UMA AVALIAÇÃO SOBRE O CONHECIMENTO EM SEGURANÇA DA INFORMAÇÃO

Cleberton Soares Soares[1]; Paulo Caetano da Silva[2].

[1]Mestre em Sistemas e Computação, Professor do Instituto Federal de Sergipe, cleberton_soares@hotmail.com; [2]Pós-Doutor em Ciências da Computação, Professor e Pesquisador da Universidade de Salvador, paulo.caetano@unifacs.br.

Resumo: A informação é um elemento fundamental às organizações e imprescindível para o planejamento estratégico. Salvaguardar informações confidenciais e sigilosas deve ser compreendido como uma ação prioritária e que transcende apenas a aquisição de ferramentas tecnológicas de proteção, mas também da capacidade das pessoas em conhecer sua responsabilidade e participação na segurança da informação. Este artigo tem por objetivo fazer uma avaliação sobre o conhecimento que programadores e analistas de sistemas e empresas têm sobre a segurança da informação. Conclui-se que o conhecimento sobre assunto, apesar de ser compreendido pelos profissionais envolvidos na pesquisa como relevante, ainda é abordado de modo incipiente e muitas vezes sem um procedimento institucionalizado.

Abstract: Information is a fundamental element to organizations and essential for strategic planning. Safeguarding confidential and confidential information should be understood as a priority action that transcends only the acquisition of technological protection tools, but also the ability of people to know their responsibility and participation in information security. This article aims to make an assessment of the knowledge that programmers and systems analysts and companies have about information security. It is concluded that knowledge about subject, despite being understood by the professionals involved in the research as relevant, is still addressed in an incipient way and often without an institutionalized procedure.

INTRODUÇÃO

A segurança da informação transcende a tecnologia, e rotineiramente sugere novos paradigmas organizacionais (SÊMOLA, 2003). Ela consiste em garantir que a informação confidencial, independentemente de seu teor e formato, esteja protegida contra o acesso por pessoas não autorizadas (confidencialidade), sempre disponível quando necessária (disponibilidade), bem como ser autêntica (integridade). Estes três elementos: confidencialidade, integridade e disponibilidade, formam a tríade da segurança da informação (SÊMOLA, 2003), conforme ilustrado na Figura 1, que é a base dos conceitos e práticas relacionados à gestão da segurança da informação.

Figura 01 - Figura 1 - Tríade da Segurança da Informação

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

- Autenticação: propriedade de garantir a fonte e o teor da informação.
- Autorização: propriedade de permitir ou negar o acesso.
- Identificação: propriedade de registrar algo ou alguém no sistema.

- Não repúdio: propriedade de garantir ao autor sua respectiva responsabilidade pelo que fez.

Ainda com base em padronizações definidas pela International Oganization for Standardization (ISO), é possível acrescentar outras propriedades à tríade de segurança da informação, definidas na característica denominada de "Segurança" na norma ISO/IEC 25010:2011, as quais avaliam a qualidade do produto de software. São elas:

- Autenticidade: legitimidade para os processos de controle de acesso.

- Responsabilidade: ética e dever na prestação de contas.

- Conformidade: ação de acordo com a legislação, com regras ou instruções.

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: a integridade das informações; à prevenção de ataques e ao furto dos dados; assegurar que os sistemas sejam reestabelecidos; e que o acesso seguro às informações seja garantido mesmo quando houver êxito em ataques ao sistema computacional.

Roubo de informações tem sido tema de matéria muito recorrente na mídia em geral, o que certamente contribui para aumentar a incerteza quanto ao uso de tecnologias de software. Contudo, existem grupos de trabalho que atuam para contribuir com a implementação de aplicações web com níveis mais elevados de segurança. Entretanto, convém que tanto empresas quanto profissionais da engenharia de software devam estar em constante estudo e pesquisa sobre a segurança da informação.

É importante ressaltar que nem toda informação requer confidencialidade ou sigilo (são consideradas de domínio público). À gestão de riscos cabe 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).

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, que ocorre o intercâmbio de informações por meio do uso de aplicações Web. Portanto, as ameaças presentes através da 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.

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. Contudo, há dificuldades para sua plena implantação, uma vez que a facilidade de uso e a segurança caminham sempre em sentidos opostos (SÊMOLA, 2003). Este artigo apresenta uma ava-

liação sobre o conhecimento que programadores e analistas de sistemas e respectivas empresas têm sobre a segurança da informação. Na segunda seção deste artigo será apresentado como a pesquisa foi conduzida, cujos resultados são discutidos na seção seguinte. A seção Conclusões, aborda as considerações finais e conclusões do trabalho.

MATERAIS E MÉTODOS

Para desenvolvimento deste trabalho foi elaborado um questionário como objetivo aferir a aceitação, o conhecimento e o envolvimento dos profissionais em empresas no estado de Sergipe sobre a segurança da informação, principalmente aquelas que atuam como analistas de sistemas e programadores de aplicações Web com intercâmbio e manipulação de informação confidencial e sigilosa.

Para inibir quaisquer prejuízos aos profissionais e as empresas que se dispuseram a contribuir com a pesquisa deste trabalho, será preservada qualquer referência que promova algum tipo de identificação daqueles que atenderam ao convite feito e responderam ao questionário.

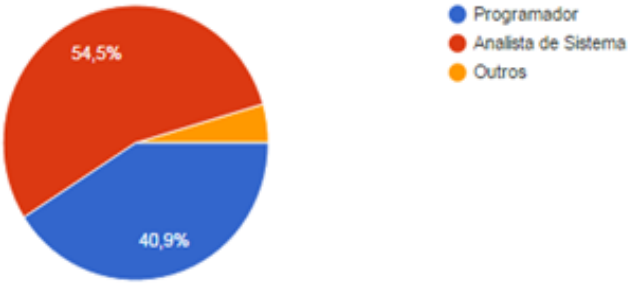
A aplicação do questionário, contendo 16 questões, sendo 15 questões objetivas e 1 aberta, foi através de recursos eletrônicos, acessível pela internet, direcionado exclusivamente a profissionais da engenharia de software que estejam ou já tiveram oportunidade de desenvolver aplicações Web. De um grupo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

RESULTADOS E DISCUSSÃO

Para esta seção, a discussão será com foco individualizado nas questões dispostas aos participantes da pesquisa. Um gráfico antecede os relatos da análise de dados, permitindo melhor visualização do perfil das respostas.

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

Gráfico 1 - Perfil dos participantes na pesquisa



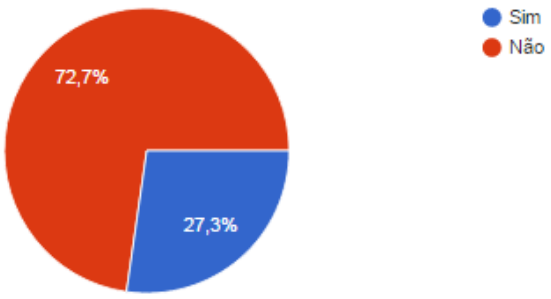
Conforme visualizado no Gráfico 1, a maioria dos entrevistados é analista de sistemas (54,5%), depois temos 40,9% que são programadores, e 4,5% (1 profissional) Arquiteto de Software. Conclui-se que o perfil dos participantes na pesquisa está adequado ao desejado, uma vez que a pesquisa trata sobre aplicações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

Q2. Atua(ou) em função de Teste 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 à 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.

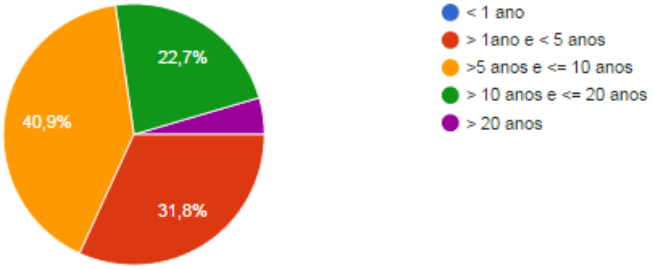
Gráfico 2 - Percentual de profissionais que atua(ou) com testes de software



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

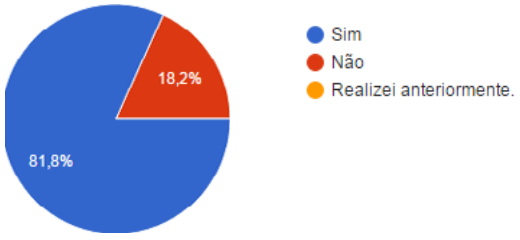


A questão "Q3" tem por objetivo identificar o nível de experiência do profissional da engenharia de software. E, conforme é ilustrado no Gráfico 3, o grupo respondente do questionário possui experiência profissional que podemos considerar relevante na engenharia de software, uma vez que a maioria (40,9%) 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 atuam 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?

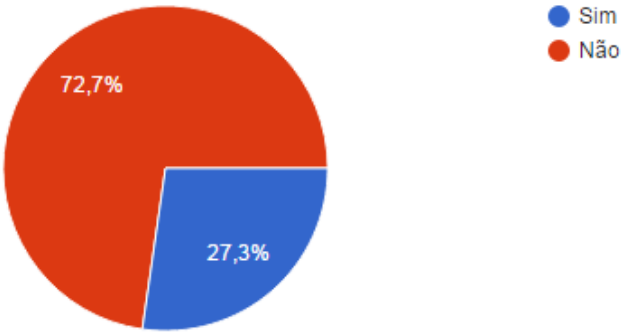
Gráfico 4 - Percentual de profissionais que desenvolvem aplicações Web



Conforme é mostrado no Gráfico 4, 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 neste artigo. 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.

Convém ressaltar que o uso de metodologia de framework representa um modelo adequado para abordagens relacionadas à processos de gestão da segurança da informação, conforme definem ISACA (2012) e MARTINS et al (2009).

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 (OWASP Top 10) se mantenham nas aplicações Web. As empresas devem atentar-se a dirimir essa falha.

Q6. Qual, dentre 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

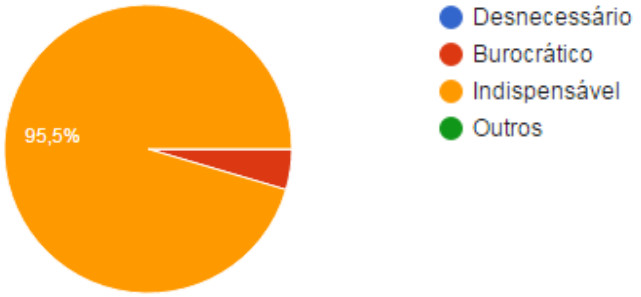
Apesar da importância dispensada pelas empresas no que se refere ao processo e atividades vinculadas à gestão da segurança da informação, a pergunta "Q6" avalia a opinião dos profissionais de engenharia de software quanto a aceitabilidade de estarem envolvidos com frameworks de gestão da segurança da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

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 deficiência quanto a capacitação dos analistas de sistemas e programadores sobre os mecanismos da segurança da informação, conforme destaca SOARES & SILVA (2016). 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.

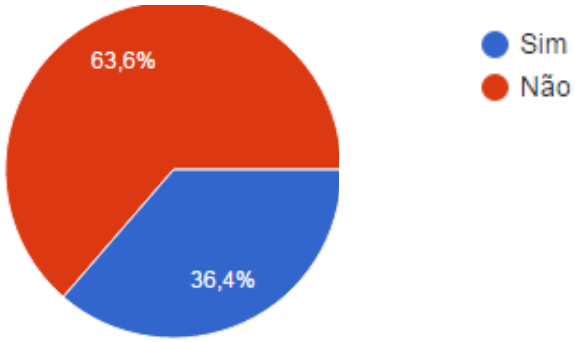
Q8. A empresa que atualmente você trabalha dispõe de uma Política de Gestão da Segurança da Informação, a qual está inserida no contexto da atividade de análise de sistemas e desenvolvimento de Aplicações Web?

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

Pelos percentuais que se visualiza 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?

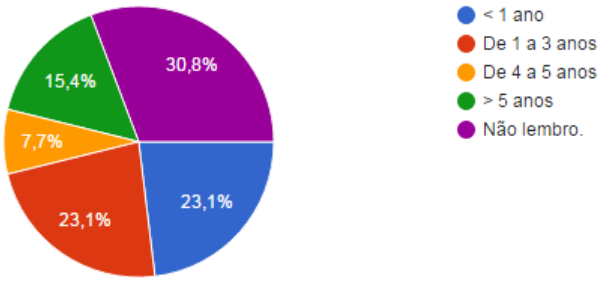
Gráfico 9 - Participação em capacitação com abordagem na gestão da segurança da informação



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% dos 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 contribuição que pode ser dada por este trabalho de pesquisa.

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 há 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

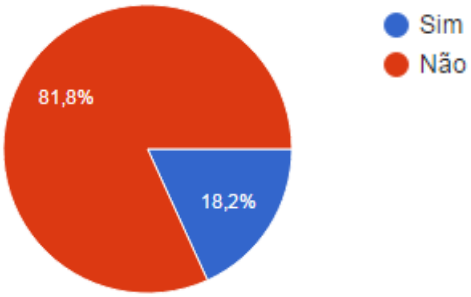
Os demais profissionais que foram capacitados, 23,1% informaram que tiveram a capacitação re-

centemente (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?

Relacionado à atividade de gestão de riscos, que é considerada uma etapa fundamental para a gestão da segurança da informação, apenas 18,2% dizem realizar, conforme mostra o Gráfico 11.

Gráfico 11 - Realiza alguma atividade de gestão de riscos



Conforme já anteriormente citado, 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.

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

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

O OWASP Top 10 é uma publicação que identifica, caracteriza e propõe contramedidas para as dez principais vulnerabilidades que expõe aplicações web a riscos que envolvem, dentre outras, o roubo de informações. Compreende-se então que tem um perfil adequado para analistas de sistemas e programadores identificar e até mesmo testar seus produtos de software, tornando-os menos vulneráveis.

Gráfico 12 - Conhece o documento OWASP Top 10

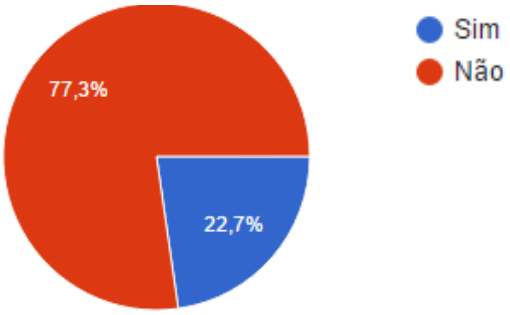


Gráfico 13 - Conhece o documento OWASP Top 10

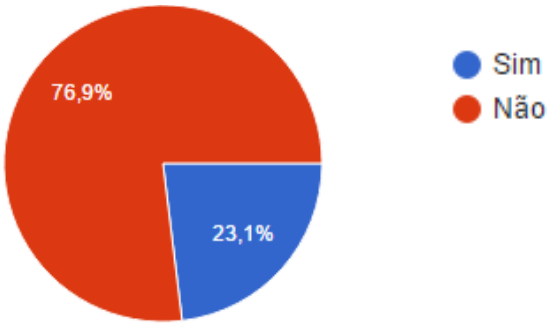
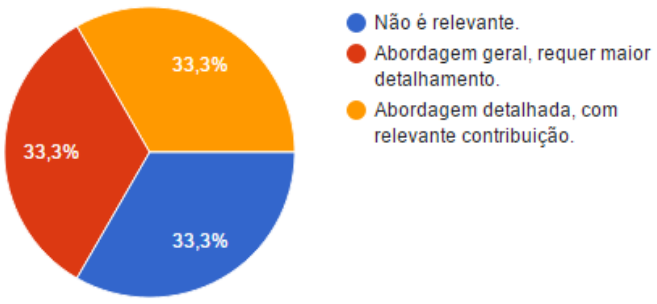


Gráfico 14 - Conclusão sobre o documento OWASP Top 10



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 dos 77,3% dos analistas de sistemas e programadores que responderam ao questionário sobre a pesquisa e leitura da literatura que aborda como alcançar níveis mais elevados de segurança da informação em aplicações Web; porém, serve como alerta para que se realize e/ou amplie o tempo destinado à consulta de artigos, documentos e demais iniciativas alusivas à segurança da informação.

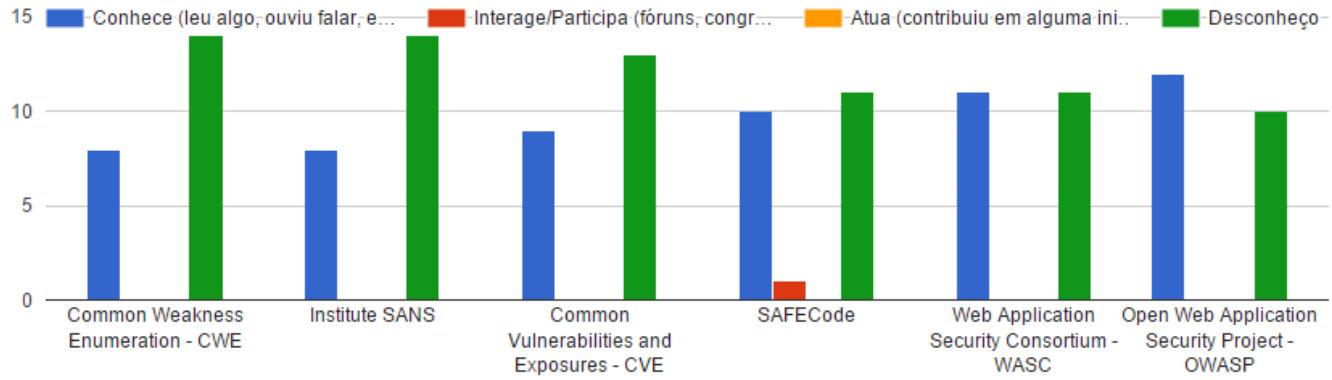
Como tivemos um número relevante de participantes que nunca realizaram uma atividade de gestão de risco (Gráfico 11), convém que os profissionais da engenharia de software estejam atentos à necessidade da melhoria contínua em relação às ameaças, porque, por exemplo, mesmo que já as conheça, elas podem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

A questão 15 tratou de identificar sobre o conhecimento e envolvimento dos participantes da pesquisa em instituições que atuam no apoio ao desenvolvimento de aplicações Web com níveis mais elevados de segurança, conforme relaciona SILVA & SOARES (2016) são elas: a CWE[1] (Common Weakness Enumeration); (ii) o Institute SANS[2] ; (iii) a Common Vulnerabilities and Exposures (CVE)[3]; (iv) a SAFECode[4]; (v) o Web Application Security Consortium (WASC)[5]; e (vi) a Open Web Application Security Project (OWASP)[6] . Destas, a última é a responsável pelo OWASP Top 10.

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



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

1. Conhece > Já leu algo a respeito ou ouviu falar sobre a instituição.

2. Interage/Participa > Participa de fóruns, congressos, seminários, etc., realizados pela instituição.

3. Atua > Contribuiu com o desenvolvimento ou outra iniciativa mantida pela instituição.

4. Desconhece > Nunca teve qualquer informação da instituição.

[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/

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, desta amostra do estado de Sergipe, não têm procurado envolvimento com as instituições citadas ou as desconhece. 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 se trata de uma questão aberta, não foi respondida para nenhum dos participantes. O objetivo era obter sugestões sobre a pesquisa realizada, 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.

CONCLUSÕES

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 que participaram, e não está intrínseca ou é incipiente à cultura organizacional.

A falta de atenção das empresas, bem como dos profissionais da engenharia de software, no que se refere a conhecer e discutir sobre gestão da segurança da informação, reiteradamente considerado como importante, conforme referenciado através das respostas obtidas ao questionário, representa um risco potencial no âmbito da segurança da informação. A negligência ao tema, inclusive, pode acobertar a imperícia, por não saber se os analistas de sistemas ou programadores conhecem, pesquisam e estudam sobre a segurança da informação.

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 de algum framework de gestão da segurança da informação como mecanismos de institucionalizar processos e atividades atinentes 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.

Este trabalho foi executado em uma amostra dos profissionais da área do estado de Sergipe; para podermos tirar conclusões mais precisas e com bases estatísticas em uma população maior é preciso expandir a consulta para outros estados do Brasil, assim poderemos usar métodos de análise estatísticas que embasem melhor as conclusões.

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

FERNANDES, J. H. C. **Segurança da Informação: nova disciplina na ciência da informação?** XI Encontro Nacional de Pesquisa em Ciência da Informação. 2010.

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.** IX SEGeT. Simpósio de Excelência em Gestão e Tecnologia. 2012.

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.

OWASP. **Metodologia de Cálculo de Risco.** https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

OWASP **The Open Web Application Security Project.** https://www.owasp.org/index.php/Main_Page.

OWASP Top 10 2013. **OWASP Top Ten Project.** http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

PRESSMAN, R. **Engenharia de Software – Uma Abordagem Profissional. 7ª Edição.** Porto Alegre: AMGH, 2011.

SÊMOLA, M.. **Gestão da Segurança da Informação – Uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores.** 5ª Edição. Pearson. 2011.

SOARES, Cleberton C. SILVA, Paulo Caetano. **Contramedidas A Riscos Que Expõem As Aplicações Web A Vulnerabilidades: Uma Revisão Da Literatura.** 13th International Conference On Information Systems & Technology Management – CONTECSI. DOI: 10.5748/9788599693124-13CONTECSI/RF-4145. 2016.