UNIVERSIDADE FEDERAL DE SANTA CATARINA

CAMPUS ARARANGUÁ

Jesiel Bitencourt

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: DESAFIOS E PERSPECTIVAS

Araranguá, Abril de 2018.

Jesiel Bitencourt

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: DESAFIOS E PERSPECTIVAS

Trabalho de Curso submetido à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Tecnologias da Informação e Comunicação.

Orientador: Prof. Dr. Giovani Mendonça Lunardi.

Araranguá, Abril de 2018.

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

CITTADIN, JESIEL DE OLIVEIRA BITENCOURT
GESTÃO DA SEGURANÇA DA INFORMAÇÃO: DESAFIOS E PERSPECTIVAS / JESIEL DE OLIVEIRA BITENCOURT CITTADIN ; orientador, Giovani Mendonça Lunardi, 2018.
70 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá, Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2018.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Segurança da informação. 3. Cenários da Segurança. 4. Gestão da Informação. 5. Mundial. I. Mendonça Lunardi, Giovani. II. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. III. Título.

TÍTULO: Gestão da Segurança da Informação: Desafio e Perspectivas

Este Trabalho Conclusão de Curso foi julgado adequado para obtenção do Título de **"Gestão da Segurança da Informação: Desafio e Perspectivas"** e aprovado em sua forma final pelo Programa ...

Araranguá, 22 de junho de 2018.

Prof.ª Dr.ª Patricia Jantsch Fiuza
Coordenador do Curso

Banca Examinadora

Prof. Dr. Giovani Mendonça Lunardi
Orientador
Universidade UFSC

Prof. Msc Rangel Machado Simon
Universidade UFSC

Prof.ª Dra. Angelita Darela Mendes
Universidade UFSC

Este trabalho é dedicado aos meus pais, meus grandes amigos.

AGRADECIMENTOS

Agradeço imensamente aos meus pais, por terem sido mais do que educadores, eles foram exemplos claros de vida e de caráter, me orgulho muito por ser seu filho.

Agradeço à minha esposa, minha companheira e amiga, por compreender que minha ausência era necessária, mas que seria recompensada quando esse momento de dificuldade e luta fossem vencido.

Agradeço a todos os amigos e familiares que, de alguma forma, contribuíram para que eu pudesse alcançar essa conquista, sem o amor e apoio de vocês, eu não teria sido capaz.

Agradeço ao meu professor orientador, Giovani Lunardi, por ter me acompanhado com paciência, atenção e companheirismo nesse percurso. Obrigado professor por me orientar, guiar e seguir comigo por todo o caminho.

Agradeço, acima de tudo, a Deus, pela vida, saúde e oportunidades.

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis” (JOSÉ DE ALENCAR).

RESUMO

Este estudo trata-se de uma pesquisa bibliográfica com foco na segurança da informação na sociedade atual, na qual cada vez mais dados circulam pelas redes que conectam indivíduos, empresas e governos em todo o mundo. Essas tecnologias permitem que estudos, trabalho, negócios e lazer sejam conduzidos de forma simples, prática e facilitada, porém, não se pode afirmar que não existam riscos envolvidos. Diante disso, o objetivo geral foi definido como: investigar os principais desafios e perspectivas na gestão da segurança de informação. Os objetivos específicos, por sua vez, foram assim estabelecidos: a) identificar os principais conceitos de gestão de segurança da informação; b) verificar os desafios para a gestão da segurança de informação; e c) apontar perspectivas futuras para a gestão da segurança da informação. Verificou-se que área de segurança da informação evoluiu grandemente ao longo dos anos, todavia, os conhecimentos de usuários com intuitos ilícitos também foram expandidos e, assim, o cenário demanda de constantes melhorias. Enquanto os maiores desafios residem na necessidade de desenvolver barreiras que protejam os usuários de ataques diversos, as perspectivas recaem sobre a capacidade de obter, armazenar e proteger os dados disponíveis, tornando as empresas e instituições mais efetivas, com melhores resultados na tomada de decisões e capazes de se destacar das demais existentes no mercado.

Palavras-chave: Segurança da informação. Desafios. Perspectivas.

ABSTRACT

This study is a bibliographical research focused on information security in today's society, where more and more data circulate through the networks that connect individuals, companies and governments around the world. These technologies allow studies, work, business and leisure to be conducted in a simple, practical and easy way, but it can not be said that there are no risks involved. Therefore, the general objective was defined as: to investigate the main challenges and perspectives in the management of information security. The specific objectives, in turn, were established as follows: a) identify the main concepts of information security management; b) verify the challenges for information security management; and c) indicate future perspectives for the management of information security. It was verified that information security area has evolved greatly over the years, however, the knowledge of users with illicit intentions has also been expanded and, thus, the scenario demands constant improvements. While the major challenges lie in the need to develop barriers to protect users from various attacks, the prospects lie with the ability to obtain, store and protect available data, making enterprises and institutions more effective, with better decision-making able to stand out from the others in the market.

Keywords: Information security. Challenges. Perspectives.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Na sociedade atual a informação está disseminada em todos os seus setores e, cada vez mais, vem sendo vista como um recurso para empresas e pessoas que desejam alcançar resultados em sal vida pessoal, acadêmica, profissional ou social. Muitas dessas informações podem ser acessadas de forma aberta, sem custos e sem limitações, porém, existem dados que precisam ser resguardados e protegidos, em função dos riscos que acarretaria seu amplo acesso por outros indivíduos ou empresas (SILVA; STEIN, 2007).

Diante dessa realidade, cada vez mais estudos vêm sendo conduzidos no sentido de encontrar formas de aumentar a segurança da informação, para que seu uso ocorra apenas por entidades e pessoas autorizadas a fazê-lo e, assim, evitando que sejam disseminadas livremente, colocando em risco os indivíduos aos quais esses dados se referem (SILVA; STEIN, 2007).

Segurança da informação refere-se ao desenvolvimento de formas de proteger os dados dos quais uma empresa, instituição ou indivíduos em geral fazem uso em suas atividades. Atualmente a informação trata-se de um produto no mercado, essencial para empresas que comercializam bens e serviços e podem englobar estoque, clientes, contas a pagar, a receber, etc. (MARCIANO, 2006).

Ocorre que essas informações podem representar o sucesso ou fracasso de uma empresa, além de sua privacidade e de seus clientes, de modo que protegê-las é indispensável para que a empresa mantenha-se competitiva no mercado e para que seus clientes estejam completamente seguros (MARCIANO, 2006).

Rigon e Westphall (2011) esclarecem que tamanha é a importância das informações que circulam no mercado, que cada vez mais sistemas de proteção vêm sendo criados, porém, ao mesmo tempo, cada vez mais pessoas vêm se especializando em formas de invadir os sistemas de diferentes companhias para obter esses dados.

A segurança da informação, de forma geral, está atrelada às pessoas que coletam, registram e armazenam esses dados. Há uma relação entre informação, segurança e cuidados assumidos pelos indivíduos para que esses dados sejam resguardados continuamente. Assim como as pessoas podem proteger as

informações, elas também podem colocá-las em risco, caso assumam condutas inadequadas (SILVA; STEIN, 2007).

Gerenciar as informações, bem como a segurança das mesmas, é atividade essencial para que os dados sejam protegidos e possíveis invasões não venham a colocar em risco empresas e pessoas cujos dados estão ali armazenados. Diante disso, o gerenciamento de segurança vem tomando uma relevância cada vez maior e diferentes ferramentas de proteção vêm sendo desenvolvidas (RIGON; WESTPHALL, 2011).

Marciano (2006) acredita que muitas pessoas e empresas questionam a segurança da informação, porém, os esforços para alcançar essa segurança, apesar de apresentarem desenvolvimento constante, ainda não alcançaram os patamares desejados e, assim, o tema merece apreciação contínua para que se altere o cenário e se alcance segurança, confiabilidade e possibilidade cada vez maior de atividades por meio das Tecnologias de Informação e Comunicação com os menores riscos envolvidos.

Neste sentido, inúmeros desafios permeiam a área, todos relacionados ao desenvolvimento de tecnologias e ferramentas que permitam elevar a segurança da informação e, assim, assegurar aos usuários dessas tecnologias de que suas informações não serão indevidamente utilizadas, o que poderia causar-lhes constrangimentos, riscos e prejuízos diversos. Não obstante, as perspectivas de futuro na área são ainda mais amplas, envolvendo tecnologias cada vez mais avançadas, com esforços constantes e globais para que a segurança não seja apenas uma teoria, mas se torne uma realidade em todos os níveis das tecnologias da informação (OLIVEIRA; MOURA; ARAÚJO, 2012).

Proteger os usuários é proteger as empresas que fazem uso de seus dados e, assim, cada vez mais esse é um objetivo das instituições, pessoas e governos, não apenas no Brasil, mas em todo o mundo.

1.1 JUSTIFICATIVA

Este trabalho justifica-se pela necessidade de verificar de que forma as empresas protegem suas informações de possíveis invasões e roubo de dados. A perda de dados pode significar perda de clientes, fornecedores, baixa na qualidade

das obras, riscos nas mesmas, além do comprometimento de dados de suas atividades ou dados pessoais de seus clientes que, desprotegidos, podem ser utilizados em atividades ilícitas, prejudicando as pessoas e as empresas.

Não obstante, processos judiciais podem ter início em função do uso inadequado das informações de clientes e, assim, cada vez mais existe uma preocupação no sentido de resguardar esses dados de uso ilícito e proteger os indivíduos a que se referem, bem como as instituições que estão de posse deles. Quanto mais informações encontram-se disponíveis no mercado, maior se torna o interesse de alguns indivíduos e empresas de obter esses dados, porém, quando não há autorização para seu uso, esta se torna uma atividade ilegal, passível de punições e com leis desenvolvidas em boa parte dos países do mundo (SILVA; STEIN, 2007).

Sabe-se que informação é patrimônio, tem valor e é disputada no mercado, por apoiar a tomada de decisões e ter a possibilidade de melhorar os resultados dos detentores desses conhecimentos. Em face disso, a segurança da informação é essencial para que os clientes não deixem de proceder de suas atividades por medo de terem sua privacidade e seus dados pessoais invadidos e utilizados ilicitamente (OLIVEIRA; MOURA; ARAÚJO, 2012).

Diante disso, é preciso analisar de que forma a relevância da segurança das informações é vista por governos, empresas e indivíduos, quais as ferramentas utilizadas por eles para que os dados sejam mantidos em sigilo e de que forma buscam melhorar essa segurança diariamente em suas atividades. Com isso, torna-se possível destacar quais são os desafios do setor e as perspectivas na área para os próximos anos.

1.2 PROBLEMA DE PESQUISA

Diante do exposto, coloca-se o principal problema a ser investigado: Quais os desafios e perspectivas para a gestão da segurança da informação na sociedade atual?

1.3 OBJETIVOS

Para responder ao problema de pesquisa proposto foram discriminados os seguintes objetivos:

1.3.1 Objetivo geral

Investigar os principais desafios e perspectivas na gestão da segurança de informação.

1.3.2 Objetivos específicos

Identificar os principais conceitos de gestão de segurança da informação;
Verificar os desafios para a gestão da segurança de informação;
Apontar perspectivas futuras para a gestão da segurança da informação.

1.4 METODOLOGIA

A metodologia usada na pesquisa pode ser descrita como o processo de coleta e armazenamento de informações relevantes e confiáveis a respeito do assunto estabelecido como o tema da pesquisa. Para que uma pesquisa alcance o objetivo de confirmar uma teoria, descartá-la ou desenvolver uma teoria diferenciada é preciso que o pesquisador agrupe as informações disponíveis e forme uma base de conhecimentos ampla e confiável para seu trabalho.

O processo de pesquisa como um procedimento desenvolvido de modo racional e sistemático, tendo como objetivo proporcionar respostas aos problemas propostos. “A pesquisa é requerida quando não se dispõe de informação suficiente para responder ao problema [...]” (GIL, 2007, p. 17).

A pesquisa como um “conjunto de procedimentos sistemáticos, baseado no raciocínio lógico, que tem por objetivo encontrar soluções para problemas propostos, mediante a utilização de métodos científicos” (ANDRADE, 2003, p. 121).

A metodologia de pesquisa deve ser uma das primeiras decisões de um pesquisador, pois antes de iniciar seus estudos, ele deverá saber se procederá de um

estudo bibliográfico, de campo, ambos, enfim, ele deverá ter consciência de como irá atuar para obter os dados que o conduzirão aos resultados esperados. Sem esse conhecimento, o pesquisador poderá iniciar seus trabalhos, porém, suas chances de finalizá-los de forma bem-sucedida são reduzidas (SANTOS, 2001).

Desta forma, a metodologia de trabalho abordará os seguintes assuntos: categorização da pesquisa, plano de coleta de dados, plano de análise e de interpretação dos dados e apresentação da organização.

1.4.1 Categorização da pesquisa

A pesquisa realizada por cientistas, pesquisadores profissionais e estudantes, não pode diferir em qualidade e confiabilidade. A diferença essencial deve encontrar-se, somente, nos propósitos.

> A diferença entre os trabalhos dos cientistas e o dos estudantes universitários não deveria residir no método, mas nos propósitos. Os cientistas já estão trabalhando com o intuito de promover o avanço da ciência para a Humanidade; os estudantes ainda estão trabalhando para o crescimento de sua ciência. Ambos, porém, devem trabalhar cientificamente. Os estudantes trabalham cientificamente quando realizam pesquisas dentro dos princípios estabelecidos pela metodologia científica, quando adquirem a capacidade não só de conhecer as conclusões que lhes foram transmitidas, mas se habilitam a reconstituir, a refazer as diversas etapas do caminho percorrido pelos cientistas (SANTOS, 2001, p. 47).

Durante a condução do presente trabalho procedeu-se de observação direta dos escritos disponíveis na área de pesquisa selecionada, o estoque, como forma de obter conhecimentos abrangentes sobre o tema e, assim, levar ao desenvolvimento de um controle efetivo e organizado.

> A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar duplicações e certos erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações. (MARCONI E LAKATOS, 2007, p. 24).

Para Santos (2001), a pesquisa bibliográfica traz consigo uma importante vantagem para o pesquisador, considerando-se que permite a expansão de conhecimentos e, ao mesmo tempo, leva o pesquisador a verificar como outros autores se posicionam sobre o tema. Com isso, a pesquisa bibliográfica não se trata

apenas da leitura de materiais de outros autores, mas da organização e seleção dos mais adequados, bem como o desenvolvimento de uma nova obra.

Não basta, porém, selecionar o tipo de pesquisa a ser conduzida, é preciso também escolher um tipo de pesquisas e um método de coleta de dados adequados e compatíveis ao objetivo da pesquisa. O tipo de pesquisa deve ser estabelecido com base nas necessidades de informação do pesquisador.

A pesquisa pode ser qualitativa, quando sua abordagem é basicamente teórica, ou quantitativa, quando sua abordagem baseia-se em dados numéricos obtidos a partir da coleta de dados. A pesquisa quantitativa é de grande utilidade quanto o tema da pesquisa refere-se à uma teoria já existente e esclarecida. Segundo Marconi e Lakatos,

> A metodologia qualitativa preocupa-se em analisar e interpretar aspectos mais profundos, descrevendo a complexidade do comportamento humano. Fornece análise mais detalhada sobre as investigações, hábitos, atitudes, tendências de comportamento, etc. (2007, p. 269).

No entanto, caso o pesquisador necessite desenvolver gráficos, tabelas ou quaisquer outros conjuntos numéricos, visando estabelecer sua teoria por meio de uma base matemática, a coleta quantitativa de dados certamente irá atender melhor suas necessidade.

A pesquisa quantitativa é a análise que utiliza as informações numéricas obtidas na investigação e apresenta esta informação em forma de conjuntos. Esses dados são muito relevantes quando se deseja apresentar uma realidade ou situação específica que por meio da análise qualitativa de dados não poderia ser realizada. Dados específicos tornam-se mais facilmente compreensíveis quando os dados são analisados sob um enfoque quantitativo, pois é possível compreender o percentual de uma tendência dentro de um determinado grupo, por exemplo (MARCONI; LAKATOS, 2007).

O uso da quantificação na coleta e no tratamento das informações, com base em técnicas estatísticas, tem por objetivo evitar possíveis distorções tanto na análise como na interpretação, possibilitando uma maior margem de segurança. Isso é muito relevante quando o pesquisador deseja apresentar dados específicos, quantidades ou percentuais encontrados por seus estudos e que podem ser representantes de um grupo, de uma situação ou de uma realidade (DIEHL, 2004).

O presente trabalho é composto por uma pesquisa qualitativa descritiva, desenvolvida com o intuito de fornecer uma base teórica confiável.

1.4.2 Plano de coleta de dados

Segundo Prodanov e Freitas (2013), coletar dados é uma atividade essencial para todos os tipos de pesquisa, nas mais diversas áreas do conhecimento:

> Na coleta de dados, o leitor deve ser informado sobre como o pesquisador pretende obter os dados de que precisa para responder o problema. Não devemos deixar de correlacionar os objetivos aos meios para alcançá-los, bem como de justificar a adequação de uns ou outros (PRODANOV; FREITAS, 2013, p. 97).

Os dados coletados servem como base para todo o estudo e, assim, são de extrema relevância e devem ser mantidos dentro de parâmetros claros e confiáveis.

1.4.3 Plano de análise e interpretação dos dados

Após a adequada coleta dos dados relevantes para o estudo conduzido, é indispensável que esses dados sejam organizados, agrupados e analisados sob o enfoque que melhor corresponde aos questionamentos do pesquisador. Analisar os dados coletados é um passo muito relevante para a obtenção dos resultados, sendo que sem essa análise, os dados estarão soltos e, provavelmente, não farão sentido (SANTOS, 2001).

Antes de iniciar a análise dos dados coletados, deve-se proceder de uma visão geral de tudo que foi obtido e, assim, sempre que possível ou necessário, dividir os dados em categorias. Essa categorização torna o estudo mais fácil de ler e compreender e, assim, o material elaborador pelo pesquisador torna-se mais confiável (MARCONI; LAKATOS, 2007).

Conforme Martins e Lintz (2000), existem diferentes formas de analisar os dados coletados, podendo proceder-se de uma comparação entre esses dados e a base teórica previamente desenvolvida, a comparação com os resultados de outros estudos, a utilização de gráficos e tabelas que, por si só, demonstram os resultados obtidos, seguida por uma análise baseada na compreensão que o pesquisador obteve através de seu trabalho, entre outras opções. Cabe a cada pesquisador conhecer as

formas de análise de dados e selecionar aquela ou aquelas que melhor se enquadram no intuito de responder aos seus questionamentos.

1.5 ESTRUTURA DO TRABALHO

Este estudo foi desenvolvido em forma de capítulos, com o intuito de torná-lo mais organizado e, assim facilitar a leitura e compreensão do tema abordado.

O capítulo 2 traz dados sobre os conceitos de segurança da informação e ferramentas de gestão da segurança da informação.

O capítulo 3 refere-se aos desafios da gestão da segurança da informação, os desafios atuais com base nos crimes virtuais, bem como a confiabilidade do mercado.

Na capítulo 4 aborda-se as perspectivas futuras para a gestão da segurança da informação, o cenário atual, a segurança da informação para pessoas, empresas e governos, bem como o cenário futuro.

No capítulo 5 são evidenciadas as conclusões obtidas pelo pesquisador e, por fim, são apresentadas as referências consultadas para o estudo.

2 SEGURANÇA E GESTÃO DA INFORMAÇÃO

2.1 CONCEITO DE DADOS

Muitas vezes ocorre uma confusão entre dados e informação e, ainda, são comuns casos em que se acredita que ambos os conceitos são iguais. Ressalta-se que dados são conceitos que não levam ao alcance de uma compreensão. Cada palavra inserida em um sistema é um dado, porém, os dados só fazem sentido quando são agrupados e podem ser analisados como informações (PERINI, 2011).

Pode-se afirmar que dados são soltos, não estão conectados e, assim, a partir deles não se pode alcançar uma conclusão específica sobre um tema. Cada número, nome e data dentro de um sistema refere-se a um dado, porém, somente se pode compreender quando eles são agrupados e organizados e, assim, pode-se saber, por exemplo, em que data a empresa adquiriu um produto, quanto pagou por ele, qual o valor dos impostos incidentes, etc. (SILVA; STEIN, 2007).

Não se pode afirmar que os dados não são importantes, de fato, eles são indispensáveis para que as informações possam ser obtidas, todavia, os dados são o ponto de partida e, assim, são apenas uma pequena parcela de um processo maior, no qual há uma alimentação de dados em uma base ou sistema e, posteriormente, esses sistema ou a análise de relatórios permite que informações sejam geradas (MARCIANO, 2006).

2.2 CONCEITO DE INFORMAÇÃO

Para que se possa falar em segurança da informação, primeiramente é relevante abordar a informação em si. Perini (2011, p. 3) afirma que “informação é um conjunto de fatos organizados de modo a ter valor adicional, além de fatos propriamente ditos”. Nesse sentido, compreende-se que a informação não abrange apenas os dados dos clientes, mas também dados da própria empresa, de seus produtos, serviços, preços, estratégias, etc.

Silva e Stein (2007) afirmam que praticamente tudo que existe na sociedade atual está atrelado à informação e, do mesmo modo, inúmeras atividades dependem desses dados para serem realizadas. Em qualquer área, saúde, educação, economia,

políticas, ou tantas outras, as informações circulam rapidamente e, muitas delas, representam segurança, desenvolvimento e lucratividade, de modo que são consideradas, no presente, como uma espécie de patrimônio intangível.

Sêmola (2003) afirma que tudo é informação, um telefone, endereço, um diagnóstico, preços, prazos, tudo que se encontra no entorno dos indivíduos está permeado por informações diversas. Todos os dias o número de informações aumenta, assim como o valor delas para empresas, instituições diversas e para as pessoas.

Cada tipo de informação possui uma aplicabilidade específica dentro da empresa e, conforme essa aplicabilidade, a empresa valoriza essas informações, ainda que todas elas tenham importância em suas atividades. As informações podem ser de cunho operacional, que permitem a execução e monitoria de atividades da empresa, bem como oferecem subsídio ao planejamento e tomada de decisões em nível operacional (PERINI, 2011).

Podem apresentar cunho intermediário, quando oferecem aos gerentes a possibilidade de monitorar e avaliar os processos por eles desenvolvidos, aplicados ou controlados, o que permite uma tomada de decisões muito mais efetiva no nível de gerência (PERINI, 2011).

Marciano (2006) afirma que o uso da informação difere entre instituições ou indivíduos, o que para alguns é essencial para aquisição de conhecimentos, para outros forma sua base de clientes, oferece vantagens competitivas, expande a compreensão sobre fatores sociais, econômicos e pessoais específicos, e assim por diante. Compreende-se, assim, que uma mesma informação pode apresentar variadas utilidades e aplicações, de acordo com a área na qual seu uso é feito.

Quanto às tipologias as informações podem, ainda, ser vistas como institucionais, aquelas que permitem aos dirigentes monitorar e avaliar o desempenho geral, bem como oferecem subsídios para a tomada de decisões de alto nível, que impactam sobre a instituição de forma mais ampla. Não significa que tais dados não tenham valor fora do ambiente institucional, porém, nesses locais se fazem essenciais para a manutenção de suas atividades e alcance de resultados (PERINI, 2011).

As informações que circulam nas empresas e na sociedade de forma geral podem ser classificadas como formais, aquelas oriundas de fontes conhecidas e seguras, sendo passíveis de verificação para confirmação de sua veracidade e

organização. Essa verificação tem como base jornais, revistas, artigos científicos, informações técnicas, documentos de uma empresa, etc. Dados formais tendem a ser citados como mais confiáveis e, assim, são os que mais despertam o interesse de diferentes parcelas do mercado e das instituições (PERINI, 2011).

As informais, por sua vez, são importantes, mas não existe uma fonte específica para sua verificação. Essas informações são prestadas por clientes, pacientes, obtidas em congressos, seminários, visitas, ou outros meios. As informações informais são muito comuns dentro e fora das empresas e não devem ser ignoradas, apenas é preciso apreciá-las de forma criteriosa e atenta, visando eliminar aquelas que demonstram não ser de uso seguro. Como esses dados não podem, em muitos casos, ser verificados, a aplicação de análise criteriosa se faz indispensável para evitar que tragam problemas aos seus usuários (PERINI, 2011).

Sêmola (2003) afirma que a informação, quando bem aproveitada, tende a trazer excelentes resultados para seus usuários. Aqui é preciso ampliar o olhar, pois em geral existe a visão de que empresas são as maiores beneficiadas pela informação. De fato, hospitais precisam delas todos os dias para verificar as condições de seus pacientes, dentistas fazem uso da informação para definir a melhor conduta de tratamento de cada caso, construtoras as utilizam como forma de realizar projetos seguros, confiáveis e rentáveis, e assim por diante.

Carocia (2009) enfatiza que no âmbito acadêmico a informação tem valor máximo, já que o ensino se baseia quase que exclusivamente em informações, exceto por atividades práticas que são realizadas em alguns cursos, porém, seu sucesso também depende de informações sobre cada experimento. Cada vez mais a educação vem fazendo uso e se beneficiando dessas informações, já que conhecimentos passam a ser disseminado se, assim, beneficiam um número crescente de usuários.

Não obstante, a informação, no âmbito acadêmico, vem sendo usada como ferramenta de conhecimento, desenvolvimento e informação. Isso decorre do fato de que no presente, muitos cursos de formação, atualização e especialização utilizam-se de ferramentas relacionadas às tecnologias da informação e, não são raros os casos em que as pessoas estudam, fazem provas e entregam trabalhos acadêmicos por meio dessas ferramentas (CAROCIA, 2009).

Com o advento dos computadores e da internet, existe a possibilidade de criar, salvar, compartilhar informações entre indivíduos e empresas e tal possibilidade tem

valor inestimável. Artigos científicos sobre variados temas estão disponíveis e podem melhorar o aprendizado e o conhecimento de diversos profissionais, é possível estudar à distância, os indivíduos podem se comunicar com pessoas de todas as partes do mundo ou realizar compras em empresas de países distantes, de forma segura e rápida (PERINI, 2011).

Todas essas atividades dependem da troca de informações e, assim, é preciso ver a informação como uma peça essencial na engrenagem que movimenta as sociedades e a economia de todo o mundo. É essencial recordar, porém, que nem todas as informações são direcionadas a todos os públicos e, assim, existem algumas que precisam ser protegidas, já que seu vazamento poderia trazer inconvenientes e mesmo riscos (como no caso de informações de Estado), nesse sentido, a segurança da informação trata-se de uma preocupação crescente em todo o mundo (SÊMOLA, 2003).

A informação já não pode ser vista como algo secundário e superficial, atualmente os dados disponíveis e bem utilizados por uma empresa, por exemplo, podem representar maior competitividade, destaque no mercado, conquista de clientes e manutenção de suas condições econômicas e financeiras e, assim, a informação deve ser vista como patrimônio e recurso essencial (SILVA; STEIN, 2007).

Gerir a segurança da informação refere-se ao modo como medidas diversas são adotadas e acompanhadas no sentido de garantir que dados confidenciais e sigilosos não sejam indevidamente divulgados ou acessados (RIGON; WESTPHALL, 2011).

Sobre o tema, Netto e Silveira (2007, p. 477) afirmam que:

> A fim de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança. Grande parte dos dados importantes ao negócio da empresa está armazenada em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema.

Com a evolução das tecnologias, um fluxo cada vez maior está disponível no mercado, já que as empresas necessitam dessas informações para suas atividades diversas. A informação não é útil para um tipo de empresa, apenas. De fato, qualquer instituição, tenha ela foco em produtos ou serviços, com ou sem fins lucrativos, precisa

de dados diversos para que suas atividades sejam conduzidas com eficiência (UNB, 2010).

Por outro lado, porém, passa a surgir um maior interesse sobre essas informações e, assim, os riscos tornam-se maiores. As ameaças tomam proporção muito maior, considerando-se que o vazamento desses dados poderia comprometer empresas e clientes, inclusive o âmbito econômico e financeiro de suas atividades. Com isso, a forma de proteger essas informações também vem sendo reavaliada e reestruturada para que a segurança desses dados seja relativamente maior (UNB, 2010).

2.3 SEGURAÇA DA INFORMAÇÃO

O ambiente tecnológico que envolve computadores, internet e dados diversos, vem se alterando e novas possibilidades de uso surgem todos os dias. Cada uma delas apresenta relevância para seus usuários, porém, também traz consigo alguma carga de riscos envolvendo possibilidades de invasão e acesso indevido de dados salvos (KAUFMAN, 2009).

> 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 (OLIVEIRA; MOURA; ARAÚJO, 2012, p. 3).

Do mesmo modo como as organizações são geridas para a obtenção dos melhores resultados, a segurança da informação também pode e deve ser gerenciada e administrada visando assegurar que as empresas e pessoas não terão seus dados expostos. Esses dados precisam ser vistos como confidenciais, integrais e disponíveis para o uso a que se destinam, porém, ser riscos de exposição inadequada (OLIVEIRA; MOURO; ARAÚJO, 2012).

Ocorre, porém, que a capacidade de muitas empresas de proteger seus dados ainda é limitada, seja por falta de conhecimentos, seja por falta de investimentos na área, muitas empresas ainda colocam em risco não apenas as próprias informações, mas dados de seus clientes, fazendo com que ao invés de serem protegidos estejam em constante risco de utilização inadequada e ilícita de seus dados (UNB, 2010).

> A segurança da informação trata da proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados à informação, preservando a confidencialidade, integridade / autenticidade e disponibilidade de informações. O objetivo é mitigar riscos e proteger a informação das ameaças que têm impacto negativo sobre a continuidade do negócio e, em última instância maximizar o retorno sobre investimentos e oportunidades de negócios (SOUZA et al, 2016, p. 241).

Dados confidenciais são aqueles que só devem ser utilizados por usuários autorizados e, caso isso não ocorra, colocam em risco a segurança dos indivíduos a quem se referem. Números de documentos, de contas bancárias, cartões de crédito, endereço, telefones, entre outros, são dados que devem ser mantidos em sigilo, já que seu vazamento poderá causar problemas diversos e, com isso, colocar em risco as finanças e a vida, de forma geral, dos indivíduos.

> [...] 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 (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 3).

No que tange a integridade, esta refere-se a forma como as informações são tratadas por uma empresa:

> [...] 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 (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 3).

Por fim, abordando-se a disponibilidade, esta se refere ao fato de que as informações possam ser utilizadas quando e onde se fizerem necessárias, desde que por usuários autorizados.

> 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 (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 3).

Existem pilares essenciais para que a segurança da informação deixe de ser apenas uma abordagem teórica e torne-se uma realidade dentro das instituições que fazem uso de dados dos clientes. Sobre os pilares que constroem a segurança da informação, Paula e Cordeiro (2015, p. 59) afirmam que:

> Confidencialidade: é responsável por garantir que o acesso às informações das organizações só se darão pelas pessoas permitidas. É também,

> assegurar o valor da organização. Quando outras pessoas cujo não tem permissão de acessar as informações da organização tem acesso a elas, ocorre a quebra de confidencialidade.
> Integridade: é a garantia de que as informações das organizações estarão corretas, verídicas, não podendo ser alteradas ou excluídas. A informação que for corrompida, falsificada, roubada ou destruída acarretará na quebra de integridade.
> Disponibilidade: a disponibilidade de informações das organizações deve ser realizada somente às pessoas autorizadas, e devem estar disponíveis sempre que os usuários precisarem. Se um usuário necessita de uma informação da organização e ela não está disponível para o uso, ocorrerá à quebra de disponibilidade.

Compreende-se, assim, que toda a comunicação entre as partes, bem como os dados transmitidos entre elas são confidenciais, só dizem respeito aos envolvidos. Esses dados devem ser mantidos com integridade, sem desvios, corretos e confiáveis e, por fim, só podem estar disponíveis para os usuários que, de fato, têm autorização para acessá-los (PAULA; CORDEIRO, 2015).

2.4 GESTÃO DA SEGURANÇA INFORMAÇÃO

Em face do papel da informação para as empresas e da necessidade de resguardar essas informações de qualquer forma de uso indevido, surge a gestão da segurança da informação, como forma de organizar e direcionar os esforços da empresa no sentido de evitar invasões, vazamentos e outras ocorrências que poderiam ser extremamente prejudiciais.

Para Rocha (2008, p. 25), é preciso ampliar um pouco esses conceitos, ultrapassando apenas a confidencialidade, integridade e disponibilidade, outros fatores também se fazem essenciais, tais como:

> 1. Disponibilidade: a informação deve estar acessível para o funcionamento da organização.
> 2. Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
> 3. Confidencialidade: a informação deve ser acessada exclusivamente por aqueles que estão autorizados e necessitam dela.
> 4. Legalidade: a informação deve estar dentro das normas que regulam a sociedade e a organização.
> 5. Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito.
> 6. Não repúdio de autoria: o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua autoria.

Diante disso, verifica-se que a gestão da segurança da informação não é apenas uma atividade, mas um processo permeado de cuidados, ações e medidas

que envolvem cautela, atenção e uma busca para que os dados dos quais uma empresa disponibiliza não sejam utilizados de modo inadequado, colocando em risco os verdadeiros donos dessas informações (UNB, 2010).

Gerir é administrar, de modo que a gestão da segurança da informação refere-se ao modo como são administradas as ferramentas desenvolvidas e aplicadas no sentido de proteger e assegurar as informações constantes de determinado sistema. Essa gestão é um processo amplo, composto de inúmeras etapas e indispensável no contexto atual, dentro do qual a informações dá poder aos seus detentores (SÊMOLA, 2003).

Para Rocha (2008), gerir a segurança da informação de uma empresa significa proteger todos os dados dos quais ela dispõe, não apenas os dados de seus clientes, fornecedores e parceiros, mas dados internos, relativos ao seu funcionamento, atividades e setores, evitando que seu vazamento se transforme em uma vantagem competitiva para outras empresas no mercado.

> [...] 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 (OLIVEIRA; MOURO; ARAÚJO, 2012, p. 4).

É preciso que se desenvolva no Brasil uma cultura que integre a gestão da segurança da informação nas atividades de todas as empresas e órgãos públicos, considerando-se que apenas da preocupação com o tema ser real, medidas abrangentes e cautelosamente criadas ainda são bastante incomuns. A cultura empresarial no país ainda assume a informação como sendo apenas uma série de dados disponíveis, não como um patrimônio a ser protegido (ROCHA, 2008).

Enquanto não houver a compreensão de que a informação é patrimônio e, como tal, deve ser protegida, preconizada e resguardada da invasão de usuários não autorizados, já que esta pertence ao consumidor, que ofereceu esses dados e à empresa que recebeu os mesmos. Não deve haver intermediários, outras pessoas ou

empresas que alcancem essas informações e delas façam uso de acordo com suas demandas particulares (OLIVEIRA; MOURO; ARAÚJO, 2012).

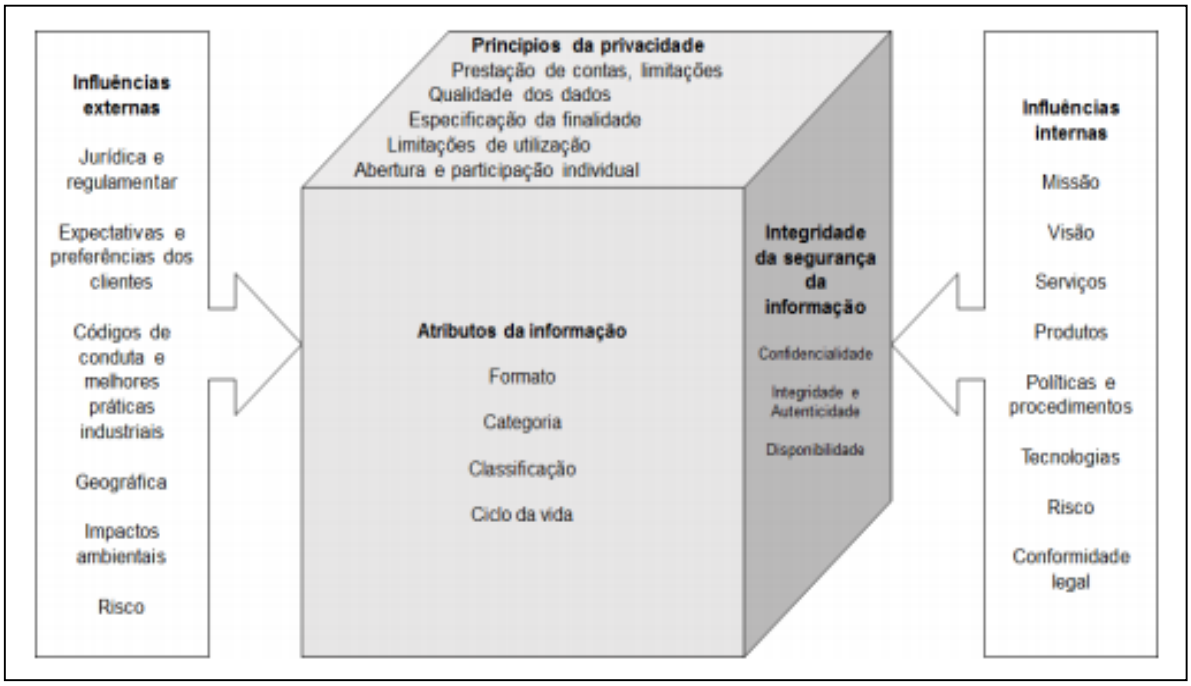

Figura 1: Atributos da informação pela perspectiva da privacidade e segurança
Fonte: Souza et al (2016, p. 244).

As empresas precisam considerar a segurança física, ou seja, referente ao local onde estão instalados os softwares nos quais as informações são armazenadas, a segurança lógica, composta pelo modo de utilização desses recursos para o trabalho, a segurança humana, que se refere às pessoas capazes de acessar esses dados e que, assim, também poderão colocá-los em risco para que definam criteriosamente suas normas de segurança e as formas de acompanhar e conferir se essas normas vêm sendo seguidas, respeitadas e melhoradas sempre que necessário (NETTO; SILVEIRA, 2007).

Para uma melhor compreensão, apresenta-se o quadro 1, que segue:

Quadro 1: Tipos de segurança da informação

Segurança física	Especificamente voltada aos locais nos quais se encontram as informações. Refere-se à necessidade de proteger equipamentos e programas dentro de um local adequado a eles.

Segurança lógica	Baseia-se na forma de utilização dos recursos nas diversas atividades cotidianas da instituição que se encontra de posse deles.
Segurança humana	Todos esses recursos são utilizados por pessoas, de modo que elas devem entender seu papel na manutenção das informações dentro de parâmetros de segurança e confiabilidade.

Fonte: Adaptado de Netto e Silveira (2017).

Bertolini Júnior et al (2010) destacam que ainda que as pessoas sejam as responsáveis pelo uso dos dados e pela aplicação dos protocolos de segurança definidos por uma instituição, elas são as responsáveis pelo vazamento de informações, seja de forma intencional ou acidental e, assim, prepará-las para que compreendam a importância da segurança das informações e apliquem as medidas necessárias deve ser um dos primeiros passos em uma empresa que deseja manter seus dados em sigilo.

Quando existe a preocupação com apenas um tipo de segurança, abre-se espaço para que ocorram vazamentos decorrentes de outros fatores, ou seja, ainda que o local de armazenamento dos dados seja cuidadosamente protegido, quando as pessoas não são preparadas para utilizar os dados e mantê-los em sigilo, a proteção existente perde sua efetividade (NETTO; SILVEIRA, 2007).

Um sistema de gestão de segurança da informação deve abordar as seguintes etapas:

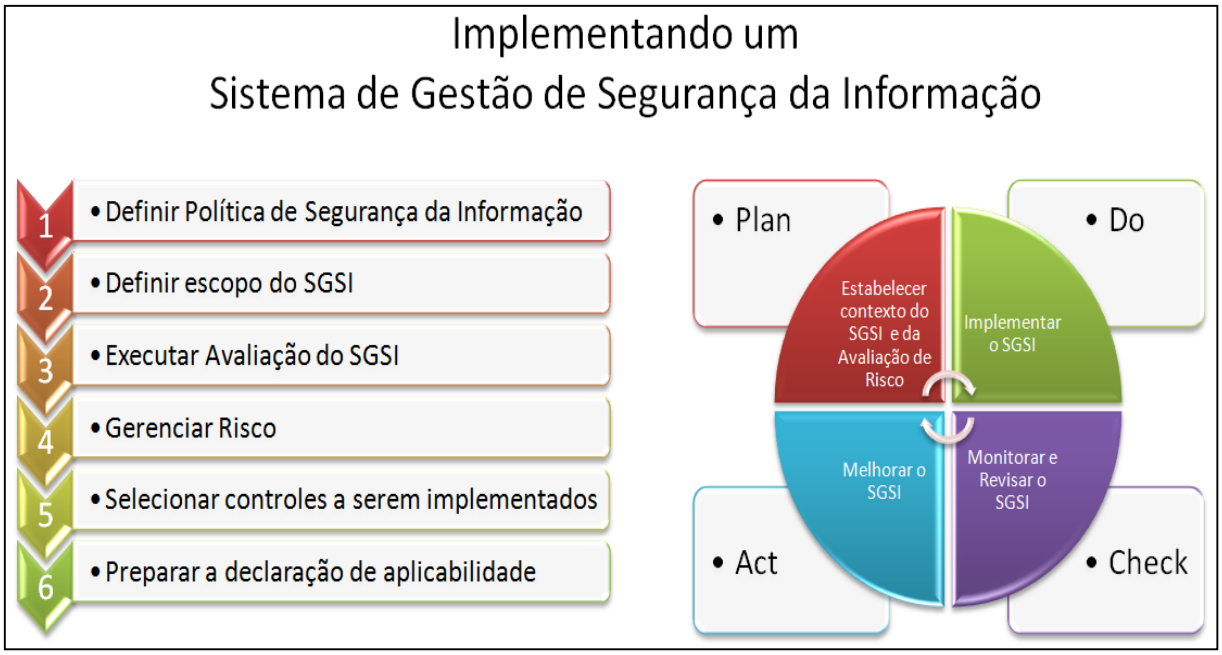

Figura 2: Sistema de gestão de segurança da informação
Fonte: Adães (2010).

PDCA é uma sigla que se refere a um ciclo utilizado como uma ferramenta gerencial para a tomada de decisões. As decisões tomadas por meio do PDCA estão voltadas a garantia do alcance das metas necessárias à sobrevivência da organização (VIEIRA FILHO, 2003).

Cada letra da sigla corresponde, segundo Vieira Filho (2003) à uma palavra em inglês, sendo P referente à palavra Plan – planejar, D referente à palavra Do – Fazer, C referente à palavra Check – conferir e A referente à palavra Act – agir. O PDCA apresenta elevado potencial no sentido de melhorar a qualidade das ações de segurança e reduzir os riscos envolvidos.

Quanto ao ciclo de PDCA, Paz et al (2017, p. 2) ressaltam que se trata de:

> [...] um método criado por Walter Andrew Shewart, mas amplamente divulgado por William Edwars Deming, principalmente nos anos 1950, quando o Japão se utilizou do método para melhorar o controle de qualidade, sendo ele a base para o sistema Toyota de produção.

Compreende-se, assim, que o ciclo envolve as atividades de planejar (PLAN – P), fazer (DO – D) conferir (CHECK – C) e agir (ACT – A). Cada etapa é muito importante para o alcance do resultado final nas mais diversas áreas em que a metodologia é aplicada (PAZ et al, 2017).

D'Avila (2015) afirma que o ciclo de PDCA, além de aumentar a organização das atividades, auxilia grandemente os gestores na tomada de decisões, pois a a partir

dessa análise conseguem visualizar com clareza os pontos fortes e fracos de uma atividade e, assim, podem decidir com segurança como atuar frente a cada um deles.

Na sequência apresentam-se ferramentas de gestão de segurança da informação.

2.1 FERRAMENTAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Uma ferramenta de gestão de segurança é o *firewall*, um conjunto de componentes alocados em uma extremidade da rede de uma empresa ou instituição. Por ele passam os dados da organização para o exterior dela e sua finalidade é oferecer segurança, controle, autenticação e registros de tráfego (ARAÚJO, 2014).

Petry (2013, p. 18) afirma que “um firewall possui três objetivos principais, que são: ser imune a penetração, controlar todo o tráfego de entrada e de saída e ser o único caminho de entrada/saída dos dados de uma rede”.

Cada componente do *firewall* apresenta funcionalidade específica, com papel diretamente incidente sobre o nível de segurança do sistema como um todo. Como funcionalidades do *firewall* destaca-se os filtros, Proxy, bastion hosts, zonas desmilitarizadas (DMZ), network adress translation (NAT), rede privada virtual (VPN), autenticação e certificação (ARAÚJO, 2014).

Os filtros procedem do roteamento seletivo de pacotes, aceitando ou descartando pacotes após uma análise das informações constantes de seus cabeçalhos. As regras de filtragem são definidas pela organização (ARAÚJO, 2014).

> Atua na verificação dos endereços IP e nas portas TCP/UDP, trabalhando com uma lista de controle de acesso, a qual é verificada antes que o pacote seja encaminhado para a rede interna. Possui vantagens como rapidez, eficiência, transparência e facilidade de compreensão, mas possui desvantagens como a aplicação de muitos testes para verificar suas funcionalidades, sintaxe difícil devido a complexidade das listas de acesso e por dificultar a aplicação das políticas e a análise é feita em um pacote por vez (PETRY, 2013, p. 20).

Os proxies são servidores capazes de agir como sistema intermediário entre a Internet e a rede interna das empresas, intermediando as solicitações de usuários e o ambiente externo.

> À medida que o servidor Proxy faz estes encaminhamentos ele também pode iniciar o processo de cache das páginas web em disco local. Com isso, da próxima vez que um usuário fizer a requisição para a mesma página web, o servidor Proxy não precisa mais ir a Internet para obter a página, pois ela já

> está armazenada localmente, proporcionando economia de banda de Internet e maior agilidade para as pesquisas dos usuários (ARAÚJO, 2014, p. 50).

Sobre os proxies, Petry (2013) esclarecem que são servidores que atuam na intermediação da comunicação entre os equipamentos que compõem a rede interna e a rede externa. As vantagens são o balanceamento de carga, recursos de cachê e isolamento todas entre as redes, porém, como desvantagens pode-se citar a lentidão, inflexibilidade e alta configuração.

> Os principais tipos de Proxy são os proxies de aplicação (WWW, FTP, TELNET, MAIL, SQL, etc); proxies de circuito que estejam em rede (endereços IP e protocolos TCP/UDP); Proxy reverso (trabalham de forma reversa, permitindo acesso a recursos internos) e proxy de cachê (armazena os sites mais usados para reúso) (ARAÚJO, 2013, p. 21).

Os bastions hosts, por sua vez, caracterizam-se como servidores nos quais se instalam serviços oferecidos aos usuários externos da organização. Em função de seu contato com ambiente externos, eles precisam ser protegidos ao máximo para que execute apenas serviços e aplicações para as quais são destinados.

> Assim, os bastions hosts podem ser chamados também de servidores fortificados, com a minimização dos possíveis pontos de ataque. Uma grande interação ocorre entre os bastions hosts e a zona desmilitarizada (DMZ), pois os serviços que serão oferecidos pela DMZ devem ser inequivocamente instalados em bastion hosts (ARAÚJO, 2014, p. 50).

No que tange as zonas desmilitarizadas, estas podem ser compreendidas como redes localizadas entre o ambiente interno e externo, na qual são instalados hardwares e softwares com o papel de realizar a interface entre serviços que os usuários externos utilizam e os serviços internos da empresa. Tal segmentação permite que quando um equipamento da rede desmilitarizada (bastion host) for comprometido, a rede interna continuará segura (ARAÚJO, 2014).

O NETWORK ADDRESS TRANSLATION não foi desenvolvido como um componente de segurança, seu intuito inicial era de tratar problemas em grandes redes com escassez de endereços de IP.

> Dessa forma, a rede interna pode utilizar endereços IP privados, sendo o NAT o responsável pela conversão desses endereços inválidos e reservados para endereços válidos e roteáveis quando a rede externa é acessada. Sob o ponto de vista de segurança, o NAT pode esconder os endereços dos equipamentos da rede interna e, consequentemente, sua topologia de rede, dificultando os eventuais ataques externos (ARAÚJO, 2014, p. 50).

A rede privada virtual (VPN) permite que informações trafeguem de forma segura pela internet. Araújo (2014, p. 50) afirma que:

> Os conceitos fundamentais da VPN são a criptografia e o tunelamento. A criptografia é utilizada para garantir a autenticidade, o sigilo e a integridade das conexões e é a base da segurança dos túneis, que permitem que os dados organizacionais trafeguem por uma rede pública através de um túnel criptografado.

A autenticação é um processo por meio do qual se garante que algo é autêntico, ou seja, existe uma verificação do que se apresenta para, então, definir sua autenticidade ou a falta dela. A validação da identidade é baseada em endereços de IP, senhas, certificados digitais, tokens, smartcards ou mesmo biometria. Trata-se de uma ferramenta que aumenta consideravelmente a segurança dos usuários e é bastante aplicada (ARAÚJO, 2014).

> Na autenticação, o usuário deve apresentar algo que só ele saiba ou possua, podendo até envolver a verificação de características físicas pessoais. A maioria dos sistemas atuais solicita uma senha (algo que, supostamente, só o usuário conhece), mas já existem sistemas mais modernos utilizando cartões inteligentes (algo que o usuário possui) ou ainda características físicas (algo intrínseco ao usuário), como o formato da mão, da retina ou do rosto, impressão digital e reconhecimento de voz (BRASIL, 2012, p. 20).

O balanceamento de cargas e alta disponibilidade de um *firewall* trata-se de um mecanismo que busca a divisão do tráfego entre dois *firewalls* que atuam paralelamente. “Os firewalls com cargas balanceadas devem operar exatamente com as mesmas regras de segurança” (ARAÚJO, 2014, p. 50).

Cada ferramenta citada apresenta especificidades e auxilia no alcance dos objetivos mais amplos, porém, deve-se ressaltar que se tornam mais eficientes quanto utilizadas de forma conjunta, ou seja, mais de um esforço deve ser realizado prezando a segurança das informações que se encontram de posse de uma instituição, empresa ou governo (PETRY, 2013; ARAÚJO, 2014).

Essas ferramentas são muito importantes para a política de segurança de informações de uma empresa, um agrupamento de princípios que norteiam a gestão de segurança das informações de uma empresa, devendo ser observado pelos usuários internos e externos. A política de segurança define as diretrizes a serem seguidas pela instituição visando assegurar os recursos computacionais e informações ali disponíveis (BRASIL, 2012).

3 DESAFIOS PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO

3.1 DESAFIOS ATUAIS: CRIMES VIRTUAIS

Um desafio a ser considerado no que tange a segurança da informação refere-se ao combate aos crimes realizados por meio das ferramentas tecnológicas, qualquer que seja sua especificidade e características.

A internet é uma ferramenta de informação e comunicação que permite a troca de informações em geral, por meio da qual as pessoas podem exercer abertamente sua liberdade de expressão, e que, em face disso, permite que os indivíduos venham a cometer atividades delituosas, de controle extremamente difícil (UNB, 2010).

Além disso, como é uma ferramenta relativamente recente, já que faz poucos anos que a internet se tornou amplamente disponível e que em algumas regiões ainda não existe acesso irrestrito a ela, as leis ainda vêm sendo desenvolvidas e alteradas para que possam abranger essas ocorrências, inexistentes até poucos anos no passado (JORGE, 2011).

> Observando-se pelo prisma jurídico, a Internet pode ser entendida como uma rede transnacional de computadores interligados, com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar dato jurídico, gerando consequências inúmeras nas mais variadas localidades (ROSA, 2005, p. 35-36).

No que tange o início dos crimes virtuais, cometidos a partir do uso das tecnologias de informação e comunicação, pode-se ressaltar que são percebidos desde a década de 50, por meio do desenvolvimento de vírus que se espalharam e comprometeram dados de forma acentuada em todo o mundo.

> Os primeiros casos de uso do computador para a prática de delitos datam da década de 50. Os crimes virtuais, ou cibercrimes, que são quaisquer atos ilegais onde o conhecimento especial de tecnologia de informática é essencial para as suas execuções, consistiam basicamente, nessa época, em programas que se auto-reaplicavam, ou seja, defeituosos. Não houve, num primeiro momento, a intenção de se criar um vírus. Na verdade, o que ocorreu foi uma falha na compilação de determinado código fonte (instrução de comandos que faz um programa funcionar de determinada forma) gerando algum tipo de transtorno, o que se assemelha ao resultado danoso que o vírus que conhecemos hoje proporciona (LIMA, 2014, p. 1).

Apesar de serem crimes graves, os crimes de internet ainda não são conceituados de forma ampla, abrangendo todas as ocorrências que envolvem, inclusive considerando-se o fato de que a cada novo dia surgem novos crimes,

indivíduos desenvolvem novas e ilícitas formas de tirar proveito dessas ferramentas e, assim, sabe-se que a legislação que rege o tema deverá ser atualizada com frequência (ROSA, 2005).

> Dentro desse sub-tema, é imperioso consignar que ainda não se definiu um conceito uniforme de Delito Informático. Aliás, nem mesmo uma singela denominação se estabeleceu, pois há quem o trate por 'Criminalidade Mediante Computadores' Criminalidade do Computador, Delito Informático, Criminalidade da Informática, Delitos Cibernéticos, entre outros (ESPM, 2002, p. 137-138).

Existem características específicas que envolvem o ambiente virtual, considerando-se que não existe um ambiente físico, tangível. Nesse sentido, é preciso definir com maior clareza o que os crimes de informática representam.

> Ouso denominá-los 'delitos informáticos', pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível 'conexão' à Rede Mundial de Computadores.
> Aliás, no âmbito da internet, a denominação seria 'delito cibernético ou telemático'. 'Delitos informáticos', então, seriam gênero, do qual 'delito cibernético' seria espécie. E em razão da recenticidade do assunto, outras denominações podem surgir com o amadurecimento da questão (ESPM, 2002, p. 137-138).

Em 1985 Tiedemann (*apud* ESPM, 2002, p. 138) procedeu de uma análise a respeito dos chamados crimes eletrônicos e conceituou essas condutas extremamente ilícitas e prejudiciais como:

> Criminalidad Mediante Computadoras: se alude a todos los actos, antijuridicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados com el empleo de un equipo automático de procesamiento de datos.

Verifica-se, analisando o supracitado, que há mais de 30 anos já havia uma visão de atos que poderiam prejudicar uma pessoa ou um grupo delas por meio das tecnologias, de forma intencional, com ou sem obtenção de lucros financeiros, mas sempre afetando negativamente a parte atingida por esses atos.

Jorge (2011) afirma que muitas pessoas ainda entendem a violência como a agressão física cometida contra outras pessoas, porém, é preciso recordar que a violência pode ser produzida de formas diferentes, como por exemplo, a agressão moral, assédio, chantagem e ameaças, praticadas por instrumentos eletrônicos (ou cibernéticos), uso e divulgação de dados não autorizados, etc.

> As tecnologias da informação e comunicação (TIC) estão a mudar as sociedades, em todo o mundo: melhoram a produtividade dos sectores industriais tradicionais; revolucionam os métodos de trabalho e remodelam os movimentos de capitais, acelerando-os. Apesar disso, este rápido crescimento propiciou, também, o aparecimento de novas formas de crime informático (UNISVIENA, 2005, p. 1).

Assim como a informática e suas diversas ferramentas trouxeram inovações e melhorias ao cotidiano dos indivíduos, também trouxeram perigos que precisam ser considerados reais e para os quais a lei precisa ser direcionada, para que esses criminosos não sejam deixados impunes.

> [...] o surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Würzburg, à década de 1960, época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas. Somente na década seguinte é que se iniciariam os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial (NETO; GUIMARÃES, 2003, p. 68).

Os delitos eletrônicos são inúmeros, porém, de forma geral, podem ser divididos e classificados em três categorias distintas. Essas categorias são: a utilização de métodos eletrônicos para obter um resultado ilícito, utilização da tecnologia eletrônica como meio para condutas criminais ou a utilização da tecnologia eletrônica como fim, sendo a máquina eletrônica ou seu material o objetivo a ser alcançado (NETO; GUIMARÃES, 2003).

> Alguns crimes informáticos são dirigidos diretamente contra as TIC, tal como servidores e websites; os vírus informáticos de difusão mundial causam prejuízos consideráveis às redes das empresas e de particulares.
> Vandalismo eletrônico e falsificação profissional ou contra facção.
> Roubo ou fraude, por meio de ataques a bancos ou sistemas financeiros, e fraudes que implicam transferências eletrônicas de capitais.
> Os computadores são usados para facilitar uma ampla série de práticas de telemarketing e de investimentos fraudulentos que envolvem práticas enganosas.
> O phishing ou o envio em massa de mensagens eletrônicas não solicitadas que contêm ligações com sites na Internet falsificados, para parecerem autênticos aos consumidores.
> Milhões destas mensagens provêm supostamente de bancos, de sites de vendas por leilão ou de outros sites legítimos e têm como objetivo induzir o utilizador a responder, fornecendo dados financeiros ou pessoais ou ainda a indicar as suas palavras-passe.
> A difusão de material ilegal e nocivo. Durante os últimos anos, a Internet tem sido usada para fins comerciais pela ‘indústria de diversões para adultos’. Contudo, a Internet é hoje, cada vez mais, utilizada para a distribuição de material considerado obsceno à luz da lei, em vários países. Outra área que suscita preocupação é a pornografia infantil. Desde finais dos anos 80, a sua

> distribuição tem aumentado substancialmente através de redes informáticas, utilizando uma vasta gama de serviços disponibilizados pela Internet, nomeadamente websites. Uma parte da distribuição de pornografia infantil está associada ao crime organizado transnacional.
> Para além de a Internet ser utilizada para a difusão de propaganda que incita ao ódio e de mensagens xenófobas, alguns dados sugerem que a Internet serve também para facilitar o financiamento de grupos terroristas e para difundir propaganda terrorista (UNISVIENA, 2005, p. 01).

Fica evidente, assim, que ainda que a internet esteja amplamente difundida e se trate de uma ferramenta aplicável ao trabalho, estudos, lazer e tantas outras possibilidades, existem indivíduos e empresas que fazem uso dela para outras finalidades, como o cometimento de crimes virtuais e, assim, o desenvolvimento de leis, bem como de políticas para reduzir e eliminar essas ocorrências se faz indispensável em todo o mundo.

3.2 DESAFIOS ATUAIS: CONFIABILIDADE NO MERCADO

Um dos maiores desafios da atualidade refere-se ao desenvolvimento de programas, ferramentas e programas dispositivos totalmente seguros, que possam ser utilizados para atividades de comunicação, compra, venda, entre outras, alcançando o público esperado, sem que esse amplo alcance deixe falhas aproveitáveis para acesso e uso indevido de informações (OLIVEIRA; MOURA; ARAÚJO, 2012).

Não obstante, outro desafio muito claro na sociedade comercial atual refere-se a conquistar a confiança dos clientes por meio de demonstrações de segurança e proteção de suas informações. Cada vez mais o comércio eletrônico é comum, porém, ainda existe muito receio para seu uso e, assim, as empresas que procedem dessa atividade como sendo seu foco precisam provar aos clientes que estão protegidos, que são confiáveis e que atuam continuamente para aumentar ainda mais a segurança oferecida a eles (OLIVEIRA; MOURA; ARAÚJO, 2012).

Diante do exposto compreende-se que a segurança da informação precisa se tornar cada vez maior, pois os indivíduos que desejam fazer uso ilícito delas estão se especializando cada vez mais, alcançando dados que as empresas consideram protegidos.

Compreende-se, assim, que inúmeros são os desafios que envolvem a gestão da segurança da informação e englobam não apenas a proteção das informações das

quais as empresas e instituições dispõem, mas também no sentido de proteger as pessoas que fazem uso dessas tecnologias para diferentes atividades. Impedir crimes diversos, desde uso indevido de informações até a disseminação de fatos caluniosos, todas são ações necessárias e que devem envolver políticas e práticas amplas (OLIVEIRA; MOURO; ARAÚJO, 2012).

Atualmente, mais do que produtos e serviços, existe dentro das empresas outro insumo considerado essencial, a informação. Todas as atividades de uma empresa são registradas em seus sistemas, permitindo que controles sejam desenvolvidos, planejamentos possam ser definidos, entre outras possibilidades (MARCIANO, 2006).

Não obstante, é preciso considerar que os indivíduos também se utilizam das tecnologias de informação e comunicação para suas atividades diversas, para compras, vendas, pagamentos, recebimentos, entretenimento, etc. Diante disso, seus dados pessoais são disponibilizados para consulta pelas empresas a que se destinam, porém, caso haja alguma falha de segurança, esses dados poderão ser apropriados de forma indevida (RIGON; WESTPHALL, 2011).

O acesso à internet e a possibilidade de conexão de diferentes dispositivos a essa tecnologia são fatores crescentes ao longo dos últimos anos. Com isso, atividades diversas podem ser desenvolvidas por meio desses recursos tecnológicos, de forma rápida e prática, dentro das empresas, escolas, residências e demais locais. Muitos foram os avanços relacionados à segurança dessas redes ao longo dos anos, porém, a especialização dos invasores também aumentou e, assim, muitos ainda conseguem passar pelos sistemas de segurança e acessar dados que deveriam ser preservados (TANENBAUM; WETHERALL, 2011).

Torres (2014) afirma que a segurança da informação deve ser uma das maiores preocupação das empresas, considerando-se que a perda de dados pode comprometer seus lucros, seus resultados, sua confiabilidade no mercado e, assim, reduzir ou eliminar suas chances de se firmar no mercado. Na realidade, qualquer que seja a área de atuação de uma empresa, zelar pela segurança deve ser uma de suas buscas primárias para que, posteriormente, seus bancos de dados sejam alimentados e mantidos.

Sobre o tema, Netto e Silveira (2007, p. 377) enfatizam que:

> [...] podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade,

> disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

Uma informação segura é aquela que pode ser utilizada pela instituição ou pessoa autorizada a fazê-lo, sem colocar em risco dados pessoais e sigilosos sobre os envolvidos, como clientes, alunos, parceiros, fornecedores, etc. Caso seja possível o acesso desses dados por outras partes, que não tenham autorização e direito legal a fazê-lo, compromete-se a segurança e o sistema torna-se pouco confiável, afetando diretamente a reputação daqueles que se encontram em posse desses dados (SILVA; STEIN, 2007).

Diante da importância das informações para as empresas, é essencial que elas tenham foco máximo em sua segurança, ou seja, assumam todas as medidas possíveis para que as informações que possuem não sejam perdidas, alteradas indevidamente, utilizadas fora da empresa, entre outras situações que prejudicam a empresa e podem atingir seus clientes (CAROCIA, 2009).

Neste sentido, Silva e Stein (2007, p. 48) afirmam que a segurança da informação (SI):

> [...] não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

A segurança da informação, por muitos, é vista como a proteção de dados oferecidos ou recebidos por alguém, porém, é preciso compreender que esta significa muito mais do que isso, pois engloba o desenvolvimento de medidas e práticas que façam com que esses dados sejam resguardados mesmo dentro da empresa, já que mesmo ali existem usuários não autorizados a utilizar essas informações e, caso tenham acesso a elas, poderão fazer um uso inadequado, fornecendo-as a quem não tenha direito a isso (OLIVEIRA; MOURO; ARAÚJO, 2012).

Marciano (2006) enfatiza que a segurança da informação não existe apenas para proteger os indivíduos aos quais se referem, seus donos por direito, mas as instituições e pessoas que fazem uso desses dados para suas atividades cotidianas, Quando este uso respeita os princípios legais e evita sua disseminação descuidada, então todas as partes são protegidas e beneficiadas por tais cuidados.

Diante disso, buscando-se compreender os objetivos da segurança da informação, ressalta-se que:

> A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas aos controles de acesso [...] (BRASIL, 2012, p. 9).

Hallberg (2003) destaca que a segurança de dados não se refere apenas às empresas, mas aos dispositivos e a forma de acesso à internet que eles utilizam. Como no presente existem veículos, televisores, telefones e outros objetos que podem se conectar com a internet, todos eles estão expostos a algum risco de roubo de informações, de modo que os cuidados precisam ser maiores e mais bem definidos para assegurar os resultados.

> 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 *apud* OLIVEIRA; MOURO; ARAÚJO, 2012, p. 4).

Uma informação segura é aquela que está disponível para seu usuário destino quando necessários, porém, com a certeza de que não será indevidamente divulgada ou acessada por pessoa ou empresa sem autorização para tal. Ao mesmo tempo em que as informações movimentam o mercado, essa movimentação precisa ocorrer de forma segura, considerando-se que seu uso indevido poderá ter consequências diversas, algumas simples, outras extremamente graves (SÊMOLA, 2003).

De acordo com Canongia e Mandarino Júnior (2009), a evolução da internet traz consigo a preocupação com a segurança dos dados por ela transmitidos. A internet permite que pessoas de todo o mundo tenham contato e possam fazer negócios em diferentes áreas, porém, como ali circulam dados importantes, sigilosos e muitas vezes que precisam ser mantidos em segurança, as empresas que participam desse mercado precisam buscar formas de deixar seus clientes seguros. Dados pessoais, bancários, de trabalho, entre tantos outros, são transmitidos pela internet e, assim, caso sejam acessados por invasores, todas as partes da negociação podem ser prejudicados.

Ressalta-se que quanto mais informações circulam nos mercados todos os dias, maior atratividade elas assumem e, assim, a preocupação com sua segurança

deve conduzir, necessariamente, ao desenvolvimento de ações, políticas e programas capazes de resguardá-las, mantê-las dentro dos limites impostos por seus usuários e proprietários ou responsáveis (SILVA; STEIN, 2007).

> O volume de informações eletrônicas utilizadas pelas empresas é cada vez maior, tornando complexo seu gerenciamento produtivo e adequação da qualidade de acesso, confiabilidade e conformidade com vistas a atender os objetivos organizacionais, assim como há a preocupação com sua exposição, cuja segurança pode ser comprometida por incidentes que representariam prejuízos financeiros ou para a imagem das organizações (SOUZA et al, 2016, p. 242).

O objetivo da segurança é evitar o acesso indevido às informações e recursos das empresas e pessoas, de modo que somente envolvidos autorizados possam ter acesso a elas. As ameaças que envolvem a segurança das informações podem ser divididas em três classes mais amplas, quais sejam: vazamento (aquisição de informações por destinatários não autorizados), falsificação (alteração não autorizada da informação) e vandalismo (interferência na operação correta de um sistema, sem ganho para o invasor) (LANG et al, 2007).

Sêmola (2003) esclarece que a palavra segurança está diretamente ligada ao conceito de proteção, Aquilo que está seguro pode ser visto como algo protegido, livre de riscos. Com a informação a realidade é a mesma, a segurança da informação permite sua proteção para que não sejam utilizadas de maneira inadequada.

No que tange as maiores dificuldades da segurança da informação, Rigon e Westphall (2011, p. 93-94) destacam que:

> O desafio está em definir objetivos de segurança da informação, alcançá-los, mantê-los e melhorar os controles que os suportam, para assegurar a competitividade, a lucratividade, o atendimento a requisitos legais e a manutenção da imagem da VII Simpósio Brasileiro de Sistemas de Informação organização junto à sociedade e ao mercado financeiro. Modelos de maturidade podem ajudar a enfrentar este desafio.

Manter a informação em segurança é protegê-la de acessos indevidos, uma medida considerada essencial no mercado e na vida pessoal. Existem diferentes formas de aumentar a segurança da informação, ferramentas desenvolvidas com essa preocupação específica, visando tranquilizar empresas e clientes sobre a confidencialidade de suas ações e de seus dados particulares. Esse cuidado enquadra-se dentro da gestão da segurança da informação (RIGON; WESTPHALL, 2011), a ser apresentada na sequência.

Cordeiro e Lima (2015, p. 59) destacam:

> A segurança da informação visa à proteção das ameaças para garantir a continuidade dos negócios, minimizando as perdas e maximizando o retorno de seus investimentos. Ameaças surgem quando os ativos estão vulneráveis, acarretando em um incidente indesejável. Essa área não deve ficar restrita aos aspectos tecnológicos, ela deve proteger a informação em qualquer meio que se encontre.

Percebe-se em todo mundo a ocorrência de alguma vulnerabilidade no que tange a segurança da informação, porém, existem esforços constantes para que essa realidade seja alterada e esses dados não sejam comprometidos, divulgados inadequadamente ou invadidos por indivíduos que se especializam nessa área (OLIVEIRA; MOURO; ARAÚJO, 2012).

No Brasil o cenário ainda demanda de muitas melhorias, já que diariamente são disponibilizados dados na internet que não deveriam ser divulgados, alguns jamais são utilizados de forma ilícita, enquanto outros causam problemas graves aos seus donos, inclusive permitindo o ajuizamento de ações judiciais contra a empresa que não defendeu esses dados adequadamente, ou contra os usuários que invadiram seus sistemas e obtiveram esses dados de forma ilícita (UNB, 2010; OLIVEIRA; MOURO; ARAÚJO, 2012).

> Embora, na prática, não se possa erradicar completamente o risco de uso impróprio ou mal-intencionado de qualquer informação, muitos esforços já foram feitos no sentido de aprimorar os sistemas de SI. Apesar disso, durante muito tempo, houve pouca ou nenhuma preocupação com as capacidades e limitações humanas dos usuários desses sistemas (SILVA; STEIN, 2007, p. 48).

Moraes, Guerini e Serra (2006) enfatizam que em todas as áreas do mercado a informação apresenta. Diante disso, é preciso verificar de que forma as empresas dessa área de atuação buscam proteger suas informações, inclusive visando manter vantagens competitivas diante de seus concorrentes (MORAES; GUERINI; SERRA, 2006).

> Na maior parte dos setores econômicos, os avanços da tecnologia de informação proporcionaram formas eficazes de gerenciar o fluxo de informações entre empresas. Diante desse cenário, o setor da construção civil, frequentemente conhecido como conservador com relação à adoção de novas tecnologias, vem passando por mudanças significativas (MORAES; GUERINI; SERRA, 2006, p. 1).

Governos, comércio, indústria e todas as demais áreas do desenvolvimento social e econômico de um país apresentam ligação com as informações que circulam no mercado todos os dias. Diante disso, compreende-se que a informação segura é

aquela que poderá ser acessada por quem tem autorização para fazê-lo sem que sejam utilizadas em outras situações que colocam em risco as pessoas (RIGON; WESTPHALL, 2011).

A segurança da informação tem sete pilares essenciais, que precisam ser conhecidos e compreendidos para melhorar a proteção das informações dentro de uma empresa ou instituição específica:

> **Infraestrutura robusta –** Para garantir um bom nível de segurança, é fundamental ter uma infraestrutura robusta. Portanto, deve-se investir em vários aspectos: arquitetura, design de um esquema de proteção, operações e práticas seguras, além de uma boa gestão de riscos.
> **Arquitetura –** Pense na análise do projeto de uma prisão ou de uma base militar. Sempre devemos levar em consideração qual é a finalidade de um edifício. Ele abrigará réus de alta periculosidade? Que informações e objetos ficarão dentro de uma área militar?
> **3. Design –** O sistema precisa ser projetado como um todo, já que ele é formado por um conjunto de componentes que devem ser protegidos individualmente. Uma infraestrutura segura leva em conta um design geral da solução sem deixar de prestar atenção à proteção dos dados. Dessa forma, há uma segurança específica para cada um dos elementos: servidores, computadores, a rede, os componentes de comunicação etc.
> **4. Operações seguras –** Ao configurar um serviço ou registrar um usuário, essas ações estão relacionadas a uma interação com um sistema e também devem ser feitas com segurança. Uma pessoa pode até ter um automóvel extremamente seguro e equipado com os melhores acessórios de segurança, mas acabará sofrendo um acidente se dirigir bêbado ou ultrapassar o limite de velocidade da via.
> **5. Boas práticas –** É preciso considerar as “boas práticas” que estabelecem qual é a melhor forma de atuar na maioria dos casos e das vezes. Precisamos saber como são essas boas práticas e adotá-las para ter uma referência de aprimoramento. Sem ter um objetivo, é impossível melhorar. E isso também é aplicável à segurança.
> **6. Gestão de riscos –** Todas as empresas são diferentes. Cada setor tem suas próprias ameaças e exposições a riscos específicos. Por isso, é importante contar com uma referência. Quais seriam as circunstâncias de uma PME? Depende da área de atuação e da importância das informações com as quais essa empresa trabalha. Traçar um panorama de riscos gera certeza na hora de avaliar até que ponto deve-se otimizar o sistema e o que é preciso priorizar.
> **7. Computação na nuvem –** A nuvem possibilita a realização de operações seguras por causa de sua arquitetura e de seu design de soluções. A arquitetura da nuvem assemelha-se a uma fortaleza. Ela já fica armada, e as operações e configurações são feitas pelo provedor, motivo pelo qual há menos exposição aos riscos (COMPUTERWORLD, 2016).

Ainda que todas as informações disponibilizadas para uma empresa devam ser protegidas, o fato é que aquelas que se constituem em mais importantes devem receber esforços ainda mais específicos e efetivos, considerando-se que seu vazamento acarretará danos para a própria instituição. Não existe segurança parcial para as informações, essa preocupação deve ser ampla, porém, é possível e

necessário direcionar os esforços de formas mais específicas (NETTO; SILVEIRA, 2007).

Em qualquer área do mercado a segurança da informação é indispensável, considerando-se que todas as empresas se utilizam de dados diversos para conduzir suas atividades de compra, venda, serviços, pagamentos, folha de pagamento, cadastro de clientes, etc. (STEHLING, 2012). Para isso, diferentes estratégias estão disponíveis e devem ser conhecidas, compreendidas e devidamente aplicadas. Proteger a informação é proteger as pessoas ou empresas às quais ela se refere e, assim, é direito dos mesmos e dever dos usuários que têm acesso a ela (SILVA; STEIN, 2007).

Após a análise de todos os dados expostos, é possível compreender que a segurança da informação trata-se de uma área de estudos a respeito das tecnologias, com objetivo de desenvolver meios para que sejam compartilhadas entre as partes envolvidas em uma determinada comunicação (compra, venda, etc.), reduzindo os riscos de uso indevido desses dados. Todavia, o grande desafio da atualidade é encontrar formas de impedir sua divulgação ou acesso indevido, protegendo as pessoas e as empresas de golpes que vêm se tornando cada vez mais comuns (OLIVEIRA; MOURA; ARAÚJO, 2012).

De fato, os desafios são muitos e variados, envolvendo a vida pessoal dos usuários das tecnologias, suas atividades comerciais e o contato com outras pessoas ou empresas dentro e fora do país. Não obstante, é preciso proteger as próprias redes para que crimes de ofensa, calúnia e desrespeito não se tornem cada vez mais comuns e fiquem sem as punições necessárias para alterar essas condutas (SILVA; STEIN, 2007; JORGE, 2011; OLIVEIRA; MOURA; ARAÚJO, 2012).

Para alcançar uma visão sumarizada, porém específica dos desafios que permeiam o mercado, apresenta-se a tabela 1, que segue.

Tabela 1: Desafios da gestão de segurança da informação

DESAFIOS ATUAIS	
Crimes virtuais	Crimes virtuais vêm se tornando comum em diferentes áreas, seja com imagens, ofensas, ou outros. O desafio é identificar esses indivíduos e aplicar a penas cabíveis.

Confiabilidade no mercado	Superar os concorrentes demonstrando a segurança dos clientes trata-se de um grande desafio para as empresas. Quanto maior a confiabilidade que apresentam, mais clientes conquistarão.
Proteção dos usuários	Cada vez mais é possível proceder de negócios através das ferramentas tecnológicas. Nesse sentido, além de proteger as empresas para evitar invasões, é preciso desenvolver dispositivos que protejam também os usuários, seus equipamentos e as redes que utilizam, para que não deixem de proceder desse tipo de negócios.

4 PERSPECTIVAS FUTURAS PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

4.1 O CENÁRIO ATUAL

Desde o surgimento dos dispositivos tecnológicos e da internet, existe uma busca por segurança de dados. Inicialmente essa segurança era apenas uma expectativa, algo que precisava ser desenvolvido, porém, com o passar dos anos ela torna-se uma realidade, já que diferentes ferramentas foram desenvolvidas para que os dados sejam mantidos com maior confiabilidade e segurança em diferentes áreas do mercado (TANENBAUM; WETHERALL, 2011).

No mercado atual a informação confere grandes possibilidades aos seus detentores, sejam elas no sentido de alcançar maiores vantagens competitivas, seja como forma de desenvolverem um banco de dados completo e capaz de oferecer embasamento para atividades e negócios futuros (TANENBAUM; WETHERALL, 2011; REZENDE, 2018).

Os computadores foram criados na década de 40, a internet começou a ser utilizada pelas forças armadas na década de 60 e a primeira chamada realizada de um telefone móvel foi em 1973. Quando de sua criação, essas tecnologias eram extremamente caras e não estavam ao alcance da população em geral. Atualmente elas se tornaram extremamente comuns, estando presentes na maioria das casas, empresas e instituições, permitindo sua comunicação mais ampla e a eliminação de limites e barreiras para sua atuação (RISCHPATER, 2001).

Logo do surgimento dessas tecnologias o acesso indevido a informações não era comum, até por não haver indivíduos com conhecimentos suficientes para agir dessa forma, porém, conforme os indivíduos passaram a conhecer e se especializar nessas ferramentas, surgiu a percepção de que poderia tirar proveito delas para alcançar benefícios em proveito próprio, mesmo que isso significasse invadir sistemas e utilizar ilicitamente as informações neles contidas(TANENBAUM; WETHERALL, 2011).

Para compreender melhor a evolução dessas tecnologias, apresenta-se a figura a seguir.

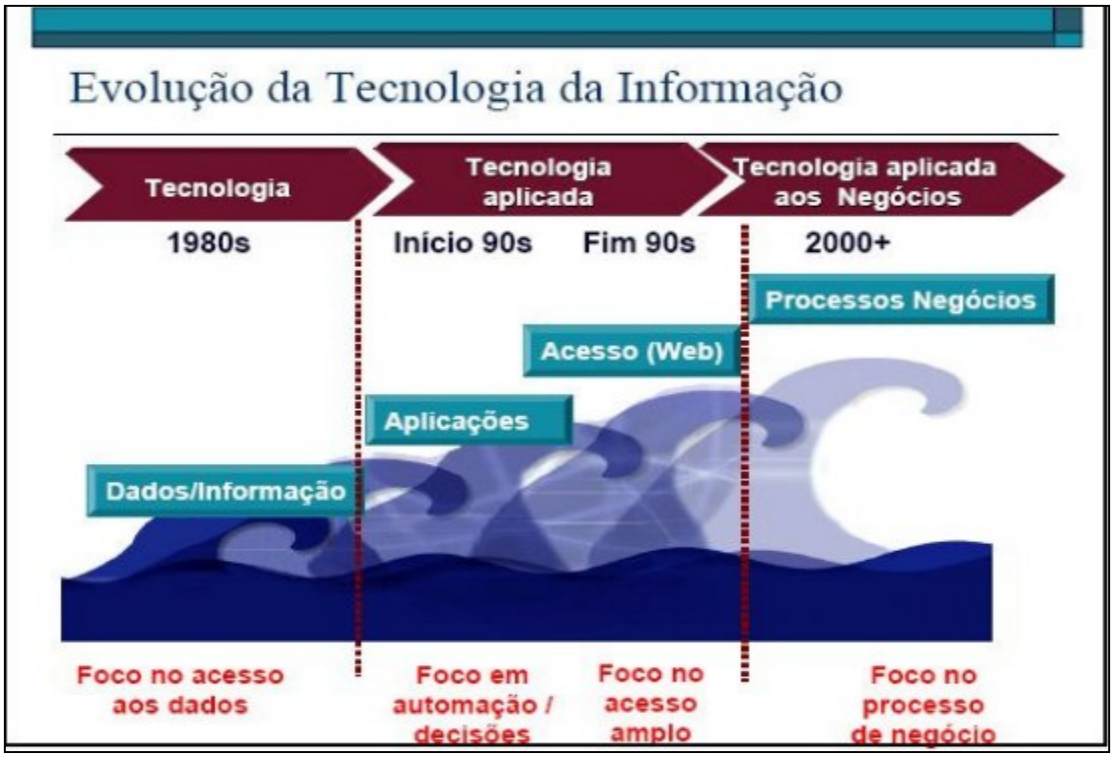

Figura 3: Evolução das tecnologias de comunicação
Fonte: Rezende (2018, p. 1).

A análise da figura 4 permite compreender que as tecnologias da informação evoluíram grandemente ao longo dos últimos anos, o que aumentou as demandas por maior segurança dessas informações dentro das instituições nas quais são aplicadas. Essa preocupação surgiu e tornou-se tão acentuada, justamente, pelo fato de que assim como as empresas se beneficiam com esses dados, usuários não autorizados buscam acessá-los para obter benefícios próprios e, muitas vezes, prejudiciais para os clientes e para as empresas nas quais ocorreram os vazamentos (TANENBAUM; WETHERALL, 2011; REZENDE, 2018).

Para Carocia (2009), desde que as empresa perceberam o quão importantes as informações são para seu desenvolvimento e para seu sucesso, elas buscam formas de proteger essas informações. Ao longo dos anos, com a evolução das tecnologias e dos sistemas de informação, a segurança também se tornou maior, porém, um longo caminho ainda deve ser percorrido para que as empresas possam sentir-se totalmente seguras no que tange suas informações.

Soares et al (1995) afirmam que as redes disponíveis são muitas e, conforme essas tecnologias vão se desenvolvendo, mais opções serão percebidas. A segurança dessas redes aumenta a cada ano, porém, não se pode dizer que isso evita riscos já

que, na realidade, os conhecimentos e possibilidades de uso dessas informações por invasores vêm crescendo e tende a aumentar a cada ano.

Laudon e Laudon (2004) destacam que nessa nova era do mercado, na qual as tecnologias estão presentes em todas as atividades do mercado, ou na expressiva maioria delas, é preciso gerir as empresas com foco nessas tecnologias e sua aplicabilidade, como forma de otimizar os negócios e melhorar os resultados alcançados.

Silva (2014) ressalta que a segurança da informação evoluiu a partir de demandas de diferentes setores do mercado, dentre os quais destaca-se o setor financeiro, em face da ocorrência de atividades ilícitas de acesso aos bancos de dados e uso de informações de clientes para finalidades criminosas, visando a obtenção de recursos a partir de dados de outros indivíduos.

Sabe-se que em todos os períodos da sociedade o homem deseja manter para si alguns dados e informações, porém, no passado havia uma facilidade maior, já que não eram registradas em sistemas que poderiam ser invadidos. Com o surgimento das tecnologias de informação e comunicação, surgem também especialistas em tomar posse de dados privados de muitos indivíduos e, assim, inicia-se o processo de desenvolvimento de ferramentas para aumentar a segurança dessas informações (SILVA, 2014).

Silva (2014, p. 33) afirma que:

> Durante a década de 1960, devido o crescente uso dos computadores surgiu a necessidade de obter privacidade e proteger a informação em formato digital. No entanto, até o início dos anos 1970 as técnicas de criptografia estavam apenas a serviço das agências de segurança, como a NSA (National Security Agency). O fato de que os mainframes eram acessíveis por múltiplos usuários e compartilhado por vários departamentos das organizações deu início as preocupações com o risco de vazamento de informações ou de ataques internos, causados, até mesmo, por um funcionário mal intencionado. Com isso os computadores eram alocados em salas isoladas ou até mesmo em prédios exclusivos, denominados CPDs (Centro de Processamento de dados), onde apenas pessoas autorizadas tinham acesso.

Quanto mais os computadores (em suas variadas configurações) se tornaram acessíveis à sociedade, maiores os riscos de uso indevido de informações e, assim, a preocupação com sua segurança tornou-se mais ampla.

> A década de 1980 representa o período onde as oportunidades de inovar no setor de segurança da informação começam a surgir de forma mais intensa. Devido a propagação dos microcomputadores e do desenvolvimento das redes, que aumentou consideravelmente o desafio de TI de proteger o processamento de dados (SILVA, 2014, p. 35).

Neste ponto destaca-se que Schneider (2012) leciona que quanto mais as tecnologias evoluem e os indivíduos se aperfeiçoam no uso dessas tecnologias, maiores se tornam as necessidades de desenvolvimento de segurança da informação, não apenas como uma política de proteção às empresas, mas acima de tudo como uma forma de proteger os clientes de ataques e uso inadequado de dados.

Ao abordas as perspectivas da segurança da informação para os próximos anos, é preciso ressaltar o cenário em uma perspectiva específica, ou seja, entre pessoas, empresas e governos, já que essas diferentes esferas apresentam necessidades, dificuldades e perspectivas das mais variadas.

4.2 SEGURANÇA DA INFORMAÇÃO PARA PESSOAS, EMPRESAS E GOVERNOS

A importância da segurança da informação é elevada tanto no setor privado (pessoas e empresas) quanto público (instituições e governos). Todos os dados transmitidos pela internet precisam ser preservados, evitando-se seu uso para fins inadequados e possíveis prejuízos para as partes envolvidas (NETO; SILVEIRA, 2007; PERINI, 2011).

No que tange a segurança da informação, ressalta-se:

> 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 (OLVEIRA; MOURA; ARAÚJO, 2012, p. 3-4).

Diante dessa realidade, procede-se de uma análise específica para cada um desses públicos e, assim, busca-se uma compreensão mais ampla e clara sobre o tema.

4.2.1 O valor da informação para as pessoas

Praticamente todas as informações disponíveis na rede referem-se às pessoas, ainda que estejam contidas nos bancos de dados de empresas ou governos, referem-se, em sua maioria, a clientes, consumidores ou contribuintes (PERINI, 2011).

A relação dos clientes com as empresas deve ser de confiança e, assim, caso não ocorra a devida proteção das informações, os clientes podem ser prejudicados, perdendo a confiança nas empresas e, muitas vezes, iniciando processos judiciais em função dos prejuízos sofridos. Não obstante, recorde-se a essa empresa poderá ser prejudicada no mercado, passando a ter uma imagem de desorganizada ou pouco confiável (ESPÍRITO SANTO, 2018).

As pessoas, ao realizarem negócios com empresas por meio da internet, esperam não apenas receber seu produto no prazo, com qualidade e excelentes condições, mas confiam que informações como seu endereço, documentos e outros dados estejam seguros, evitando os riscos de fraudes diversas por parte de pessoas ou empresas mal intencionadas. Neste sentido, o cliente confia na empresa e essa confiança deve ser valorizada e preservada (ESPÍRITO SANTO, 2018).

Fonseca (2009) ressalta que a segurança da informação deve ser sempre priorizada pelas pessoas quando desejam realizar qualquer tipo de negócios pela internet. O vazamento de seus dados, mesmo que não sejam utilizados para fraudes, pode causar transtornos diversos, falsificação de suas informações, contatos de empresas com as quais o cliente não tem interesse em se relacionar, etc. Assim sendo, o próprio cliente precisa pesquisar sobre as empresas, verificando seu histórico para ocorrências de vazamento de informações.

De acordo com Oliveira, Mouro e Araújo (2012, p. 2), deve-se ter em mente que:

> 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.

Oliveira, Moura e Araújo (2012) são muito enfáticos a respeito da necessidade de proteger as informações para que as pessoas que fazem negócios com elas sejam protegidas e, assim, negócios ilícitos utilizando seus dados possam ser controlados e eliminados. Uma empresa não sobrevive sem seus clientes, de modo que é preciso proteger as pessoas para que continuem a adquirir seus produtos e serviços e, assim, todas as partes envolvidas são beneficiadas.

4.2.2 O valor da informação para as empresas

Gurgel (2006) esclarece que, no presente, a informação precisa ser vista como um patrimônio da empresa, um bem da qual ela dispõem e sobre o qual ela deve apoiar-se para definir muitas de suas práticas e políticas de mercado. Mesmo empresas que oferecem produtos ao mercado precisam ter a consciência que além dos bens tangíveis que elas oferecem elas lidam com bens intangíveis, as informações.

De acordo com Perini (2011, p. 3) “um administrador eficaz em qualquer área de negócios deve entender que a informação é um dos recursos organizacionais mais preciosos e importantes que uma organização possui”.

Neste sentido, compreendendo-se a informação como um recurso e patrimônio da empresa, é essencial destacar que esta apresenta valor no ambiente no qual é utilizada. Uma mesma informação apresenta diferentes valores dentro de situações variadas, sempre se considerando seu uso para definir qual é, de fato, sua importância nos contextos nas quais os dados estão inseridos (SILVA; STEIN, 2007).

Qualquer que seja o porte de uma instituição, ela demanda de informações diversas para que suas atividades sejam conduzidas. Neste sentido, ainda que existam diferenças entre o valore de dados diversos de acordo com cada empresa, aquelas informações que são foco de suas atividades apresentam valor acentuado e, justamente por isso, demandam de maior cuidado, apreciação e segurança (NETTO; SILVEIRA, 2007).

Empresas que reconhecem o valor da informação e sabem fazer com uso dela tendem a apresentar maior sucesso no mercado. Com o surgimento e desenvolvimento de diversas tecnologias de comunicação, as empresas possuem

uma maior facilidade de acesso às informações, além de haver uma gama muito maior de informações circulando no mercado (GURGEL, 2006).

Certamente que não se pode afirmar que esta era da informação apresenta apenas vantagens, na verdade existem riscos e desvantagens, porém, estão ligados com a segurança, no que tange o valor da informação para empresas e sociedade, existe uma inquestionável percepção de que esses dados não são apenas importantes, mas essenciais (GURGEL, 2006).

Carocia (2009) afirma que as tecnologias de informação tornaram os mercados mais amplos e, por consequência, mais competitivos e, diante desse cenário, as empresas que possuem informações claras e completas sobre o mercado, clientes, concorrências, economia e ambiente empresarial, conseguem se manter mais equilibradas, sabem o que precisam fazer para superar seus clientes e atender às demandas do mercado.

Para Kaufman (2009), os sistemas de informação são agrupamentos das informações das quais as empresas dispõem, de forma organizada, em um mesmo local, com possibilidade de acesso dessas informações sempre que necessário. Seria incorreto afirmar que apenas empresas de grande porte são beneficiadas pelas informações. Cada vez mais hospitais, por exemplo, utilizam-se dessas ferramentas para o registro de seus pacientes e, com base nele, se dá todo seu acompanhamento de saúde.

Nesse sentido, todas as áreas sociais são beneficiadas pelas tecnologias e por seu uso no sentido de armazenar e proteger informações diversas. O mais importante é que exista um reconhecimento sobre o valor dessas informações para cada instituição a seu modo, além de uma busca constante para que sua preservação e proteção seja uma realidade em qualquer setor de atuação de seus usuários (KAUFMAN, 2009).

Dentro de uma empresa as informações podem ser utilizadas em diferentes setores em sob diferentes formas. Elas podem ser utilizadas para definir políticas de vendas, de preços, de marketing, etc. O importante é que para cada finalidade existe uma gama específica de informações a ser utilizada. Dentro da gestão estratégica das empresas, as informações assumem valor elevado, considerando-se que a definição de estratégias não pode ser feita de modo intrínseco, deve ser apoiada sobre dados diversos (CAROCIA, 2009).

A estratégia de uma empresa refere-se a suas políticas e práticas com vistas ao futuro, dentro delas encontra-se sua visão, missão, valores, etc. Nesse sentido, como são condições que deverão ser conhecidas, compreendidas e alcançadas no futuro, definir as estratégias demanda de informações diversas para que o gestor saiba se será possível cumpri-las ou não (CAROCIA, 2009).

Além disso, é preciso destacar que uma tomada de decisões efetiva e vantajosa para uma empresa depende das informações das quais ela dispõem e da forma como se utiliza delas. Possuir as informações e não saber como utilizá-las de modo efetivo não traz qualquer vantagem para as empresas. “O valor das informações para as organizações está diretamente ligado a como elas auxiliam os tomadores de decisão a atingir seus objetivos organizacionais” (PERINI, 2011, p. 5).

Identifica-se, assim, que a informação serve como base para a tomada de uma série de decisões, muitas delas decisivas para o desenvolvimento e o futuro das empresas. Com isso, dispor de informações se torna indispensável, enquanto protegê-las passa a ser mais do que um diferencial, mas se trata de um dever de todas as empresas que armazenam esses dados (OLIVEIRA; MOURA; ARAÚJO, 2012).

Fonseca (2009) esclarece que dentro de cada empresa, nem todos os setores têm autorização para acesso e utilização das informações dos clientes e, assim, essa hierarquização se faz muito necessária, para que mesmo dentro do ambiente não ocorra uma utilização inadequada ou mesmo ilegal de dados que as empresas se comprometem com seus clientes a proteger e resguardar de ameaças diversas.

Não basta que indivíduos e organizações de fora sejam barradas, as pessoas dentro da empresa também não podem fazer uso dessas informações em benefício próprio, o que demonstra que a preocupação com a segurança da informação envolve tanto questões internas da empresa quanto externas, envolvendo ambientes sobre os quais ela poderá não ter controle (FONSECA, 2009).

Ocorre, porém, que muitas informações indevidamente utilizadas são acessadas, divulgadas ou aplicadas por membros de uma equipe de trabalho, aqueles que deveriam atuar para sua proteção acabam atuando par ao uso indevido e, assim, é indispensável que dentro das próprias instituições sejam desenvolvidas e aplicadas políticas rígidas de confidencialidade, sigilo e proteção de dados diversos (OLIVEIRA; MOURA; ARAÚJO, 2012).

Na sequência apresenta-se a hierarquia das informações conforme sua utilização pelas empresas.

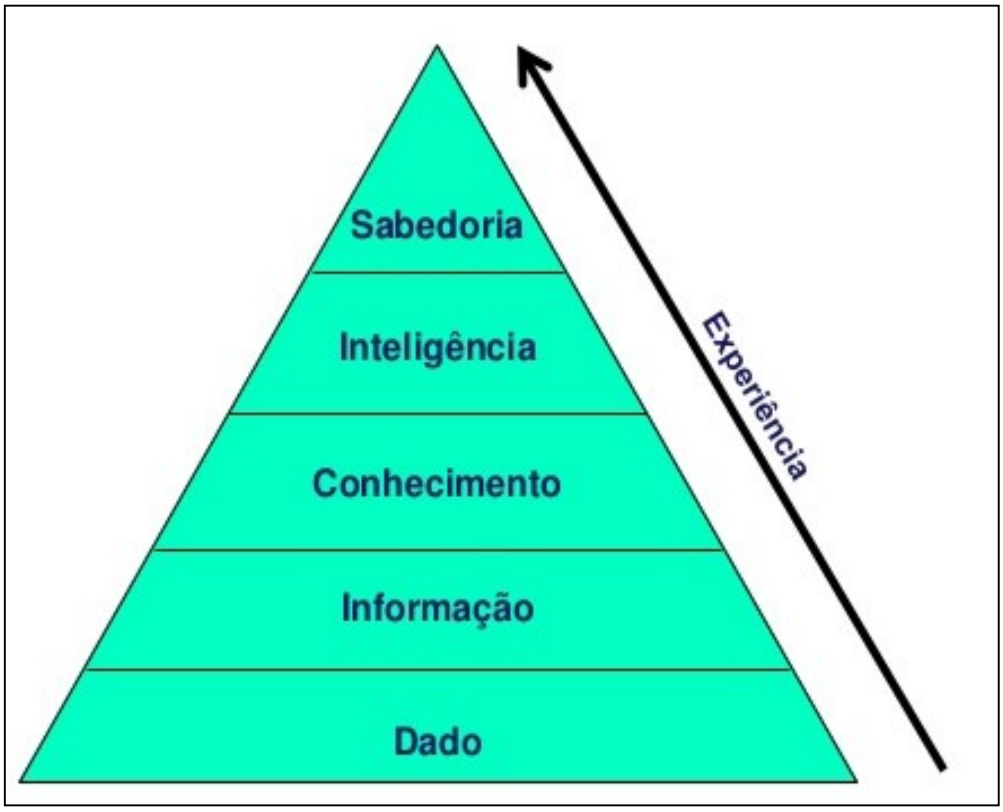

Figura 4: Hierarquia da informação
Fonte: Adaptado de Perini (2011).

Compreende-se, assim, que a hierarquia da informação deve ser conhecida e respeitada, mantendo-se os pontos considerados essenciais para sua aplicação organizada e que permita o sucesso dos resultados. Percebe-se que a experiência, o conhecimento sobre as tecnologias existentes, suas características e aplicações, trouxe consigo a possibilidade de melhoria nas formas como são vistas, valorizadas e consideradas dentro de uma instituição (FONSECA, 2009; PERINI, 2011; OLIVEIRA; MOURA; ARAÚJO, 2012).

Sobre o tema, destaca-se o disposto por Brasil (2014, p. 8):

> A TI evoluiu de um posicionamento clássico de suporte administrativo para um lugar de desempenho estratégico dentro das instituições. A área muitas vezes ultrapassa a função de ferramenta e assume papel de fator crítico de sucesso. A aplicação efetiva de TI pressupõe a integração entre a estratégia de tecnologia da informação alinhada às metas institucionais.

Compreende-se, assim, que as informações permitem que as empresas alcancem seus objetivos e metas, porém, ainda que sejam essenciais para isso, as

empresa não podem fazer uso delas da forma como lhes parecer mais adequado, existem leis e códigos de ética que precisam ser conhecidos e respeitados como forma de proteger os clientes e seus interesses.

Perini (2011) esclarece que a informação é patrimônio das empresas, qualquer que seja seu porte ou sua área de atuação. Nesse sentido, além de saber como fazer o melhor uso dessas informações, é preciso definir formas de proteger essas informações, para que não sejam utilizadas de forma indevida e, assim, acabem por se tornar uma vantagem para os concorrentes.

Fonseca (2009) ressalta que além das preocupações e aquisição de programas para aumentar a segurança dentro de suas atividades, as empresas devem treinar seus funcionários para que eles compreendam que também apresentam um importante papel na segurança da informação. Por melhores que sejam os sistemas de segurança, quando as pessoas que os operam não seguem as instruções e parâmetros necessários, os riscos continuam existindo e as empresas podem ser grandemente prejudicadas.

4.2.3 O valor da informação no setor público

O setor público refere-se aos governos do país, bem como das instituições que representam suas atividades. Com isso, deve-se ressaltar que os dados que essas instituições possuem são amplos, muito completos e encampam os contribuintes, os cidadãos e suas atividades na vida pública. Quando há um vazamento desses dados, o comprometimento pode ser grande e, em muitos casos, trazer resultados graves, como o uso dessas informações para fraudes capazes de prejudicar essas pessoas (PAULA; CORDEIRO, 2015).

Todos os pilares e preceitos aplicáveis à segurança da informação no setor privado devem, necessariamente, ser aplicados ao setor público, já que a preocupação deve ser a mesma, evitar que esses dados sejam acessados e utilizados por pessoas não autorizadas.

De acordo com Souza (2013, p. 2):

> A informação, sendo um dos principais motores da atividade humana, é a principal causa da existência da organização, pois independentemente de sua natureza, tamanho ou atividades ela precisa de informações para poder executar e prosseguir a sua missão cumprindo os seus objetivos. Assim, é fundamental existir na organização uma infraestrutura adequada para a

> manipulação desta massa de dados. Além disso, a organização precisa conhecer os conceitos essenciais sobre o funcionamento dos Sistemas de Informação e as suas aplicações para que a gestão da TI no serviço público possa avançar com desenvoltura frente ao avanço das leis.

Fica evidente, assim, que as organizações públicas necessitam de informações para que suas atividades possam ser realizadas. Sem dados específicos suas atividades não podem ser conduzidas de modo adequado e completo, prejudicando os contribuintes e a própria instituição.

Por outro lado, como possuem dados extremamente pessoais, completos e específicos sobre os contribuintes, os órgãos públicos precisam preocupar-se grandemente com a segurança das informações das quais estão de posse, o que se configura como um desafio considerável. Todos os dias novas ferramentas de segurança são desenvolvidos e passam a ser utilizadas por esses órgãos, porém, na mesma velocidade surgem ferramentas e práticas capazes de colocar em risco essas informações (SOUZA, 2013).

Informações conferem efetividade às atividades, estratégias e resultados de uma empresa, seja pública ou privada e, assim, devem ser utilizadas com critérios, cuidados e excelência para a obtenção de vantagens, sem o desrespeito aos clientes, contribuintes, fornecedores ou demais envolvidos com uma instituição (PAULA; CORDEIRO, 2015).

> Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações (BRASIL, 2012, p. 10).

As instituições públicas devem definir um servidor responsável pela gestão da segurança da informação, cuja atuação tenha foco em verificar as ferramentas disponíveis, sua aplicação e os riscos envolvidos, visando evitar que esses riscos venham a se tornar ocorrências negativas (BRASIL, 2012).

As pessoas envolvidas com setores críticos, nos quais o fluxo de informações é elevado ou que tenham acesso a informações confidenciais, também precisam ser treinadas, preparadas, além de participar do desenvolvimento dos sistemas de gestão da segurança da informação. Assim como esses servidores conhecem os pontos

críticos, eles poderão prestar esclarecimentos importantes para que sistemas de segurança efetivos sejam desenvolvidos e implantados (BRASIL, 2012).

Souza et al (2016, p. 242) enfatizam que:

> No Brasil, mais especificamente no setor público, a segurança da informação é agenda estratégica, existindo uma gama de dispositivos legais e normas que tratam de sua aplicação nos órgãos vinculados ao Governo Federal e cuja observância é obrigatória.

Para o setor público, a segurança da informação é mais do que a oferta de um diferencial, trata-se de uma obrigação legalmente prevista e a ocorrência de falhas no setor pode apresentar resultados desastrosos, o que faz com que nesse setor a perspectiva de crescimento da segurança seja acentuada (BRASIL, 2012; SOUZA et al, 2016).

Compreende-se, assim, que no setor público a segurança da informação não se trata de uma opção visando à satisfação dos clientes, de fato, trata-se de uma medida legalmente exigida para que dados importantes não sejam colocados em risco e as pessoas não sejam prejudicadas devido a seu acesso inadequado a partir de falhas nos órgãos públicos (SOUZA et al, 2016).

4.3 O CENÁRIO FUTURO: PERSPECTIVAS

Em face de toda a evolução que permeia continuamente as tecnologias de informação e comunicação, a segurança da informação precisa acompanhar a tendência de inovação e desenvolvimento de novas práticas e medidas para aumentar a certeza dos usuários de que os dados que compartilham com empresas ou pessoas específicas são serão utilizados inadequadamente. Oliveira, Moura e Araújo (2012) destacam que a informação vem se tornando um bem cada vez mais valioso no meio social e, diante disso, o interesse em acessá-la e utilizá-la vem crescendo.

“A concentração de esforços relativa à segurança e à preservação da informação é uma condição **sine qua non** para se assegurar que as organizações estabeleçam eficazmente as suas linhas de ação, objetivos, missão e estratégia” (SOUSA, 2014, p. 93).

Um dos princípios da segurança da informação refere-se à confidencialidade, de modo que os dados compartilhados entre as partes, sejam físicas, jurídicas ou ambas, devem ser considerados confidenciais, sua divulgação não pode ocorrer sob

nenhuma hipótese sem a autorização da pessoa a quem as informações se referem. Diante disso, uma perspectiva que vem se desenvolvendo refere-se à criação de meios para que essas informações estejam, de fato, asseguradas (OLIVEIRA; MOURA; ARAÚJO, 2012).

Accorsi (2014) ressalta que ainda que todas as informações sejam importante e todas as instituições devam atuar para sua proteção, uma preocupação crescente no momento encampa as instituições financeiras. Essas empresas contam com dados amplos e muito importantes e, quando utilizados de forma indevida, podem trazer elevados prejuízos financeiros para os clientes. Tanto dados pessoais de clientes como números de contas, senhas, cartões de créditos, todas são informações armazenadas nessas instituições e, assim, o desafio que vem sendo visto como de grande dificuldade, mas elevada necessidade, refere-se à proteção das informações que essas instituições armazenam em seus bancos de dados.

> No entanto, as questões suscitadas pela segurança da informação colocam-se a outros níveis e, para serem efetivamente asseguradas, têm que ser equacionadas proporcionalmente à importância da informação, como ativo crucial em qualquer organização, e refletir o seu papel, presença e requisitos ou atributos que lhe são exigidos no seio e fora da Organização que a produz, recebe e acumula (SOUSA, 2014, p. 94).

Aprimorar a segurança da informação é um desafio, mas acima de tudo uma necessidade. Não basta desenvolver tecnologias que permitem inúmeras atividades, contatos com clientes e fornecedores de locais distantes, derrubando as barreiras geográficas, é preciso que todo o desenvolvimento tecnológico venha acompanhado de segurança, de medidas pensadas, desenvolvidas, aplicadas e continuamente melhoradas para que o ambiente virtual, de fato, permita bons negócios e contatos e não se torne solo fértil para uso indevido, ilícito e capaz de enriquecer alguns com base em atos ilegais e criminosos contra outros (BRASIL, 2014).

O cenário futuro pode tornar-se extremamente promissor e positivo, ou conduzir a uma regressão nos hábitos de utilização das tecnologias para as mais variadas atividades do cotidiano, tudo depende da forma como a gestão da segurança da informação desenvolverá ferramentas de proteção efetivas e de forma contínua. Não basta conquistar a preferência dos consumidores com bons preços ou prazos diferenciados, é preciso muito mais. Eles devem sentir-se seguros e terem certeza de que, ao compartilhar seus dados pessoais com empresas, instituições e governos,

não estão colocando sua privacidade, finanças e a segurança de forma geral em risco (OLIVEIRA; MOURA; ARAÚJO, 2012).

Informação gera conhecimento e, assim, trata-se de mais do que um emaranhado de informações, mas uma ferramenta de desenvolvimento e destaque. Empresas que possuem informações sólidas, claras e confiáveis sobre seus clientes, concorrentes e mercado tendem a se tornar mais competitivas, lucrativas e bem sucedidas, enquanto aquelas que não valorizam as informações rapidamente serão ultrapassadas (RODRIGUE; BLATTMANN, 2014).

Diante dessa percepção, é indispensável ressaltar que quando existe o acesso a essas informações de forma ilícita, invade-se a privacidade e a seguranças dos usuários, incorrendo em crime. Por outro lado, essas invasões trazem resultados extremamente negativos para as pessoas atingidas e, assim, se tornam motivos para a perda de confiança e encerramento das atividades com a instituição que não protegeu esses dados adequadamente (OLIVEIRA; MOURA; ARAÚJO, 2012; BRASIL, 2014; SOUSA, 2014).

Souza (2013) acredita que as perspectivas futuras são inúmeras, praticamente ilimitadas, considerando-se que os esforços para melhorar a gestão da segurança da informação são contínuos. Tanto as empresas que usam esses sistemas quanto aquelas responsáveis por sua criação e fornecimento ao mercado vêm trabalhando para aumentar os níveis de segurança, impedindo o acesso e uso indevido das informações armazenadas.

Apesar disso, porém, seria totalmente inadequado afirmar que os patamares mais elevados de segurança já foram alcançados, de fato, o caminho é longo e, constantemente, falhas são percebidas e aproveitadas por aqueles que buscam um caminho fácil para a obtenção de vantagens ilícitas. Diante disso, acredita-se que os estudos, esforços e ferramentas nessa área tendem a ser desenvolvidos constantemente, até que barreiras sólidas e impenetráveis sejam alcançadas (SOUZA, 2013; BRASIL, 2014; SOUSA, 2014).

Diante disso, acredita-se que uma das perspectivas mais fortes para o futuro no que tange a gestão de segurança da informação refere-se ao estudo aprofundado dos acontecimentos atuais, buscando verificar os pontos falhos existentes e, assim, desenvolver ferramentas para que sejam suprimidos, assegurando a todos os usuários que suas informações serão utilizadas única e exclusivamente por quem tem

autorização para fazê-lo (OLIVEIRA; MOURA; ARAÚJO, 2012; ACCORDI, 2014; SOUSA, 2014).

5 CONSIDERAÇÕES FINAIS

A sociedade atual encontra-se permeada pelo uso constante das tecnologias de informação e comunicação para as mais diversas atividades. Compras, vendas, serviços, estudos, trabalho, todas essas ações podem ser conduzidas a partir de um computador ou celular conectado à internet, o que faz com que as barreiras geográficas deixem de ser limitantes e pessoas de todo o mundo possam entrar em contato entre si em tempo real.

Com essas tecnologias, surgiram oportunidades de mercado extremamente importantes e muitas empresas vêm se especializando em comércio virtual. Os clientes fazem seus negócios a partir de suas casas ou escritórios e não precisam deixar o conforto e a segurança para pagar ou retirar os produtos, tudo é muito rápido e fácil para todas as partes.

Em face disso, o montante de informações que circulam nas redes todos os dias é muito alto, dados relacionados aos indivíduos, empresas, instituições e governos, fotos, vídeos, enfim, uma vasta gama de dados, alguns compartilhados abertamente, outros mantidos em sigilo visando à proteção e segurança dos usuários das tecnologias.

Pessoas, empresas e governos fazem uso dessas informações e apresentam bancos de dados virtuais contendo dados, o que passou a chamar a atenção de indivíduos com intuitos escusos, ilícitos, interessados nessas informações como modo de obterem vantagens, o que trouxe consigo a ocorrência de invasões e roubo de informações.

O que era para ser um grande benefício para todos os envolvidos passa a apresentar uma carga de inseguranças e riscos que, muitas vezes, afastam pessoas e empresas. Diante da ameaça de ter os dados acessados e utilizados indevidamente, surge o receio de prejuízos pessoais, morais e financeiros e os usuários passam a buscar as oportunidades virtuais que apresentam maiores índices de segurança, confiabilidade e satisfação relatados por outros clientes.

Em face dessa realidade, surge a segurança da informação, um esforço verificado em todos os países do mundo, por meio do qual a busca central refere-se ao desenvolvimento de tecnologias e ferramentas que se tornem barreiras entre os bancos de dados existentes e as pessoas interessadas em acessá-los, mesmo não sendo autorizadas para isso.

Diante dessa percepção, este estudo foi desenvolvido com o objetivo central de investigar os principais desafios e perspectivas na gestão da segurança de informação.

Os estudos realizados permitiram verificar que a gestão de segurança da informação vem evoluindo continuamente ao longo dos anos e os esforços na área jamais são interrompidos, constantemente as empresas, governos e pessoas, assim como os desenvolvedores desses sistemas, vêm buscando formas de tornar suas atividades virtuais mais seguras, mantendo a si e a quem atuam com elas em segurança.

Atualmente existem desafios consideráveis na área, como a prática de crimes virtuais. Esses crimes envolvem fraudes, roubos, desvios de verbas, mas também atingem a dignidade das pessoas quando são voltados ao âmbito moral. Ofensas, ameaças, calúnias, todas são formas de ação criminosa que podem não comprometer as finanças dos indivíduos, mas certamente atingem sua vida e comprometem sua satisfação.

Práticas de estelionato com uso de informações alheias, como documentos, números de contas bancárias ou cartões de crédito também são comuns e podem gerar prejuízos imensos para a vítima, além de levar ao enriquecimento ilícito dos criminosos. De forma geral, as ocorrências envolvendo recursos financeiros são as mais combatidas, considerando-se a dificuldade de recuperar esses valores, porém, nos últimos anos leis vêm sendo desenvolvidas para punir aqueles que causam danos morais às vítimas escondidos atrás de recursos virtuais.

Fica evidente, assim, que os maiores desafios existentes estão relacionados ao desenvolvimento de medidas efetivas que protejam todos os usuários dessas tecnologias, sem impedir o desenvolvimento social, econômico e pessoal que elas podem trazer quando são bem utilizadas. Manter seu uso reduzindo os riscos e ameaças é a preocupação mais comum na área no momento e jamais poderá deixar de ser assim.

No que tange as perspectivas futuras, verifica-se que a segurança se torna um ideal buscado por todos os envolvidos nesse meio, como forma de assegurar o crescimento de suas atividades, fazendo com que os usuários alcancem máxima confiança e passem a indicar a outros determinados negócios como sendo seguros, eficazes e protegidos.

Empresas, instituições e governos capazes de obter e proteger essas informações para seu uso, de acordo com a autorização dos indivíduos, tendem a proceder de uma tomada de decisões muito mais efetiva, sólida e pautada em dados reais e, assim, também seus resultados são amplamente beneficiados.

A área de segurança da informação tende a crescer continuamente, pois sabe-se que quanto mais barreiras são desenvolvidas, mais usuários mal-intencionados buscam se especializar para poder ultrapassá-las, o que demonstra que a área não permanecerá estática sob nenhuma circunstância.

REFERÊNCIAS

ACCORSI, André. O banco do futuro: perspectivas e desafios. **R.Adm**. São Paulo, v.49, n.1, p.205-216, jan./fev./mar. 2014.

ADÃES, Marcelo. A maturidade da segurança da informação. 23 fev. 2010. Disponível em: < https://tecnoativa.wordpress.com/2010/02/23/a-maturidade-da-seguranca-da-informacao/> Acesso em: 17 abr. 2017.

ARAÚJO, Rubens. **Política de segurança da informação**: instrumento de defesa cibernética. Rio de Janeiro: RJ, 2014. Disponível em: <http://www.esg.br/images/Monografias/2014/ARAUJO.pdf> Acesso em: 30 mer. 2017.

BERTOLINI JÚNIOR, Hélio et al. **Segurança da informação**. Universidade Federal de Minas Gerais. 2010.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação.** Tribunal de Contas da União. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

_____. Ministério da Cultura. **Planejamento Estratégico de Tecnologia da Informação 2014-2016**. Out. 2014. Disponível em: < http://www.cultura.gov.br/documents/10180/646838/PETI+-+Vers%C3%A3o+Final+-+2014.pdf/92efa495-4318-4de8-b0d0-8d661a2fb087> Acesso em: 19 mar. 2018.

CANOGIA, Cláudia; MANDARINO JÚNIOR, Rafael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parc. Estrat**. Brasília-DF. V. 14; n. 29; p. 21-46, jul-dez, 2009. Disponível em: < http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342> Acesso em: 4 dez. 2016.

CAROCIA, Marcel. **Sistemas de informação**. São Paulo: Pearson Education do Brasil, 2009.

COMPUTERWORLD. **Sete pilares da segurança da informação, segundo a Microsoft**. 9 set. 2016. Disponível em: <http://computerworld.com.br/sete-pilares-da-seguranca-da-informacao-segundo-microsoft> Acesso em: 30 mar. 2017.

D'ÁVILA, Márcio. **PMBOK e Gerenciamento de Projetos**. Gestão de TI, 2015. Disponível em: <http://www.mhavila.com.br/topicos/gestao/pmbok.html>. Acesso: em 20 mar. 2018.

ESPÍRITO SANTO, Adriele Fernanda Silva do. **Segurança da informação**. Disponível em: <http://www.ice.edu.br/TNX/encontrocomputacao/artigos-internos/aluno_adrielle_fernanda_seguranca_da_informacao.pdf> Acesso em: 14 mar. 2018.

ESPM – Escola Superior do Ministério Público do Estado de São Paulo. **Direito e Internet**. Caderno Jurídico. Ano 2 Vol. 1 – Nº 4 – Julho/2002. Disponível em: <http://www.esmp.sp.gov.br/2010/caderno_4.pdf> Acesso em 9 mar. 2017.

FONSECA, Paula Fernanda. **Gestão da segurança da informação**: o fator humano. Nov. 2009. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf> Acesso em: 11 mar. 2018.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2007.

GURGEL, Giovane Montine Moreira. O valor estratégico da informação para a gestão das organizações. **XIII SIMPEP**. Bauru, SP, Brasil, 06 a 08 de Novembro de 2006. Disponível em: < http://www.simpep.feb.unesp.br/anais/anais_13/artigos/967.pdf> Acesso em: 15 abr. 2017.

HALLBERG, Bruce A. **Networking**: rede de computadores teoria e prática. Rio de Janeiro: Alta Books, 2003.

JORGE, Higor Vinícios Nogueira. **Crime cibernético não é sinônimo de impunidade**. 15 maio 2011. Disponível em: <http://www.conjur.com.br/2011-mai-15/policia-possue-ferramentas-investigar-crime-internet> Acesso em 9 mar. 2017.

KAUFMAN, Lori M. Data Security in the World of Cloud Computing. **IEEE Security & Privacy**. Volume: 7, Issue: 4, July-Aug. 2009. Disponível em: < http://ieeexplore.ieee.org/abstract/document/5189563/> Acesso em: 11 abr. 2017.

LANG, Andreas et al. Future perspectives: the car and its IP address – a potential safety and security risk assessment. **Safecomp**, 2007, p. 40-53. Disponível em: <http://link.springer.com/chapter/10.1007/978-3-540-75101-4_4#page-1> Acesso em: 5 dez. 2016.

LAUDON, K. C; LAUDON J. P. **Sistemas de informação gerenciais**: administrando a empresa digital. 5. Ed. Tradução de Arlete Simille Marques. São Paulo: Pearson Prentice Hall, 2004.

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. In: **Âmbito Jurídico**, Rio Grande, XVII, n. 128, set. 2014. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 26 mar. 2018.

LÜDKE, Menga; ANDRÉ, Marli. **Pesquisa em educação**: abordagens qualitativas. São Paulo: EPU, 1986.

MARCIANO, João Luiz Pereira. **Segurança da Informação**: uma abordagem social. Brasília, 2006. Disponível em: < http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf> Acesso em: 15 jan. 2017.

MARCONI, Marina de Andrade. LAKATOS, Eva Maria. **Metodologia científica**. 5 ed. São Paulo: Atlas, 2007.

MARTINS, Gilberto de Andrade; LINTZ, Alexandre. **Guia para elaboração de monografias e trabalhos de conclusão de curso**. São Paulo: Atlas, 2000.

MELHADO, S. B. **Gestão, cooperação e integração para um novo modelo voltado à qualidade do processo de projeto na construção de edifícios**. – Tese (Livre Docência), Escola Politécnica da USP, 2001.

MORAES, Rosa Maria M; GUERINI, Fábio; SERRA, Sheyla M. B. **Aplicação de tecnologia de informação no setor da construção civil**. XII SIMPEP - Bauru, SP, Brasil, 06 a 08 de novembro de 2006. Disponível em: < http://www.simpep.feb.unesp.br/anais/anais_13/artigos/334.pdf> Acesso em: 22 jan. 2017.

NASCIMENTO, Luiz Antônio; SANTOS, Eduardo Toledo. A indústria da construção na era da informação. **Ambiente Construído**. 2003; 3(1):69-81. Disponível em: < http://www.seer.ufrgs.br/ambienteconstruido/article/download/3443/1857> Acesso em: 6 dez. 2016.

NETO, Mario Furlaneto. GUIMARÃES, José Augusto Chaves. Crimes na internet: elementos para reflexão sobra a ética informacional. **R. CEJ**, Brasília, n. 20, p. 67-73, jan./mar. 2003. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/523/704> Acesso em 11 mar. 2017.

NETTO, Abner da Silva; SILVEIRA, Marco Antônio Pereira da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**. Vol. 4, No. 3, 2007, p. 375-397. Disponível em: <http://www.redalyc.org/html/2032/203219581007/> Acesso em: 15 fev. 2018.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Caroline Gaudêncio de; ARAÚJO, Francisco de Assis Norberto Galdino de. **Gestão da segurança da informação**: perspectivas baseadas na tecnologia da informação. 2012. Disponível em: < http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311> Acesso em: 11 mar. 2017.

PAULA; Lorena Pires de; CORDEIRO, Douglas Farias. Políticas de segurança da informação em instituições públicas. Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica. 2015; v. 6, n. 2; p. 58-69.

PELACANI, Valmir Luiz. **Responsabilidade na construção civil**. Curitiba: CREA-PR, 2010.

PERINI, Luis Cláudio. **Administração de sistemas de informação**. São Paulo: Pearson Prentice Hall, 2011.

PETRY, Anderson Cunha. **Desenvolvimento de firewall com hardware de baixo desempenho e fácil configuração em nível de usuário**. Santa Maria: UFRGS, 2013. Disponível em: <http://www.redes.ufsm.br/docs/tccs/Anderson_Petry.pdf> Acesso em: 13 abr. 2017.

PRODANOV, Cleber Cristiano. FREITAS, Ernani Cesar de. **Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico.** 2 ed. Novo Hamburgo: Feevale, 2013.

REZENDE, Denis Alcides. **A evolução da tecnologia da informação nos últimos 45 anos**. Disponível em: < https://www.joinville.udesc.br/portal/professores/pfitscher/materiais/Evolu__o_da_TI.pdf> Acesso em: 14 mar. 2018.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle. **Modelo de avaliação da maturidade da segurança da informação**. VII Simpósio Brasileiro de Sistemas de Informação. 2011. Disponível em: < http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2011/modelodeavalicao.pdf> Acesso em: 12 jan. 2017.

RISCHPATER, Ray. **Desenvolvendo wireless para a Web**. São Paulo: Makron. Books, 2001.

ROCHA, Paulo César Cardoso. Segurança da informação: uma questão não apenas tecnológica. Brasília: Universidade de Brasília, 2008. Disponível em: < http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/paulo_cesar.pdf > Acesso em: 10 mar. 2017.

RODRIGUE, Charles; BLATTMANN, Úrsula. Gestão da informação e a importância do uso de fontes de informação para geração de conhecimento. **Perspectivas em Ciência da Informação**. v.19, n.3, p.4-29, jul./set. 2014. Disponível em: <http://www.scielo.br/pdf/pci/v19n3/a02v19n3.pdf> Acesso em: 23 mar. 2018.

ROMANO B. **Programas da qualidade da construção civil no Brasil**: uma análise da teoria sob a ótica da teoria institucional. Vila Velha: UFES, 2002.

ROSA, Fabrízio. **Crimes de informática**. 2. ed. Campinas: Bookseller, 2005.

SANTOS, Antonio Raimundo dos. **Metodologia científica**: a construção do conhecimento. Rio de Janeiro: DP & A editora, 2001.

SCHNEIDER, Luiz Carlos. **Avaliação dos processos de segurança da informação na integração das áreas de controladoria e de tecnologia da informação**. São Leopoldo: UNISINOS, 2012. Disponível em:

<http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/3367/avaliacao_processos.pdf?sequence=1&isAllowed=y> Acesso em: 18 mar. 2018.

SÊMOLA, Marcos. **Gestão da segurança informação**: uma visão executiva. 2. ed. Rio de Janeiro: Campus, 2003.

SILVA, Denise R. P. da; STEIN, Lilian M. Segurança da informação: uma reflexão sobre o componente humano. **Ciências & Cognição**. 2007; Vol 10: 46-53. Disponível em: <http://pepsic.bvsalud.org/pdf/cc/v10/v10a06.pdf> Acesso em: 15 fev. 2018.

SILVA, Fábio Alves da. **A evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro**. Curitiba: UFPR, 2014. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/38336/R%20-%20D%20-%20FABIO%20ALVES%20DA%20SILVA.pdf?sequence=3&isAllowed=y> Acesso em: 18 mar. 2018.

SOARES, Luiz FG et al. **Redes de computadores**: das LANs, MANs e WANs às redes ATM. Rio de Janeiro: Campus, 1995.

SOUSA, Evaldo Silva de. A gestão da TI dentro do serviço público. **Gestão e Tecnologia para a Competitividade**. Out. 2013. Disponível em: < https://www.aedb.br/seget/arquivos/artigos13/25218236.pdf> Acesso em: 15 mar. 2018.

SOUSA, Paula Maciel Carvalho de. **Gestão da Informação**: do modelo de segurança e preservação ao repositório confiável. PÁGINAS a&b. S.3, 1 (2014) 03-13. Disponível em: < http://ojs.letras.up.pt/index.php/paginasaeb/article/viewFile/572/572> Acesso em: 18 mar. 2018.

SOUZA, Jackson Gomes Soares et al. Gestão de riscos da segurança da informação em uma instituição pública federal: um estudo de caso. **ENIAC Projetos**, Guarulhos (SP),V.5, n.2, jun.- dez. 2016. Disponível em: < https://www.governodigital.gov.brplone/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/seguranca-da-informacao> Acesso em: 12 mar. 2018.

TANENBAUM, Andrew S.; WETHERALL, David J. **Rede de computadores**. 5. ed. São Paulo: Saraiva, 2011.

TORRES, Gabriel Torres. **Rede de computadores**. 2. ed. Rio de Janeiro: Nova terra, 2014.

UNB – Universidade Brasília. **Gestão da segurança da informação e comunicações**: volume 1. Jorge Henrique Cabral Fernandes, organizador. Brasília: Faculdade de Ciência da Informação, c2010.

UNISVIENNA. Gabinete das Nações Unidas contra a droga e a criminalidade. **Crimes informáticos**. Disponível em: <http://www.unis.unvienna.org/pdf/fact_sheet_6_p.pdf> Acesso em 10 mar. 2017.

VIEIRA FILHO, Geraldo. **GQT – Gestão da qualidade total**: uma abordagem prática. São Paulo: Alínea, 2003.