportamental pode interferir no contexto geral da segurança da informação, potencializando as falhas e vulnerabilidades existentes, sendo então, considerado ponto focal na Gestão de Segurança da Informação nas Organizações.

Diante de todo o exposto, definiu-se os seguintes objetivos para este artigo científico: explicar a importância da governança de TI na gestão de segurança da informação, apresentar a importância do fator humano, associada aos controles e práticas voltadas para a conscientização e educação, como pilar fundamental na gestão de segurança da informação e apontar as abordagens utilizadas na hora de sensibilizar as pessoas sobre segurança da informação nas organizações.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 A Importância da Governança de TI na Gestão de Segurança da Informação

A Globalização trouxe consigo uma revolução tecnológica, levando as empresas a se repensarem constantemente. Mas mesmo com toda a evolução, a tomada de decisão ainda é uma prerrogativa humana. Para desenvolver e administrar os projetos, as empresas precisam das pessoas. Coordenar tudo isso e ainda entregar valor é uma função de um gestor competente (Theecnetwork, 2009).

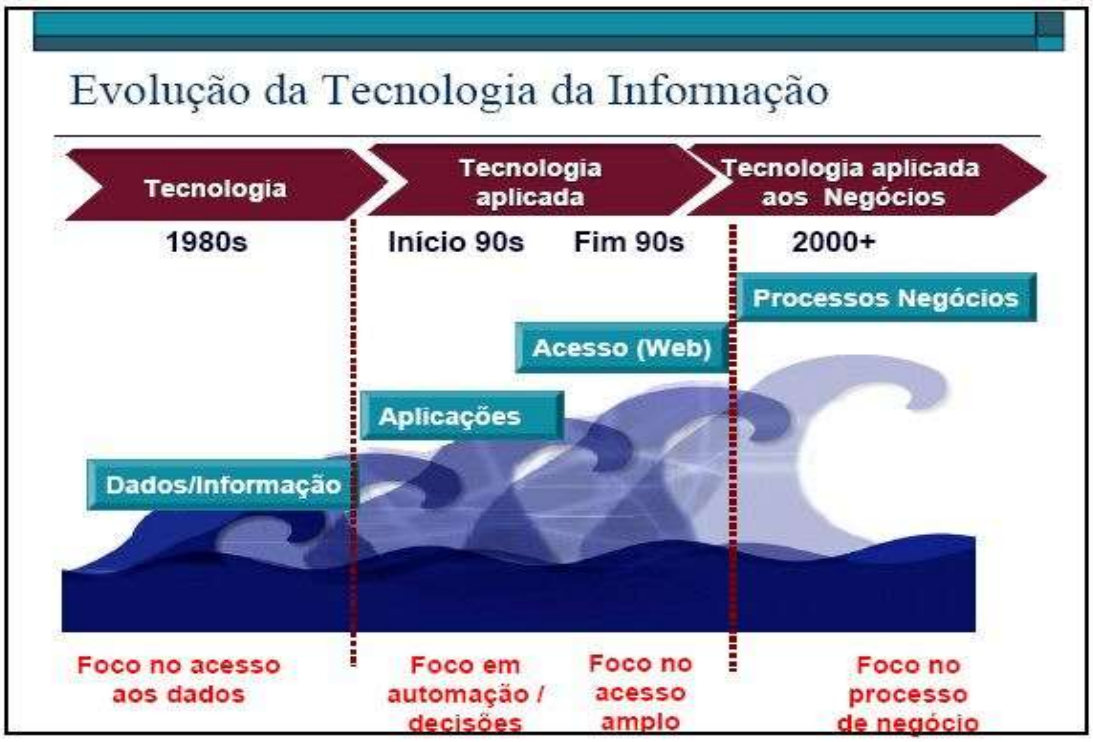

Figura 1 - A evolução da tecnologia da informação nos últimos 45 anos

Fonte: Rezende (2018)

A Governança de TI alinha seus planos com os de negócio gerenciando os riscos, os recursos, o desempenho, otimizando os resultados para entregar valor permitindo o uso mais racional e eficiente da TI dentro das organizações.

Segundo o *Information Technology Governance Institute* – ITGI (2007, p. 7) “governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização”.

A utilização da TI estrategicamente pode aumentar a vantagem competitiva das empresas passando a ser um instrumento de diferenciação com relação aos seus concorrentes. E a informação se tornou uma ferramenta valiosa para o sucesso, o aumento de produtividade e a redução de custos no mercado em que essas empresas atuam. “O maior valor das informações é sua vantagem competitiva no mercado.“ (Horton; Mugge, 2003, p. 07).

Figura 2 - Áreas de foco na Governança de TI
Fonte: ITGI (2007)

As informações de uma empresa são essenciais para garantir a continuidade do negócio, pois são assuntos pertinentes ao seu funcionamento. Contudo, a segurança dessas informações, o gerenciamento de seus riscos, apesar de tão essenciais para as empresas, na grande maioria, ainda não são vistos como estratégicos para as áreas de negócios.

Atualmente, já existem várias recomendações na literatura que, se implementadas, permitem a redução dos riscos e podem garantir a segurança das informações nas empresas, tais como:

- Definir regras considerando o ciclo de vida das informações
- Criar o departamento de Segurança da Informação
- Realizar treinamentos de todos os funcionários, inclusive os da área de segurança da informação
- Implementar soluções de proteção da informação
- Configurar as ferramentas corretamente e monitorar os canais de informação constantemente
- Definir o departamento de Segurança da Informação como “contrapeso” ao departamento de Tecnologia da Informação

Pessoas, processos e tecnologias são de vital importância para a manutenção da segurança da informação. O processo de manter segura a informação requer muito mais do que avanços tecnológicos. A segurança da informação passa por questões que vão além do setor de TI. É preciso trabalhar fortemente as questões humanas e culturais para que, em conjunto com processos e procedimentos bem estruturados, os riscos sejam minimizados.

Em virtude desse cenário e na busca por otimização de processos, a Gestão de Segurança da Informação nas organizações precisa trabalhar continuamente o fator humano associado aos controles e práticas voltadas para a conscientização e educação na Segurança da Informação. E é nesse contexto, que a Governança é de suma importância para a efetiva implementação desses controles e práticas.

Figura 3 - Dimensões da Governança em TI
Fonte: Santos; Baruque (2010)

O objetivo da governança é criar meios eficientes de gerenciamento (alinhamento estratégico) em que o foco está em garantir que as ações implementadas sejam alinhadas aos interesses dos envolvidos e a busca de maiores resultados, alinhados à estratégia fim da organização. “A reunião de gestores com visões do mesmo objeto, mas de pontos diferentes, é fundamental para a obtenção real dos problemas, desafios e consequências.” (Ferreira; Araújo, 2008, p. 70).

Um dos principais atores da Governança é a alta administração e uma de suas principais preocupações é garantir a adesão dos colaboradores da organização a códigos de conduta, políticas e normas pré-acordados, através de mecanismos que tentam reduzir ou eliminar os conflitos de interesse. É muito importante que a empresa promova de forma sincronizada, ações para que exista aderência às melhores práticas de gestão, as quais devam ser observadas e aplicadas em todos os níveis organizacionais.

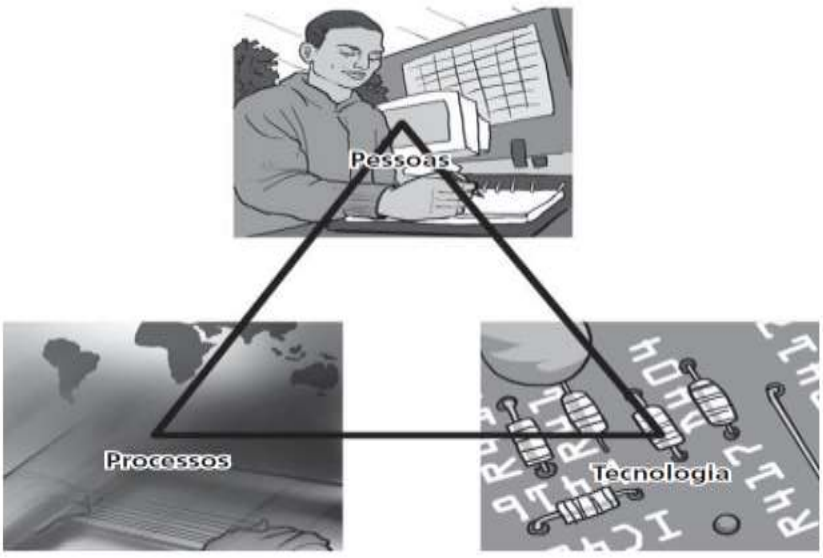

Figura 4 – Pessoas, Processos e Tecnologia
Fonte: Santos; Baruque (2010)

E nesse contexto, a Gestão de Segurança da Informação nas organizações precisa do apoio da governança, de seu comprometimento, para fazer uma boa implementação de segurança da informação. Os controles e práticas voltadas para a conscientização e educação dos colaboradores precisam estar alinhados com os objetivos da empresa, bem como com a Governança. Os colaboradores precisam ver que a Governança está totalmente comprometida com essa implementação. “A Governança de TI eficaz estimula e amplifica a engenhosidade dos funcionários no emprego da Tecnologia da Informação e assegura a observância da visão e dos valores gerais da empresa. “ (Weill; Ross, 2006, p. 2).

2.2 A Importância do Fator Humano, Associada aos Controles e Práticas Voltadas para a Conscientização e Educação, Como Pilar Fundamental na Gestão de Segurança da Informação

A segurança da informação pode ser definida por meio de seus três pilares:

- Confidencialidade: assegura que as informações confidenciais e críticas não sejam acessadas por quem não possui o acesso devido
- Integridade: corresponde à preservação da precisão, consistência e confiabilidade das informações
- Disponibilidade: os dados podem ser acessados a qualquer momento por quem possui acesso aos mesmos

Essas definições se complementam e norteiam políticas e normas nas organizações gerando controles efetivos. A implementação de uma política de segurança da informação e a avaliação dos riscos, definindo quais informações precisam ser protegidas, quais as ameaças e os danos que podem atingir a organização, têm um papel muito importante. Essas políticas devem ser apropriadas ao ambiente e aos objetivos de negócio da empresa, mas a sua efetividade depende de uma boa gestão da segurança da informação, considerando ainda a estratégia, o planejamento e principalmente os aspectos humanos nas organizações.

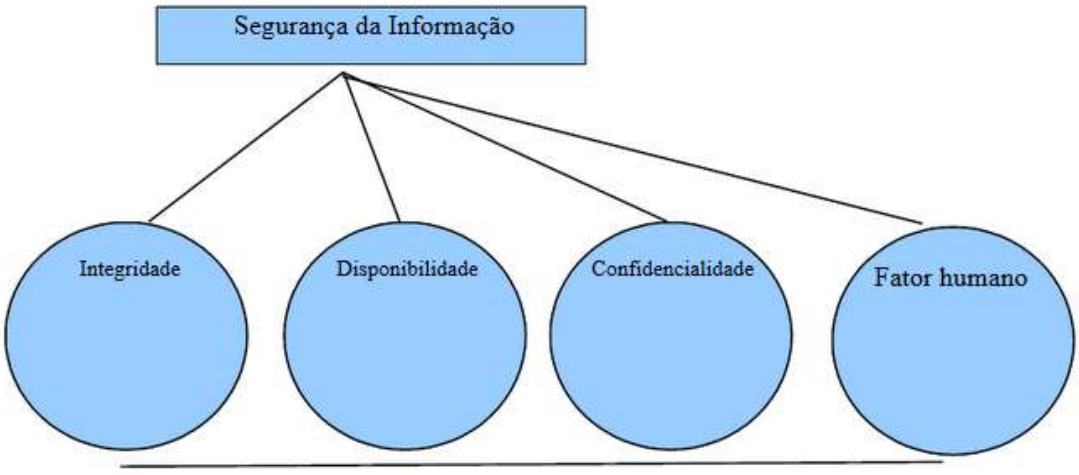

Figura 5 – Proposta para um novo olhar sobre segurança da informação com o fator humano como base
Fonte: Silva; Costa (2009)

As pessoas exercem um forte impacto sobre a confidencialidade, a integridade e a disponibilidade da informação, pois, por exemplo, o usuário que não mantiver a confidencialidade de sua senha, registrá-las em papéis que não estão guardados em locais seguros, utilizar senhas de baixa qualidade, senhas consideradas fracas, que podem ser facilmente exploradas, ou ainda que compartilhar senhas individuais, pode comprometer a segurança da informação.

Práticas como autorização de usuários que permitem acessos a dados e objetos, se malconduzidas, fragilizam a segurança, uma vez que muitas pessoas acabam tendo acesso a informações importantes, colocando em risco a segurança da informação. Além dessas falhas, erros

humanos têm sido relatados com frequência cada vez maior, interferindo na segurança da informação. “Nenhuma área ou instalação de TI será cem por cento invulnerável a fatores naturais ou ações feitas pela mão do homem”. (Ferreira; Araújo, 2008, p. 189)

As ameaças tecnológicas podem interromper, temporariamente, o trabalho de uma empresa, suas comunicações e o contato com os clientes, mas tudo isso pode ser resolvido rapidamente. Por outro lado, um colaborador mal-intencionado, possuindo acesso a dados secretos, documentos financeiros e outros dados, pode causar sérios danos ao negócio. “O tipo de ameaça pode ser intencional (humana), acidental (humana) ou natural”. (Horton; Mugge, 2003, p. 30). É importante mapear os diversos cenários que podem configurar ameaças à segurança da informação, conhecendo assim as principais fontes de riscos.

Uma forma conhecida de ataque cibernético, ameaça constante às informações, é a chamada engenharia social, que tem por objetivo manipular pessoas e/ou acessar informações para fins dos mais diversos: desde um sequestro até uma simples abordagem para um relacionamento pessoal. Um simples e-mail malicioso pode instalar no computador do usuário um *malware* (programa malicioso com o intuito de causar danos) e pode colocar em risco uma segurança fragilizada. Apesar da capacitação e do treinamento dos usuários reduzirem a probabilidade de sucesso de uma abordagem desse tipo, de nada adianta, se a conscientização não partir do colaborador.

Figura 6 – Golpes na Internet
Fonte: Cert.br (2012)

Mesmo com as melhores tecnologias e todos os processos bem arquitetados na empresa, os colaboradores precisam estar engajados, conscientes de que fazem parte e de que são responsáveis pela segurança da informação da empresa como um todo. Segundo Lyra (2015), um ótimo motivador nesse caso é explicar como a participação das pessoas beneficiará não apenas a empresa, mas também os empregados em si, pois como a empresa detém informações particulares sobre cada funcionário, quando os colaboradores fazem a sua parte para proteger as informações ou os sistemas de informações, na verdade eles estão protegendo também as suas próprias informações. Não são apenas as empresas que estão sujeitas ao roubo de dados, as pessoas físicas também podem ser afetadas.

Os parceiros de negócios da área de TI e de outras áreas também precisam estar inseridos quando o assunto é segurança. As organizações precisam adotar critérios para seleção e monitoramento da segurança da informação desses parceiros, pois tanto os colaboradores internos como externos se utilizam de alguma forma dos recursos de TI e precisam ser vistos pela gestão de segurança da informação da organização. Os colaboradores externos são corresponsáveis pelos princípios da segurança da informação. Uma das formas pode ser a aplicação de termos de confidencialidade. Segundo Fernandes e Abreu (2008), quanto mais interligada com seus

fornecedores, clientes e usuários a empresa estiver, maiores são as chances de ocorrência de incidentes em segurança da informação que possam trazer perdas financeiras.

A ausência ou o desconhecimento das regras de segurança e a utilização, muitas vezes despercebida, de itens maliciosos são alguns dos erros mais comuns dos usuários. Por isso, além das soluções de TI voltadas para a segurança, que através de mecanismos tecnológicos controlam as ações dos usuários, existe a necessidade de treinamentos claros e objetivos sobre segurança da informação nos ambientes corporativos, para conscientização e alertas sobre vulnerabilidades e ameaças.

2.3 As Abordagens Utilizadas na Hora de Sensibilizar as Pessoas Sobre Segurança da Informação nas Organizações

Várias são as recomendações sobre procedimentos para viabilizar a segurança da informação nas organizações visando assegurar um nível de segurança adequado ao negócio, tais como:

- Definir e implementar uma Política de Segurança da Informação alinhada com os objetivos de negócios e conectada com a cultura da empresa
- Implementar um Sistema de Gestão de Segurança da Informação eficiente
- Implementar controles e o monitoramento da Política de Segurança da Informação
- Definir planos de capacitação efetiva para os usuários

As boas práticas representam um caminho rápido para alcançar bons resultados, pois já estão testadas e aprovadas por várias organizações em todo o mundo. “Outra característica importante é o fato de que as chamadas boas práticas são distribuídas e compartilhadas de forma gratuita” (Viana, 2010, p. 13). Vale ressaltar que as boas práticas devem estar conectadas aos princípios e diretrizes da organização.

Ferreira e Araújo (2008) dizem que alguns itens de muita importância devem ser utilizados para o sucesso de uma Política de Segurança:

- Formalização dos processos e instruções de trabalho;
- Utilização de tecnologias capazes de prover segurança;
- Atribuição formal das responsabilidades e das respectivas penalidades;
- Classificação das informações;
- Treinamento e conscientização constantes.

As pessoas costumam enxergar a segurança da informação como algo burocrático, que atrapalha. Consideradas como o elo mais fraco da segurança da informação, as pessoas podem estar sendo abordadas de forma incorreta na hora de sensibilizá-las sobre essa importante área. Porém, se conseguirmos relacionar o tema com o dia a dia das pessoas, com situações rotineiras, pode ser muito mais interessante para os usuários, e neste momento, a percepção da importância dessa segurança pode mudar.

Nos dias atuais, a maioria das pessoas, até em sua vida particular, não possuem a real percepção dos riscos a que estão expostas em função do mundo digital e da velha e perigosa engenharia social. A conectividade atual junta com a engenharia social contribui bastante para a elevação desses riscos, como por exemplo os sites de relacionamento que se apresentam como um ambiente propício para uso de informações falsas.

As pessoas precisam saber quais são as informações que devem ser protegidas e como devem protegê-las, para que estejam aptas a identificar situações de riscos. Definir planos de capacitação efetiva para os usuários, já a partir da admissão, divulgando políticas, normas e procedimentos de segurança da informação, com ações gradativas e constantes, com avaliação de aprendizado, visando criar e fortalecer uma cultura sobre o assunto, pode ajudar nesse contexto.

Figura 7 – Aspectos da Segurança da Informação
Fonte: Skylan (2010 *apud* Alves, 2018)

A consciência e o preparo das pessoas diminuem com o tempo, por isso é importante estabelecer programas de treinamento básico e avançado, trabalhando com a tecnologia e os processos existentes na organização, de forma continuada, direcionados aos diferentes grupos de colaboradores, tais como: a governança, os gerentes, o pessoal de TI, os usuários de computadores, os assistentes, os recepcionistas e o pessoal de segurança física, entre outros, com avaliação periódica e revisão de metodologias, para que se possam identificar as melhorias necessárias. Toda a organização precisa ser envolvida. “As condicionantes psicológicas que movem os agentes fraudadores são variadas e requerem análise para efeito de compreensão”. (Gil, 1996, p. 178).

Neste sentido, para que os planos de capacitação/treinamento dos colaboradores atinjam todos os níveis da organização, faz-se necessária uma combinação de diversos elementos nestes planos: seminários; cursos e capacitação; campanhas de divulgação da política de segurança (folders, e-mails, divulgação de notícias ou campanhas no site ou portal); procedimentos específicos em caso de demissão e admissão de funcionários; termos de responsabilidade e de confiabilidade; software de auditoria de acessos e de monitoramento e filtragem de conteúdo, para que se consiga altos índices de compreensão sobre o assunto.

Além disso, as consequências pelo não-cumprimento das políticas e dos procedimentos de segurança também devem ser consideradas importantes. Precisam ser definidas, divulgadas e implementadas para os usuários nestes mesmos planos. “A própria Política de Segurança deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com sua severidade, amplitude e tipo de infrator que a executa”. (Ferreira; Araújo, 2008, p. 155). Por sua vez, a empresa também pode apresentar um programa de recompensa, que deve ser criado para os empregados que demonstram boas práticas de segurança ou que reconhecem e relatam um incidente de segurança. E sempre que houver essa recompensa, isso também deve ser amplamente divulgado como exemplo para toda a empresa.

Como muitos aspectos da segurança da informação envolvem tecnologia, é muito fácil para os colaboradores acharem que problemas nessa área não envolvem as pessoas. A capacitação, então, deve criar em cada empregado a consciência sobre a importância dele na segurança geral da organização e como reagir em caso de situações de riscos presentes em determinadas situações.

Diante de situações de risco, muitas vezes, as pessoas costumam modificar seus comportamentos, e suas decisões são baseadas em confiança ou grau de criticidade da situação. Será que realizar atividades de engenharia social reversa para expor e corrigir as falhas com os usuários seria uma boa opção? Realizar uma série de testes para verificar o comportamento dos usuários, incluindo novas técnicas e como lidar com cada uma delas, demonstrando efetivamente o que estão fazendo de errado e, mais do que isso, comunicando diretamente àqueles que realmente “caíram” nas armadilhas, pode ser muito mais efetivo do que as campanhas educacionais?

Um método para manter a segurança sempre na mente do empregado é fazer com que a segurança das informações seja parte específica da função de todas as pessoas que trabalham na empresa. Isso as encoraja a reconhecer o seu papel crucial na segurança geral da empresa. Há uma

forte tendência de os usuários acharem que a segurança não é problema deles, é uma particularidade somente da TI.

Outro ponto importante a ser tratado é o monitoramento dos sistemas de informação, que é feito, normalmente, mediante registros de *log* (registros cronológicos de atividades do sistema), trilhas de auditoria ou outros mecanismos capazes de detectar invasões. “O domínio dos controles de *logs* e de aplicativos, tanto por profissionais de informática quanto por usuários, é fundamental para minimizar a possibilidade de ocorrência de fraudes informatizadas”. (Gil, 1996, p. 70). Inabilidade técnica também gera vulnerabilidades de hardware e software. Esse monitoramento é essencial à equipe de segurança de informações, já que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários.

Portanto, políticas, capacitações, treinamentos, testes, monitoramentos, dentre outros, são práticas que podem contribuir para a segurança da informação nas organizações, considerando o envolvimento de todos da organização, do nível estratégico ao operacional. Mas, tudo isso não será suficiente, se não levarmos em conta o comportamento humano e suas particularidades, promover ações proativas, em vez de reativas, tendo em vista a garantia da segurança da informação e a defesa dos interesses da empresa.

3 METODOLOGIA

A metodologia empregada para o desenvolvimento do presente trabalho se constituiu em uma pesquisa bibliográfica que procurou investigar em referências teóricas publicadas em livros, artigos científicos, documentos etc., para explicar, com maior aprofundamento, os assuntos contidos no corpo do artigo à luz das contribuições cientificas pré-existentes.

Segundo Lakatos e Marconi (1991), a pesquisa bibliográfica é o levantamento de toda a bibliografia já publicada, em forma de livros, revistas, publicações avulsas e imprensa escrita.

A sua finalidade é fazer com que o pesquisador entre em contato direto com todo o material escrito sobre um determinado assunto, auxiliando o cientista na análise de suas pesquisas ou na manipulação de suas informações. Ela pode ser considerada como o primeiro passo de toda a pesquisa científica.

Dentre as contribuições pesquisadas, destacam-se as obras de autores como por exemplo: Ferreira; Araújo (2008), Weill; Ross (2006), Lyra (2015).

Sabe-se que uma boa base teórica é o alicerce para se olhar os dados bibliográficos levantados e desenvolver um estudo, indo além do que a realidade nos mostra simplesmente.

A orientação do estudo, deu-se pelo questionamento acerca dos benefícios trazidos às empresas quando se leva em conta o comportamento humano nos controles e práticas voltadas para a conscientização e educação sobre a segurança das informações nas organizações.

Desta forma, o domínio dos autores pesquisados contribuiu de forma precisa no desenvolvimento desse artigo já que, por meio deles, foi possível saber o que se produziu de importante sobre o objeto de estudo e sobre os avanços alcançados a respeito dele.

4 CONSIDERAÇÕES FINAIS

Após criteriosa pesquisa, o que se pode perceber é que as empresas estão cada vez mais vulneráveis aos acessos maliciosos em seus ativos, principalmente através das pessoas, consideradas atualmente também, um dos seus principais ativos, podendo resultar em perdas de dados e informações e que a gestão de segurança da informação ainda não é uma prática comum nas empresas.

Nesse contexto, contar com uma efetiva e comprometida Governança de TI pode contribuir de forma considerável para prover uma direção estratégica à empresa, assegurando que os objetivos sejam alcançados e seus riscos gerenciados apropriadamente, proporcionando uma gestão de segurança da informação bem-sucedida, com redução nos riscos, uma vez que essa área requer o envolvimento de todos da organização, do estratégico ao operacional.

Nos dias atuais, o cenário da Tecnologia da Informação passa por uma série de mudanças que exigem eficiência e rapidez na solução de problemas. Os acessos estão cada vez mais remotos e descentralizados, com processamento mais virtual gerando assim uma quantidade de riscos que precisam ser gerenciados. Os benefícios podem ser alcançados quando envolvem técnicas de gerenciamento e ferramentas que agilizem o processo.

Outro ponto a considerar é que a segurança da informação, apesar de ser um tema tão comentado, ainda é pouco pesquisado. Encontramos pouca literatura referente a usuários e segurança da informação, com foco no comportamento humano.

Objetivamente, o que se pôde observar é que as pessoas interferem diretamente no sucesso da gestão da segurança da informação, por isso não podem ficar em segundo plano. Elas podem representar uma barreira para prevenir incidentes nessa área. Por isso, é importante que as empresas criem uma cultura de segurança e fortaleçam a sua influência no comportamento dos seus colaboradores, trabalhando melhor os controles e práticas voltadas para a conscientização e educação dessas pessoas, pois sem conhecimento, não há comprometimento.

A discussão sobre a Influência humana e os controles e práticas voltadas para a conscientização e educação das pessoas na gestão de segurança da informação nas organizações, além de ser importante do ponto de vista prático, é um assunto relevante para o desenvolvimento de estudos e pesquisas.

Considerando que a produção científica tem como objetivo contribuir para o aperfeiçoamento da vida social, esse estudo pode colaborar para a divulgação desse assunto e para a construção de um saber novo.

REFERÊNCIAS

Alves, Cássio Bastos. (2018). *Segurança da informação vs. Engenharia Social* - Como se proteger para não ser mais uma vítima. Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm>. Acesso em 26 out. 2018.

CERT.br. (2012). *Cartilha de Segurança para a Internet:* v4.0. São Paulo: Comitê Gestor da Internet no Brasil.

Fernandes, Aguinaldo Aragon; Abreu, Vladimir Ferraz de. (2008). *Implantando a governança de TI:* da estratégia à gestão dos processos e serviços – 2ª ed. Rio de Janeiro: Brasport.

Ferreira, Fernando Nicolau Freitas; Araújo, Márcio Tadeu de. (2008). *Política de Segurança da Informação* – Guia Prático para Elaboração e Implementação. 2ª ed. Revisada. Rio de Janeiro: Ciência Moderna Ltda.

Gil, Antônio de Loureiro. (1996). *Fraudes Informatizadas.* São Paulo: Atlas.

Horton, Mike; Mugge, Clinton. (2003). *Hack Notes:* Segurança de Redes – Referência Rápida. Rio de Janeiro: Elsevier.

ITGI. (2007). CobiT 4.1.

Lakatos, E.M.; Marconi, M. A. (1991). *Fundamentos da Metodologia Científica.* 3ª ed., São Paulo: Atlas.

Lyra, Mauricio Rocha. (2015). *Governança da Segurança da Informação*. Brasília.

Prestes, Vladimir. (2018). *Fator Humano na Segurança.* Disponível em: <https://www.baguete.com.br/noticias/12/06/2018/o-fator-humano-na-seguranca>. Acesso em: 24 set. 2018.

Rezende, Denis Alcides. (2018). *A evolução da tecnologia da informação nos últimos 45 anos.* Disponível em: <http://www.joinville.udesc.br/portal/professores/pfitscher/materiais/Evolu__o_da_TI.pdf> Acesso em: 10 set. 2018.

Santos, Luis Cláudio dos; Baruque, Lúcia Blondet. (2010). *Governança em Tecnologia da Informação.* v. 1. Rio de Janeiro: Fundação CICIERJ.

Silva, Maicon Herverton Lino Ferreira da; Costa, Veridiana Alves de Sousa Ferreira. (2009). *O Fator Humano como Pilar da Segurança da Informação:* uma proposta alternativa. IX Jornada de Ensino Pesquisa e Extensão (JEPEX) da UFRPE.

Theecnetwork. (2009). *A Governança de TI em um Mundo Globalizado*.

Viana, Helder de Souza. (2010). *Governança de TI e suas Metodologias dentro do Mundo Corporativo.* Rio de Janeiro.

Weill, Peter; Ross, Jeanne W. (2006). *Governança de TI, Tecnologia da Informação.* São Paulo: M. Books do Brasil Editora Ltda.