SIC 2022
X Seminário de Iniciação Científica do IFNMG
II Seminário da Pós-Graduação do IFNMG
8 a 10 de junho de 2022 Evento online
INSTITUTO FEDERAL
Norte de Minas Gerais
Campus Diamantina

APLICAÇÃO DE SEGURANÇA DA INFORMAÇÃO EM AMBIENTES VIRTUAIS DE APRENDIZAGEM

OTONI, B.O.G.[1]; PEREIRA, L.D.L.[2]; ALVES, A.F.S. [2]

[1]Discente do curso de Análise e Desenvolvimento de Sistemas do IFNMG – campus Teófilo Otoni; [2] Docente do IFNMG – campus Teófilo Otoni

Palavras chaves: Ambientes virtuais de aprendizagem; Segurança da informação; Educação; Ensino à Distância.

Introdução

Indubitavelmente, as tarefas cotidianas mais simples encontram grande apoio no aparato digital disponível às sociedades contemporâneas, de modo que considerável parte de seus avanços residem e dependem do concomitante progresso de tecnologias oriundas do referido mundo digital. Assim sendo, o contexto tecnológico representa um valor imensurável para a contemporaneidade.

Tendo como base essa premissa, observa-se que o avanço tecnológico também adentrou no âmbito da educação, de modo que, atualmente, há incontáveis ambientes online de aprendizagem. Nesse novo contexto, portanto, novas considerações e também indagações ganham notório destaque, de modo que a presente obra se dedica a elucidar as questões concernentes aos critérios de segurança da informação dos referidos ambientes virtuais de aprendizagem.

Assim sendo, o presente resumo prioriza o debate sobre a empregabilidade da segurança da informação em ambientes virtuais de aprendizagem, evidenciando componentes primordiais para uma abordagem expressiva e fundamentada, a fim de apresentar aspectos responsáveis pela relevância do tema.

Material e métodos /Metodologia

Com o objetivo de esclarecer tais questões, através de uma revisão bibliográfica, este resumo dedica-se a esclarecer importantes questões acerca dos Ambientes Virtuais de Aprendizagem, caracterizados por constituírem um modo de integração entre o ensino e o aluno, valendo-se, para tanto, do meio digital. Por fim, inclinando-se nas temáticas acerca da segurança da informação, expõe a importância de se possuir mecanismos de averiguação de riscos e ameaças, bem como métodos de prevenção nos ditos ambientes virtuais de aprendizagem.

Resultados e discussão

Segurança da Informação

Nos Ambientes Virtuais de Aprendizagem, é importante que o usuário se sinta seguro, e que as informações disponibilizadas por ele sejam destinadas para fins anteriormente estabelecidos e aceitos. Para que isso ocorra, é imperativo que se aplique nos ambientes princípios estabelecidos pela Segurança da Informação, os quais abrangem questões como: tratar a informação presente no ambiente como um bem institucional; controlar e monitorar o acesso à informação; manter a responsabilidade perante os usuários, gestores e administradores da informação; preparar-se para agir de maneira preventiva e repressiva, estando apta a agir em emergências e garantir a privacidade do

usuário; e, finalmente, adotar uma conduta ativa de modo a instituir medidas disciplinares caso as regras não sejam seguidas (MEDEIROS, 2001).

Fatores comportamentais exercem grande influência sobre a segurança de determinada informação. Entre eles estão, por exemplo, a forma com que o usuário lida com as funções destinadas a ele, o ambiente, a infraestrutura definida ou mesmo ações de indivíduos mal-intencionados. A tríade CIA (*Confidentiality, Integrity and Availability*) – Confidencialidade, Integridade e Disponibilidade – representa a estrutura por trás de elementos responsáveis pela análise, planejamento e a implementação da segurança para o grupo de informações estabelecido. A confidencialidade consiste em limitar o acesso da informação aos indivíduos autorizados pelo detentor da informação. A integridade visa garantir a legitimidade das informações que sofreram manipulação, mantendo as características originais designadas pelo proprietário, abrangendo o controle de mudanças e a garantia de que funções como a inserção, manutenção e destruição de determinada informação sejam preservadas. Quanto à disponibilidade, entende-se que ela garante que determinada informação esteja sempre disponível para uso apropriado e que não interfira na proteção das informações que foram atribuídas pelo proprietário (REIS, 2010).

Mecanismos de proteção contra riscos e ameaças

Métodos designados a explorar brechas e vulnerabilidades são cada vez mais utilizados e, consequentemente, aprimorados, uma vez que quando determinado meio não consegue exercer com sucesso a finalidade para a qual foi desenvolvido, um novo método é aplicado a fim de suprir essa função. Com intuito de realizar testes que evidenciassem vulnerabilidades, um estudo elencado pela *Open WEB Application Security Project* (OWASP), entidade que possui reconhecimento internacional e concebida visando a melhoria da segurança de softwares e aplicativos, detalha as dez vulnerabilidades mais comuns em aplicações web, é caracterizado por realizar a utilização de mais de 500 mil aplicações, providas por um número de organizações não divulgado, sendo algumas delas anônimas. As vulnerabilidades indicadas pelo estudo foram: quebra de controle de acesso, falhas criptográficas, injeção, design inseguro, configuração incorreta de segurança, componentes vulneráveis e desatualizados, quebra de identificação e autenticação, falhas de software e integridade de dados, falhas de registro e monitoramento de segurança e *server-side request forgery* (OWASP, 2013).

Contrapondo-se aos elementos que constituem os riscos e ameaças pertinentes ao ambiente virtual, estão os mecanismos de segurança e os métodos de averiguação, que possuem como propósitos primordiais a segurança e integridade do ambiente onde são introduzidos.

Conclusão(ões)/Considerações finais

Mediante a discussão proposta, concluiu-se que os ambientes virtuais de aprendizagem necessitam de uma série de abordagens provindas de boas técnicas e métodos, de um ciclo de desenvolvimento que priorize práticas que preveem possíveis riscos e ameaças. E que compreendam, também, os erros provenientes da má utilização oriunda do usuário, que é capaz de ocasionar problemas expressivos, destoando do propósito principal dos ambientes que é mediar a aprendizagem com o auxílio da tecnologia.

Assim como exposta a demanda por métodos preventivos, os principais riscos conceituados e listados pelo OWASP evidenciam o quanto os ataques a aplicações web são expressivos, mesmo que os métodos de prevenção estejam disponíveis para aplicação. Revelam também a necessidade de desenvolvimento e aprimoramento de mecanismos da segurança da informação aptos a proverem a devida segurança do sistema.

Agradecimentos

Os autores agradecem ao Instituto Federal do Norte de Minas Gerais pelo apoio financeiro através do Programa Institucional de Bolsas de Iniciação Científica.

Referências

MEDEIROS, C. D. R. **Segurança da informação: implantação de medidas e ferramentas de segurança da informação.** Joinville: Universidade da Região de Joinville – INIVI; Departamento de Informática, 2001. Disponível em: <http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf>. Acesso em: 14 de fev. de 2022.

OWASP. **Welcome to the OWASP Top 10 - 2021**. Disponível em: https://owasp.org/Top10/ . Acesso em: 14 de fev. de 2022.

REIS, H.T.E. **Segurança da informação e a Educação a distância**. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2688/2641. Acesso em: 14 de fev. de 2022.