UNIFACS UNIVERSIDADE SALVADOR
MESTRADO PROFISSIONAL EM SISTEMAS E COMPUTAÇÃO

CLEBERTON CARVALHO SOARES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM APLICAÇÕES WEB

Salvador
2016

CLEBERTON CARVALHO SOARES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM APLICAÇÕES WEB

Dissertação apresentada ao programa de Mestrado em Sistemas e Computação da UNIFACS Universidade Salvador, Laureate International Universities, como requisito parcial para a obtenção do título de Mestre.

Orientador: Prof. Dr. Paulo Caetano da Silva.

Salvador
2016

FICHA CATALOGRÁFICA
Elaborada pelo Sistema de Bibliotecas da UNIFACS Universidade Salvador, Laureate International Universities)

Soares, Cleberton Carvalho

Gestão da segurança da informação em aplicações Web./ Cleberton Carvalho Soares.- Salvador: UNIFACS, 2016.

107 f. : il.

Dissertação Programa de Pós-Graduação em Sistemas e Computação de UNIFACS Universidade Salvador, Laureate International Universities como requisito parcial à obtenção do título de Mestre.

Orientador: Prof. Dr. Paulo Caetano da Silva.

1. Segurança da Informação. 2. Aplicações Web. I. Silva, Paulo Caetano da Silva, orient. II. Título.

CDD: 004.62

UNIFACS
UNIVERSIDADE SALVADOR
LAUREATE INTERNATIONAL UNIVERSITIES

FOLHA DE APROVAÇÃO

CLEBERTON CARVALHO SOARES

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM APLICAÇÕES WEB

Dissertação aprovada como requisito parcial para obtenção do grau de Mestre em Sistemas e Computação, Universidade Salvador - UNIFACS, do Curso de Mestrado Profissional em Sistemas e Computação, pela seguinte banca examinadora:

Prof. Dr. Paulo Caetano da Silva - Orientador
Universidade Salvador – UNIFACS

Prof. Dr. Bruno Carreiro da Silva
Universidade Salvador – UNIFACS

Prof. Dr. Glaudio José Couri Machado
Universidade Federal de Sergipe - UFS

Salvador, 28 de dezembro de 2016

Universidade Salvador - UNIFACS
R. Alameda das Espatódias, 915 – Caminho das Árvores – 41820-860 / Salvador – BA
Telefax: (71) 3330-4630 / ppgcomp@unifacs.br

Dedico este trabalho àqueles que representam a maior expressão do amor de Deus para comigo nesta terra; a quem coube a minha formação de valores e fé de ser humano: ao meu avô, Francisco Dantas Soares, referência de coragem, determinação e força; e à minha avó, que faleceu em 2011, Rosalva Maturano Soares, que demonstrou o poder que há na caridade e o diferencial existente na verdade. Amarei sempre vocês. Minha eterna gratidão!

AGRADECIMENTOS

Deus, porque me amas e continua a me dar força e fé para continuar, amparo e carinho para me recuperar, e propor desafios para fazer-me mais do que vencedor, receba o meu louvor e honra. Consagro-Te tudo o que sou e o que vier a ser! Sozinho eu não posso.

Ao meu amor nesta terra, minha linda esposa (carinhosamente, "*minha filha"*), Lenyangelles, a qual é exemplo de fidelidade; aos meus filhos que fazem ainda mais feliz minha existência: Rebeca (minha bebê) e Isaías (meu campeão). Obrigado pelo amor, abraço, afeto e sorriso. Tê-los comigo é fundamental!

Agradeço incomensuravelmente a minha "tia Mim" (Marineide Dantas), que como uma verdadeira presença de mãe, desde os meus primeiros contatos com a escola, dedicou atenção e carinho para que eu pudesse desenvolver prazer e habilidade com as letras e os números. Jamais! Jamais conseguirei alcançar valor material que possa pagar o que fizestes por mim. Eu sou um fruto seu! Obrigado por ter acreditado em mim quando tudo era incerto e em cenário tão adverso.

Meu agradecimento também ao orientador deste trabalho, Prof. Dr. Paulo Caetano, a quem coube a tarefa de acompanhar-me por toda a jornada, ajustando e contribuindo valorosamente para que minhas ideias e produção textual estivessem adequadas para um trabalho acadêmico de um mestre. As lições aprendidas, que se misturaram à experiência vivida durantes esses anos, jamais serão esquecidas; em especial, para o que está planejado vir a seguir, referente ao próximo degrau na vida acadêmica.

Carinhoso agradecimento também a minha prima-irmã-sobrinha e jornalista Késia Bezerra, a qual abriu as portas da sua residência ("My Dubai"), com tamanha atenção e simpatia, para que eu pudesse estar muito bem acomodado durante as semanas de aulas e demais atividades acadêmicas, quando era requerido estar em Salvador/BA.

Àquelas pessoas que cederam também seus préstimos e créditos para que pudesse honrar meus compromissos financeiros junto à UNIFACS. São eles: nobre amigo e admirável pessoa: Carlos Alberto (Beto); e aos queridos e sempre marcantes e presentes familiares, meus queridos irmãos: "tia Pipi" (Maria Dantas); "Misa" (Misael Dantas) – sempre um "paitrocinador"; e ao meu pai "Dié" (Daniel Dantas) – uma pessoa que se preocupa comigo; ao casal a qual também tenho tanto apreço, Ulzias e Jô - meu sogro e sogra, que destinam sempre atenção, respeito e afeto. Todos vocês continuam sendo verdadeiramente incríveis e abençoadores para mim e aos meus.

Agradeço ao meu primo-irmão, Flávio André, e o irmão “Tega” (Natanael Dantas), os quais me ajudaram nas traduções dos artigos na língua inglesa, e nas revisões textuais de toda a produção científica nestes anos de Mestrado.

Externo também agradecimento ao grupo Estácio de Ensino Superior, a quem coube parte do aporte financeiro e de liberação nas semanas de aula e demais atividades presenciais, necessários para conseguir concluir esse programa de Mestrado. Registro aqui, em especial, o agradecimento aos meus gestores imediatos, Prof. Dr. Paulo Rafael Nascimento e Prof. Dr. Fernando Monteiro, dos quais houve a permissão para as ausências do posto de trabalho, permitindo-me conciliar a agenda de trabalho e estudo, e a compreensão que foi preciso mais tempo do que o comumente previsto para atingir o objetivo: titulação de Mestre.

Aos meus irmãos espirituais da Terceira Igreja Batista de Aracaju, em especial, ao Pastor, escritor e tio (por consideração), Antônio Martins Soares Bezerra, o qual esteve sempre dando o apoio e acompanhando (dividindo a ansiedade) até alcançar o fim dessa jornada!

Para concluir, gostaria de fazer menção a duas pessoas que gostaria muito de abraçar neste momento, mas que apenas presenciaram meu ingresso no Mestrado, e não mais vive neste mundo: a querida anciã D. Anita (avó da minha esposa), que sempre me cercou de carinho; e a flor ceifada ainda na mocidade, Míriam Rafaela - minha irmã, a qual a vida não nos propiciou muitos encontros, mas que permitiu-nos constituir admiração e respeito de quem procura fazer o que é certo.

As lágrimas agora são de alento, satisfação, memórias, agradecimento e, sobretudo, de alcançar o que, por vezes, pareceu incerto e quase impossível. Chegar até aqui foi muito e intensamente desafiador! Mas, continuo feliz por tudo e por todos, por isso desejo prosseguir!

Sinceramente, OBRIGADO!

Deus é quem aperfeiçoa o meu caminho e me faz vencer!

RESUMO

A informação é uma variável influente no ambiente corporativo, potencialmente rica e fundamental para o planejamento estratégico, portanto, não podem estar expostas a riscos de alteração ou acesso indevido, não autorizado. Dentre as tecnologias da informação que manipulam e fazem intercâmbio de informações, atualmente, as tecnologias Web representam um paradigma de desenvolvimento de software cada vez mais utilizado e fazem uso da Internet como meio de comunicação para intercâmbio de informações. Contudo, a Internet é reconhecidamente um ambiente hostil e sem gestão, o que favorece ao uso de técnicas e estratégias para explorar vulnerabilidades que expõe a informação das empresas a riscos severos, comprometendo os seus negócios. Para que as aplicações Web continuem manipulando e intercambiando informações confidenciais e sigilosas é necessário obter níveis mais elevados de segurança da informação. Baseado nesse contexto é proposto nessa dissertação um *framework* de gestão da segurança da informação, preconizado na norma ABNT ISO/IEC 27002:2013 e nos principais riscos atualmente encontrados nas aplicações Web. No *framework* são propostos processos e atividades para que boas práticas e tecnologias sejam identificadas, integradas, institucionalizadas e periodicamente aperfeiçoadas, no intuito de contribuir para dirimir ou mitigar os riscos que atualmente são encontrados nas aplicações Web. Para avaliar a proposta, foi desenvolvido e aplicado um questionário a profissionais da área da engenharia de software, no intuito de identificar a opinião destes profissionais tanto no uso de *frameworks* quanto em processos vinculados à gestão da segurança da informação. Os resultados mostram que iniciativas e propostas estruturadas em *frameworks* são comuns para a engenharia de software, e que pesquisas no âmbito da gestão da segurança da informação continuam a ser importantes e devem ser fomentadas no desenvolvimento de sistemas, em especial, para aplicações que utilizem a Internet como meio para manipulação e intercâmbio de informações confidenciais e sigilosas.

Palavras-chave: Gestão da Segurança da Informação. Norma ABNT ISO/IEC 27002:2011. Aplicações Web. Segurança na Internet.

ABSTRACT

Information is an important variable in the corporate environment, potentially rich and important for strategic planning, therefore, can not be exposed to changing risks or unauthorized access. Among the information technologies that manipulate and make exchange of information, currently, the Web technologies represent a software development paradigm increasingly used and use the Internet as a means of communication to exchange information. However, the Internet is admittedly a hostile and without management environment, which favors the use of techniques and strategies to exploit vulnerabilities that exposes information from companies to severe risks, compromising their business. For Web applications continue manipulating and exchanging confidential and sensitive information it is necessary to obtain higher levels of information security. Based on this context we propose in this dissertation a framework of information security management, recommended in ISO / IEC 27002:2013 standard, and the main risk currently found in Web applications In the framework we propose processes and activities so that good practices and technologies are identified, integrated, institutionalized and regularly improved in order to help to resolve or mitigate risks that are currently found in Web applications. To evaluate the proposal we developed and applied a questionnaire to professional an in the software engineering area, in order to identify the opinion of these professionals both in the use of frameworks and in processes related to the management of information security. The results show that initiatives and proposals of structured frameworks are common for software engineering, and research in the context of information security management remain important and should be encouraged in the development of systems, in particular for applications using the Internet as a means for handling and exchange of confidential and sensitive information.

Keywords: Information Security Management. Standard ABNT ISO/IEC 27002:2013. Web applications. Internet security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AS/NZA	Australian/New Zealand Standard
BSi	British Standards
CWE	Common Weakness Enumeration
CVE	Common Vulnerabilities and Exposures
ERIC	Educational Resource Information Center
IEC	International Eletrotechnical Comission
HTTP	Hiper Text Transmission Protocol
ISACA	IT, Audit, Security & Risk
ISO	International Organization for Standardization
CSRF	Cross-Site Request Forgery
OWASP	Open Web Application Security Project
SGSI	Sistema de Gestão de Segurança da Informação
SQL	Structured Query Language
SSL	Security Socket Layer
STOPE	Strategy; Technology; Organization; People; and Environment
UML	Unified Modaling Language
URL	Uniform Resource Locator
VPN	Virtual Private Network
TLS	Transport Layer Security
XSS	Cross-Site Scripting

SUMÁRIO

1 INTRODUÇÃO

Este capítulo tem como propósito contextualizar sobre a problemática a ser tratada nesta dissertação, apresentar as justificativas e a motivação para sua elaboração, juntamente com os objetivos que se esperam alcançar com sua conclusão. Por fim, é apresentada a ordem e conteúdo a serem discutidos nos capítulos que compõem este trabalho.

1.1 CONTEXTUALIZAÇÃO

A literatura, com maior destaque a da área de administração, é enfática ao instituir o nível de relevância da informação para as organizações, independente de quaisquer similaridades ou diferenças que caracterizem uma empresa. A informação é uma variável influente no ambiente corporativo, potencialmente rica e fundamental para o planejamento estratégico. Qualquer ferramenta tecnológica que interaja ou infira com a informação, em qualquer etapa do seu ciclo de vida (BEAL, 2005), precisa utilizar-se de mecanismos que priorize o nível de segurança da informação adequado ao negócio.

O uso e desenvolvimento de tecnologias da informação são fomentados pelos sistemas de informações, os quais definem novos paradigmas para a produção, gestão e intercâmbio dos produtos de informação. Esses sistemas, segundo a norma ABNT 27002:2013, são expostos a diversos riscos a partir de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, roubo. A evolução do comércio e dos negócios eletrônicos, por exemplo, tornaram a privacidade uma grande preocupação da sociedade da informação.

A segurança da informação visa salvaguardar a informação em relação a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (ABNT 27002, 2013). A gestão da segurança da informação compreende a concepção de processos para monitorar, de maneira continuada, à integridade das informações; à prevenção de ataques e ao furto dos dados; e assegurar que os sistemas sejam restabelecidos, e o acesso seguro às informações seja garantido na incidência de ataques ao sistema computacional que tenha êxito.

É importante ressaltar que nem toda informação requer confidencialidade ou sigilo (são consideradas de domínio público), o que deixa claro que uma gestão de riscos deve definir o nível de impacto ou de incidência do risco, para que seja empreendido maior esforço de controles de segurança na informação de maior criticidade e com maior exposição aos riscos. Este nível é alcançado pela atividade de avaliação do risco (ABNT 27005, 2011).

Empreender a aplicação de um processo de gestão de riscos se torna uma medida bem adequada aos objetivos de identificar, analisar e avaliar os riscos, sendo o ponto de partida para implementação da gestão da segurança da informação (ABNT 27005, 2011). Conhecido os riscos, deve ser apurado e estabelecido um conjunto de atividades coordenadas para dirimir ou mitigá-los, que são os controles de segurança, no sentido de proteger a informação. Conclui-se, então, que a gestão da segurança da informação promove o alinhamento, por exemplo, da equipe da tecnologia da informação ao negócio da organização, porque os negócios na sociedade do conhecimento têm ampla dependência da informação.

Dentre as tecnologias relativas à engenharia de software, as aplicações Web atualmente agregam a maioria dos produtos de softwares arquitetados e construídos, porém, a Web é um lugar em que encontramos a maioria dos intrusos, espionando e tentando fazer uso indevido da informação (TANENBAUM; WETHERALL, 2011), além de ser considerada por Sêmola (2003) uma infraestrutura sem gestão. É neste contexto tecnológico de comunicação de dados inóspito em que ocorre, por exemplo, intercâmbio de informações quando do uso de aplicações Web. Portanto, as ameaças presentes na Internet expõem as informações, em seu ciclo de vida, a diversos riscos de segurança da informação, torna-se imprescindível identificá-los para dirimi-los ou mitigá-los. Muitas dessas informações são confidenciais, o que exige prevalência da segurança da informação tanto para os protocolos de comunicação como no produto de software, através da implementação de estratégicas de proteção coletivas e integradas.

No âmbito da comunicação através da Internet, encontramos vasta literatura alusiva à implementação de proteção para informação com uso dos protocolos de comunicação (e.g. VPN, SSL/TLS, IPSec, IPv6) que subsidiam proteção ao ambiente de trânsito da informação, ou seja, nas camadas de rede e transporte do modelo OSI (SILVA, 2003). Contudo, não somente a utilização de protocolos de redes de computadores seguros é suficiente para atender a demanda de segurança da informação para a Internet e para as aplicações Web; se assim o fosse, problemas alusivos ao roubo e alteração de informações como, por exemplo, senhas de

cartão de crédito ou de *Internet banking*, que transitam pela Internet, não seriam tão recorrentes, além de tantos outros tipos de ataques mencionados por pesquisas recentes, conforme observamos em Borgohain et al (2015).

No domínio da camada de software, existem instituições internacionais que visam apoiar o desenvolvimento de sistemas com atenção às questões de segurança para a aplicação de software, oferecendo publicações a respeito da implementação de segurança para o produto de software, suporte técnico e treinamentos, dentre outras atividades, e.g. (i) a CWE[1] (Common Weakness Enumeration); (ii) o Institute SANS[2]; (iii) a Common Vulnerabilities and Exposures[3] (CVE); (iv) a SAFECode[4]; (v) o Web Application Security Consortium[5] (WASC); e (vi) a Open Web Application Security Project (OWASP)[6].

A partir da análise da atuação e contribuições das instituições supracitadas, principalmente dos relatórios e documentos que por elas são disponibilizados para a comunidade da engenharia de software, constata-se o uso generalizado de uma abordagem técnica na discussão dos mecanismos de segurança, a fim de que se possa dirimir ou mitigar os riscos presentes, dentre outros, em aplicações Web. Contudo, verifica-se pouca ou inexistente menção aos conceitos alusivos à gestão da segurança da informação.

Entende-se que apesar da importância quanto à questão técnica, a sua prática de maneira exclusiva contribui e permite que os profissionais da engenharia de software continuem a desenvolver softwares com as vulnerabilidades que já são discutidas por instituições e pesquisadores. Apesar da discussão técnica já empreendida, a deficiência por parte dos programadores para desenvolver sistemas com acúmulo de vulnerabilidades é apontada na literatura em muitas pesquisas, com destaque para a escala de tempo em que foram publicadas (LAWTON, 2007; JOVANOVIC et al, 2010; BRADBURY, 2012; CARVALHO, 2014). Apesar de normalmente ser vinculada a ferramentas tecnológicas (e.g. firewalls, antivírus, IDS/IPS), que têm a sua importância, a segurança da informação transcende a questões estritamente tecnológicas, e rotineiramente sugere novos paradigmas organizacionais (SÊMOLA, 2003), envolvendo ambiente, processos e pessoas que estão vinculados ao ciclo de vida da informação. Os profissionais da área de desenvolvimento de

[1] http://cwe.mitre.org/
[2] https://www.sans.org/
[3] https://cve.mitre.org/
[4] htpp://www.safecode.org/
[5] http://www.webappsec.org/
[6] http://www.owasp.org/

sistemas podem ter deficiências no âmbito da gestão da segurança da informação, a qual proporciona imperícia e negligência sobre como e quando podem ser implementados controles de segurança eficazes, tanto de maneira isolada, como uma forma adequada de integrá-los. Convém empreender esforços para suprir essa lacuna.

1.2 JUSTIFICATIVA

A segurança da informação é um requisito fundamental para fornecedores de software, principalmente em razão das pressões exercidas pelo mercado, que requerem ambiente de proteção para suas infraestruturas e pela necessidade de instituir e resguardar a confiança no ambiente de computação. O foco de proteção deve privilegiar a segurança da informação, principalmente aquelas de cunho privado, porque a informação é caracterizada como o elemento de maior valor para as empresas.

Identificar, analisar e avaliar recursos de proteção à informação não deve ser desconsiderado ou tratado como um assunto ultrapassado, bem como se já fosse discutido e resolvido totalmente. Apesar do contexto oportuno propiciado pela Internet como meio de comunicação de dados e esforços para promover maiores níveis de proteção à informação, ela continua a ser uma infraestrutura insegura, o que expõe a informação por ela intercambiada a riscos de adulteração ou furto.

Existe a necessidade em discutir como controles de segurança podem dirimir ou mitigar os riscos presentes em aplicações Web, dentre outros, através de uma discussão que não se detenha a explanação com detalhes técnicos de implementação, uma vez que a deficiência a ser suprida é saber o que é, i.e., a criptografia e o certificado digital.

Empreendido com independência de linguagem de programação ou tecnologia, uma solução de gestão da segurança da informação pode ter uma maior abrangência e contribuição para a engenharia de software, porque pode ser utilizada por quaisquer empresas que atuem com desenvolvimento de aplicações Web, e pode também ajustada e/ou estendida para outras linguagens ou paradigma de programação disponibilizadas pela engenharia de software.

Uma abordagem que preceda a implementação de um sistema contribui para o fomento do desenvolvimento das tecnologias da informação seguras, porque habilita os profissionais envolvidos na arquitetura e construção de aplicações Web terem foco na segurança da informação. Isto contribui para dirimir ou mitigar os riscos antes mesmo da

atividade de programação do sistema. A remoção de vulnerabilidades em etapas posteriores do desenvolvimento de software favorece a custos finais maiores para o produto de software (SOMMERVILLE, 2011; SHAR, 2012).

1.3 MOTIVAÇÃO

A motivação inicial para elaboração deste trabalho foi a constatação, com base na revisão bibliográfica, de que os programadores de aplicações Web mantém as suas implementações com vulnerabilidades oriundas de riscos que já são abordados pela literatura; e que, conforme enfatizado por Shar (2012), encontrar soluções para combater riscos continua a ser um importante problema de pesquisa.

A partir da análise de relatórios fornecidos por instituições (e.g. CWE, Institute SANS, Common Vulnerabilities and Exposures, SAFECode, WASC e OWASP) constata-se que a literatura faz uso da abordagem técnica para explicitar os mecanismos de segurança que podem ser utilizados para dirimir ou mitigar os riscos. Dentre as instituições pesquisadas, motivou-nos o uso do documento emitido pela OWASP, denominado de OWASP Top 10, porque contatou-se estar sendo continuamente publicado ao longo dos últimos dez anos - que permitiu uma contextualização histórica muito rica; e pelo foco do documento ser para aplicações web e por ter aceitação acadêmica.

A motivação em empreender uma discussão a partir de uma abordagem conceitual deu-se mediante: (i) a lacuna identificada na literatura em explorar essa abordagem para discutir sobre contramedidas de segurança da informação para os principais riscos identificados nas aplicações Web; e (ii) entender que se a abordagem técnica fosse suficiente, as aplicações Web não deveriam continuar expostas a riscos que já são conhecidos e detalhados através das pesquisas relacionadas ao assunto.

A utilização de normas de gestão da segurança da informação foi motivada porque, além da utilização da abordagem conceitual, buscou-se empreender uma discussão que enfatizasse a proteção da informação que é manipulada ou intercambiada pela aplicação Web através da Internet, e não da tecnologia de paradigmas ou linguagens da engenharia de software. Kozen *et al* (2012) definem que a utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da

informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

Explorar a metodologia de *framework* foi motivada por identificar que profissionais da engenharia de software têm aceitação por propostas estruturadas nesse método; e que o uso de *frameworks* representa um modelo adequado para abordagens relacionadas à processos de gestão da segurança da informação, conforme definem Isaca (2012) e Martins *et al* (2009).

1.4 OBJETIVOS

1.4.1 Geral

O objetivo deste trabalho é propor uma solução para auxiliar à gestão de segurança da informação no desenvolvimento de aplicações Web, baseada na Norma ABNT 27005:2011, no documento OWASP e estruturada como um *framework*, de maneira que práticas e tecnologias de segurança da informação possam ser adotadas e institucionalizadas.

1.4.2 Específicos

Para se alcançar o objetivo desta dissertação é necessário que alguns objetivos específicos sejam alcançados:

a) Identificar requisitos de gestão e da segurança da informação;
b) Identificar mecanismos da segurança da informação e suas estratégias de utilização dos mecanismos da segurança da informação que sirvam como contramedidas eficazes aos riscos identificados;
c) Realizar uma gestão de riscos no âmbito qualitativo aos dez principais riscos de segurança mais críticos em aplicações Web;
d) Propor um *framework* para a gestão da segurança da informação em aplicações Web;
e) Realizar um estudo de caso para se avaliar a solução proposta.

1.5 ESTRUTURA DA DISSERTAÇÃO

O capítulo atual – Capítulo 1 – teve por finalidade apresentar e contextualizar a problemática, justificativa e motivação para escolha do assunto a ser tratado neste trabalho.

Também são apresentados os objetivos geral e específicos, e como está a organização dos capítulos que compõem essa dissertação.

Será exposta no Capítulo 2 uma visão holística relacionada ao risco e discutido um referencial teórico, que envolve conceitos, fundamentos e normas relacionadas a gestão da segurança da informação e da gestão dos riscos. A discussão também contempla os mecanismos da segurança da informação que apoiam o desenvolvimento de controles para a proteção da informação. Para contemplar plenamente a fundamentação teórica necessária para o trabalho, será também feita uma discussão sobre a concepção de *frameworks*.

A discussão dos trabalhos correlatos será no Capítulo 3.

O Capítulo 4 será destinado a discutir sobre a aplicação do processo de gestão de riscos da segurança da informação para as aplicações Web, apoiados pela norma de gestão da segurança da informação escolhida.

O Capítulo 5 será destinado a discussão referente a proposta do *framework* de gestão de segurança da informação, de maneira que agregue subsídios para alcançar níveis mais elevados de proteção no desenvolvimento de aplicações Web a partir dos mecanismos da segurança da informação.

O estudo de caso, discutido no Capítulo 6 terá como objetivo identificar o conhecimento a respeito da segurança da informação, e a aceitação e favorabilidade do uso do *framework* proposto junto a profissionais da engenharia de software.

Encerradas as discussões, serão apresentadas no Capítulo 7 as conclusões alcançadas com a pesquisa e elaboração deste trabalho, bem como a exposição de trabalhos futuros.

Na Tabela 1, é apresentada a síntese da estrutura deste trabalho.

Tabela 1 - Estrutura da dissertação

Fundamentação Teórica Exploratória	Capítulo 2: Fundamentos e Gestão da Segurança da Informação e de Gestão de Riscos Erros mais comuns e críticos para o Desenvolvimento de Aplicações Web
Revisão da Literatura	Capítulo 3: Trabalhos Correlatos
Intervenção de Pesquisa Descritiva	Capítulo 4: Gestão de Riscos da Segurança da Informação Capítulo 5: *Framework* de Gestão da Segurança da Informação
Aplicabilidade	Capítulo 6: Avaliação sobre Conhecimento em Segurança da Informação
Aspectos Conclusivos	Capítulo 7: Conclusão e Trabalhos Futuros

Fonte: Autor deste trabalho (2016).

2 A SEGURANÇA DA INFORMAÇÃO E A GESTÃO DE RISCO

O referencial teórico permite verificar o estado do problema a ser pesquisado, sob o aspecto teórico e de outros estudos e pesquisas já realizados (MARCONI; LAKATOS, 2010). Este capítulo discute o referencial teórico que envolve conceitos sobre as variáveis de pesquisa deste trabalho: riscos; segurança da informação; gestão da segurança da informação e da gestão de riscos; e *frameworks*. Além destes, a discussão aborda sobre os mecanismos da segurança da informação que apoiam o desenvolvimento de controles para a proteção da informação.

2.1 VISÃO HOLÍSTICA DO RISCO

O risco está relacionado ao tempo futuro, caracterizado pela incerteza da ocorrência (SÊMOLA, 2003), e sua ocorrência propicia alterações em um marco inicial do que estava planejado a ocorrer. O risco é um problema potencial (PRESSMAN, 2011) e com características particulares para cada sistema, mesmo que similares. Portanto, uma ou várias soluções no intuito de dirimir ou mitigar os riscos podem ser aplicadas a diversos sistemas, mas requer uma avaliação e validação para possíveis adaptações.

A proposição de contramedidas aos riscos deve ser a partir da exposição genérica do que fazer, e deve se abster em definir como fazer; pois a realização efetiva dependerá das ferramentas e mecanismos disponíveis à época, sejam manuais ou tecnológicos, bem como de habilidade para alcançar contramedidas eficazes. Inclusive, tais recursos propostos para defender-se do risco podem se tornar obsoletos, com a continuidade do mesmo risco explorado por outra estratégia de ataque. Além de estabelecer as contramedidas, faz-se necessário avalia-las periodicamente, porque a estratégia ou a própria contramedida podem ficar obsoletas.

Para eliminar ou mitigar o risco é essencial dedicar-se à sua análise para aqueles que sejam considerados comuns, certos ou óbvios (visto que por serem bastante conhecidos, têm maior chance de serem explorados); porém, convém dar maior ênfase, àqueles que promovem o impacto negativo de maiores proporções, seja na esfera da tecnologia e, principalmente, do negócio. Encontrar soluções para combater riscos continua a ser um importante problema de pesquisa (SHAR, 2012). Convém não subestimar qualquer risco, mas ter muito bem definido onde e como empreender maior esforço de combate.

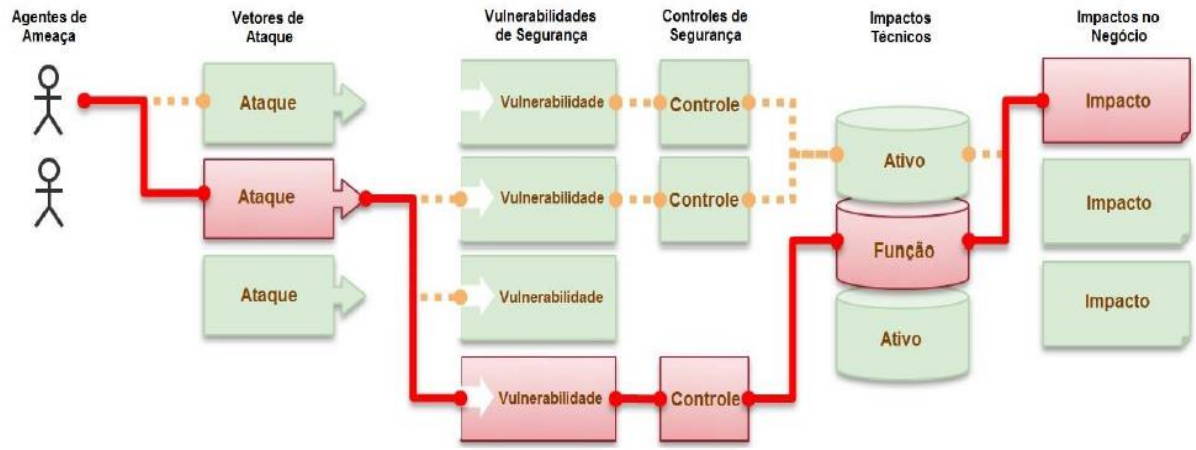
2.2 MAPA CONCEITUAL DO RISCO

Na Figura 1 é apresentado um mapa conceitual que mostra o sucesso obtido em um ataque a um sistema qualquer. A promoção de impactos técnicos e ao negócio é denominado de incidente de segurança da informação (ABNT 27005, 2011), o qual é resultado da negligência ou imperícia da aplicação efetiva de algum controle de segurança.

Observando a Figura 1, identifica-se a representação da existência de diversas possibilidades entre vetores de ataques e vulnerabilidades de segurança, que podem tanto sobrepor aos controles de segurança quanto identificar sua ausência. As possiblidades formam rotas. Todas as rotas buscam comprometer o funcionamento das tecnologias da informação, através de impactos técnicos (e.g. parada no banco de dados), bem como propiciar um impacto no negócio da empresa, comprometendo sua credibilidade e imagem diante do mercado. E exatamente a exploração destas rotas é que formam os riscos.

O risco em segurança da informação é muitas vezes expresso em termos de combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade associada de ocorrência (ABNT 27005, 2011). Através do *framework* de gestão da segurança da informação se estabelece uma biblioteca de práticas, padrões, normas, processos, atividades, objetivos, requisitos, controles e métricas dos controles de segurança, a fim de que possa coibir de maneira eficaz a ação do risco (ISACA, 2012).

Figura 1 - Mapa Conceitual dos Riscos



Fonte: OWASP Top 10 (2016).

2.3 CONCEPÇÃO DE *FRAMEWORK*

Apesar de muito abordado pela engenharia de software, *frameworks* são utilizados por várias ciências. Exemplificando o conceito traduzido por Oxford (2013), em que traduz *framework* como “armação, estrutura, sistema”, seria uma estrutura básica de apartamentos com a mesma planta ou estrutura; para a computação, seria um mesmo ponto de partida para implementação de um sistema, o qual poderia ocorrer adições, remoções ou extensões, visando uma melhor adequação.

Apesar da pluralidade de áreas que empregam o uso do termo *framework*, através da pesquisa bibliográfica, observa-se duas características comuns, as quais são destacadas nos trabalhos alusivos ao tema: ganho de produtividade e qualidade (desempenho, interoperabilidade) para o produto gerado. Essa produtividade é relacionada principalmente à questão do reuso, que é uma variável detentora de muita atenção e destaque no ciclo de desenvolvimento de software (PRESMANN; SOMMERVILLE, 2011).

Contudo, conforme abordado na contextualização deste trabalho, duas definições tiveram destaque dentre as demais encontradas na literatura, porque fazem alusão a *frameworks* com escopos vinculados à gestão da segurança da informação, a partir de uma gestão de riscos. São elas:

a) Isaca (2012) cita que no contexto de processos de gestão de segurança e governança de tecnologia da informação, podemos entender *framework* como um conjunto estruturado ou uma biblioteca de práticas, padrões, normas, processos, atividades, objetivos, requisitos, controles e métricas; e
b) Martins (2008) especifica que um *framework* de segurança da informação deve procurar integrar os principais padrões, i.e., *standards*, e suas metodologias de aplicação, as boas práticas da segurança da informação e considerar uma rigorosa metodologia de identificação e avaliação de riscos, apresentando aos tomadores de decisões das organizações uma visão macroscópica sobre a segurança da informação.

2.4 A GESTÃO DE RISCOS

A segurança da informação transcende a tecnologia, e rotineiramente sugere novos paradigmas organizacionais

Figura 2 - Tríade da Segurança da Informação

Fonte: Sêmola (2003).

Ela consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade), bem como é autêntica (integridade). Estes três elementos: confidencialidade, integridade e disponibilidade, formam a tríade da segurança da informação (SÊMOLA, 2003), conforme ilustrado na Figura 2, que é a base dos conceitos e práticas relacionados à gestão da segurança da informação.

Adicionalmente, quatro outras propriedades são associadas à tríade (FERNANDES, 2010): autenticação, autorização, identificação e não repúdio (este último, também denominado de irretratabilidade). Atuando em conjunto, estes sete elementos fundamentam a gestão da segurança da informação no intento de proteger dados, sistemas e processos.

a) Autenticação: propriedade de garantir a fonte e o teor da informação.
b) Autorização: propriedade de permitir ou negar o acesso.
c) Identificação: propriedade de registrar algo ou alguém no sistema.
d) Não repúdio: propriedade de garantir ao autor sua respectiva responsabilidade pelo que fez.

Ainda com base em padronizações definidas pela ISO, é possível acrescentar outras propriedades à tríade de segurança da informação que são definidas pela característica de "Segurança" definida pela ISO/IEC 25010:2011, que avalia a qualidade do produto de software. São elas:

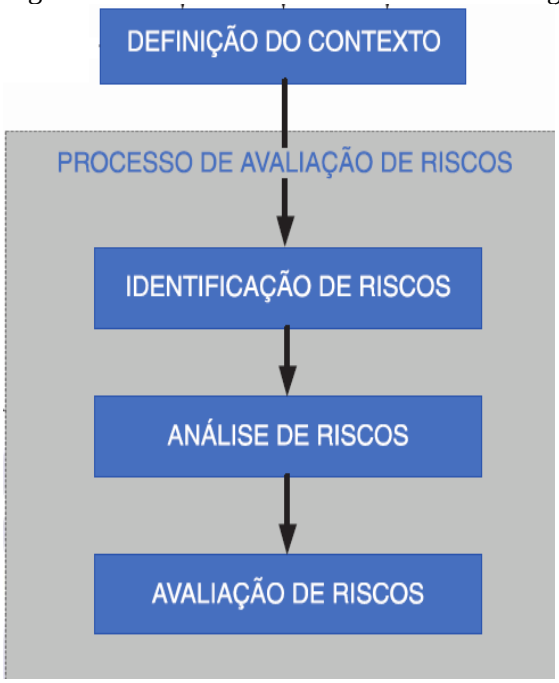
a) Autenticidade: legitimidade para os processos de controle de acesso.
b) Responsabilidade: ética e dever na prestação de contas.
c) Conformidade: ação de acordo com a legislação, com as regras ou instruções.

A implantação da gestão da segurança das informações é fundamental para minimizar os riscos e garantir a continuidade do negócio (ABNT 27002, 2013). Kozen *et al* (2012) definem que a utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

Para garantir êxito de que as questões relacionadas à segurança da informação sejam atendidas de forma satisfatória, as empresas têm aperfeiçoado e modificado, ao longo do tempo, seus modelos para desenvolvimento e uso dos sistemas computacionais; mas há dificuldades para sua plena implantação, uma vez que a facilidade de uso e a segurança caminham sempre em sentidos opostos (SÊMOLA, 2003).

A etapa inicial e fundamental para a gestão da segurança da informação é formada pelas atividades de identificação e conhecimento dos riscos inerentes ao ambiente que se deseja proteger (ABNT 27002, 2013), considerando uma rigorosa gestão de riscos, apresentando aos tomadores de decisões das organizações uma visão macroscópica sobre a segurança da informação (MARTINS, 2008). Dentre o conjunto de normas da família 27000 – que trata da implantação de um Sistema de Gestão de Segurança da Informação (SGSI), a ABNT normatiza um processo de gestão de riscos através da norma ABNT ISO/IEC 27005:2011, a qual não impõe nenhuma limitação de sua utilização.

Figura 3 - Processo de Gestão de Riscos da Segurança da Informação



Fonte: ABNT ISO/IEC 27005 (2011).

Ademais as normativas de outras instituições, a própria ABNT dispõe de duas normas para a gestão de riscos: a ISO/IEC 27005 e a ISO/IEC 31000. Veloso (2012) especifica que as diferenças entre as duas normas (27000 e 31000) são mínimas, porém destaca diferença nas áreas de aplicação, sendo a 27005 orientada para gestão de riscos para a segurança da informação e a 31000 para outras áreas de uma empresa. Por isso, a escolha pelas normas vinculadas a família 27000, com ênfase à ABNT 27005, que trata da gestão de riscos de segurança da informação.

A Figura 3 ilustra o processo de avaliação de riscos da segurança da informação definido pela norma ABNT 27005:2011. A primeira atividade desse processo é a definição do contexto, na qual deve ser caracterizada e registrada as informações relevantes do negócio ou processo que será objetivo a ser avaliado pela gestão de riscos. Uma vez definido o contexto, a próxima atividade é o processo de avaliação de riscos, o qual compreende três atividades:

a) Identificação dos riscos: evidenciar a maior quantidade de riscos possíveis; podem ser utilizadas fontes de informações internas, ou seja, produzida na própria empresa; ou externas, obtidas de outras empresas. Para fontes externas, convém que estejam correlacionadas com o tipo de aplicação que

será avaliada. Devem ser evidenciadas as ameaças, consequências, vulnerabilidades e controles existentes.

b) Análise de riscos: averiguar, a partir de distintos graus de detalhamento, o impacto gerado na exploração do risco, ou seja, quando passa a ser fato ocorrido. Esta análise de riscos pode ser quantitativa e qualitativa, ou até uma combinação entre ambas. Contudo, normalmente a análise qualitativa precede a quantitativa (ABNT 27005, 2013).

c) Avaliação de riscos: definir que contramedidas são adequadas e quais as prioridades serão empreendidas no âmbito de dirimir ou mitigar os riscos. A análise de riscos qualitativa contribuiu para instituir quais os riscos devem receber maior atenção de contramedidas de segurança da informação, uma vez que esclarece quais os riscos que propiciam maiores e menores impactos ao negócio.

2.5 MECANISMOS DA SEGURANÇA DA INFORMAÇÃO

Atualmente, os mecanismos de segurança comumente implementados em conjunto para que aplicações possam dar suporte aos postulados da segurança da informação, a fim de implantação de processos seguros aos sistemas de informação modernos, são (BURNETT; PAINE, 2002; SÊMOLA, 2003; TANENBAUM; WETHERALL, 2011):

a) Criptografia: transformação reversível da informação de forma a torná-la de impossível compreensão a terceiros não autorizados. Para a criptografia são requeridos: uso de algoritmos específicos (os quais são de domínio público); e um elemento definido como chave da criptografia (que deve ser bem gerenciada); e, a partir de um conjunto de dados não criptografados (identificados como texto claro), produzir uma sequência de dados criptografados.

b) Assinatura digital: um conjunto de dados criptografados, associados a um documento, que garante a integridade do documento associado, distinguindo eventuais alterações que podem ter ocorrido durante o trânsito entre emissor e receptor. A detecção da alteração imprópria e não autorizada é usualmente feita através de algoritmos e funções de *hashing* (BURNETT; PAINE, 2002).

c) Controle de acesso: uma referência a algum tipo de mecanismo que permita o prévio reconhecimento de quem está requerendo acesso a informação e, a partir

dos processos de identificação e autenticação, validada seu ingresso ao ambiente de informação; e, pelo processo de autorização, possa lhe ser concedida a disponibilidade à informação, de acordo com os atributos definidos. Um quarto processo também vinculado ao controle de acesso é a auditoria. A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez. Exemplos utilizados para controle de acesso: dueto composto por nome de usuário/senha; sistemas biométricos; firewalls e tokens.

d) Mecanismos de certificação: atestam a validade da informação e, principalmente, o seu autor, através de uma infraestrutura de chave pública, também citada pela sigla "PKI" (BURNETT; PAINE, 2002), a fim de associar uma pessoa ou entidade a um documento eletrônico que o represente digitalmente. O serviço bancário via Internet é o exemplo do uso de certificados digitais.

O simples fato de utilizar os referidos recursos da segurança da informação não implica nível de proteção adequado para a informação. Além de explorar estes recursos, requer integrá-los adequadamente, a fim de elevar o nível de segurança da informação que é manipulada ou intercambiada, por exemplo, pela Internet. Níveis mais elevados de segurança são alcançados a partir da integração entre tais mecanismos (SÊMOLA, 2003)

Portanto, a imperícia ou negligência em explorar estes mecanismos da segurança da informação, tanto de maneira isolada como uma forma adequada de integrá-los, expõe as aplicações Web a implementação com acúmulo de vulnerabilidades que expõe a informação a alteração não autorizadas ou roubos. Muitas vezes a empresa pode deixar a cargo do programador a responsabilidade em utilizar tais mecanismos. Esta, certamente, não é uma boa prática.

2.6 ANÁLISE DO RELATÓRIO OWASP TOP 10

O objetivo desta seção não é desmotivar o uso do OWASP Top 10 2013, bem como as edições já publicadas ou as próximas; pelo contrário, consideramos que deve ser um instrumento considerado e consultado, porque representa uma base de informações relevante, de aceitação acadêmica e do mercado, no âmbito da segurança para as aplicações Web – por isso foi selecionado como uma fonte externa para a atividade de identificação dos principais riscos deste trabalho.

Portanto, a partir da análise e estudo do referido documento, foram identificadas algumas características sensíveis que podem ser aperfeiçoadas, e contribuem para a referida produção. Portanto, o objetivo é uma contribuição visando o aperfeiçoado do documento da OWASP Top 10.

O documento OWASP Top 10 2013 é bem enfático em citar intolerância para continuidade de problemas que é definido como simples, haja vista uma década de publicação com riscos remanescentes, além de encorajar as organizações a pensarem em segurança em suas aplicações e na gestão de riscos.

Contudo, analisando a abordagem utilizada pela OWASP, não localizamos nenhuma ênfase à segurança da informação e aos seus mecanismos para proteção à informação. Pode ser que empreender esforços de proteção a aplicação Web favoreça a segurança da informação; mas, conforme já vimos na contextualização deste trabalho, normalmente, o foco das empresas está em salvaguardar a informação e não o produto de software em si. Isto não é enaltecido no documento OWASP Top 10 2013. Apesar de apresentar uma classificação, explanação e diagnóstico referente aos riscos mais críticos, não é disponibilizado nenhum dado quantitativo quanto a ocorrência dos riscos, nem detalhes sobre o tipo de aplicação Web em que foi identificada a vulnerabilidade.

Outro aspecto relevante é quanto a periodicidade da publicação do relatório OWASP Top 10. Apesar de percebermos uma organização para atualização do relatório a cada 3 anos, não existe sinalização do compromisso em manter esta periodicidade, e não foi encontrada uma justificativa para a definição do intervalo trienal.

2.7 CONSIDERAÇÕES FINAIS

Neste capítulo foram discutidos conceitos e fundamentos a respeito da gestão da segurança da informação e da gestão de riscos. A discussão relacionada aos riscos, possibilitou conhecimento sobre as etapas que norteiam a ação do ataque contra um sistema, e da obrigatoriedade de implantação de controles de segurança, conforme apresentadas por um mapa conceitual dos riscos em aplicações, para dirimir ou mitigar tais riscos.

As definições obtidas na literatura referentes ao emprego do termo *framework*, em especial, de Isaca (2012) e Martins (2008), propiciaram a clareza das etapas que propormos

seguir para atingir o objetivo geral deste trabalho, inclusive que arvoram a decisão do processo de gestão de riscos da norma ABNT ISO/IEC 27005:2011.

Para os controles de segurança, discutimos sobre os mecanismos apresentados na literatura para a gestão da segurança da informação, os quais podem ser implantados em contramedida aos riscos: criptografia; assinatura digital; controle de acesso e certificado digital. Identificamos que estes mecanismos não são concorrentes, ou seja, realizam funções distintas, e que podem ser complementares entre si. Como níveis mais elevados de segurança são alcançados a partir da integração entre tais mecanismos (SÊMOLA, 2003), o *framework* a ser proposto neste trabalho deve privilegiar a formação de boas práticas entre tais mecanismos de segurança.

No próximo capítulo, serão discutidos os trabalhos correlatos que foram encontrados na literatura, durante a revisão da literatura requerida para elaboração desta dissertação.

3 NORMAS E FRAMEWORKS PARA A GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO

O objetivo principal deste capítulo é discutir sobre propostas que sejam correlatas ao tema desta dissertação. Na pesquisa bibliográfica não foi encontrado um *framework* da gestão da segurança da informação para aplicações Web, todavia muitos trabalhos que abordam contramedidas que representam ações para dirimir ou mitigar os riscos são apontados na literatura.

3.1 NORMAS PARA A GESTÃO DE SEGURANÇA DA INFORMAÇÃO E DE GESTÃO DE RISCOS

Durante a pesquisa bibliográfica identificamos que normas para gestão de riscos é um assunto muito abordado pela literatura, motivado principalmente pela preocupação cada vez maior com perdas ou furtos de informações por falha em sistemas computacionais, com destaque para os governos e empresas em geral.

Para esta seção, como critério de seleção, foram consideradas propostas que tivessem respaldo de órgãos com ênfase na segurança da informação, e que não houvesse limitação quanto ao seu uso para a engenharia de software. As questões de pesquisa que nortearam a atividade de busca por trabalhos correlatos estão citadas a seguir

a) Quais as normas disponíveis para a gestão da segurança da informação?
b) Existem processos de gestão de risco vinculado a segurança da informação?

Dentre as organizações que emitem normas sobre segurança da informação, podemos destacar a ISO[7] (International Organization for Standardization), a BSi[8] (British Standards) e a AS/NZS (Australian/New Zealand Standard). No Brasil, conforme já referenciado, a ABNT é a responsável pela recomendação dos padrões técnicos e membro da ISO.

As principais recomendações de segurança reforçam a adoção de boas práticas de gerenciamento de sistemas computacionais e representam importantes instrumentos de orientação, observando a área de atuação. As normas com recomendações de segurança mais conhecidas são:

[7] http://www.iso.org
[8] http://www.bsi-global.com

a) Série BS 7799 do BSi (BS 1: 1999; BS2: 2002; e BS3: 2005) – que posteriormente foram revistos e reorganizados na série ISO/IEC 17799. São normas desenvolvidas pelo governo britânico, cujo foco é a segurança da informação. É a norma que serviu de base para o desenvolvimento da norma da ABNT ISO/IEC 27002, vinculadas à implantação de um sistema gestor da segurança da informação (SGSI). Também pode ser utilizada como um guia prático para desenvolver os procedimentos de segurança da informação nas empresas; contudo, não especifica uma gestão de riscos como a norma ABNT 27005:2011.
b) A especificação AS/NZ 31000:2009, desenvolvida pelos governos da Austrália e Nova Zelândia, trata o risco como um elemento para o equilíbrio entre as oportunidades de ganho e a redução das perdas. Esta abordagem conceitual de risco difere dos demais conceitos encontrados na literatura na gestão de risco. Seu antecessor, AS/NZS 4360:2004, foi publicado em 1995 e revisto pela última vez em 2004, quando uma comissão mista formada pelos dois países que participam da sua elaboração decidiu que, em vez de proceder a uma revisão similar em 2009, preferiram promover o desenvolvimento de uma norma internacional sobre gestão de risco, que poderia então ser adotada localmente.
c) No tocante à ABNT, adicionalmente à norma 27005, atualizada em 2011, temos todos as normas que compõe a família 27000 que busca dar subsídios a implantação do SGSI. São elas: 27001, 27002. Conforme discutido no Capítulo 2, estas três normas não são concorrentes, mas sim complementares e apoiam a implantação de um sistema de gestão da segurança da informação, sendo a 27005, a normativa referente a gestão de riscos.
d) A ISO também tem a norma 31000:2009, porém com abordagem mais voltada a governança corporativa, e não para fins da segurança da informação. O padrão ISO 31000:2009 pode ser aplicado em toda a vida de uma organização, e para uma ampla gama de atividades, incluindo estratégias e decisões, operações, processos, funções, projetos, produtos, serviços e bens.

3.2 FRAMEWORKS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Para esta seção, utilizamos para a identificação de trabalhos correlatos o portal de documentos EBSCOhost, pois o mesmo agrega trabalhos publicados em diversas áreas e

linhas de pesquisa, em especial, o ERIC – Educational Resource Information Center, e a Academic Seacher Elite; além destes, consideramos a busca por trabalhos de mestrado e doutorado com viés na segurança da informação. As questões de pesquisa que nortearam a atividade de pesquisa por trabalhos correlatos foram:

a) Há propostas de *frameworks* de gestão de segurança da informação na literatura?
b) Quais as características e motivos para propostas de *frameworks* de gestão de segurança da informação?
c) Há propostas de *frameworks* de gestão de segurança da informação vinculados a engenharia de software, em especial, para aplicações Web?

Como as iniciativas relacionadas à segurança da informação buscam, dentre outras, o aperfeiçoamento da cultura organizacional, Alhogail (2015) apresenta uma proposta de framework baseado em uma estrutura denominada de STOPE (Strategy; Technology; Organization; People; and Environment) de modo a melhor preparar o *peopleware*[9] para questões alusivas à segurança da informação. A abordagem utilizada no trabalho contribui para uma ampla visão no tocante a segurança da informação, porém não se detém e estudar vulnerabilidades específicas vinculadas a tecnologias Web ou quaisquer outras.

Sipior e Ward (2008) alertam para a preocupação continuada de questões inerentes a segurança da informação, o que fomenta a necessidade em empreender a gestão da informação como recurso para atender a referida premissa. Os autores destacam no trabalho sobre os ataques internos à segurança da informação, ou seja, emitidos por aqueles que pertencem à organização. Ataques internos ocorrem também pela negligência ou desconhecimento de como proceder para dirimir riscos da segurança da informação, portanto, o trabalho reforça que a conscientização a partir de uma abordagem com viés na segurança da informação favorece a ambientes mais seguros.

Martins (2008), propõe um framework de segurança para sistemas de informação (SI) que proteja os SIs organizacionais dos métodos de ataque produzidos com base em ameaças e tipo de estratégias utilizadas em três esferas: físicas, de sintaxe e semânticas, porém não dispõe de uma gestão de riscos no escopo da atuação de um SI. Já Santos e Nunes (2012) propõe um framework de gestão de segurança da informação para organizações militares. O trabalho visa identificar as mais relevantes dimensões e categorias de controles de segurança da informação a aplicar nas organizações militares em ambiente categorizado por “Guerra de

[9] Pessoas que interagem com os sistemas de informações modernos.

Informação" (destaca a relevância da informação), e de que forma a doutrina militar em vigor limita ou promove a aplicação das normas de segurança da informação disponíveis.

Marciano (2009) afirma que a tecnologia da informação é capaz de apresentar parte da solução a este problema, mas não é capaz de resolvê-lo integralmente, e propõe um modelo para a formulação de políticas de segurança da informação baseadas em moldes afetos ao domínio das ciências sociais e construídas com ênfase na observação dos sistemas de informação e no contexto em que se inserem. Segundo o autor, pelos resultados alcançados na observação de uma abordagem de caráter humanista, centrada nos pontos de vista do usuário e que se contraponha aos modelos tecnicistas atuais, demonstrou relevância significativa para o sucesso na implantação da segurança da informação. Abordagens conceituais são mais intrínsecas ao lado humano do que da tecnologia.

3.3 PROPOSTAS DE CONTRAMEDIDAS DE SEGURANÇA PARA APLICAÇÕES WEB

No âmbito dos trabalhos correlatos catalogados, apesar da incipiente disponibilidade de publicações da engenharia de software que promova uma abordagem no contexto da segurança da informação, foi possível identificar quantitativo expressivo de pesquisas que abordam sobre riscos que estão contidos em aplicações Web.

Para esta seção, a questão de pesquisa que norteou a atividade de busca por trabalhos correlatos foi:

- Há literatura disponível que discuta sobre como dirimir ou mitigar os riscos apresentados pelo documento da OWASP em aplicações Web, com uso de uma abordagem técnica?

Os critérios de seleção definidos foram: trabalhos aceitos e publicados em periódicos, os quais foram publicados a partir da primeira edição do OWASP Top 10, e que tratasse de riscos vinculados restritamente a aplicações Web. Como a abordagem deste trabalho não é vinculada a especificação técnica, e para evitar que o trabalho fique prolixo por causa do quantitativo de riscos, não avaliaremos correlatos de todos os riscos que estão citados no OWASP Top 10.

No intuito de definir quais seriam os riscos mais relevantes a serem pesquisados para compor essa seção, foram considerados os três primeiros riscos definidos pelo documento da

OWASP; e, adicionalmente, todos os riscos cuja classificação relacionado ao impacto nos negócios ou tecnologia tenha a classificação como “Severo”. Com base nesse critério, foram identificados quatro riscos, sendo a discussão dos trabalhos, identificados na revisão da literatura, relacionados a esses riscos feita individualmente.

- **Cross-Site Scripting (XSS)**

Foi possível identificar na revisão da literatura que a discussão sobre como os desenvolvedores e analistas de sistemas lidam com a questão da segurança da informação é um tema já abordado no que se refere aos produtos de software baseados em tecnologias Web. Conry-Murray (2006), esclarece sobre formas de ataques do XSS e sugere a necessidade de desenvolvedores de aplicações Web realizarem capacitação, pois não apresentam habilidades para implementar contramedidas eficazes, além de destacar também sobre a necessidade de realização de testes de vulnerabilidades antes do atacante, ou seja, o que denota inobservância a processos estabelecidos da engenharia de software (testes dos sistemas).

Semelhantemente, Lawton (2007) discute riscos de segurança vinculados com a natureza interativa e colaborativa da Web 2.0, e.g. o XSS e CSR (Cross-Site Request Forgery). É sugerido que os programadores desenvolvam as aplicações Web usando técnicas de programação que tenham foco nas questões de segurança. O autor destaca que a popularização da Web impõe desafios ainda maiores para qualquer aplicação que a utilize como meio de comunicação.

Jovanovic et al. (2010) ressalta que aplicações Web têm se tornado um dos canais de comunicação mais importantes entre vários tipos de prestadores de serviços e clientes na Internet; porém, em geral, possuem grande vulnerabilidade a ataques do tipo XSS e Injeção de Código (SQL). Como contramedida, os autores apresentam uma ferramenta denominada de “Pixy”, que serve para detectar vulnerabilidades por meio de análise de fluxo de dados.

Sood e Enbody (2011), discutem sobre a situação adversa relacionada a iniciativas dos bancos para proteção das transações dos seus clientes ao XSS e CSRF, por exemplo, são vetores de ataque que permitem o roubo de uma seção estabelecida entre cliente e servidor em intercâmbio de informações. Como contramedida de segurança da informação proposta, é apresentado o resultado de avaliação de segurança declarativa, a qual propõe melhorias ao protocolo HTTP para controlar o estado do browser e proteger a seção do usuário (cliente).

Saiedian e Broyle (2011), rechaçam a premissa que o modelo SOP (Same-Origin Policy)[10] é eficiente contramedida ao XSS, ao contrário, ele propicia um aumento nas vulnerabilidades.

Bradbury (2012) discute que parte dos problemas relacionados ao XSS, apesar de ser uma vulnerabilidade bem compreendida, é proveniente da pouca conscientização sobre segurança da informação pelos desenvolvedores; e que há uma tendência de se aumentar a fragilidade dos sistemas com a evolução e inovação tecnológica, pois repercutem em novas vulnerabilidades a partir do respectivo agente de ameaça. Shar e Tan (2012) apresentam várias contramedidas de combate aos riscos do XSS, mas ressaltam que há continuidade das vulnerabilidades nas aplicações Web pela falta de familiaridade dos desenvolvedores na compreensão do problema e na limitação de implementar os mecanismos de contramedidas.

Fraiwan et al. (2012) apresentam uma técnica para identificação de dados maliciosos, a partir de características comuns nos malwares, a fim de que seja possível à aplicação Web identificar ataques de XSS, por exemplo, a partir de listas de características comuns criadas a partir da coleta e armazenamento desses dados caracterizadores. Em trabalho mais atual alusivos ao XSS, Das et al. (2015) discutem sobre vulnerabilidades oriundas do XSS, bem como práticas atuais de contramedidas de segurança da informação. Os autores apresentam como contramedida uma proposta a partir da criação de listas com características coletadas a partir da análise da forma de exploração do XSS. Por se tratar de uma solução estática, semelhante a assinaturas de site maliciosos presentes nos *firewalls*, requer que as listas sejam geridas periodicamente, sob pena de que a desatualização promova a vulnerabilidade da aplicação Web, a partir de inovações na estratégia ou no método de ataque.

- **Injeção de Código**

Gary e Zhendong (2007) esclarecem que a Injeção de Código é um tipo identificado como comum de ataques às aplicações Web, que promove a execução de consultas não autorizadas, por exemplo, em banco de dados. Os autores fazem críticas quantos aos modelos propostos para prevenir, de maneira estática e dinâmica, o risco da Infeção de Código. Como alternativa de resolução, apresenta uma proposta baseada em uma política denominada de "conversadora", a fim de avaliar se o código a ser executado após o intercâmbio entre cliente e servidor estão com algum ataque de Injeção de Código.

[10] Protocolo para troca de informações estruturadas em uma plataforma descentralizada e distribuída.

Halfond et al (2008) discutem sobre a problemática da evolução do cenário das aplicações Web, que por consequência se tornaram alvos de ataques de segurança. Halfond et al (2008) apresentam uma ferramenta denominada Web Application SQL-injection Preventer (WASP), a qual atua no conceito que os autores definem como sintaxe-aware. Mais recentemente, Lee et al (2012) apresenta um método de detecção ao ataque a partir da injeção, através da análise estática e dinâmica combinada, conforme Gary e Zhendong (2007), em que é removido o valor do atributo no momento da execução da consulta SQL, utilizando uma comparação a parâmetros pré-determinados.

Dorai e Kannan (2011) empreendem uma abordagem menos tecnicista sobre a Injeção de Código, eles discutem a necessidade em observar a seguridade do banco de dados. Os autores discutem ainda sobre a importância dos desenvolvedores Web e outros profissionais na área da tecnologia da informação erradicarem as vulnerabilidades a partir do agente de injeção. Porém, não faz uso de nenhuma norma da gestão da segurança da informação.

De igual modo, Cho (2015) especifica que usuários mal-intencionados podem roubar o conteúdo do banco de dados, aproveitando-se de erros cometidos por programadores. Como estratégia para mitigar a Injeção de Código, propõe a criação de um ambiente Web de avaliação na divulgação de informações de uma aplicação Web, a fim de apoiar tanto o emissor como o receptor. Contudo, notamos uma deficiência nas especificações que permitissem uma caracterização da referida aplicação Web de validação, e dos requisitos para sua implementação.

- **Cross-Site Request Forgery (CSRF)**

Larkin (2007) cita que tem ocorrido aperfeiçoamentos com este método de ataque. O autor sugere a necessidade de desenvolvedores de aplicações web realizarem capacitações, e que deve ser observado a realização de testes de vulnerabilidades antes do atacante. Nesta mesma ênfase, Mao et al. (2009) mencionam sobre a necessidade de contramedidas de segurança da informação contra o CSRF, em especial, para aplicações web com viés financeiro. Para tanto, propõem uma inspeção nos tokens de autenticação, a fim de avaliar se as requisições são legítimas através de uma técnica que foi denominada de Browser-Enforced Authenticity Protection (BEAP).

Vinculado à relação da aplicação web com protocolos redes, Rocchetto et al. (2014) fazem menção a posição de destaque do CSRF no relatório OWASP Top 10, e enfatizam que

desenvolvedores devem atuar em contramedidas de segurança da informação. Apesar da existência de muitos recursos de proteção contra o CSRF, existem vulnerabilidades mais complexas que contribuem para o atacante alcançar seu objetivo. A proposta de contramedida feita no artigo é apresentar como deve ser especificada uma aplicação web, a fim de que seja mais fácil a identificação de sua exposição a ataques CSRF.

A dificuldade em identificar a ocorrência do CSRF ou de um conteúdo autorizado é discutida por Ryck et al (2011), os quais destacam que a implementação de contramedidas de segurança costuma apresentar dificuldade com relação ao controle de acesso, quando existe a dependência de autenticações em diversas aplicações para permissão da operação. O artigo apresenta uma proposta de tratar os servidores das aplicações web com base em indicadores que apontem a atividade não-maliciosa, assim como Telikicherla et al (2014) que apresentam uma proposta de uma política de como aplicações web podem acessar dados no servidor de maneira mais segura.

- **Exposição de Dados Sensíveis**

Gritzalis et al (1999) propõem observar questões de segurança alusiva a Internet, principalmente para intercâmbio de dados vinculados a saúde das pessoas. A partir do pressuposto que a segurança se refere a um conjunto de medidas, que podem ser classificadas como processual, lógico e físico, e que visam a prevenção, a detecção, a indicação, e correção de certos tipos de má utilização do sistema, tanto acidental como deliberado, o artigo utiliza uma arquitetura composta por certificados digitais e criptografia para propor uma boa prática para desenvolvimento de aplicações Web para a área médica.

Hamann et al (2001) apresentam uma proposta para alcançar níveis mais elevados de segurança da informação através de mecanismo de autenticação através do uso de *smarts card*. Anane et al (2008) destacam sobre a relevância da criptografia para evitar o acesso não autorizado e garantir a integridade dos dados. Identifica-se que o artigo não apresenta menção às normas de segurança da informação, porém apresenta um esquema de fragmentação que envolve proteger apenas o dado que é confidencial, e não todo o texto como rotineiramente são implementados nos sistemas computacionais. Entende-se que esta é uma proposta relevante, principalmente para a busca de soluções eficientes, neste caso, relacionada ao custo de processamento.

Ainda relacionado aos mecanismos da segurança da informação, Kanso et al (2012) destacam o papel fundamental para aplicações Web das funções de *hash* no âmbito da integridade da informação. Através das simulações, mostram que a função de *hash* não representa impacto considerável no custo de processamento e atende aos requisitos para proteção dos dados confidenciais. Sakhare (2015) cita sobre estratégias que as empresas estão usando para solucionar o problema da segurança em aplicações Web. Ressaltam que deve ser entendido como uma questão crítica de pesquisa, uma vez que as aplicações Web estão cada vez mais sendo utilizadas nas rotinas de negócios das empresas. O autor disponibiliza um ambiente de teste e validação para aplicações Web, contudo, não apresenta todos os riscos citados pelo OWAP Top 10 2013, nem deixa claro como identificaram tais riscos ou qual o método de gestão de riscos foi utilizado.

3.4 CONSIDERAÇÕES FINAIS

A revisão da literatura permitiu identificar que há muitas publicações vinculadas aos riscos citados pelo documento OWASP Top 10 2013. Conforme disposto na Tabela 2, onde dispomos do resumo quantitativo dos trabalhos localizados com base nos critérios previamente descritos, foram identificados 24 (vinte e quatro) trabalhos.

Tabela 2 – Quantitativo de trabalhos correlatos alusivos aos riscos em aplicações Web

Agente de Ameaça	**ANO DE PUBLICAÇÃO**					
	2003	**2004**	**2005 a 2007**	**2008 a 2012**	**A partir de 2013**	**Total**
Cross-Site Scripting (XSS)	-	-	02	06	01	09
Cross-Site Request Forgery (CSRF)	-	-	01	03	02	06
Exposição de Dados Sensíveis	02			02	01	05
Injeção de Código	-	-	01	02	02	05

Fonte: Autor deste trabalho (2016).

Analisando a Tabela 2, percebemos a preponderância de trabalhos vinculados ao Cross-Site Scripting (XSS), com mais de um terço da produção com abordagem para este risco. O agente de ameaça definido como Cross-Site Request Forgery (CSRF) recebeu a

atenção na proposição de contramedidas de segurança em 25% dos trabalhos identificados. Os demais trabalhos referem-se à “Exposição de Dados Sensíveis”, com cinco trabalhos localizados; e a cinco publicações alusivas ao tema “Injeção de Código”, representando também 25% do total localizado. Então podemos considerar, a partir desses resultados, que as pesquisas e publicações de trabalhos têm contribuído para discutir sobre os agentes de ameaça que expõe a aplicação Web a vários riscos.

Ademais às questões quantitativas, a revisão da literatura permitiu identificar que existem muitas iniciativas de pesquisa para a segurança de aplicativos móveis, porém, a abordagem técnica tem característica de perenidade menor em relação a abordagem conceitual (porque a tecnologia vai sendo adaptada e modificada); também ficou evidente que os profissionais da área de análise e desenvolvimento de sistemas são responsabilizados pela ineficiente proteção às aplicações Web; e que a gestão da segurança da informação é pouco abordada pelos desenvolvedores de software.

Conforme postulado pela norma ABNT 27002:2013, para uma adequada gestão da segurança da informação deve-se inicialmente proceder com uma gestão de riscos. Portanto, no próximo capítulo, teremos a discussão a respeito da implementação da gestão de riscos da segurança da informação para os principais riscos em aplicações Web, nas atividades de identificação, análise e avaliação de riscos.

4 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO PARA APLICAÇÕES WEB

A etapa inicial e fundamental para a gestão da segurança da informação é formada pelas atividades de identificação e conhecimento dos riscos inerentes ao ambiente que se deseja proteger (ABNT 27002, 2013), considerando uma rigorosa gestão de riscos, apresentando aos tomadores de decisões das organizações uma visão macroscópica sobre a segurança da informação (MARTINS, 2008).

Este capítulo será destinado a discutir sobre a implementação de uma gestão de riscos de segurança da informação para os riscos encontrados em aplicações Web. Essa gestão de riscos é um pré-requisito para a definição do *framework* de segurança da informação, objetivo geral deste trabalho. Arvorado pelo que preconiza a norma ABNT 27005:2011, conforme discutido no Capítulo 2, a gestão de riscos da segurança da informação é constituída a partir da definição do escopo de três etapas: identificação, análise e avaliação do risco.

O escopo desta gestão de riscos de segurança da informação são as ameaças encontradas em aplicações Web que expõem informações sigilosas e confidenciais a riscos, causados pela negligência ou imperícia dos profissionais da engenharia de software na implementação de mecanismos eficazes da segurança da informação para dirimir ou mitigar tais riscos.

4.1 IDENTIFICAÇÃO DOS RISCOS

A norma ABNT 27005 define que a identificação de riscos deve seguir por cinco etapas: identificação dos ativos; identificação das ameaças; identificação dos controles existentes; identificação das vulnerabilidades; e identificação das consequências. A discussão destas etapas será feita nas quatro seções a seguir.

4.1.1 Identificação dos Ativos

O propósito da identificação dos ativos é determinar os ativos dentro do escopo estabelecido. Um ativo é algo que tem valor para a organização e que, portanto, requer proteção (ABNT 27005, 2011). Com base neste conceito, os ativos considerados neste trabalho são as aplicações Web, as quais atuam no ciclo de vida da informação confidencial e

sigilosa, principalmente na produção, gestão ou intercâmbio da informação através da Internet.

4.1.2 Identificação das Ameaças

Uma ameaça tem potencial de comprometer os ativos e, por isso, também as organizações. Com base no documento OWASP Top 10 2013, a negligência ou imperícia dos profissionais da engenharia de software em relação à segurança informação, expõem as aplicações Web às ameaças apresentadas na Tabela 2. A ordem na citação das ameaças segue um ranking com base no quantitativo de aplicações Web que foram identificadas vulneráveis às respectivas ameaças.

Tabela 1 - Ameaças mais críticas encontradas em aplicações Web

AMEAÇAS
Injeção de código
Quebra de Autenticação e Gerenciamento de Sessão
Cross-Site Scripting (XSS)
Referência Insegura e Direta a Objetos
Configuração Incorreta de Segurança
Exposição de Dados Sensíveis
Falta de Função para Controle de Nível de Acesso
Cross-Site Request Forgery (CSRF)
Utilização de Componentes Vulneráveis Conhecidos
Redirecionamentos e Encaminhados Inválidos

Fonte: OWASP Top 10 (2013).

4.1.3 Identificação dos Controles Existentes

Conforme explanado no Capítulo 2, os mecanismos da segurança da informação disponíveis são: criptografia; assinatura digital; controle de acesso; e o certificado digital. A literatura especifica que estes mecanismos são negligenciados ou, por imperícia, implementados incorretamente. A aplicação destes controles será discutida no Capítulo 5, através do *framework* de segurança da informação, a fim de fornecer aos profissionais que desenvolvem aplicações Web as boas práticas para implementação eficaz dos mecanismos de segurança da informação.

4.1.4 Identificação das Vulnerabilidades e das Consequências

As vulnerabilidades representam fragilidades que podem ser exploradas pelas ameaças a fim de comprometer ou ativos ou a organização. Convém salientar que um controle implementado incorretamente já pode ser considerado uma vulnerabilidade (ABNT 27005:2011). Com base na edição mais atual do OWASP Top 10, na Tabela 4 são apresentadas as vulnerabilidades e consequências de cada ameaça identificada.

Tabela 4 - Lista de vulnerabilidades e consequências presentes nas aplicações Web

AMEAÇAS	VULNERABILIDADES	CONSEQUÊNCIAS
Injeção de código	Exposição de uma referência à implementação interna de um objeto, como um arquivo, diretório, ou registro da base de dados.	Manipulação nos dados pode fazer com que o interpretador execute comandos indesejados ou permita o acesso a dados não autorizados por meio dos objetos identificados.
Quebra de Autenticação e Gerenciamento de Sessão	Autenticação e gerenciamento de sessões implementadas de forma incorreta ou não presente.	Assumir a identidade de usuários, principalmente maiores privilégios (administrador, por exemplo), sem autenticar-se ou para má implementação da aplicação.
Cross-Site Scripting (XSS)	Execução de scripts recebidos com instruções não confiáveis e que não foram validados ou filtrados.	Assumir sessões do usuário, alterar informação ou redirecionar o usuário para sites com dados maliciosos.
Referência Insegura e Direta a Objetos	Referenciar inadequadamente um objeto, como um arquivo, diretório, ou registro da base de dados sem controle de acesso definido.	Manipular estas referências para expor e explorar o objeto referenciado, inclusive tornando-o público.
Configuração Incorreta de Segurança	Configuração padrão costuma ser insegura. Implementar qualquer aplicação sem observar maiores níveis de segurança ou atualizações.	Aplicação Web com baixo nível de segurança, com estrutura baseada em legado com várias lacunas de segurança da informação.
Exposição de Dados Sensíveis	Proteção fraca ou indevida aos dados sensíveis, tanto no seu armazenamento como em trânsito.	Roubar ou modificar dados desprotegidos com o propósito de realizar fraudes de cartões de crédito, roubo de identidade, ou outros crimes.
Falta de Função para Controle de Nível de Acesso	Verificar os direitos de acesso em nível de função antes de tornar essa funcionalidade visível na interface do usuário.	Forjar as requisições, com o propósito de acessar a funcionalidade sem autorização adequada.
Cross-Site Request Forgery (CSRF)	Forçar o navegador da vítima a criar requisições que a aplicação vulnerável aceite como requisições legítimas realizadas pela vítima.	Forjar requisição HTTP, incluindo o cookie da sessão da vítima e qualquer outra informação de autenticação incluída na sessão.
Utilização de Componentes Vulneráveis Conhecidos	Utilizar componentes (bibliotecas, *frameworks*, e outros módulos de software) que dispõem de vulnerabilidades conhecidas - componentes rotineiramente requer privilégios elevados para serem executados.	Aplicação sensível a uma gama de possíveis ataques já conhecidos contando com uma sessão com elevados privilégios, visto que não foram aplicadas as contramedidas de segurança.
Redirecionamentos e Encaminhados Inválidos	Páginas de destino resultado de redirecionamentos e encaminhamentos inválidos, não validados.	Redirecionar as vítimas para sites de “phishing” ou “malware”, ou usar encaminhamentos para acessar páginas não autorizadas.

Fonte OWASP Top 10 2013 (2013).

4.2 ANÁLISE DE RISCOS

A norma ABNT 27005:2011 define que a análise de riscos deve ser empreendida a partir de uma metodologia qualitativa ou quantitativa, ou uma combinação de ambas. A metodologia deve ser aquela que tenha vínculo relacionado ao(s) ativo(s) da gestão de riscos. Na Seção 4.2.1, será discutida a metodologia OWASP Risk Rating Methodolgy [11] e a justificativa para sua escolha para a análise qualitativa. Nas duas seções seguintes, dar-se-á a discussão sobre as etapas de: análise qualitativa; avaliação das consequências; e avaliação das probabilidades dos incidentes.

4.2.1 OWASP Risk Rating Methodology

Além do documento OWASP Top 10, a OWASP define uma metodologia própria de análise de riscos, cuja estrutura é apresentada na Tabela 5.

Tabela 5 - Estrutura da análise qualitativa do risco

Agentes de Ameaça	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos	Impactos no Negócio
Específico da Aplicação	Fácil	Generalizada	Fácil	Severo	Específico do Negócio/ Aplicação
	Média	Comum	Média	Moderado	
	Difícil	Rara	Difícil	Pequeno	

Fonte: OWASP Top 10 (2013).

A estrutura apresentada pela OWASP Risk Rating Methodology representa a análise qualitativa através de termos (e.g. “Fácil”, “Generalizada”, “Severo”, “Moderado”, “Rara”), os quais representam uma incidência do agente de uma ameaça.

Os agentes de ameaças e os impactos no negócio são específicos e, por isso, devem ser estabelecidos pelo proprietário ou gestor da aplicação de software ou do negócio. Ademais, são apresentadas quatro propriedades para agentes de ameaça, de acordo com o mapa conceitual de riscos: vetores de ataque; prevalência da vulnerabilidade; detecção da vulnerabilidade; e impactos técnicos.

Todas estas propriedades dispõem de uma representação através de três atributos qualificadores, que possuem uma nomenclatura correlacionada ao grau de dano a ser causado.

[11] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Cada um dos atributos recebe destaque através da utilização de uma cor como um plano de fundo (Tabela 4), no intuito de enfatizar maior ou menor gravidade do dano causado pela materialização do risco, sendo divididas nas seguintes tonalidades:

a) Vermelho: Risco/dano **MAIS** acentuado/maior.
b) Laranja: Risco/dano **MÉDIO**.
c) Amarelo: Risco/dano **MENOR**.

Os vetores de ataques são as alternativas e/ou estratégias para introdução do ataque contra a aplicação Web. A facilidade em explorar os vetores de ataques implica em maior condição de risco, por isso recebe o destaque da cor vermelha para o atributo "Fácil". Aos demais qualificadores, temos: "Média" com a tonalidade laranja e "Difícil" com o amarelo.

A prevalência da vulnerabilidade está vinculada à manutenção nas aplicações Web de riscos já estudados e amplamente tratados na literatura, os quais podem ser resultado da negligência ou imperícia dos mecanismos de segurança da informação. O atributo de maior relevância na propriedade "Prevalência da Vulnerabilidade" é classificado como "Generelizada", ou seja, em que se encontra muita prevalência da vulnerabilidade; posteriormente temos como de médio risco (laranja) o termo "Comum" e, por fim, "Rara" (amarelo), definido como a vulnerabilidade com menor reincidência.

A detecção da vulnerabilidade tem a função em demonstrar a facilidade do atacante em identificar que a aplicação Web está vulnerável ao vetor do ataque utilizado, ou seja, define o nível de exposição ao risco. Portanto, a escala de qualificadores é inversamente proporcional: quanto mais fácil identificar, mais grave será o risco. Por isso, o qualificador "Fácil" recebe a tonalidade vermelha, e na ordem de gravidade, temos o "Média" (laranja), e o "Difícil" com o amarelo.

A última propriedade é designada de "Impactos Técnicos", onde se busca apresentar o dano potencial causado pela incidência da ameaça, ou seja, caso o atacante tenha êxito no seu objetivo. O qualificador com maior relevância é o "Severo" (vermelho), em que temos incidência de relevante prejuízo para a empresa. Os demais, na ordem de impacto, são o moderado (laranja), e o amarelo que é o de "pequeno" impacto.

A partir de uma correlação entre os conceitos vinculados a estrutura da metodologia de riscos da OWASP (Tabela 5), e das etapas de identificação de riscos preconizados pela norma

ABNT 27005:2011, conseguimos perceber semelhanças entre as propostas, conforme apresentado no comparativo da Tabela 6.

Tabela 2 - Comparativo entre elementos da análise de riscos OWASP e ABNT 27005:2011

OWASP Risk Rating Methodoly	ABNT 27005:2011
Agentes de Ameaças	Escopo
Vetores de Ataques	Ameaças
Detecção da Vulnerabilidade	Vulnerabilidades
Impactos Técnicos	Consequências

Fonte: Autor deste trabalho (2016).

A norma de gestão de riscos ABNT 27005:2011 define que a análise qualitativa deve utilizar-se de uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais e a probabilidade de tais ocorrências ocorrerem. Contudo, pela característica inerente de uma normativa que define apenas o que fazer, mas não como, a escolha do método para a análise qualitativa dos riscos é livre, desde que tenha vínculo ao escopo da gestão de riscos.

Mediante a flexibilidade permitida pela norma ABNT 27005:2011 quanto à metodologia a ser utilizada na análise qualitativa, e por identificar adequada aderência para a realização de uma gestão de riscos da segurança da informação, foi escolhido utilizar a metodologia definida pela OWASP através da OWASP Risk Rating Methodology para realizar a análise qualitativa da gestão de riscos.

4.2.2 Análise Qualitativa

A análise qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo, pequena, média e grande) e a probabilidade dessas consequências ocorrerem (ABNT 27005, 2011).

O OWASP Top 10 2013 apresenta uma análise qualitativa referente aos riscos mais críticos encontrados em aplicações Web, a qual está baseada na OWASP Risk Rating Methodology. Na Tabela 7 está disposta a análise qualitativa dos riscos apresentadas no relatório OWASP Top 10 2013 em relação aos agentes de ameaça encontrados em aplicações Web.

Tabela 3 - Análise qualitativa dos riscos

Agentes de Ameaça	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos
Injeção de código	Fácil	Comum	Média	Severo
Quebra de Autenticação e Gerenciamento de Sessão	Média	Generalizada	Média	Severo
Cross-Site Scripting (XSS)	Média	Muito Difundida	Fácil	Moderado
Referência Insegura e Direta a Objetos	Fácil	Comum	Fácil	Moderado
Configuração Incorreta de Segurança	Fácil	Comum	Fácil	Moderado
Exposição de Dados Sensíveis	Difícil	Rara	Média	Severo
Falta de Função para Controle de Nível de Acesso	Fácil	Comum	Média	Moderado
Cross-Site Request Forgery (CSRF)	Média	Comum	Fácil	Moderado
Utilização de Componentes Vulneráveis Conhecidos	Média	Generalizada	Difícil	Moderado
Redirecionamentos e Encaminhados Inválidos	Média	Rara	Fácil	Moderado

Fonte: OWASP Top 10 9 (2013).

O estudo do OWASP Top 10 2013 permitiu-nos concluir que a ordem apresentada na Tabela 7 está vinculada à quantidade de aplicações Web que apresentaram estar vulneráveis às ameaças, porque o foco do documento é a identificação dos riscos vinculado a uma gama de organizações distintas no tocante ao negócio. Por isso é necessário, a fim de adequar à gestão de riscos de segurança da informação proposto pela norma ABNT 27005:2011, empreender uma análise no âmbito qualitativo. Para a análise de riscos qualitativa, deve-se levar em consideração o envolvimento dos fatores de magnitude do impacto e probabilidade de ocorrência, a partir dos atributos de vetores de ataque: prevalência da vulnerabilidade; detecção da vulnerabilidade e impactos técnicos.

Como estratégia para apresentar as ameaças classificadas a partir da análise qualitativa preconizada pela norma ABNT 27005:2011, substituiremos os termos apresentados na Tabela 7 (“Médio”, “Severo”, “Raro”, etc.) por valores compreendidos em uma escala entre 1 (um) a 4 (quatro), a partir das cores que representam a intensidade da ameaça em relação aos atributos do mapa conceitual de risco, seguindo o protocolo disposto na Tabela 8. Essa substituição será necessária para realização do cálculo do risco total. Na Tabela 9, é

apresentado o resultado dessa substituição, o que já permite estabelecer uma visão quantitativa com relação às ameaças.

Tabela 4 - Valoração das propriedades para avaliação dos riscos

Cor	Valoração
Roxa	4
Vermelha	3
Laranja	2
Amarela	1

Fonte: Autor deste trabalho (2016).

Tabela 5 – Tabela com atributos qualificadores valorados

Ameaça	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos
Injeção de código	3	2	2	3
Quebra de Autenticação e Gerenciamento de Sessão	2	3	2	3
Cross-Site Scripting (XSS)	2	4	3	2
Referência Insegura e Direta a Objetos	3	2	3	2
Configuração Incorreta de Segurança	3	2	3	2
Exposição de Dados Sensíveis	1	1	2	3
Falta de Função para Controle de Nível de Acesso	3	2	2	2
Cross-Site Request Forgery (CSRF)	2	2	3	2
Utilização de Componentes Vulneráveis Conhecidos	2	3	1	2
Redirecionamentos e Encaminhados Inválidos	2	1	3	2

Fonte: Autor deste trabalho **(2016).**

A partir da valoração dos atributos qualificadores com respectivas magnitudes referentes aos riscos é possível estabelecer uma visão qualitativa, conforme preconiza a norma ABNT 27005:2011, através de “uma escala que considere a magnitude das consequências

potenciais (impactos), juntamente com a probabilidade de ocorrerem (vetores de ataque, detecção da vulnerabilidade e prevalência da vulnerabilidade) ”.

Para definir uma escala que permita inferir a análise qualitativa dos riscos citados pelo relatório OWASP Top 10 2013, consideramos calcular o produto entre as questões probabilísticas (os vetores de ataques; a detecção e a prevalência da vulnerabilidade); como a magnitude das consequências (impactos técnicos).

A escolha pelo cálculo através da multiplicação se deu mediante a discussão no Capítulo 2 a respeito do Mapa Conceitual de Riscos (Seção 2.2), que define os riscos como sendo todas as rotas possíveis para se atacar. Assim sendo, conclui-se que cada atributo qualificador representa *“n”* vezes a possiblidade de se obter novo risco. Portanto, se temos dois atributos, teremos **“*x* . *y*”** possibilidades de riscos. Assim sendo, a escala para a análise qualitativa, a qual denominados de “Risco Total” e cujo resultado está apresentado na Tabela 10, é o resultado da seguinte equação:

RISCO TOTAL = VETORES DE ATAQUE * PREVALÊNCIA DA VULNERABILIDADE * DETECÇÃO DA VULNERABILIDADE * IMPACTOS TÉCNICOS

Tabela 6 - Cálculo do risco total

Ameaças	Vetores de Ataque	Prevalência da Vulnerabilidade	Detecção Vulnerabilidade	Impactos Técnicos	Risco Total
Injeção de código	3	2	2	3	36
Quebra de Autenticação e Gerenciamento de Sessão	2	3	2	3	36
Cross-Site Scripting (XSS)	2	4	3	2	48
Referência Insegura e Direta a Objetos	3	2	3	2	36
Configuração Incorreta de Segurança	3	2	3	2	36
Exposição de Dados Sensíveis	1	1	2	3	6
Falta de Função para Controle de Nível de Acesso	3	2	2	2	24
Cross-Site Request Forgery (CSRF)	2	2	3	2	24
Utilização de Componentes Vulneráveis Conhecidos	2	3	1	2	12
Redirecionamentos e Encaminhados Inválidos	2	1	3	2	12

Fonte: Autor deste trabalho (2016).

Baseado no risco total das ameaças, identificamos que, sob a visão qualitativa da gestão de riscos da segurança da informação com base na norma ABNT 27005:2011, a ordem de classificação para as ameaças mais críticas nas aplicações Web está apresentada na Tabela 11.

Conforme preconiza a norma ABNT 27005:2011, a ordem das ameaças definidas no método qualitativo é o instrumento de entrada para a determinação de nível de risco, porque estabelece uma condição de identificar e conhecer os riscos a partir da magnitude dos impactos gerados, caso o atacante tenha êxito na implementação da sua estratégia.

Tabela 7 – Classificação dos riscos pelo cálculo do risco total

Ranking	Risco Total	Ameaça
A1	48	Cross-Site Scripting (XSS)
A2	36	Injeção de código Quebra de Autenticação e Gerenciamento de Sessão Referência Insegura e Direta a Objetos
A3	24	Configuração Incorreta de Segurança Falta de Função para Controle de Nível de Acesso Cross-Site Request Forgery (CSRF)
A4	12	Utilização de Componentes Vulneráveis Conhecidos Redirecionamentos e Encaminhados Inválidos
A5	6	Exposição de Dados Sensíveis

Fonte: Autor deste trabalho (2016).

4.2.3 Avaliação das Consequências

A avaliação das consequências pode ser determinada a partir de uma análise do impacto técnico ou ao negócio (ABNT 27005, 2011). A Tabela 12 apresenta os impactos técnicos gerados pelo incidente de segurança, de acordo com o documento OWASP Top 10 2013. Observa-se um cenário para a segurança da informação que pode ser considerado preocupante, pois em nenhum caso este atributo classificatório possui o indicador que represente um prejuízo para a aplicação ou ao negócio de menor expressão; pelo contrário, os impactos classificados como “Moderado” (laranja) são em 70% dos riscos, e 30% como “Severo” (vermelho).

Tabela 8 - Avaliação das consequências

Impactos Técnicos	Frequência	%
Moderado	7	70
Severo	3	30
Total geral	**10**	**100**

Fonte: Autor deste trabalho (2016).

Nos três casos cujo impacto foi classificado como “Severo”, a partir da análise das ameaças apresentadas pelo OWASP Top 10 2013 (Tabela 7), um deles apresenta-se como uma ameaça difícil de ser aplicado (ataques a criptografia), o que permite concluir que a criptografia representa um mecanismo de segurança com nível elevado para a proteção da

segurança da informação. Porém, convém a atenção na definição adequada, por exemplo, na definição do tipo de chave e algoritmo de criptografia, confirmo explica Burnet e Paine (2003).

O incidente de segurança a partir da ameaça XSS, que obteve o maior risco total na análise qualitativa, é uma das sete ameaças que geram um impacto moderado. A ameaça "Quebra de Autenticação e Gerenciamento de Sessão" aparece na segunda colocação tanto no documento OWASP Top 10 2013, como pelo cálculo do risco total.

Merece destaque o risco que ocupa o primeiro lugar no ranking do OWASP Top 10 2013 ("Injeção de Código"), e que imputa riscos técnicos também classificados como "Severo" e de fácil exploração pelo atacante (vetores de ataque). Entendemos que negligenciar um mecanismo de segurança para essa ameaça, imputa à aplicação Web um baixo nível de proteção para a informação.

4.3 AVALIAÇÃO DOS RISCOS

Convém ressaltar que os critérios de avaliação de riscos utilizados na tomada de decisões sejam consistentes com o contexto definido, externo ou interno, relativo à gestão de riscos de segurança da informação, e levem em conta os objetivos da organização (ABNT 27005:2011).

A Tabela 14 apresenta a lista de ameaças as aplicações Web que leva em consideração, inicialmente, as ameaças que têm maior nível de impacto; ou seja, primeiro as ameaças com nível classificado como "Severo" e, posteriormente, "Moderado". Após essa primeira classificação, as ameaças são listadas com base no "Risco Total" (Tabela 11), definindo uma nova ordem de prioridades para implementação de mecanismos de segurança para a aplicação Web.

Portanto, entendemos que os esforços para alcançar níveis mais elevados de segurança para as aplicações Web devem ser empreendidos na implementação de contramedidas contra as ameaças classificadas com base na Tabela 14. Como utilizamos uma norma voltada à gestão da segurança da informação, e como a informação é definida como uma base fundamental para os negócios, entendemos que a proposta de classificação definida promove um melhor alinhamento da equipe de engenharia de software com o negócio da empresa.

Tabela 9 - Avaliação dos riscos

Ranking	Nível de Impacto	Risco Total	Ameaça
01	Severo	48	Cross-Site Scripting (XSS)
02		36	Injeção de código
03		6	Exposição de Dados Sensíveis
04			Quebra de Autenticação e Gerenciamento de Sessão
05		36	Referência Insegura e Direta a Objetos
06			Configuração Incorreta de Segurança
07	Moderado	24	Falta de Função para Controle de Nível de Acesso
08			Cross-Site Request Forgery (CSRF)
09			Utilização de Componentes Vulneráveis Conhecidos
10		12	Redirecionamentos e Encaminhados Inválidos

Fonte: Autor deste trabalho (2016).

4.4 CONSIDERAÇÕES FINAIS

Neste capítulo foi discutida a implementação da gestão de riscos de segurança da informação, com base na norma ABNT 27005:2011, nas ameaças mais críticas encontradas em aplicações Web definidos pelo OWASP Top 10 2013.

A implementação da gestão de riscos discutida neste capítulo contribui para ratificar a importância, já apresentada pela literatura, no tocante a importância de uma gestão de riscos para a gestão da segurança da informação. Essa análise permite avaliar a maturidade quanto a ação das ameaças, o que torna-se relevante para a proposição de contramedidas eficazes de proteção, que compõem o *framework* a ser proposto.

Também foi possível evidenciar que o uso da norma ABNT 27005:2011 é adequado para o intuito de empreender uma gestão de riscos com ênfase na gestão da segurança da informação. Como resultado da gestão de riscos de segurança da informação, classificou-se o risco pela sua ameaça no âmbito qualitativo pelo “Risco Total” (Tabela 11) e pelo “Nível de Impacto” (Tabela 14), sendo esta última com ênfase na ameaça propiciada a segurança da informação.

Percebe-se que o *ranking* da abordagem qualitativa e quantitativa apresenta algumas diferenças, mas com poucas variações, conforme observa-se na Tabela 15. Destaque maior ocorre quando há ênfase do nível de riscos vinculado à segurança da informação, uma vez que

a ameaça “Exposição de Dados Sensíveis” é elevada como a ameaça de maior impacto para o negócio, mediante a preponderante importância da informação para qualquer empresa.

Tabela 10 - Comparativo entre a análise de risco qualitativa e quantitativa

Ameaças	Análise de Riscos Quantitativa	Análise de Riscos Qualitativa Risco Total	Análise de Riscos Qualitativa Nível de Impacto
Injeção de código	A1	A2	A2
Quebra de Autenticação e Gerenciamento de Sessão	A2	A3	A4
Cross-Site Scripting (XSS)	A3	A1	A1
Referência Insegura e Direta a Objetos	A4	A4	A5
Configuração Incorreta de Segurança	A5	A5	A6
Exposição de Dados Sensíveis	A6	A10	A3
Falta de Função para Controle de Nível de Acesso	A7	A6	A7
Cross-Site Request Forgery (CSRF)	A8	A7	A8
Utilização de Componentes Vulneráveis Conhecidos	A9	A8	A9
Redirecionamentos e Encaminhados Inválidos	A10	A9	A10

Fonte: Autor deste trabalho (2016).

O comparativo apresentado através da Tabela 15 é importante no intuito em se estabelecer as prioridades de defesa, ou seja, onde deve-se empreender maior esforço no que se refere à implantação de contramedidas de segurança eficazes, cuja ênfase é na segurança da informação. Vale reiterar a discussão que, a partir da visão holística dos riscos, eles podem vir de diferentes formas e variados métodos, o que sugere que não se consegue ou é muito difícil gerir todos eles.

Em prol de apoiar o desenvolvimento de aplicações Web, no próximo capítulo, faremos a proposta do *framework* de gestão da segurança da informação contra os riscos que expõem as aplicações Web a situações de insegurança, a fim de apresentar processos e atividades para explorar e integrar os mecanismos de segurança da informação para alcançar níveis mais elevados de proteção à informação.

5 FRAMEWORK DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Este capítulo é dedicado a apresentar e discutir a proposta do *framework* de gestão da segurança da informação, com o objetivo de contribuir para que profissionais da engenharia de software possam alcançar índices mais elevados de segurança da informação no desenvolvimento de aplicações Web.

A exposição das contramedidas de segurança da informação será dividida entre os mecanismos de segurança disponíveis para proteção à informação. Portanto, cada mecanismo de segurança será discutido em uma seção específica, quando será feita correlação entre mecanismos de segurança e respectivos riscos que podem ser dirimidos ou mitigados.

É importante reiterar que a aplicabilidade do *framework* pode ser estendida a equipes de analistas de sistemas e programadores em geral, ou seja, não somente a aplicação Web, uma vez que a gestão da segurança da informação abstrai a questão tecnológica. Contudo, convém levantar as questões específicas ou adaptações, oriundas do paradigma ou linguagem de programação utilizados, bem como os protocolos de comunicação.

5.1 VISÃO GERAL FRAMEWORK DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Com base na discussão conceitual do Capítulo 2, sabemos que a gestão da segurança da informação tem o compromisso de provê à informação três elementos básicos que formam a tríade da segurança da informação. A tríade da segurança da informação, conforme discutido no Capítulo 2 é composto pela:

a) Confidencialidade
b) Integridade
c) Disponibilidade

Para alcançar os atributos alusivos à segurança da informação, devem ser implementados nas aplicações mecanismos de segurança. Estes mecanismos podem ser utilizados individual ou em conjunto, sendo a segunda opção o modo de alcançar índices mais elevados de proteção (SÊMOLA, 2003). Portanto, para a gestão da segurança da informação, os mecanismos de segurança servem de contramedida aos riscos que atualmente envolvem as aplicações Web. Os mecanismos de segurança já discutidos são:

a) Criptografia
b) Assinatura Digital
c) Controle de Acesso
d) Certificado Digital

Na Figura 4 temos a visão geral do *framework* de gestão de segurança da informação proposto, o qual será discutido nas seções seguintes.

Figura 1 – Framework de Gestão Segurança da Informação: Confidencialidade, Integridade e Disponibilidade

Fonte: Autor deste trabalho (2016).

Correlacionando os mecanismos de segurança e os processos do *framework*, temos:

1. Criptografia

   a. Gestão de Chaves de Criptografia. As chaves de criptografia detêm reiterada relevância no processo para proteção da informação, e que são mais fáceis de serem conseguidas do que alcançar o êxito na promoção de ataques ao algoritmo de criptografia. Portanto, a escolha, atualização e uso das chaves de criptografia deve receber processo específico.
   b. Escolha de Algoritmos de Criptografia. Os algoritmos de criptografia são públicos e, após ação de ataques que consiga destituir sua prevalência quanto a segurança, têm suas fragilidades largamente divulgadas. Convém que a escolha esteja pautada em processo que envolva pesquisa na literatura específica, e avaliação.

2. Assinatura e Certificado Digital
   a. Seleção de recursos de Integridade da Informação. Mediante sua contribuição na segurança da informação serem especificas e distintas, o uso de assinatura e certificado digital exige um conhecimento sobre como eles apoiam na proteção da informação, e qual a informação deve ser protegida (i.e., o autor e/ou o teor da informação).
3. Controle de Acesso
   a. Auditoria e Gestão do Controle de Acesso. Além de proteção à informação, a devida identificação e controle da liberdade de ação que os usuários detêm, bem como o registro do que, quando e por quem foi realizado, exigem o armazenamento de dados que permitam a auditoria aos sistemas de informação, bem como a definição de processos que evitem fraudes ou erros que permitam ao não-autorizado o acesso ou inferência à informação.

Adicionalmente, são propostos ao *framework* processos que (a) fazem vínculo a proteção a nível de protocolo de comunicação, através do processo “Escolha dos Protocolos de Comunicação”; (b) estão relacionados a capacitação da equipe da engenharia de software, o qual é o processo denominado de “Plano de Capacitação à Equipe”; (c) compreende a manutenção de um plano de melhoria contínuo, visto principalmente da inovação tecnológica que propicia métodos e técnicas de implementação dos mecanismos de modo mais aperfeiçoado (“Identificar Melhorias”); e (d) deve ser institucionalizado um comitê gestor de segurança da informação, o qual segue os requisitos da norma ABNT ISO/IEC 27002:2011, que estabelece a necessidade de existir uma equipe responsável em capitanear as ações

alusivas à segurança da informação. O comitê gestor é um elemento fundamental para a gestão da segurança, pode ser substituído por algum outro órgão que a empresa já tenha, o qual disponha de desígnios semelhantes ao que será caracterizado e discutido neste capítulo.

A seguir, discutiremos cada uma das atividades as quais propomos em cada um dos processos do *framework* de gestão de segurança da informação para a implementação de aplicações Web.

5.2 CRIPTOGRAFIA

Para dirimir ou mitigar os riscos oriundos da "Exposição de Dados Sensíveis", a premissa mais fundamental de contramedida é a utilização da criptografia. A imperícia ou negligência ao correto uso da criptografia implica ao atacante total condição de ter acesso a toda informação manipulada ou intercambiada na aplicação Web. Certamente tal situação é altamente indesejada – por isso se trata da ameaça com maior nível de risco (ilustrada na Tabela 15) identificada na gestão de risco apresentada no Capítulo 4, e que sugere que deve-se iniciar explorando as etapas do *framework* que possam ser contramedidas de segurança da informação.

Inicialmente qualquer linguagem ou tecnologia de desenvolvimento de aplicações Web sem especificação formal ou suporte a criptografia torna-se imprópria para manipular ou intercambiar dados sensíveis; com isso, deve ser desconsiderada. Contudo, o simples uso da criptografia não representa a contramedida definitiva para dirimir o risco da "Exposição de Dados Sensíveis", porque a imperícia na definição dos requisitos alusivos à criptografia (algoritmos e chaves de criptografia) também promovem vulnerabilidades.

É comum que as linguagens de programação disponibilizem pacotes vinculados à segurança pela criptografia, tanto simétrica como assimétrica. Porém, convém ressaltar que as utilizações desses pacotes também representam outras ameaças, por exemplo, a "Configuração Incorreta de Segurança" e "Utilização de Componentes Vulneráveis Conhecidos", os quais constam no documento OWASP Top 10 2013. Convém não apenas utilizar esses pacotes, mas também avaliar sua especificação.

Normalmente os atacantes não buscam investir contra os algoritmos da criptografia, inclusive, eles são de domínio público, uma vez que há questões vinculadas ao tempo de processamento necessário para decifrar uma mensagem criptografada. Também não é

aconselhável realizar implementações particulares de criptografia, porque dificilmente se alcançará o nível de proteção promovido pelos principais algoritmos atualmente existentes (e.g., RSA e AES). Os algoritmos de domínio público dispõem de maturidade suficiente no âmbito da proteção aos dados, formado a partir da experiência adquirida por profissionais e métodos científicos de criptografia.

No que concerne a criptografia, o elo mais fraco para obtenção de dados é tentar roubar as chaves utilizadas na criptografia. Entretanto, os avanços tecnológicos impõem um aumento considerável no tamanho das chaves criptográficas para que se mantenha um nível de segurança adequado, resultando efeitos indesejáveis em tempo de processamento, largura de banda e armazenamento.

Apoiados pelo que sugere a norma ABNT 27002:2013, o *framework* propõe estabelecer uma política de controle criptográfico, cuja responsabilidade é da empresa, através do comitê gestor da segurança da informação, em discutir e definir as especificações sobre algoritmos e a política das chaves de criptografia. Ou seja, as escolhas quanto ao algoritmo a ser utilizado; ou o pacote de criptografia que será adotado; ou o próprio algoritmo criptográfico, serão instituídos pelo comitê gestor de segurança da informação. Caso seja observado inexperiência necessária para realizar tal processo com o apoio da equipe da engenharia de software, convém obter suporte de um especialista externo para avaliar a decisão tomada.

Assim como ocorrerá com os demais processos a serem discutidos nas seções seguintes deste capítulo, todo o portfólio gerado através dos processos de “Gestão de Chaves de Criptografia” e “Escolha de Algoritmos de Criptografia” devem ser integrados aos processos de “Plano de Capacitação à Equipe” e “Identificação Melhorias”.

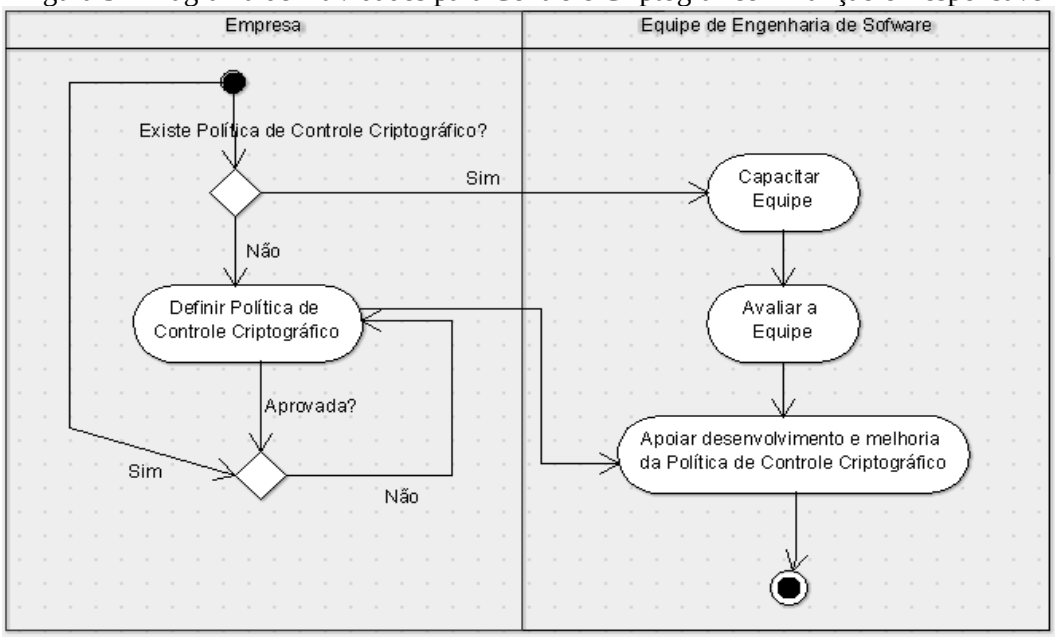
Essa etapa do *framework* visa definir a política da empresa em explorar a criptografia para subsidiar o desenvolvimento de aplicações Web no pilar da confidencialidade da informação. Na Figura 5, temos uma representação da proposta referente ao processo de controle criptográfico do *framework* de gestão da segurança da informação.

Figura 2 - Framework da Segurança da Informação: Controle Criptográfico

Fonte: Autor deste trabalho (2016).

A Figura 6 ilustra um conjunto de atividades que podem ser empreendidas, a fim de contemplar o processo de controle criptográfico.

Figura 3 - Diagrama de Atividades para Controle Criptográfico – Função e Responsável



Fonte: Autor deste trabalho (2016).

A empresa não deve deixar para o programador a decisão quanto ao algoritmo de chave de criptografia a ser utilizado. Cabe a ela (empresa) institucionalizar a política de controle criptográfico, manter e cobrar que ela seja aplicada aos seus produtos da engenharia de software (as aplicações Web) que sejam desenvolvidos. Convém que sejam registrados e

arquivados registros do planejamento e realização de todas as atividades, e que tenham sempre responsáveis por cada uma delas.

Para o controle criptográfico as atividades a serem empreendidas, ilustradas na Figura 6, possuem o seguinte sequenciamento e funções:

1. Definir Política de Controle Criptográfico – Na segurança da informação, a política é essencial e primordial para a institucionalização de medidas, para isso é necessário inicialmente verifica-se se há políticas de controle criptográfico; caso contrário, deve-se empreender esforços para defini-la.
2. Uma vez existente e/ou aprovada a política de controle criptográfico, deve ser promovida a capacitação da equipe de engenharia de software na referida política.
3. Ao término da capacitação, deve ser aplicada uma avaliação da equipe capacitada.
4. Deve-se ter previsto na própria "Política de Controle Criptográfico" a sua periódica atualização, e o(s) responsável(eis) por essa ação. Este é o objetivo da etapa "Apoiar desenvolvimento e melhoria da Política de Controle Criptográfico".

5.3 ASSINATURA DIGITAL

A criptografia atua como recurso de confidencialidade à informação, mas é preciso também atender aos demais pilares da segurança da informação: integridade e disponibilidade. Conforme estabelece a norma 27005:2011, requisitos de integridade de mensagens em aplicações devem ser identificados e controles apropriados identificados e implementados. A norma ABNT 27002:2013 esclarece que precisa ser considerada toda a legislação relevante ao uso da assinatura digital, em particular àquela que descreve as condições sob as quais é legalmente aceita.

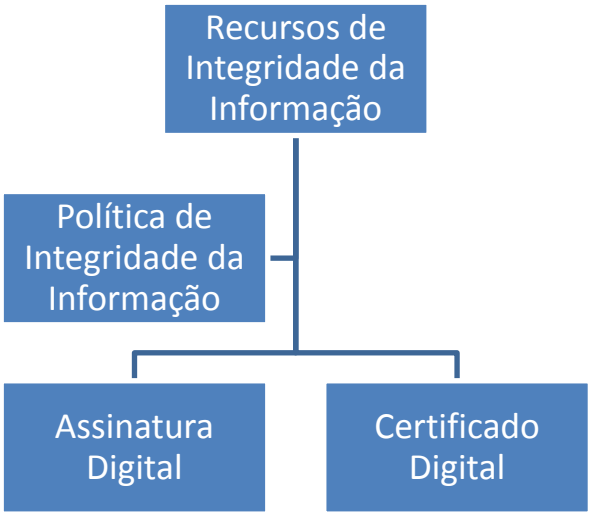
Para elevar o nível de segurança de uma aplicação Web, a assinatura digital é atualmente um recurso que pode contribuir na garantia da integridade da informação, além também da autoria do documento que está sendo compartilhado e explorado pela aplicação Web. A criptografia protege o teor da mensagem e a assinatura protege toda a mensagem, identificando se houve alguma alteração não autorizada, por exemplo. Adicionalmente, em detrimento ao foco potencial do ataque contra a chave de criptografia, convém identificar recursos da segurança da informação que proteja a chave de criptografia, ou, ao menos

permita identificar possíveis alterações no teor da mensagem (criptografado ou não). Tal proteção não se consegue com a criptografia.

Além de elevar o nível de segurança da informação apoiando a criptografia, os recursos de integridade podem ser utilizados para validação dos dados que estão sendo recebidos pelo serviço da aplicação Web. Portanto, pode-se empreender esforços para dirimir ou mitigar ameaças como, por exemplo, “Injeção de código”, “XSS”, “CSRF”, uma vez que pode validar se houve alteração no código que corresponde à requisição que deve ser respondida.

Portanto, ao *framework* de gestão da segurança da informação, propomos incluir o processo “Recursos de Integridade da Informação”, com as atividades que estão representadas através da Figura 7.

Figura 4 – Processo de Integridade da Informação



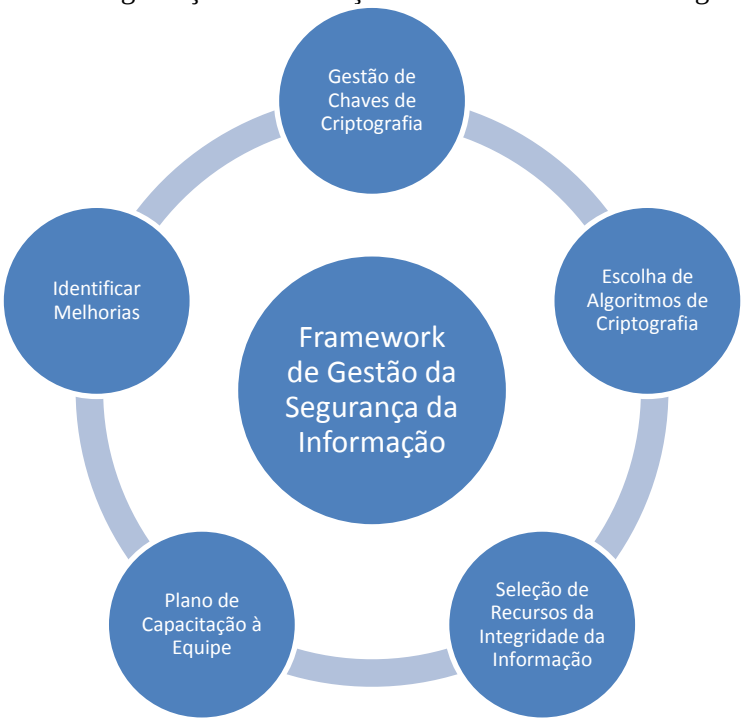
Fonte: Autor deste trabalho (2016).

No âmbito dos recursos da integridade da informação, podem ser adotadas duas técnicas: chaves públicas ou de chaves secretas. Pela técnica de chave pública a solução com ampla utilização é o certificado digital, o qual será discutido na próxima seção deste capítulo. Quanto a técnica de chaves secretas, a empresa deve incluir na política de controle criptográfico quais as estratégias serão adotadas e qual o algoritmo de assinatura digital a ser utilizado (e.g. SHA, MD5). Assim como proposto na gestão de controle criptográfico, cabe a empresa institucionalizar o uso dos recursos de integridade da informação através da definição da política de integridade da informação.

Uma vez que a mensagem a ser enviada para o destinatário já conta com o resultado do processo de controle criptográfico, é possível elevar o nível de proteção através dos recursos de integridade da informação, visto que ambos os processos são complementares. Por exemplo, realizar a criptografia da mensagem (confidencialidade), e assinar digitalmente o texto criptografado, a fim validar a integridade da mensagem ao término do intercâmbio da informação entre emissor e receptor.

Portanto, adicionamos ao *framework*, conforme mostra a Figura 8, o processo de recursos de integridade da informação, contemplando os pilares de confidencialidade (criptografia) e integridade (assinatura digital) da segurança da informação.

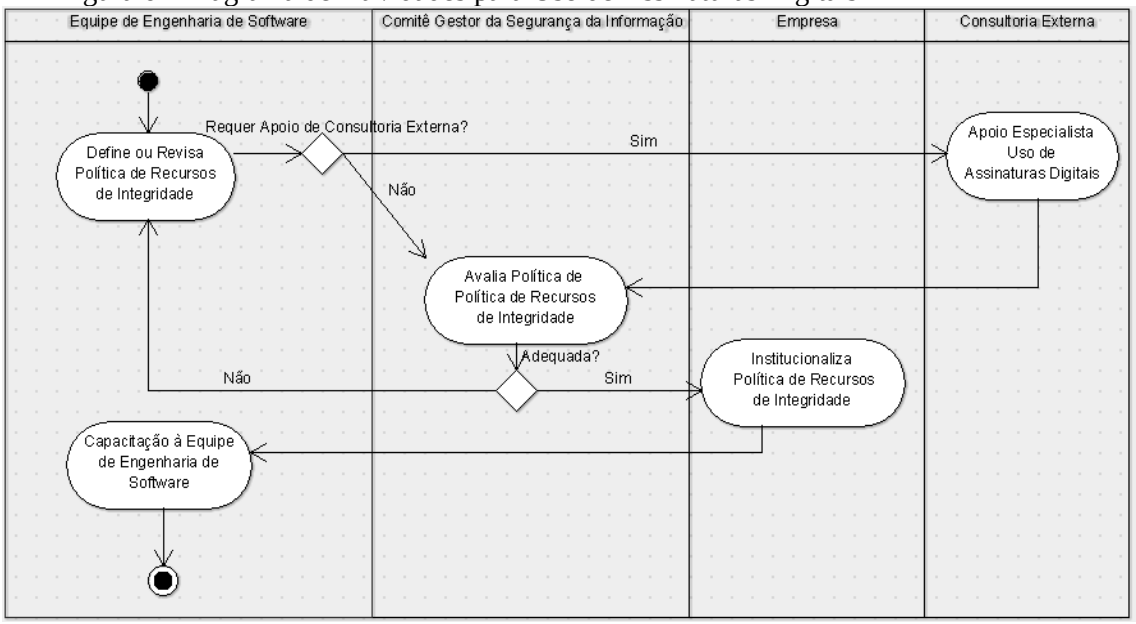
Figura 5 - Framework da Segurança da Informação: Confidencialidade e Integridade



Fonte: Autor deste trabalho (2016).

As definições alusivas a assinatura digital, de igual modo ao que discutimos sobre a criptografia, não devem ficar exclusivamente a cargo dos programadores, mas sim discutidos e analisados por toda a equipe de engenharia de software. Sendo necessário, poder ser utilizado algum serviço de consultoria externa sobre o assunto, a fim de que a política de recursos de integridade da informação possa ser suficientemente capaz de propiciar a segurança da informação requerida para aplicações Web que manipulam ou que fazem intercâmbio de dados confidenciais e sigilosos.

Figura 6 - Diagrama de Atividades para Uso de Assinaturas Digitais



Fonte: Autor deste trabalho (2016).

Referente ao processo de "Seleção de Recursos de Integridade", no âmbito da assinatura propõe-se que sejam empreendidas as seguintes atividades, ilustradas na Figura 9:

a) Definição ou revisão da Política de Recursos de Integridade.
b) Caso seja necessário, deve buscar apoio especialista sobre o uso de assinaturas digitais.
c) Encaminhar a Política de Recursos de Integridade para avaliação do comitê gestor da segurança da informação.
d) Sendo avaliada como adequada, a Empresa institucionaliza a Política de Recursos de Integridade.
e) De posse da Política de Recursos de Integridade, cabe a equipe de engenharia de software promover a capacitação para todos os membros envolvidos no desenvolvimento de aplicações Web.

Durante a revisão da literatura referente a assinatura digital, foi identificado que diversos órgãos governamentais brasileiros utilizam a assinatura digital para a verificação da integridade de documentos intercambiados eletronicamente através da Internet. Exemplos são a Advocacia Geral da União e do Tribunal de Contas da União. Ambos, em publicações internas[12]-[13], explicam o apoio da assinatura digital como sendo indispensável para atuação jurídica e de auditoria dos seus membros e auditores. Merece destaque que nos referidos

[12] Manual de Boas Práticas Consultivas. Fonte: Advocacia Geral da União.
[13] Boas Práticas de Segurança da Informação. Fonte: Tribunal de Contas da União.

órgãos, existe um setor vinculado à Governança da Tecnologia da Informação para atuar na definição das políticas de como explorar recursos da segurança informação.

Portanto, com a constatação que órgãos não vinculados a tecnologia da informação empreendem esforços para formação de equipe que pensem e disseminem as práticas da segurança da informação, é pouco entendível ou injustificado que empresas que atuam com implementação de produtos de software, como aplicações Web, por exemplo, não tenham iniciativa e preocupação semelhantes. É preciso haver consciência de que as empresas almejam e precisam salvaguardar a informação. A política estabelecida no processo de "Recursos da Integridade da Informação" deve ser adicionada ao "Plano de Capacitação à Equipe" e à "Identificar Melhorias".

5.4 CERTIFICADO DIGITAL

Conforme ilustra a Figura 7, o uso de certificado digital deve estar contido no processo "Recursos da Integridade da Informação", porém a escolha da utilização do mecanismo de chaves públicas para a assinatura digital da mensagem a ser intercambiada deve seguir as definições especificadas no processo de "Gestão de Chaves de Criptografia", a qual está institucionalizada na "Política de Controle Criptográfico".

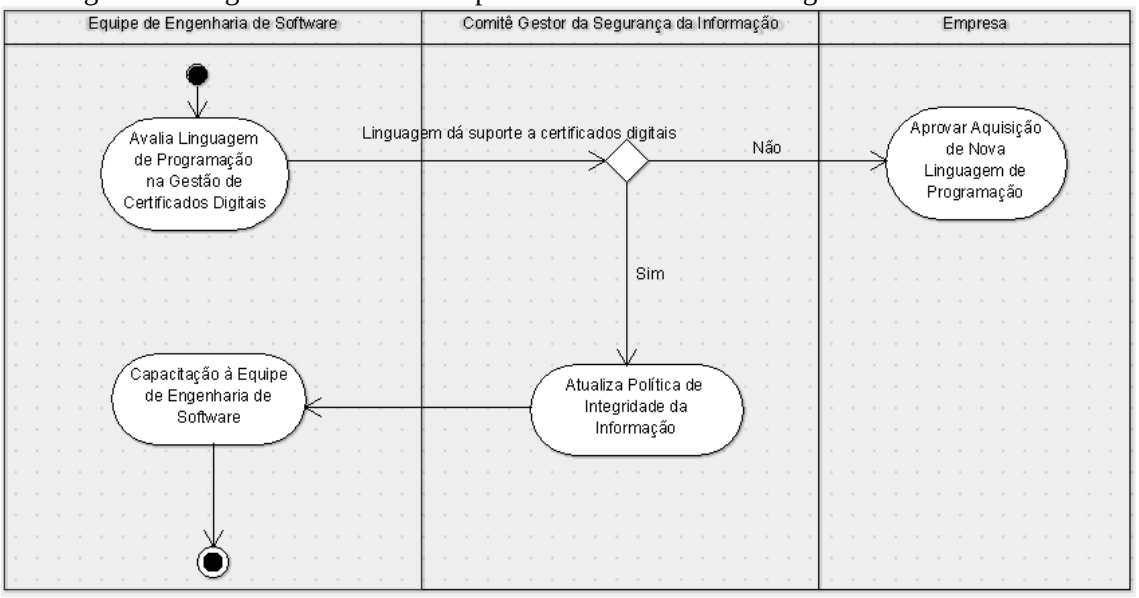
Explorar o uso do certificado digital está vinculado em garantir a autoria do conteúdo, ou seja, comprovar a quem recebe uma mensagem a identidade do emissor, a fim de que tenha garantia de que o conteúdo recebido seja daquele que o emitiu. Com o uso do certificado digital busca-se identificar seguramente pessoas, empresas, sistemas e informações no contexto do ambiente digital, apoiando na proteção às transações online e a troca virtual de documentos, que é um dos focos do desenvolvimento de aplicações Web, bem como também atualmente já provê validade jurídica.

O processo de certificado digital exige cuidados na gestão da emissão dos certificados, os quais podem ser tanto feito de maneira particular, como também através de uma infraestrutura de chave pública (ICP ou PKI – em inglês). A ICP atua como um terceiro elemento entre emissor e destinatário, cuja missão é promover a confiança através da garantia de certificar-se quem enviou o documento.

As etapas propostas para o processo de "Seleção de Recursos de Integridade", ilustradas na Figura 10, são:

a) Deve ser avaliada como a linguagem de programação utilizada para desenvolvimento de aplicações Web suporta a gestão de certificados digitais. Caso não ofereça recursos de certificados digitais, deve ser recomendada a modificação da linguagem de programação; para tanto, deve ser aprovado pela empresa, principalmente no que se refere a custos, por exemplo, licenciamento.
b) A partir da definição quanto a linguagem de programação, de como e quando serão utilizados os certificados digitais, cabe ao comitê gestor da segurança da informação atualizar a Política de Integridade da Informação.
c) Posteriormente, a equipe de engenharia de software deve promover a capacitação junto aos seus membros.

Figura 7 - Diagrama de Atividades para Uso de Certificados Digitais



Fonte: Autor deste trabalho (2016).

Convém salientar que fornecedores de linguagens de programação disponibilizam componentes que auxiliam no uso de assinatura e certificados digitais. No entanto, para dirimir o risco "Utilização de Componentes Vulneráveis Conhecidos", requer que a engenharia de software possua e avalie detalhes da implementação e gestão de certificados digitais do componente fornecido pela linguagem de programação. Essa avaliação do componente deve estar contida na "Política de Integridade da Informação", inclusive, anexado os detalhes disponibilizados pelo fornecedor da linguagem de programação. Sempre que houver a atualização da Política de Recursos de Integridade, dentre outras verificações, convém que seja verificado junto ao fornecedor as especificações sobre certificados digitais pelo componente a ser utilizado na implementação da aplicação Web.

5.5 CONTROLE DE ACESSO

A fim de promover a completude do *framework* no que concerne aos três pilares da segurança da informação, iremos discutir sobre a etapa que contempla o pilar da disponibilidade, que é o controle de acesso. De maneira genérica, entende-se que o controle de acesso deve reconhecer e disponibilizar ao usuário restritamente aquilo que lhe é de direito, através de uma gestão de perfil de usuário.

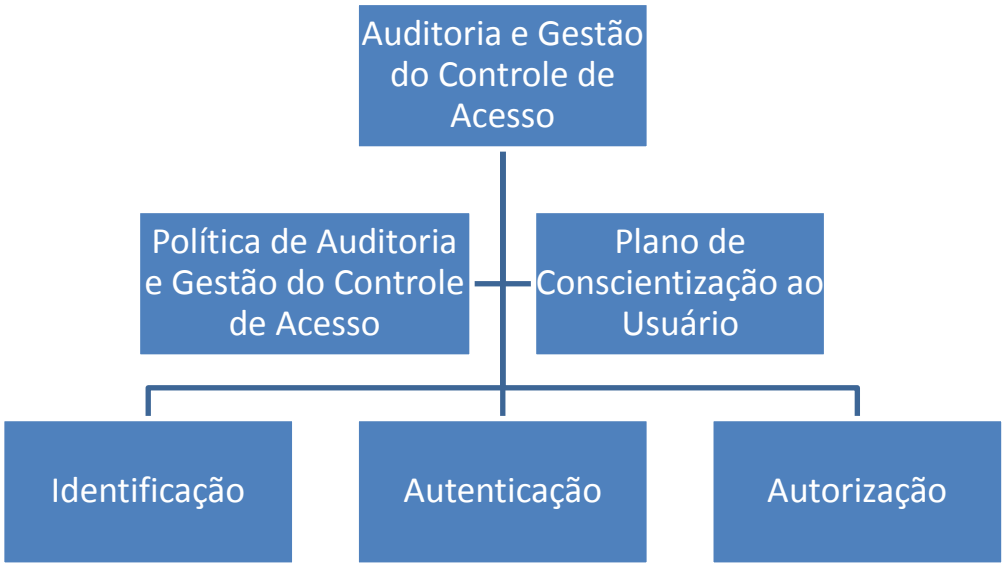
A partir do que identificamos através das pesquisas na revisão da literatura sobre o tema, existe uma motivação pela autenticação consolidada, também reconhecida como "única" em detrimento à diversidade de software que compõe a arquitetura de aplicações da empresa; o que requer a ação deliberativa constante do controle de acesso. Além do aspecto burocrático e repetitivo, temos o agravante em obrigar ao usuário ter quantidade significativa de credenciais de acesso (e.g. nome de usuário e senha).

Expor o usuário a um cenário burocrático para a concessão do seu respectivo e devido acesso devido pode ser entendido como uma ação contrária à disponibilidade. Portanto, é sensato desenvolver um método de autenticação integrado. Porém, convém que para ambientes operacionais que manipulem ou faça intercâmbio de informações confidenciais e sigilosas tenha nível seguridade elevado. Se a integração da autenticação representar um agravo ao nível de segurança da informação, deve ser requerida a implementação de nova autenticação à aplicação Web.

Duas ameaças são quantitativamente encontradas quanto a vulnerabilidades no controle de acesso: "Quebra de Autenticação e Gerenciamento de Sessão", que obteve o segundo posto na escala quantitativa do documento OWASP Top 10 2013, e "Falta de Função para Controle de Nível de Acesso" – na sétima posição do ranking.

No intuito de dirimir ou mitigar as ameaças oriundas à disponibilidade da informação, propomos o processo "Auditoria e Gestão do Controle de Acesso", conforme ilustrado na Figura 11. Neste processo, temos três atividades já comumente vinculadas ao controle de acesso: identificação, autenticação e autorização. Adicionalmente, por estarmos tratando de uma gestão da segurança da informação, compõem o processo: "Política de Auditoria e Gestão do Controle de Acesso"; e o "Plano de Conscientização ao Usuário". A seguir, faremos a discussão sobre essas etapas do Processo de Auditoria e Gestão do Controle de Acesso.

Figura 8 – Processo de Auditoria e Gestão do Controle de Acesso



Fonte: Autor deste trabalho (2016).

A identificação é a atividade de grande relevância para um sistema de informação, e.g. é imprescindível tornar o responsável pelo cadastro ciente da importância da sua adequada atuação no momento em que se inclua os registros dos usuários e seus respectivos perfis. Convém ter instituído na política de auditoria e gestão do controle de acesso a clara especificação de cada perfil de usuário, a fim de que a associação usuário/perfil seja sempre mais fidedigna possível. Torna-se frágil esforços em elevar o nível de segurança da informação no âmbito tecnológico, seja através de um controle criptográfico ou de recursos de integridade, se os usuários estão em perfis distintos àqueles que lhe devem ser conferidos, bem como se existe ou se permite o compartilhamento de senha.

Por compartilhamento de senha, convém estabelecer ao plano de conscientização do usuário ações que explique e recomende ao usuário se ter um nível maior de compreensão sobre a importância de não a compartilhar. Não somente por determinações punitivas, mas demonstrar a importância da atuação correta como contribuição para a seguridade do ambiente de manipulação ou intercâmbio de dados confidenciais e sigilosos. Também nesta política, reiteramos atenção para enfatizar a importância da informação para a empresa, e que cada usuário da aplicação Web torna-se um ativo, uma vez que detém credenciais que o habilita ao acesso à informação.

Ainda no tocante a identificação, é diferencial a definição de política de senhas que sejam dinâmicas, ou seja, que sejam solicitadas trocas com periodicidade, e que tenham

formatos que envolva letras (maiúsculas e minúsculas), números e caracteres especiais (e.g. $, !, %, &, etc.). Por exemplo, não instituir senha com tamanhos padronizados, mas sim flexibilizar entre número mínimo e máximo. Caso contrário, o atacante, a partir de um processo de observação, pode identificar qual a política adotada. Mais especificamente para as aplicações Web, convém que sejam auditadas a questão temporal das requisições que chegam ao servidor, a fim de minimizar a vulnerabilidade de ataques de diferentes fusos horários.

Reitera-se a necessidade em prever uma política de alteração de senha que contemple uma sistemática de informações que não sejam facilmente obtidas por pesquisas simples de dados pessoais, que atualmente são cada vez mais disponibilizados em larga escala na Web. Caso contrário, a ação do atacante será facilitada no seu intento mal-intencionado de acesso a aplicação Web, e obter acesso com privilégios do perfil do usuário que conseguiu alterar a senha. Como contramedida de segurança, convém a utilização de que a manutenção do cadastro envolva algum tipo de dado menos conhecido ou uma posterior confirmação.

Todas estas e outras ações realizadas para a atividade de identificação devem ser auditadas periodicamente. Neste sentido, uma política de auditoria e gestão do controle de acesso contribui para instituir o plano de atuação da empresa em averiguar a devida adequação entre usuário e perfil; da verificação da política de senha – e de alteração; além do cumprimento do plano de conscientização do usuário. Convém que sejam estabelecidos os critérios e as métricas para cada uma das ações, a fim de se medir o nível de segurança da informação na atividade de identificação.

Na atividade de autenticação, cuja responsabilidade é específica da equipe de engenharia de software, deve-se obrigatoriamente fazer uso de protocolos de comunicação (e.g. VPN, SSL/TLS, IPSec, IPv6) que permita a proteção no âmbito da comunicação através da Internet, ou seja, que subsidiam proteção ao ambiente de trânsito da informação. Por isso, ao *framework* foi adicionado o processo “Escolha de Protocolos de Comunicação”, que será discutido na Seção 5.6.

Relacionado a atividade de autorização, entendemos que seu nível de segurança se apoia nas atividades de identificação e autenticação. Contudo, devemos ressaltar sobre a possibilidade da anomalia da aplicação Web, ou seja, em razão da ação do atacante em alterar indevidamente a codificação, a aplicação privilegiar ao usuário um perfil não autorizado, concedendo permissões de acesso e manipulação de informação confidencial e sigilosa superior ao que o usuário detém. Ademais a ameaça ser de procedência externa, deve-se

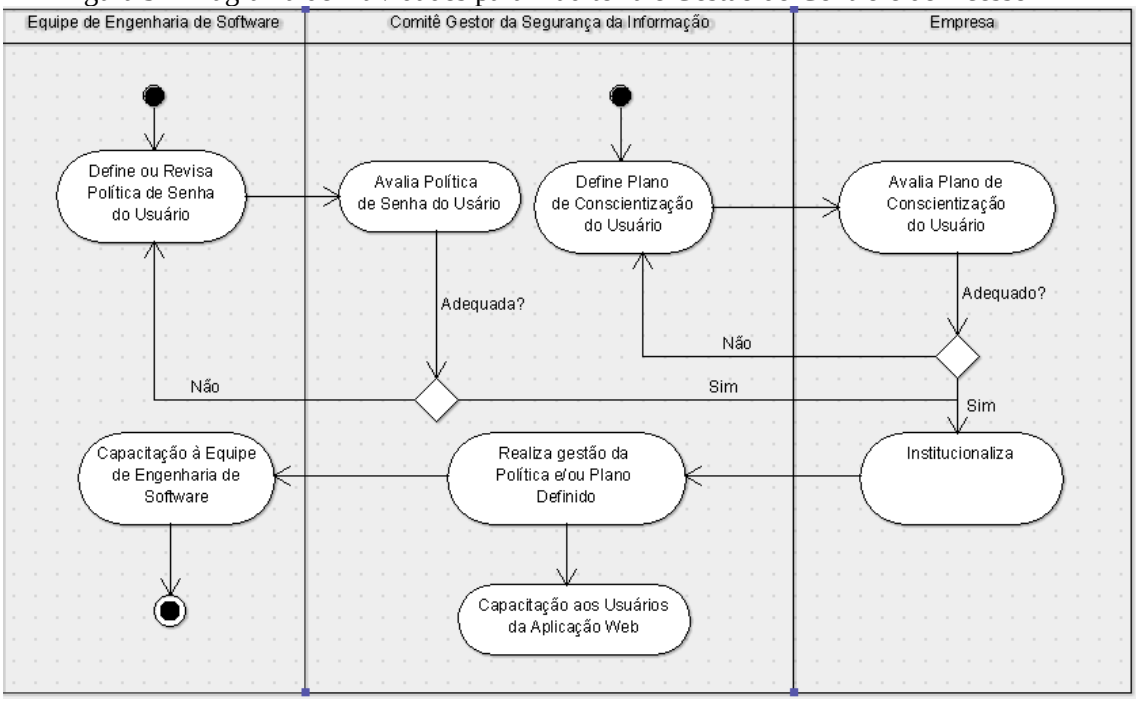
considerar o ataque interno, onde o vetor do ataque é um membro da própria equipe de engenharia de software. A dificuldade na prévia identificação de um ataque interno é um desafio para qualquer processo ou atividade vinculada a segurança da informação.

O ataque interno é motivado, dentre outros, por alguma insatisfação do profissional. Portanto, sugerimos atuar com o plano de conscientização do usuário, a fim de que possa estabelecer e fortalecer toda a equipe de engenharia de software sobre os valores esperados pelos seus membros, enquanto detentores de um perfil de acesso privilegiado. Convém também empreender um plano de registro para o acesso ao código fonte após a homologação da aplicação Web. Para fortalecer a política de auditoria e gestão de controle de acesso, entendemos que a empresa não pode negligenciar, ao contrário, é preciso ser transparente sobre a existência do ataque interno, e dos respectivos impactos gerados ao negócio; todavia, deve ser muito incisiva e não tolerar desvios de conduta de funcionários, independente do seu nível funcional ou hierarquia organizacional.

Conforme ilustra a Figura 12, as seguintes etapas são propostas para o processo de "Auditória e Gestão do Controle de Acesso":

a) A equipe de engenharia de software deve definir, ou revisar caso exista, a política de senha do usuário e submete ao comitê gestor da segurança da informação.
b) O comitê cabe iniciar o "Plano de Conscientização do Usuário" e, quando receber da equipe de engenharia de software, deve avaliar a "Política de Senha do Usuário".
c) A análise do "Plano de Conscientização" cabe a empresa.
d) Uma vez avaliados como adequados, a empresa institucionaliza o "Plano de Conscientização do Usuário" e a "Política de Senha do Usuário".
e) O comitê gestor deve realizar a gestão e aplicação do Plano e da Política institucionalizados, e promover a capacitação aos Usuários da Aplicação Web sobre a Política de Senha do Usuário e o Plano de Conscientização.
f) À equipe de engenharia de software, mediante a características mais técnica, cabe treinar seus membros sobre Política de Senha do Usuário e o Plano de Conscientização.

Figura 9 - Diagrama de Atividades para Auditoria e Gestão do Controle de Acesso



Fonte: Autor deste trabalho (2016).

Convém que o comitê gestor de segurança da informação apoie a capacitação da equipe de engenharia de software no âmbito da abordagem conceitual, deixando para o analista de sistema ou programador a etapa técnica. Recomenda-se que um membro da equipe de engenharia de software, principalmente quem esteja responsável pela elicitação de requisitos da aplicação Web, possa acompanhar o comitê gestor de segurança da informação na capacitação junto aos usuários. Entende-se que essa participação possa contribuir para que seja identificado o êxito da "Política de Senha do Usuário" e/ou "Plano de Conscientização do Usuário", ou até mesmo alguma lacuna que requer adições ou ajustes ao processo.

5.6 ESCOLHA DE PROTOCOLOS DE COMUNICAÇÃO

A comunicação através das redes de computadores exige a utilização de protocolos. É amplamente discutido na literatura que nem todo o protocolo de comunicação é adequado para o intercâmbio de informações seguras, o que impõe muita responsabilidade na escolha do protocolo a ser utilizado no meio de comunicação.

A atividade alusiva a "Escolha de Protocolos de Comunicação" envolve selecionar, a partir de características técnicas que sejam aderentes ao paradigma de desenvolvimento Web, protocolos de comunicação que atentam aos requisitos de segurança na comunicação através

da Internet. Com a expansão do e-commerce, por exemplo, é essencial que a aplicação Web possibilite seguridade também a nível de protocolos.

Apesar de esforços referentes ao aperfeiçoamento dos protocolos de comunicação no sentido de fornecer mecanismos de segurança, problemas com a utilização de protocolos de redes de computadores não seriam tão recorrentes, além de tantos outros tipos de ataques mencionados por pesquisas recentes (i.e., ataques de negação de serviço nas camadas físicas, enlace e de rede), conforme observamos em Borgohain et al (2015).

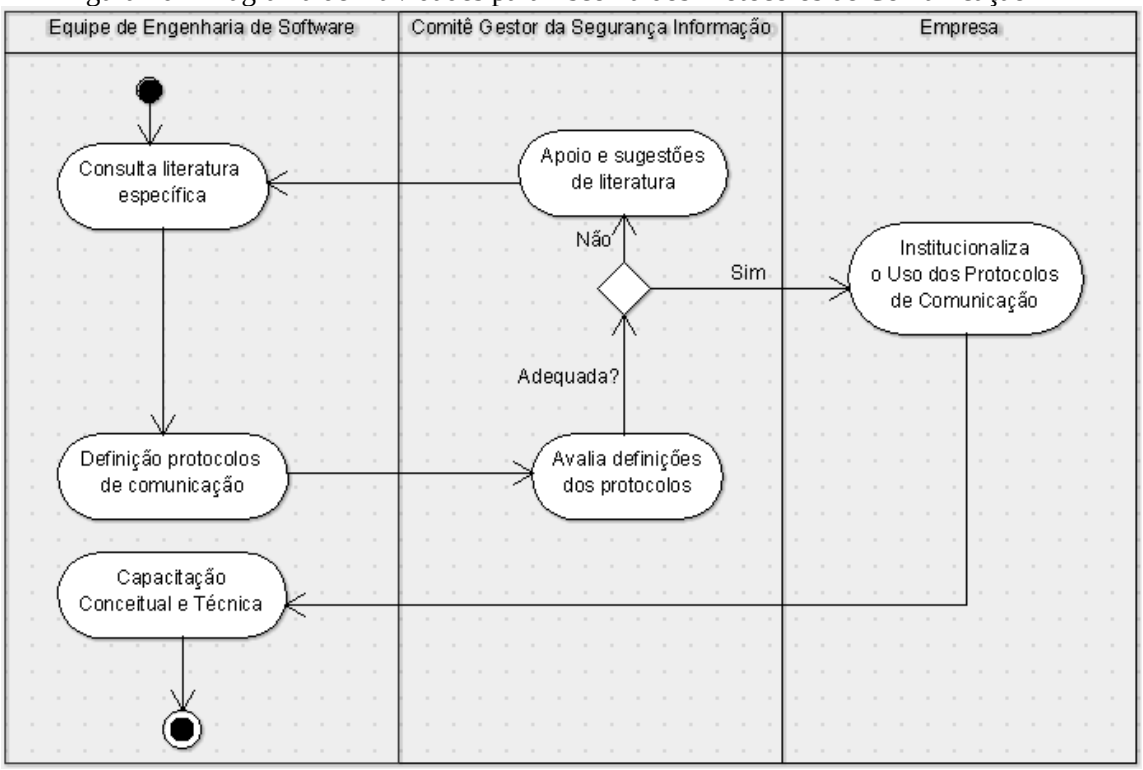
Mesmo com características técnicas, que não estão contidas em um *framework* de gestão, a ênfase pretendida é que a escolha seja através da consulta à literatura específica sobre opções com melhores avaliações de segurança. Semelhantemente aos processos discutidos nas seções anteriores, a proposta é que exista a participação do comitê gestor da segurança da informação juntamente com a equipe de engenharia de software para a escolha do(s) protocolo(s).

A Figura 13 mostra um diagrama de atividades proposto para o processo de "Escolha de Protocolos de Comunicação":

a) A equipe de engenharia de software deve empreender consulta a literatura específica, a qual trate sobre especificações de protocolos de comunicação.
b) A partir da análise da documentação, deve definir sobre o(s) protocolo(s) que será(ão) utilizado(s) na aplicação Web. Deve-se produzir então um documento que especifique e justifique a(s) escolha(s).
c) O comitê gestor de segurança da informação deve avaliar a(s) escolha(s) da equipe de engenharia de software. Caso não esteja adequada, o comitê gestor deve apoiar a equipe de engenharia de software na identificação e sugestões de novas fontes de informação e documentações alusivos aos protocolos de segurança.
d) Uma vez definido como adequado pelo comitê gestor de segurança da informação o documento que define e justifica a escolha do(s) protocolo(s) de comunicação, feito pela equipe de engenharia de software, a empresa deve institucionalizar o referido documento.
e) Cabe a equipe de engenharia de software, realizar a capacitação conceitual e técnica aos seus membros sobre a utilização do(s) protocolo(s) de comunicação. Caso seja necessário, a equipe de engenharia de software pode

solicitar o apoio e participação de um membro do comitê gestor de segurança da informação para a capacitação na etapa conceitual.

Figura 10 - Diagrama de Atividades para Escolha dos Protocolos de Comunicação



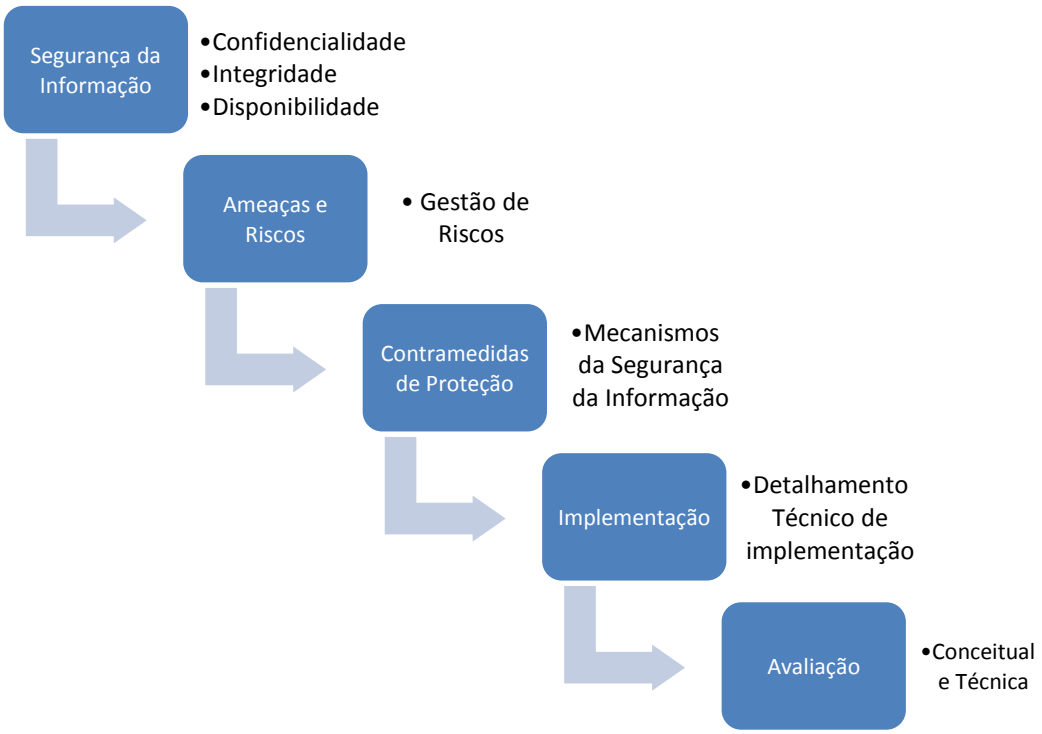
Fonte: Autor deste trabalho (2016).

5.7 PLANO DE CAPACITAÇÃO À EQUIPE

O processo “Plano de Capacitação à Equipe” tem relevante importância quanto tratamos sobre da gestão da segurança da informação, uma vez que a formação consciente do profissional é imprescindível para que tenhamos sucesso em implementações de aplicações Web mais seguras.

Conforme citado no capítulo da revisão da literatura (Capítulo 3), vários trabalhos faziam citações sobre a necessidade de capacitar os analistas de sistemas e programadores, e o *framework* proposto neste capítulo faz menção sempre a necessidade de capacitação. As etapas do plano de capacitação estão representadas na Figura 14 e serão discutidas a seguir. Adicionalmente às etapas, são sugeridos aos tópicos que devem citar citados quando da oferta de capacitações.

Figura 11 - Atividades do Plano de Capacitação à Equipe



Fonte: Autor deste trabalho (2016).

É proposto que a capacitação tenha sempre seu início com a apresentação através de uma abordagem conceitual e não técnica, que envolva: (a) os pilares da informação; (b) o resultado de uma gestão de risco; e (c) mecanismos de segurança da informação que serão utilizados para dirimir ou mitigar as ameaças que expõem a aplicação Web aos riscos. Entendemos que o amadurecimento conceitual propiciará que o entendimento técnico seja facilitado, isto porque o analista de sistema ou programador conhecerá a razão e a estratégica da contramedida de cada mecanismo da segurança da informação na aplicação Web.

Findo a primeira etapa, segue a abordagem técnica da capacitação, onde devem ser explicadas como explorar os mecanismos de segurança na linguagem que será utilizada para a implementação da aplicação Web. Portanto, a etapa de capacitação técnica ocorrerá posteriormente, de acordo com a linguagem e paradigma de desenvolvimento de software adotado. Na atividade de "Implementação" é que devem ser tratados os desígnios tecnicistas, incluindo todas as questões sobre como deve ser implementado e testado.

Todas as políticas (criptografia, integridade e controle de acesso) devem fazer parte do portfólio de capacitações a serem aplicadas aos profissionais da engenharia de software, inclusive, àqueles que estão ingressando na empresa ou à equipe recentemente; convém envolver também os terceirizados neste processo de capacitação.

5.8 CONSIDERAÇÕES FINAIS

Por estar livre de contexto tecnológico, e explorar os mecanismos de proteção atualmente existentes, o *framework* proposto pode ser aplicado a qualquer empresa que deseja a implementação de níveis de segurança em aplicações Web, atentando-se para adaptações necessárias a fim de atender as especificidades técnicas.

Entendemos que se a empresa e, principalmente, a equipe de engenharia de software estiver comprometida na implementação de todos os processos e atividades aqui apresentadas, conseguirá dirimir ou mitigar às ameaças que atualmente impõem às aplicações Web muitos riscos.

Percebemos que a ação coletiva entre os membros da equipe de engenharia de software, a qual é proposta nos processos do *framework*, representa uma contribuição relevante no âmbito de elevar o nível de segurança do produto de software. Em epígrafe, precisa haver uma colaboração dos profissionais envolvidos no projeto da aplicação Web; as regras devem estar claras, explicadas e institucionalizadas, coibindo ações individualizadas.

Também convém ressaltar que o *framework* envolve todos aqueles que detém acesso a aplicação Web, os quais são partícipes no plano de gestão da segurança da informação proposto; ou seja, não é exclusivo e/ou restrito a equipe da engenharia de software. Por isso, o *framework* é um plano para a empresa.

No próximo capítulo está discutido sobre o estudo de caso proposto, a fim de, dentre outras coisas, avaliar cobre o conhecimento em segurança da informação por parte de analistas de sistemas de programadores.

6 UMA AVALIAÇÃO SOBRE O CONHECIMENTO EM SEGURANÇA DA INFORMAÇÃO

Com o objetivo de arvorar a necessidade de se ter um *framework* para a gestão de segurança da informação, foi feita neste trabalho uma pesquisa de campo com profissionais de engenharia de software. A aplicação do questionário teve como objetivo aferir a aceitação, o conhecimento e o envolvimento dos profissionais sobre segurança da informação através de perguntas que permeiam palavras-chaves desta dissertação: segurança da informação, gestão de riscos e *framework*.

Para alcançar o objetivo proposto, incialmente buscou-se identificar empresas que atuam com desenvolvimento de software, em especial, com aplicações Web, privilegiando aquelas que desenvolvem para ambientes de intercâmbio e manipulação de informação confidencial e sigilosa.

Por razões vinculadas à sensibilidade da empresa em tratar sobre segurança da informação, sempre é um desafio que empresa e profissionais estejam disponíveis para responder questões que possam desencadear algum prejuízo de imagem para aqueles que vão responder ao questionário.

Dados da Associação de Processamento de Dados (ASSESPRO)[14] apontam que nove empresas associadas em Sergipe declaram que fazem desenvolvimento de sistemas com uma das suas principais atividades. Dentre estas, duas citam que desenvolvem soluções bancárias, inclusive com aplicações Web, as quais manipulam e fazem intercâmbio de informações sigilosas através de aplicações Web. Uma vez feitos os contatos com os profissionais com aderência ao perfil deste trabalho, estes correspondem a cinco empresas.

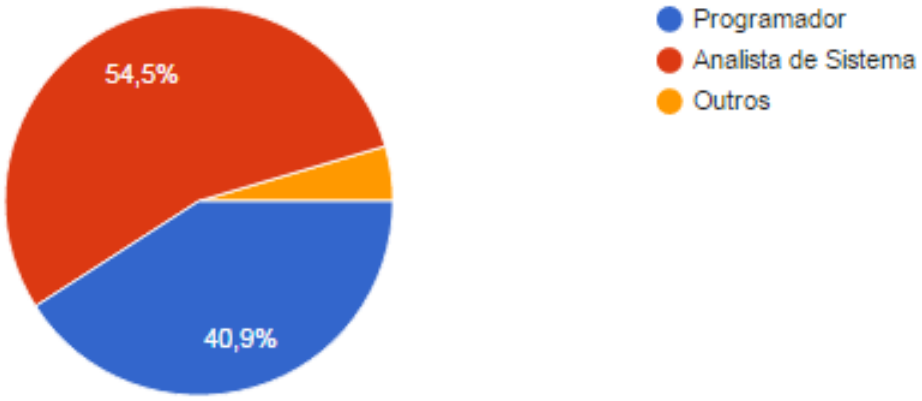
A aplicação de questionário (Anexo I) contendo 16 questões, sendo 15 questões objetivas e 1 aberta, foi através de recursos eletrônico, acessível pela Internet, e direcionado exclusivamente a profissionais da engenharia de software que estejam ou já tiveram oportunidade de desenvolver aplicações Web. De um grupo de 30 profissionais identificados com o perfil adequado para realização da pesquisa, vinte e dois (73%) realizaram a pesquisa.

[14] http://assespro.org.br/institucional/associados/sergipe/. Acesso em 20 de janeiro de 2018.

A seguir, apresentaremos as perguntas e a análise dos dados extraídos. Será utilizado gráfico em cada questão, permitindo melhor condição visual quanto ao perfil das respostas fornecidas pelos participantes.

Q1. Vinculado a engenharia de software, que função exerce(u)?

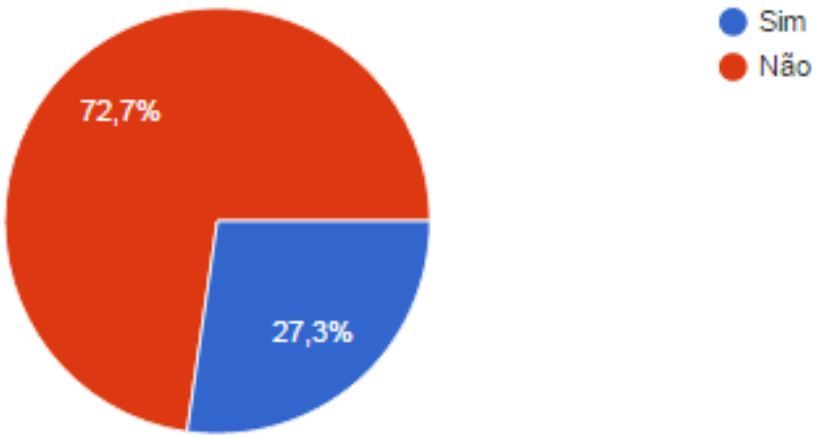
Gráfico 1 - Perfil dos participantes na pesquisa



Conforme visualizado no Gráfico 1, a maioria é analista de sistemas (54,5%), depois temos 40,9% que são programadores, e 4,5% (1 profissional) que é Arquiteto de Software – conforme discriminado pelo respondente. Conclui-se que o perfil dos participantes na pesquisa está adequado ao esperado, uma vez que a dissertação trata sobre aplicações Web; inclusive que demonstra maturidade dos profissionais que responderam ao questionário, visto que a maioria já é analista de sistemas.

Q2. Atua(ou) em função de Teste de Software?

Gráfico 2 – Percentual de profissionais que atua(ou) com testes de software

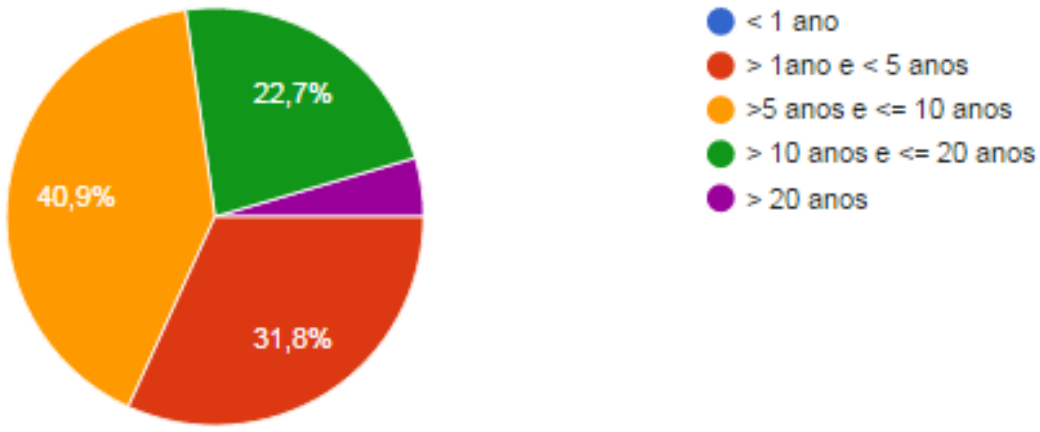


A segunda pergunta trata sobre uma atuação específica do profissional da engenharia de software que é a de Teste de Software. A motivação para essa questão foi em detrimento a menção da importância que a literatura dá para a equipe de teste de software no âmbito de obter níveis mais elevados de segurança, uma vez que avaliam se o produto de software está atendendo ao requerido. Pressman (2011) destaca a relevância da atividade de "Teste de Software" para a seguridade do software que está sendo desenvolvido.

Conforme mostra no Gráfico 2, a maioria dos profissionais (72,7%) que respondeu ao questionário não atua na atividade de teste de software; outros 27,3% têm ou já tiveram atuação na referida atividade.

Q3. Quanto tempo exerce a função vinculada a engenharia de software?

Gráfico 3 – Perfil do tempo de atuação em engenharia de software

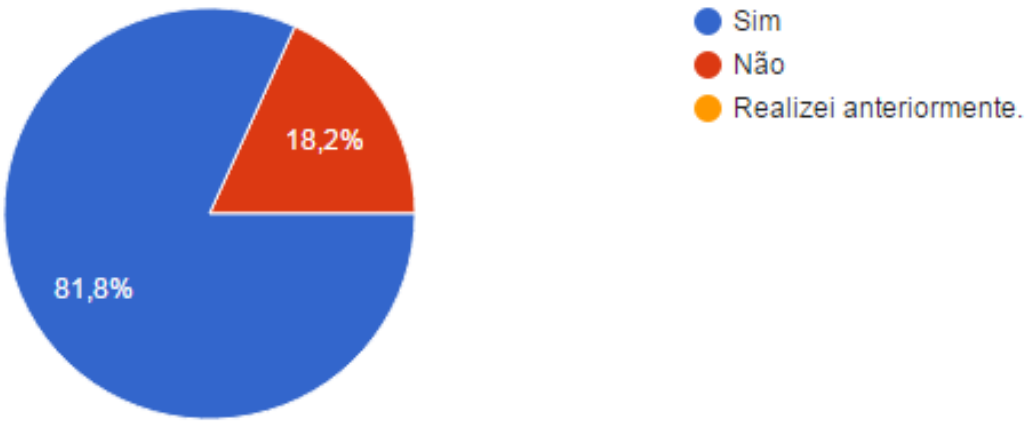


A questão “Q3” tem por objetivo identificar o nível de experiência do profissional da engenharia de software. E, conforme é ilustrado no Gráfico 3, o grupo respondente do questionário possui experiência profissional que podemos considerar relevante de atuação na engenharia de software, uma vez que a maioria (40,9%) atua entre 5 a 10 anos na área; entre aqueles que responderam, 01 deles (4,5%) tem mais de 20 anos de função; e 22,7% tem entre 10 e 20 anos.

Analisando os percentuais obtidos nas respostas da questão “Q3”, constata-se que 68% dos participantes da pesquisa tem no mínimo 5 anos que atua em funções de engenharia de software. Nenhum dos participantes da pesquisa tem tempo inferior a 1 ano de atividade, e 31,8% têm entre a 1 a 5 anos.

Q4. Desenvolve Aplicações Web que manipulam ou fazem intercâmbio de informações confidenciais/sigilosas?

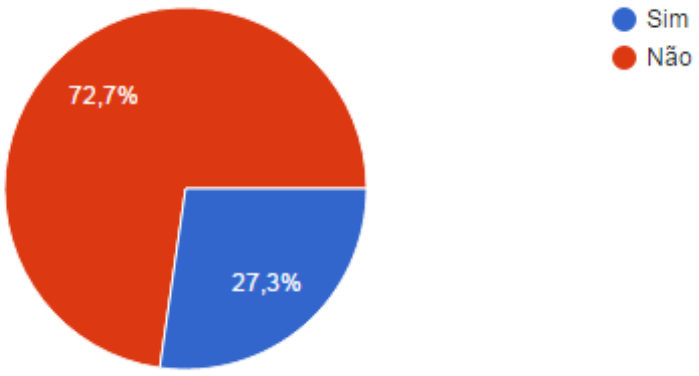
Gráfico 4 – Percentual de profissionais que desenvolvem aplicações Web



Conforme é mostrado no Gráfico 4, cerca de 18 (81,8%) dos participantes que responderam ao questionário desenvolvem aplicações Web que manipulam ou fazem intercâmbio de informações confidenciais/sigilosas. O percentual de respostas "Sim" à questão, permite concluir que o perfil dos profissionais da engenharia de software participantes do presente estudo de caso está alinhado com o perfil do assunto discutido e explorado nesta dissertação. Portanto, pode-se aferir que as respostas contribuem para o objetivo do questionário.

Q5. Para o desenvolvimento de Aplicações Web, utiliza algum Framework de Segurança da Informação?

Gráfico 5 – Percentual dos profissionais que utilizam framework de segurança da informação

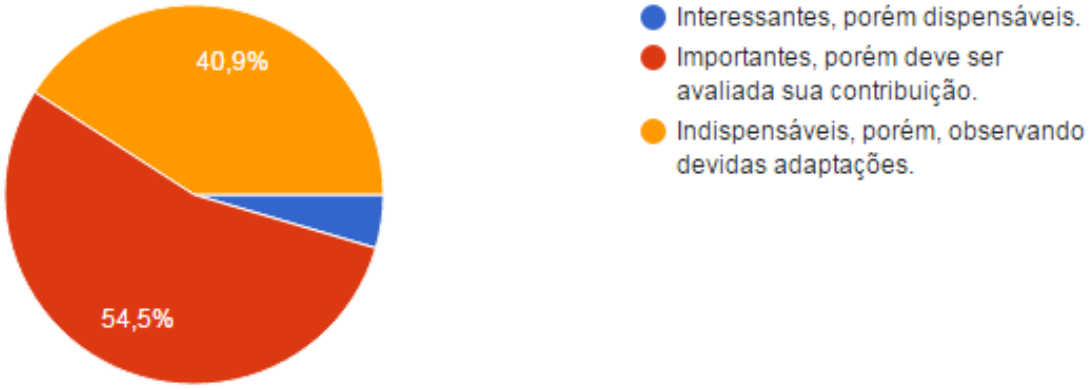


Dos participantes da pesquisa, conforme mostra o Gráfico 5, 72,7% responderam que não utilizam frameworks de segurança da informação; pelas informações extraídas do gráfico, conclui-se que apenas 27,3% declaram que utilizam um *framework*, ou seja, quase 2/3 dos respondentes não dispõem de proposta institucionalizada no âmbito da segurança da informação.

Delegar ao analista de sistema ou programador a atenção quanto à proteção da informação, sem processos e/ou atividades que apoiem e fiscalizem o profissional no desenvolvimento de aplicações Web com níveis elevados de segurança, pode contribuir consideravelmente para que os riscos já conhecidos se mantenham nas aplicações Web. As empresas devem atentar-se a dirimir essa negligência.

Q6. Qual, entre as opções abaixo, melhor adequa-se à sua opinião sobre a utilização de Frameworks de Segurança da Informação no desenvolvimento de sistemas?

Gráfico 6 – Opinião sobre utilização de framework de segurança da informação



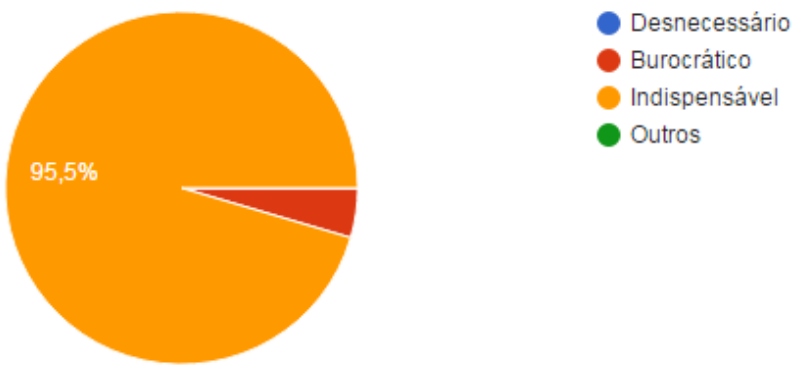
Apesar da importância dispensada pelas empresas no que se refere ao processo e atividades vinculadas à gestão da segurança da informação, a pergunta “Q6” avalia a opinião dos profissionais de engenharia de software quanto a aceitabilidade de estarem envolvidos com *frameworks* de gestão da segurança da informação.

Com exceção de 1 (um) profissional que respondeu à questão mencionado que o envolvimento com *frameworks* de gestão de segurança da informação é dispensável, os demais participantes assinalaram ser importante (40,9%) ou indispensável (54,5%) o envolvimento dos programadores ou analistas de sistemas em iniciativas vinculadas a processos e/ou atividades vinculadas à segurança da informação, conforme é mostrado no Gráfico 6.

Com base nos percentuais identificados, pode-se aferir que existe aceitabilidade dos profissionais da engenharia de software, caso as empresas tenham a iniciativa de definir e/ou utilizar, em utilizar *frameworks* vinculado à gestão da segurança da informação como, por exemplo, a proposta apresentada no Capítulo 5.

Q7. Qual, dentre as opções abaixo, melhor adequa-se à sua opinião sobre aplicação de processos vinculados à Gestão da Segurança da Informação no desenvolvimento de sistemas, por exemplo, de Aplicações Web?

Gráfico 7 – Opinião sobre utilização de framework de segurança da informação

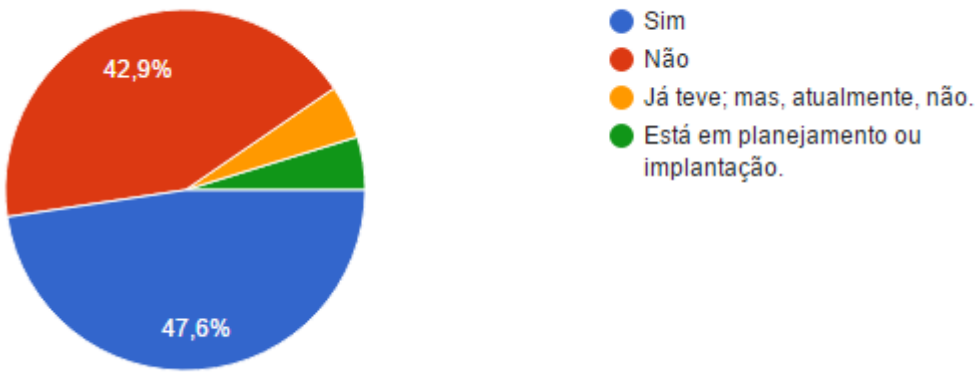


A pergunta “Q7” faz alusão à gestão da segurança da informação, uma vez que foi identificado nos trabalhos correlatos (Capítulo 2) deficiência quanto a capacitação dos analistas de sistemas e programadores sobre os mecanismos da segurança da informação. O Gráfico 7 mostra que 95,5% dos que responderam ao questionário entendem ser indispensável aplicação de processos vinculados à gestão da segurança da informação. Apenas 1 (4,5%) dos participantes classificou como “burocrático”.

O perfil identificado nas respostas às questões Q6 e Q7 torna claro que capacitações com abordagem na gestão da segurança da informação devem estar presentes no plano de cursos a serem realizados, e que processos na mesma área devem ser empreendido pelas empresas.

Q8. A empresa que atualmente você trabalha dispõe de uma Política de Gestão da Segurança da Informação, a qual está inserida no contexto da atividade de análise de sistemas e desenvolvimento de Aplicações Web?

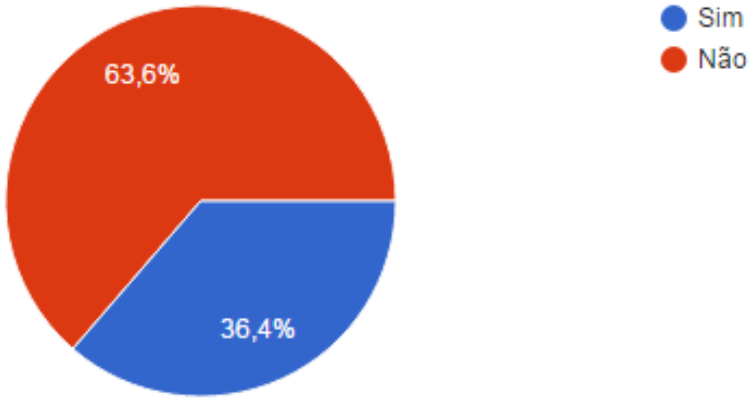
Gráfico 8 – Existência de uma política de gestão de segurança da Informação na empresa



Pelos percentuais que visualiza-se através do Gráfico 8, 47,6% das empresas em que os profissionais que responderam ao questionário trabalham dispõem de uma política de gestão da segurança da informação, que é um indicador muito bom. Porém, percebemos que quase o mesmo percentual se aplica a empresas que não tem a mesma iniciativa. Neste cenário referente a resposta “Não”, requer expressamente a iniciativa para planejar e implantar. Em outros casos, existe 1 (uma) empresa que está em fase de planejamento da política, e outra que dispunha de uma política, porém atualmente não mais a utiliza.

Q9. Já realizou capacitação(ões) com abordagem na Gestão da Segurança da Informação?

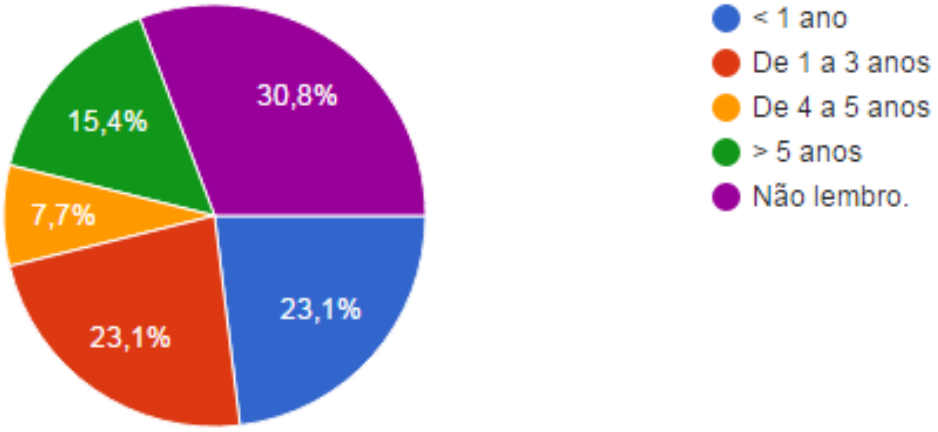
Gráfico 9 – Participação em capacitação com abordagem na gestão da segurança da informação



Apesar da aceitabilidade identificada nos profissionais da engenharia de software quanto a utilização de *framework* e de processos vinculados à gestão da segurança da informação, apenas 36,4% dos profissionais que responderam ao questionário afirmaram ter realizado alguma capacitação com abordagem na gestão da segurança da informação, conforme visualiza-se no Gráfico 9; portanto, 63,6% de analistas de sistemas ou programadores ainda não tiveram oportunidade de conhecer sobre o referido assunto, o que reitera a importância em empreender esforços quanto a capacitação com base na gestão da segurança da informação. Essa conclusão atesta a relevante contribuição dessa dissertação.

Q10. Se sua resposta à questão anterior foi "Sim", quando (em anos) ocorreu a última capacitação?

Gráfico 10 – Tempo que ocorreu a última capacitação em gestão da segurança da informação

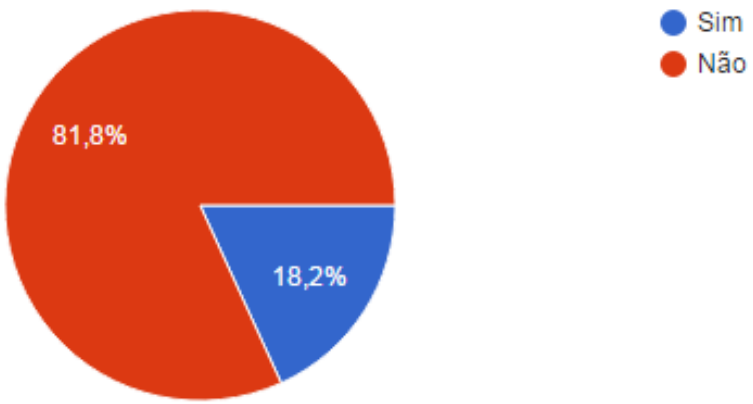


Apesar de 36,4% responderem que já foram capacitados em gestão da segurança da informação (Gráfico 8), observa-se através do Gráfico 10 que 30,8% não se lembram quando foi a capacitação ou já tem mais de 5 anos que foram capacitados (15,4%); ou seja, quase a metade dos profissionais da engenharia de software que informaram já terem participado de capacitação alusiva a gestão da segurança da informação, estão a algum tempo sem interação com novas abordagens e/ou esclarecimentos pertinentes ao referido assunto, salvo aqueles cuja empresa dispõe de uma política de gestão da segurança da informação

Os demais profissionais que foram capacitados, 23,1% informaram que tiveram a capacitação recentemente (menos de 1 ano), ou entre 1 ano e menos de 3 anos (23,1%); e 7,7% dos participantes na pesquisa informaram que foram capacitados a mais de 4 e menos de 5 anos.

Q11. Realiza alguma atividade de Gestão de Riscos com alguma periodicidade?

Gráfico 11 – Realiza alguma atividade de gestão de riscos



Relacionado à atividade de gestão de riscos, a qual foi discutida no Capítulo 4 e que é uma etapa fundamental para a gestão da segurança da informação, apenas 18,2% dizem realizar, conforme mostra o Gráfico 11.

Conforme já discutido neste trabalho, a gestão de riscos é a etapa inicial dos processos concernentes à gestão da segurança da informação, e 81,8% dos respondentes não fazem tal etapa. Entende-se que este é um indicador preocupante, em detrimento a realidade que esforços para empreender contramedidas de segurança da informação podem estar com foco em riscos com menor níveis de impactos, ou de maneira empírica aos reais níveis de impacto.

Mesmo tendo política de gestão da segurança da informação instituída e realizar capacitações vinculadas à gestão da informação, negligenciar a gestão de riscos da segurança da informação certamente não é uma boa prática. O *framework* proposto nesta dissertação contribuiu para que empresas e profissionais da engenharia de software realizem a gestão de riscos; inclusive, a gestão de riscos empreendida no Capítulo 4 contribuiu como exemplo de uma metodologia que pode ser aplicada para tal finalidade.

Q12, Q13 e Q14 – Sobre o documento OWASP Top 10

Gráfico 12 – Conhece o documento OWASP Top 10

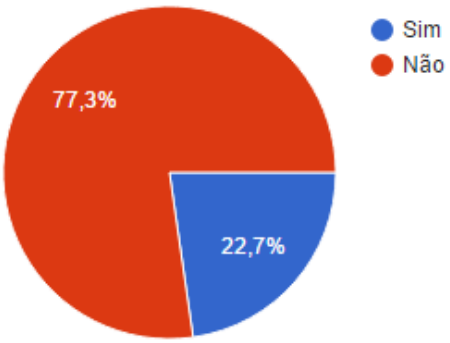


Gráfico 13 – Aplica(ou) alguma orientação do OWASP Top 10 2013

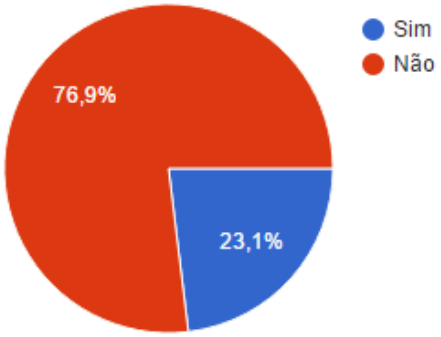
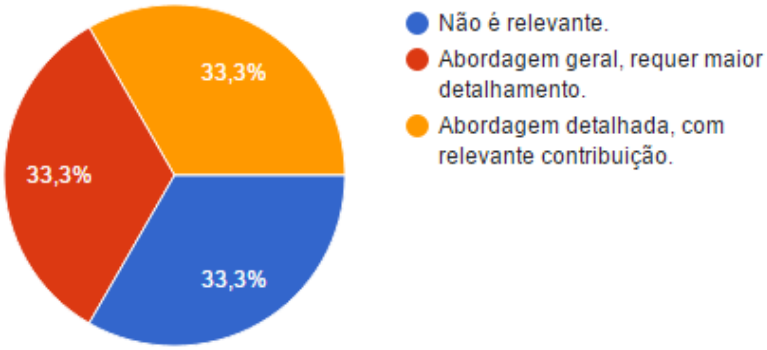


Gráfico 14 – Conclusão sobre o documento OWASP Top 10



As três próximas questões que serão discutidas estão vinculadas ao conhecimento e utilização documento OWASP Top 10 (Q12, Q13 e Q14). As questões Q13 e Q14 não eram obrigatórias, uma vez que somente responderiam aqueles que marcassem a opção “SIM” na questão Q12.

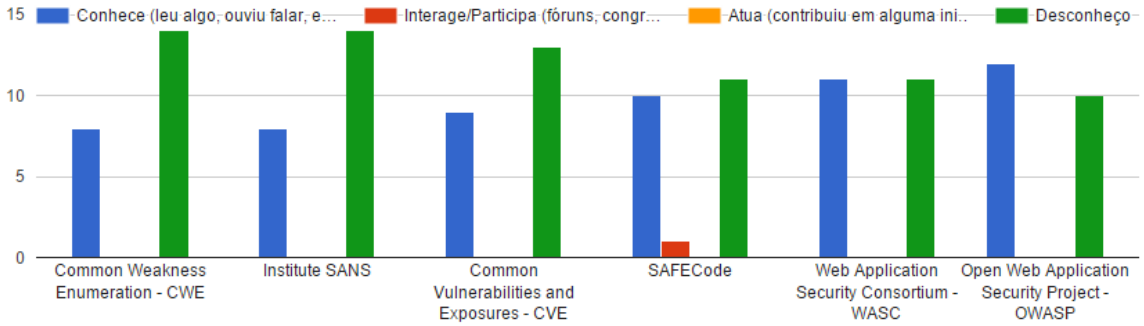
Na questão Q12, conforme o Gráfico 12, conclui-se que menos de 1/4 dos profissionais da engenharia de software que responderam ao questionário conhecem o documento OWASP Top 10. O simples fato de desconhecer um documento não permite concluir que exista negligência por parte dos 77,3% dos analistas de sistemas e programadores, que responderam ao questionário, na pesquisa e leitura da literatura que aborda sobre como alcançar níveis mais elevados de segurança da informação em aplicações Web; mas serve como alerta para que realize e/ou amplie o tempo destinado à consulta de artigos, documentos e demais iniciativas alusivas à segurança da informação.

Como tivemos um número relevante de participantes que nunca realizaram uma atividade de gestão de risco (Gráfico 11), convém que os profissionais da engenharia de software estejam atentos à necessidade da melhoria contínua em relação às ameaças, porque, por exemplo, mesmo que já as conheça, elas podem ser exploradas a partir de novas estratégias e técnicas de ataque.

A partir do Gráfico 13, observa-se que dos 22,7% que afirmam conhecer o documento OWASP Top 10 (Gráfico 12), apenas 23,1% aplicam ou aplicaram alguma orientação do documento (Gráfico 13), conforme resposta à questão “Q13”; e, através das respostas da questão “Q14”, mostrada no Gráfico 14, a conclusão em percentual semelhante para as três opções (33,3%) sobre o documento é que: 1) não é relevante; (2) dispõe de uma abordagem geral; ou (3) abordagem detalhada. Apesar de conhecerem o relatório, 76,9% responderam que nunca aplicaram uma contramedida as ameaças às aplicações Web a partir da orientação do documento.

Q15. Assinale na tabela abaixo, ação(ões) que tenha com empresas que atuam no âmbito de questões alusivas à segurança para Aplicações Web.

Gráfico 15 – Atuação dos profissionais em instituições que apoiam o desenvolvimento de aplicações Web



A questão 15 tratou de identificar sobre o conhecimento e envolvimento dos participantes da pesquisa em instituições que atuam em apoio ao desenvolvimento de aplicações Web com níveis mais elevados de segurança, as quais foram identificadas na revisão da literatura e já apresentadas no Capítulo 2.

A estrutura da questão dispõe do nome das instituições e três variáveis a serem sinalizadas pelos participantes da pesquisa no perfil abaixo especificado:

a) Conhece ➔ Já leu algo a respeito ou ouviu falar sobre a instituição.
b) Interage/Participa ➔ Participa de fóruns, congressos, seminários, etc., realizado pela instituição.
c) Atua ➔ Contribuiu com o desenvolvimento ou outra iniciativa mantida pela instituição.
d) Desconhece ➔ Nunca teve qualquer informação da instituição.

A partir da análise do Gráfico 15, que mostra a atuação dos participantes da pesquisa em instituições que apoiam o desenvolvimento de aplicações Web, principalmente em iniciativas vinculadas à segurança, identifica-se que nenhum tem atuação nas empresas relacionadas. Apenas 1 (4,5%) profissional sinalizou alguma interação com a SAFECode.

A variável mais preponderante quanto a sinalização dos participes da pesquisa foi "Desconheço", ou seja, os profissionais da engenharia de software não têm procurado envolvimento com as instituições citadas. Observa-se também que das instituições que tiveram maior quantitativo da indicação da variável "Conhece", o destaque são o WASC e o OWASP, sendo essa última com maior conhecimento entre os profissionais.

Q16. Sugestões sobre a pesquisa; sobre experiência na área de gestão da segurança da informação; ou para tecer quaisquer comentários que julgar ser importante.

A última pergunta do questionário, que trata-se de uma questão aberta, não foi respondida para nenhum dos participantes. O objetivo era obter sugestões sobre a pesquisa realizada nesta dissertação, algum relato de experiência vinculado à gestão da segurança da informação, bem como franquear ao participante a oportunidade de tecer comentários.

Como 36,4% dos respondentes do questionário nunca tiveram capacitação relacionada a segurança da informação (Gráfico 9), e dos que tiveram a oportunidade da capacitação, mais da metade afirmam que tem quatro anos ou mais que fizeram a capacitação (Gráfico 10), a

ausência de relato pode ser em detrimento ao pouco contato com o assunto de segurança da informação, uma vez que mais de 80% desenvolve aplicações Web que manipulam informações confidenciais e sigilosas (Gráfico 4), bem como evitar ou não ser adequado fazer algum relato neste sentido.

6.1 CONSIDERAÇÕES FINAIS

Após as análises e discussões empreendidas a partir das respostas do questionário, conclui-se que o tema segurança da informação é conhecido; contudo, sua abordagem não é uma rotina para as empresas e equipes da engenharia de software, e não está intrínseca ou é incipiente à cultura organizacional.

A negligência, por parte das empresas bem como profissionais da engenharia de software, quanto a conhecer e discutir sobre gestão da segurança da informação, reiteradamente considerado como importante, conforme referenciado através das respostas obtidas ao questionário e também identificado nas pesquisas de trabalhos correlatos, representa um risco potencial no âmbito da segurança da informação. A negligência, inclusive, pode acobertar a imperícia, por não saber se os analistas de sistemas ou programadores conhecem, pesquisam e estudam sobre a segurança da informação.

O *framework* proposto no Capítulo 5 trata-se de uma contramedida de gestão da segurança da informação para dirimir ou mitigar a negligência quanto ao uso e capacitação no âmbito da segurança da informação, tanto para a empresa quanto para os profissionais envolvidos no desenvolvimento de aplicações Web.

A aceitabilidade dos profissionais da engenharia de software em propostas sob a estrutura de *framework*, apurada através das respostas ao questionário, nos leva a concluir que há relevante probabilidade na aplicabilidade e institucionalização do *framework* de gestão da segurança da informação proposto no Capítulo 5.

Assim sendo, de maneira geral, conclui-se que atingimos os objetivos previstos para a elaboração dessa dissertação, a fim de promover níveis mais elevados de segurança no desenvolvimento de aplicações Web.

7 CONCLUSÃO

Este capítulo descreve as considerações finais sobre este trabalho, suas principais contribuições e possiblidades de trabalhos futuros.

7.1 CONSIDERAÇÕES FINAIS

Esta dissertação apresentou uma proposta de *framework* para o desenvolvimento de aplicações Web que contemplem processos de atividades alusivas à gestão da segurança da informação. O trabalho foi subsidiado pelas normas ABNT ISO/IEC 27002:2013 para definições de processos vinculados à gestão da segurança da informação, e pela ABNT ISO/IEC 27005:2011 para o desenvolvimento de uma gestão de riscos da segurança da informação.

Após realização de pesquisa na literatura, foram identificados dez principais riscos que são identificados pelo documento OWASP Top 10 2013. No referido documento, os riscos são classificados considerando uma análise quantitativa. Portanto, conforme preconizado pela norma ABNT 27005:2011, uma gestão de risco deve ser sempre empreendida como ponto inicial em atividades vinculadas a gestão da segurança da informação, e que a análise de risco seja realizada tanto no aspecto quantitativo quanto no qualitativo; posteriormente, seja comparado o resultado de ambas as análises. O comparativo entre a análise qualitativa e quantitativa demonstrou uma diferença na classificação do risco, o que reforça a necessidade em empreender ambas as análises quando da realização da atividade de gestão de riscos.

Entende-se que convém dar maior ênfase a análise de risco qualitativa, porque ela representa a magnitude do impacto gerado pelos respectivos riscos para a informação, principalmente aquela considerada confidencial e sigilosa. A partir de uma visão holística do risco, pode-se não conseguir implementar contramedidas para todos os riscos, portanto, deve-se privilegiar empreender maiores esforços para aqueles que representem maior impacto ao negócio.

Foram identificados vários trabalhos e instituições que apoiam ao desenvolvimento de aplicações Web mais seguras, mas quase a totalidade deles dispõem de abordagem técnica para discutir contramedidas de proteção à informação. Se a discussão feita unicamente através abordagem técnica fosse suficiente, não teríamos aplicações Web expostas continuamente aos

mesmos erros, conforme aponta a pesquisa nas edições do documento OWASP Top 10. Portanto, a abordagem conceitual discutida nessa dissertação é um elemento adicional importante para introdução de soluções que atuem no âmbito de alcançar níveis mais elevados de segurança para a informação, e supre uma lacuna que havia na literatura.

A pesquisa de campo discutida no Capítulo 6 induz que a imperícia ou negligência são questões de atenção a serem analisadas pelas empresas na sua equipe de engenharia de software, principalmente aquelas que desconsideram a segurança da informação. Portanto, iniciativas de capacitação com abordagem conceitual, e não somente técnica, e empreender esforços para definir políticas para implementação e integração dos mecanismos de gestão da segurança da informação representa um ganho adicional para a engenharia de software.

Com relação à negligência, conclui-se que é de maior responsabilidade das empresas, caso não implementem, capacitem, avaliem e busque melhorar processos vinculados à gestão da segurança da informação. Convém transformar a gestão da segurança da informação em uma diretriz e procedimento privilegiado de atuação para a equipe da engenharia de software. O *framework* proposto nesta dissertação contribuiu para essa finalidade.

Já sobre a imperícia, conclui-se que os profissionais da engenharia de software devem procurar aperfeiçoamento das suas técnicas de desenvolvimento, adotando uma postura de maior atenção tanto na abordagem conceitual como na técnica no âmbito da segurança da informação, respectivamente, através da pesquisa e leitura de trabalhos afetos ao tema.

Níveis mais elevados de segurança são alcançados através da união entre diversos mecanismos de segurança. No âmbito da gestão da segurança da informação, a qual estabelece novos paradigmas organizacionais, conclui-se que é preciso mitigar ou dirimir tanto a negligência das empresas no tocante a abordagem referente a segurança da informação, quanto a imperícia dos analistas de sistemas e programadores na implementação adequada e integrada dos mecanismos da segurança da informação.

Portanto, pode-se concluir que empresas e equipes da engenharia de software devem agir de maneira unida para empreender esforços contra aquele que pode ser o risco de maior magnitude: a negligência do desconhecimento ou a imperícia do falso conhecimento.

7.2 PRINCIPAIS CONTRIBUIÇÕES

Com a elaboração de trabalho, entende-se como principais contribuições:

a) Uma análise que busca conscientizar aos profissionais da engenharia de software que a informação é mais importante do que o produto de software (i.e., aplicação Web), porque o impacto negativo ao negócio é maior se houver roubo, perda ou adulteração da informação, em especial, a confidencial e sigilosa. Portanto, convém empreender medidas e mecanismos com foco na gestão da segurança da informação.

b) A discussão e comparação sobre a análise de riscos quantitativa e qualitativa, a partir do que preconiza a norma ABNT ISO/IEC 27005:2011, com foco na gestão da segurança da informação. Por utilizar a referida norma da ABNT, está adequada as exigências preconizadas pela norma ABNT ISO/IEC 27002:2013 para, por exemplo, estabelecer um comitê gestor da segurança da informação em qualquer empresa.

c) A proposta de um *framework* que estabelece a atuação e responsabilidade da empresa, dos profissionais e respectivas equipes vinculadas a engenharia de software, no desenvolvimento de aplicações Web com níveis mais elevados de segurança da informação.

Durante o desenvolvimento deste trabalho, houve a motivação para submissão de artigos científicos para diferentes eventos, a fim de validar na comunidade acadêmica as contribuições deste trabalho, bem como obter contribuições em prol do aperfeiçoamento da pesquisa e do seu teor. Segue abaixo relação desses eventos:

a) 13th International Conference on Information Systems and Technology Management. 2016. São Paulo, Brazil. (Aceito)

b) 56th International Conference for Computer Information System. 2016. Nashville, Tennessee. (Aceito)

7.3 TRABALHOS FUTUROS

Com a conclusão deste trabalho, percebeu-se que alguns aspectos ainda encontram-se abertos, os quais podem ser analisados no intento de ampliar o conjunto de contribuições disponibilizadas para a comunidade científica. Desta forma, relacionamos indicações de trabalho futuros a seguir:

a) Desenvolver uma metodologia de implantação do *framework*, e detalhar os processos a partir dessa metodologia. A documentação unívoca do modelo de gestão da segurança da informação contribuiu para o registro padronizado da realização de processos e atividades, respeitando as especificidades organizacionais, mas com a devida expressão e institucionalização da importância da segurança da informação.
b) Estabelecer métricas de acompanhamento e medição do nível de maturidade dos processos propostos no *framework*. Avaliar a aplicação dos processos e atividades à medida em que o produto de software está em desenvolvimento é sempre considerado uma boa prática; inclusive, constituiu um elemento de retroalimentação relevante para o aperfeiçoamento do *framework*.
c) Estender o *framework* para outros paradigmas da engenharia de software.
d) Planejamento e aplicação de um estudo experimental que possa melhor avaliar a aplicabilidade do *framework*, inclusive de pontos fortes e fracos.
e) Propor um plano de atividades para a “Identificação de Melhorias”.
f) Fazer um estudo sobre ações realizadas pelos usuários que representam riscos às aplicações Web.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013. Código de Prática para a Gestão da Segurança da Informação.** Rio de Janeiro, 2013.

_____. **ABNT NBR ISO/IEC 27005:2011 Gestão de Riscos para Segurança da Informação.** Rio de Janeiro, 2011.

ALBREIKI, H.H.; MAHMOUD, Q.H. Evaluation of static analysis tools for software **security.** Innovations in Information Technology (INNOVATIONS), In: INTERNATIONAL CONFERENCE ON, 10., 2014. **Proceedings…** 2014.

ALHOGAIL, A. Design and validation of information security culture framework. **Computers in Human Behavior,** v. 49, n.567-575, aug. 2015. ISSN: 07475632.

ANANE, R; DHILLON, S; BORDBAR, B. Stateless data concealment for distributed systems. **Journal of Computer & System Sciences,** v.74, n2, p.243-254, mar. 2008. ISSN: 00220000.

BOJINOV, H; BURSZTEIN, E; BONEH, D. The Emergence of Cross Channel Scripting. **Communications of the ACM**, v. 53, n.8, p.105-113, aug. 2010. ISSN: 00010782.

BRADBURY, D. The dangers of badly formed Websites. **Computer Fraud & Security**, 2012, v.1, p.12-14, jan. 2012. ISSN: 13613723.

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BORGOHAIN, T; KUMAR, U; SANYAL, S. Survey of Security and Privacy Issues of Internet of Things. **International Journal of Advanced Networking & Applications,** v.6, n.4, p.2372-2378, jan. 2015. ISSN: 09750290.

BURNET, Steve; PAINE, Stephen. **Criptografia e segurança:** o guia oficial RSA. Rio de Janeiro: Elsevier, 2002.

CARVALHO, Alan Henrique Pardo de. Segurança de aplicações Web e os dez anos do relatório OWASP Top 10: o que mudou? **FATEC-São Caetano do Sul,** São Caetano do Sul, v.1, n. 8, mar./set. 2014. p. 6 a 18.

CHO, Y; PAN, J. Design and Implementation of Website Information Disclosure Assessment System. **PLoS ONE,** v.10, n.3, p.1-29, mar. 2015. ISSN: 19326203.

CONRY-MURRAY, A. XSS Vulnerabilities Abound. **Network Computing,** v.17, n.16, p.16, aug. 31, 2006. ISSN: 10464468.

DAS, D; SHARMA, U; BHATTACHARYYA, DK. Detection of Cross-Site Scripting Attack under Multiple Scenarios. **Computer Journal**, v.58, n. 4, p.808-822, apr. 2015. ISSN: 00104620.

DORAI, R; KANNAN, V. SQL Injection-Database Attack Revolution and Prevention. **Journal of International Commercial Law & Technology**, v.6, n.4, p.224-231, oct. 2011. ISSN: 19018401.

FERNANDES, J. H. C. Segurança da Informação: nova disciplina na ciência da informação? In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 1., 2010. **Anais...** 2010.

FRAIWAN, M. et al. Analysis and Identification of Malicious JavaScript Coden**. Information Security Journal: A Global Perspective,** v.21, n.1, p.1-11, feb. 2012. ISSN: 19393555.

GARY, W.; ZHENDONG, S.. Sound and precise analysis of Web applications for injection vulnerabilities. In: ACM SIGPLAN CONFERENCE ON PROGRAMMING LANGUAGE DESIGN AND IMPLEMENTATION (PLDI '07), 28., 2007, New York, NY, USA. **Proceedings…** New York, NY, USA: ACM, 2007. 32-41. DOI=10.1145/1250734.1250739 http://doi.acm.org/10.1145/1250734.1250739.

GRITZALIS, S et al. Developing secure Web-based medical applications. **Medical Informatics & the Internet in Medicine,** v.24, n.1, p.75-90, mar. 1999. ISSN: 14639238.

HALFOND, W. J.; ORSO, A.; MANOLIOS, P. W. Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation. **IEEE Transactions on Software Engineering,** v.34, n.1, p.65-81, jan. 2008. ISSN: 00985589.

HAMANN, E. M. et al. Securing e-business applications using smart cards. **IBM Systems Journal**, v. 40, n.3, p. 635, jun. 2001. ISSN: 00188670.

ISACA. COBIT 5 **A Business Framework for the Governance and Management of Enterprise IT**. [S.l.]: Meadows, 2012.

JOVANOVIC, N.; KRUEGEL, C.; KIRDA, E. Static analysis for detecting taint-style vulnerabilities in Web applications. **Journal of Computer Security,** v.18, n.5, p.861-907, aug. 2010. ISSN: 0926227X.

KANSO, A.; YAHYAOUI, H.; ALMULLA, M. Keyed hash function based on a chaotic map. **Information Sciences**, v.186, n.1, p.249-264, mar. 2012. ISSN: 00200255.

KONZEN, M. P.; FONTOURA, L. M.; NUNES, R. C. Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança. In: SEGET. SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 9., 2012. **Anais…** 2012.

KHAN, M. U. A.; ZULKERNINE, M. Activity and Artifact Views of a Secure Software Development Process. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND ENGINEERING, 2009. **Proceedings…** 2009. p. 339- 404.

_____. Quantifying Security in Secure Software Development Phases. In: ANNUAL IEEE INTERNATIONAL COMPUTER SOFTWARE AND APPLICATIONS CONFERENCE, 2008. **Proceedings…** 2008. p. 905-960.

LAWTON, G. Web 2.0 Creates Security Challenges. **Computer. 40**, v.10, n.13-16, oct. 2007. ISSN: 00189162.

LEE, I. et al. A novel method for SQL injection attack detection based on removing SQL query attribute values**. Mathematical & Computer Modelling,** v.55, n.1/2, p.58-68, jan. 2012. ISSN: 08957177.

LARKIN, E. Don't Let Bad Guys Pose as You. **PC World,** v.25, n.4, p.36, apr. 2007. ISSN: 07378939.

MARCONI, M. A; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7 ed.. São Paulo: Atlas, 2010.

MAO, Z.; LI, N.; MOLLOY, I. Defeating Cross-Site Request Forgery Attacks with Browser-Enforced Authenticity Protection. **Financial Cryptography and Data Security Lecture Notes in Computer Science**, v.5628, p. 238-255, 2009.

MARTINS, J. C. L. **Framework de segurança de um sistema de informação**. 2008. Dissertação (Mestrado em Sistemas de Informação)- Programa de pós-graduação em Sistemas de Informação da Universidade do Minho, Lisboa – Portugal, 2008.

MARCIANO, J. L. P. **Segurança da informação:** uma abordagem social. 2006. Tese (Doutorado em Ciência da Informação)- Universidade de Brasília - UNB, Brasília, 2006.

OWASP. **Metodologia de Cálculo de Risco**. Disponível em: <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>. Acesso em: 12 jan. 2016.

_____. **The Open Web Application Security Project**. Disponível em: https://www.owasp.org/index.php/Main_Page. Acesso em: 12 jan. 2016.

_____. **OWASP Top 10 2013**. OWASP Top Ten Project. Disponível em: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf Acesso em: 12 jan. 2016.

PRESSMAN, R. **Engenharia de software:** uma abordagem profissional. 7. ed. Porto Alegre: AMGH, 2011.

ROCCHETTO, M.; OCHOA, M.; DASHTI, M. T. **Model-Based Detection of CSRF**. **ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology**, v.428, p. 30-43, 2014.

ROCHA, T. S.. **Detecção Automática de Ataques de Cross-Site Scripting em Páginas Web**. **Explorando linguagens de marcação para representação de relatórios de informações Financeiras**. 2003. Dissertação (Mestrado Profissional em Informática)- Programa de pós-graduação em Informática da Universidade Federal do Amazonas, 2013.

DE RYCK, P. et al.. Automatic and Precise Client-Side Protection against CSRF Attacks. **Computer Security – ESORICS 2011 Lecture Notes in Computer Science,** v. 6879, p. 100-116, 2011.

SAIEDIAN, H; BROYLE, D. Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives. **Computer,** v.44, n.9, p.29-36, sept. 2011. ISSN: 00189162.

SANTOS, H.; NUNES, P. Framework de Gestão da Segurança da Informação para Organizações Militares Orientadas pelos Principais Vetores de Ataque. In: CONFERÊNCIA DA ASSOCIAÇÃO PORTUGUESA DE SISTEMAS DE INFORMAÇÃO (CAPSI-2012), 12., 2012. **Proceedings…** Disponível em: http://www3.dsi.uminho.pt/CAPSI2012/cd/submissions/capsi2012_submission_2.pdf. Acesso em: 12 jan. 2016.

SIPIOR, J. C.; WARD, B. T. A framework for information security management based on guiding standards: a United States perspective**. Informing Science and Information Technology,** v. 5, p. 51-60, 2008.

SOOD, A; ENBODY, R. Malvertising–exploiting web advertising C**omputer fraud & security**. v.7, p.11-16, jul. 2011. ISSN: 13613723.

SÊMOLA, M.. **Gestão da segurança da informação:** uma visão executiva**.** Rio de Janeiro: Elsevier, 2003.

SHAR, L K. TAN, H B K. Predicting Common Web Application Vulnerabilities from Input Validation and Sanitization Code Patterns**.** In: IEEE/ACM INTERNATIONAL CONFERENCE ON AUTOMATED SOFTWARE ENGINEERING (ASE 2012), 27., 2012. **Proceedings…** 2012. p. 310-313.

SILVA, P. C. **Explorando linguagens de marcação para representação de relatórios de informações financeiras**. 2003. Dissertação (Mestrado Profissional em Redes de Computadores)- Programa de pós-graduação Universidade Salvador - UNIFACS, Salvador, 2003.

SOMMERVILLE, I. **Engenharia de software.** 9. ed. São Paulo: Pearson, 2011.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011.

TEIXEIRA, E. **Ferramenta de análise de código para detecção de vulnerabilidades.** 2007. Disponível em: http://www.di.fc.ul.pt/~nuno/THESIS/EmanuelTeixeira_master07.pdf . Acesso em: 12 jan. 2016.

TELIKICHERLA, K. C.; CHOPPELLA, V.; BEZAWADA, B. CORP: A Browser Policy to Mitigate Web Infiltration Attacks. **Information Systems Security Lecture Notes in Computer Science,** v.8880, p. 277-297, 2014.

VELOSO, M. A. **ISO 31000 X ISO 27005:** Comparação entre as normas para gestão de risco. MBA em Gestão de Segurança da Informação. [S.l.]: [s.n.], 2008.

WASUKAR, A. R; USMAN, Mohammad; SAKHARE, Neha. Vulnerability Management. **Web Application. International Journal For Research In Emerging Science And Technology,** v.2, Special Issue-1, mar. 2015.

XIAOLI, L. et al. Threat Modeling for CSRF Attacks," Computational Science and Engineering, 2009. CSE '09. In: INTERNATIONAL CONFERENCE ON, 3., 2009. **Proceedings…** 2009 .doi: 10.1109/CSE.2009.372.

ANEXO A – QUESTIONARIO DO ESTUDO DE CASO

OBSERVAÇÕES

Este questionário tem por finalidade exclusiva obtenção de dados quantitativos para trabalho de pesquisa do acadêmico CLEBERTON CARVALHO SOARES, vinculado ao Mestrado de Sistemas e Computação da Universidade Salvador – UNIFACS, com a matrícula 710111008, sob a orientação do Prof. Dr. Paulo Caetano da Silva.

O acadêmico declara e dá fé que não integra ou responde por quaisquer empresas de desenvolvimento de software ou áreas correlatas neste momento; e que a utilização dos dados apurados não fará qualquer menção à empresa ou ao participante da pesquisa, bem como fazer alusão que permita a identificação destes.

O questionário não requer nenhum tipo de informação pessoal e/ou profissional, por não ter nenhum vínculo com o objeto de análise do trabalho, bem como para incentivar fidelidade nas respostas. Mediante dar credibilidade a pesquisa, serão aceitos apenas os formulários preenchidos e devolvidos presencialmente.

Agradecemos sua participação!

DO TRABALHO

A gestão da segurança da informação transcende a tecnologia e propende em proteger a informação contra qualquer ameaça que transgrida os seus pilares: confidencialidade, integridade e disponibilidade. Como as tecnologias Web representam um paradigma de desenvolvimento de software cada vez mais em utilização; porém, mediante o uso da Web como meio de comunicação para intercâmbio de informações, favorece ao crescimento de pesquisa para explorar estratégias de ataques. Esses ataques torna a aplicação Web vulnerável a diversos riscos, conforme identificado na literatura que aborda sobre o assunto de segurança.

Convém empreender esforços para dirimir ou mitigar os riscos, conforme especifica a norma 27002:2013 da Associação Brasileira de Normas Técnicas (ABNT). Uma gestão de segurança da informação é um mecanismo para, independente de tecnologia, apoiar na implantação de um processo para que sejam instituídas e averiguadas ações para elevar o nível de segurança da informação, iniciando por uma gestão de risco que tenha um respaldo no mercado, conforme especifica a norma 27005:2011 da ABNT.

Este questionário é uma etapa de um trabalho acadêmico, que visa publicação em documento vinculado a área da Computação, com o objetivo averiguar o conhecimento atual de profissionais da engenharia de software sobre elementos pertinentes a pesquisa: gestão da segurança da informação; e a gestão de riscos em aplicações Web.

Após apuração dos dados, pretende-se arvorar e subsidiar uma proposta de solução estruturada como um *framework*, que auxilie a qualquer equipe vinculada ao desenvolvimento de aplicações Web na gestão de segurança da informação, de maneira que práticas e tecnologias de segurança da informação possam contribuir para implantação de um processo que propicie aplicações Web com níveis mais elevados de proteção à informação.

Questionário

Q1. Vinculado a engenharia de software, que função que exerce(u)?

( ) Programador ( ) Analista de Sistema ( ) Outro.

Se “Outro”, por favor informar, qual?

Q2. Atua(ou) em função de teste de software?

( ) Sim ( ) Não

Q3. Quanto tempo exerce(u) a função vinculada a engenharia de software?

( ) <1 ano ( ) > 1 ano e < 5 anos ( ) >5 e <=10 anos

( ) > 10 e <= 20 anos ( ) > 20 anos

Q4. Desenvolve **Aplicações Web** que manipulam ou fazem intercâmbio de informações confidenciais/sigilosas?

( ) Sim ( ) Não

Q5. Para o desenvolvimento de Aplicações Web, utiliza algum framework de segurança da informação?

( ) Não utiliza ( ) Próprio ( ) Fornecedores

Q6. Qual, entre as opções abaixo, melhor adequa-se à sua opinião sobre a utilização de *frameworks de Segurança da Informação* no desenvolvimento de sistemas?

( ) Interessantes, porém dispensáveis.

( ) Importantes, porém deve ser avaliada sua contribuição.

( ) Indispensáveis, porém, observando devidas adaptações.

Q7. Qual, entre as opções abaixo, melhor adequa-se à sua opinião sobre aplicação de processos vinculados à gestão da segurança da informação no desenvolvimento de sistemas, por exemplo, de Aplicações Web?

( ) Desnecessário ( ) Burocrático ( ) Indispensável

( ) Outro. Qual? _____

Q08. A empresa dispõe de uma política de gestão da segurança da informação para desenvolvimento de aplicações Web?

( ) Sim ( ) Não

Q9. Já realizou capacitação com abordagem na gestão de segurança da informação?

( ) Sim ( ) Não

Q10. Se realizou, por favor, quando (em anos) ocorreu a última capacitação:

( ) < 1 ano ( ) De 1 a 3 anos ( ) De 4 a 5 anos

Q11. Realiza alguma gestão de riscos rotineiramente ou com alguma periodicidade?

( ) Sim ( ) Não

Q12. Conhece o documento OWASP TOP 10?

( ) Não ( ) Sim

Q13. Se positivo, por favor responda às questões abaixo:

Aplica/Aplicou Uma Ou Mais Orientações Do OWASP Top 10 2013?

( ) Sim ( ) Não

Q14. Conclusão particular sobre o documento "OWASP Top 10"

( ) Não é relevante.

( ) Abordagem geral, sem muita profundidade.

( ) Abordagem detalhada, com relevante contribuição.

Q15. Por favor, assinale na tabela abaixo, ação(ões) que tenha com empresas que atual no âmbito de questões alusivas à segurança para aplicações Web.

Empresa	**SIGLA**	**Conhece** (leu algo, ouviu falar, etc.)	**Interage/Participa** (fóruns, congressos, lista de discussão, etc.)	**Atua** (apoia em algum projeto)
Common Weakness Enumeration	CWE	◯	◯	◯
Institute SANS	-	◯	◯	◯
Common Vulnerabilities and Exposures	CVE	◯	◯	◯
SAFECode	-	◯	◯	◯
Web Application Security Consortium	WASC	◯	◯	◯
Open Web Application Security Project	OWASP	◯	◯	◯

Q16. Espaço aberto para comentários, sugestões sobre a pesquisa, bem como expor alguma experiência ou conhecimento em segurança da informação para aplicações Web.