Revista Multidisciplinar do Nordeste Mineiro, v4,
2022/04
ISSN 2178-6925

EMPREGABILIDADE DE SEGURANÇA DA INFORMAÇÃO EM AMBIENTES VIRTUAIS DE APRENDIZAGEM

EMPLOYABILITY OF INFORMATION SECURITY IN VIRTUAL LEARNING ENVIRONMENTS

Bárbara de Oliveira Guedes Otoni
Acadêmica do curso de Análise e Desenvolvimento de Sistemas, Instituto Federal do Norte de Minas Gerais, Brasil.
E-mail: barbaraguedes10@gmail.com

Luan Diego de Lima Pereira
Docente de Engenharia Elétrica, Instituto Federal do Norte de Minas Gerais, Brasil.
E-mail: luan.pereira@ifnmg.edu.br

Americo Fernando de Souza Alves
Docente de Língua Portuguesa, Literatura e Redação, Instituto Federal do Norte de Minas Gerais, Brasil.
E-mail: americo.alves@ifnmg.edu.br

Revista Multidisciplinar do Nordeste Mineiro, v4,
2022/04
ISSN 2178-6925

Recebido 01/03/2022. Aceito 20/04/2022

Resumo

O artigo aborda, a princípio, a importância dos Ambientes Virtuais de Aprendizagem (AVA) para a construção e consolidação do conhecimento escolar e acadêmico dos indivíduos na sociedade contemporânea. E, ainda, como a utilização dos AVA evidencia que a tecnologia ocupa um espaço significativo na trajetória escolar dos estudantes. Em seguida, indica riscos apontados pelo OWASP (*Open Web Application Security Project*), caracterizado por conter amplo consenso a respeito dos riscos de segurança mais críticos para uma aplicação *web*, que podem comprometer a experiência de estudo conferida por Ambientes Virtuais de Aprendizagem, assinalado como elemento central, caracterizando todo o aspecto passível de análise e aplicação das questões aqui tratadas. Propondo-se a oferecer informações relevantes ao leitor, este trabalho realiza pontuais distinções entre a modalidade de Ensino à Distância e a Atividade Emergencial Remota, e, de forma derradeira, dispõe de métodos abrangidos pela segurança de informação, inclusive os preconizados pelo OWASP, com intuito de enfatizar que riscos e ameaças podem ser abordados e previstos antes mesmo que aconteçam, para que a integridade e segurança em meio ao método aplicado sejam estabelecidas de forma eficaz.

Palavras-chave: Ambientes virtuais de aprendizagem; Segurança da informação; Educação.

Abstract

The article addresses, at first, the importance of Virtual Learning Environments (VLE) towards the construction and consolidation of school and academic knowledge among individuals in contemporary society. And also, how the use of VLE shows that technology occupies a significant space in the school trajectory of students. It then indicates the risks identified by the OWASP (Open Web Application Security Project), characterized by having a broad consensus regarding the most critical security risks for a web application, which can compromise the study experience provided by Virtual Learning Environments, known as central element, characterizing every aspect that can be analyzed and applied to the issues discussed here. Intending to offer relevant information to the reader, this work makes punctual distinctions between the Distance Learning modality and the Remote Emergency Activity, and, lastly, it has methods covered by information security, including those recommended by OWASP, in order to emphasize that risks and threats can be addressed and predicted even before they happen, so that integrity and security in the amongst of the applied method are effectively established.

Keywords: Virtual learning environments; Information security; Education.

1. 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.

Com o objetivo de esclarecer tais questões, e com o apoio de ampla base bibliográfica, este artigo objetiva, em princípio, realizar pontuais distinções entre a modalidade de Ensino à Distância (EaD) e a Atividade Emergencial Remota (AER), visto que, em razão de similaridades, há uma constante confusão entre os dois termos no meio educacional. Posteriormente, 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.

Portanto, dentre muitos aspectos que poderiam ser abordados, priorizou-se 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.

2. Distinções fundamentais entre o Ensino à Distância e a Atividade Emergencial Remota

Inicialmente, é importante dintinguir os dois termos - EaD e AER -, os quais, apesar de serem vistos como análogos, se divergem e possuem, cada um, determinadas particularidades. O termo EaD, ao longo dos anos, tem sido conceituado de diferentes maneiras, e essa característica evidencia a falta de consenso da comunidade responsável pela especificação factual da temática em questão.

Como exemplo disso, observam-se as oscilações entre nomenclaturas nacionais e internacionais, como Estudo Independente e Educação Aberta e a Distância - EAD (Peters, 2001); Tele Educação (Foresti, 2001); Educação Semipresencial (Brasil, 2004); Aprendizagem Flexível (Formiga, 2009); Aprendizagem Imersiva ou *I-Learning* (Mattar, 2012); Aprendizagem Eletrônica ou *E-Learning* (Valente, 2009); Aprendizagem com Mobilidade ou *Mobile-Learning* (Carvalho, 2013); Aprendizagem em Pequenas Doses ou *Micro – Learning* (Richard, 2016) e, por fim, Cursos Online Massivos (Andrade & Silveira, 2016), que caracterizam alguns dos muitos conceitos aplicados, e mesmo constituindo apenas uma parte de um todo, é perceptível que a questão temporal e os avanços tecnológicos possuem implicações inteiramente relacionadas com essas variações conceituais.

A Educação a Distância possui em seu âmbito o que pode ser caracterizado como aspecto primordial, a premissa de que aluno e professor não compartilham o mesmo ambiente físico, e que o meio tecnológico é o canal que possibilita a interação entre ambos, perspectiva compartilhada por Moore e Kearsly (2010, p. 02) os quais conceituam o termo como:

> "O aprendizado planejado que ocorre normalmente em um lugar diferente do local de ensino, exigindo técnicas especiais de criação do curso e de instrução, comunicação por meio de várias

> tecnologias e disposições organizacionais e administrativas especiais."

Sendo assim, o método de Ensino à Distância traz consigo a flexibilidade necessária para estudantes que não conseguiriam estar presencialmente em um ambiente com horários fixos e estipulados pela instituição, viabilizando aos mesmos a possibilidade de determinar os próprios horários de estudo, constituídos por aulas síncronas e assíncronas, que permitem a mediação do conhecimento entre professores e alunos. Sobre a flexibilidade e a facilidade advinda do ensino online, Gilbert comenta que:

> "Há um debate constante no mundo acadêmico sobre quem é levado a estudar on-line. Tem-se como fato dado que os alunos que estudam on-line são adultos, pois essa espécie de aprendizagem, que se dá em qualquer lugar e a qualquer hora, permite-lhes continuar trabalhando em turno integral, sem deixar de também dar atenção à família. O on-line 'típico' é geralmente descrito como alguém que tem mais de 25 anos, está empregado, preocupado com o bem-estar da comunidade, com alguma educação superior em andamento, podendo ser tanto do sexo masculino quanto do feminino." (GILBERT, 2001, p.75).

A confusão conceitual foi estabelecida quando o termo *Educação à Distância* começou a ser usado popularmente para se referir a *Atividades Emergenciais Remotas*, estabelecidas na pandemia da COVID-19, as quais, apesar de possuírem similaridades, diferem-se no momento de aplicação, dado que o Ensino à Distância é uma oferta permanente da instituição de ensino, aplicação oriunda de um novo modelo educacional que se diverge, pois, de uma ação emergencial cuja finalidade seja suprir necessidades acarretadas por restrições momentâneas. As Atividades Emergenciais Remotas somente são aplicadas em situações singulares e específicas, momentos nos quais o ensino convencional ofertado pela

instituição de ensino tornou-se inviável, e toda sua aplicabilidade é propriamente delimitada por aspectos remotos de ensino.

3. Pontos fundamentais acerca dos Ambientes Virtuais de Aprendizagem

Após expor os elementos divergentes que caracterizam e definem os ambientes em xeque, é de extrema importância abordar de que maneira esses ambientes são introduzidos nas atividades escolares e acadêmicas.

Os Ambientes Virtuais de Aprendizagem (AVA) já estavam presentes nos meios acadêmicos e coorporativos de inúmeros indivíduos, entretanto, no contexto social atual, seu uso tem se tornado mais expressivo. A implementação desses ambientes não foi originada a partir de um cenário restritivo e incomum, mas sim da necessidade de novas abordagens em torno da obtenção do conhecimento, o que requer uma nova concepção de ambientes/comunidades de aprendizagem, que sejam constituídos como ambientes virtuais de aprendizagem (OKADA; SANTOS, 2004).

Segundo Santos (2003):

> "A aprendizagem mediada pelo AVA pode permitir que, através dos recursos de digitação, várias fontes de informação e conhecimento possam ser criadas e socializadas através de conteúdos apresentados de forma hipertextual, mixada, multimídia, com recursos de simulações. Além do acesso das possibilidades variadas de leituras, o aprendiz que interage com o conteúdo digital poderá também se comunicar com outros sujeitos de forma síncrona e assíncrona em modalidades variadas de iteratividade: um-um e um-todos, comuns das mediações estruturadas por suportes com impressos, vídeos, rádios, TV, e principalmente, todos-todos, própria do ciberespaço." (SANTOS, 2003, p.4)

Autores como Valentino e Soares (2005) caracterizam AVAs como um espaço social, responsável por realizar interações cognitivo-sociais abrangendo todo ou determinado segmento de um objeto do conhecimento, referindo-se a um lugar na web, onde indivíduos interagem, por intermédio de uma linguagem de hipermídia, introduzindo os fluxos de comunicação entre os indivíduos, viabilizadas pela interface gráfica. Ambientes responsáveis pela aplicabilidade de diversas ferramentas, como a troca de e-mails, chats, fóruns que introduzem discussões, avaliações individuais e propostas de interação realizadas pelos professores, além do controle de acesso delimitado pelos mesmos, apresentando assim modelos de disposição de informações que possibilitam a organização do pensamento e o desenvolvimento de novas estratégias de comunicação.

Assim sendo, é possível inferir que os AVAs são um tipo de estrutura de mescla tecnológica que tem como aspecto primordial oferecer suporte ao processo de ensino-aprendizagem (PEREIRA, 2007), de modo a aplicar variações pedagógicas em questões abordadas pela interface que torna possível a criação de espaços virtuais de aprendizagem que sejam atraentes aos estudantes (KIRNER, 2011;2012).

4. Segurança da Informação

É inegável a importância atribuída à segurança destinada à proteção de dados e informações pessoais. De acordo com Nakamura e Geus (2010), a segurança da informação abrange diversos setores, entre eles os tecnológicos, jurídicos, humanos, de negócios e processuais, elementos esses que estão introduzidos em diferentes cenários, inclusive os abordados pela presente pesquisa.

Para Ferreira, a Segurança da Informação:

> “Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios,

> reduz as perdas e maximiza o retorno dos investimentos e das oportunidades." (2003, p.162)

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: visualizar a informação como um bem institucional; possuir um controle de acesso às informações; manter responsabilidades aos usuários, à administração e ao gestor de informação; preparar-se para situações de contingência e garantir privacidade ao usuário; e, por fim, estabelecer medidas disciplinares, caso as regras sejam descumpridas (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).

4.1 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. Segundo dados do Cert.br, 01 de janeiro a dezembro de 2013, 24% dos incidentes relatados por usuários, referentes a falhas de segurança, tinham como principal objetivo tentativas de fraude e, dentre essa porcentagem, 5% estavam direcionadas a aplicações Web (CERT.BR, 2014).

A esse respeito, é importante citar a *Open WEB Application Security Project* (OWASP), entidade que possui reconhecimento internacional e caracteriza-se por não possuir fins lucrativos. Tal entidade foi concebida visando a melhoria da segurança de softwares e aplicativos, administrando um conjunto importante de informações que viabilizam a avaliação de riscos de segurança a fim de combater formas de ataques através da internet.

Com intuito de realizar testes que evidenciassem vulnerabilidades, um estudo elencado pelo OWASP (2013), que 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. Modificações foram feitas e a nova versão que lista os dez principais riscos de segurança de aplicativos web possui três novas categorias, quatro categorias com alterações de nomenclatura, escopo e alguma consolidação no Top 10 para o ano de 2021.

Quebra de controle de acesso - o controle de acesso tem como intuito impor que somente as permissões destinadas ao usuário sejam acessadas, restringindo o mesmo de ações que estão dentre as não permitidas. Falhas como divulgação,

modificação ou destruição de informações não autorizadas estão entre as abrangidas pela categoria.

Falhas criptográficas – anteriormente conhecidas como exposição de dados confidenciais, que era um sintoma amplo, em vez de uma causa raiz, a renovação dessa categoria teve como principal objetivo priorizar as falhas relacionadas à criptografia, que geralmente resultam na exposição de dados confidenciais ou comprometimento do sistema.

Injeção – categoria que contém o segundo maior número de ocorrências em aplicativos, caracterizando vulnerabilidades quando a aplicação não realiza etapas de validação, filtragem ou higienização dos dados fornecidos pelo usuário, dentre os pontos de extrema importância.

Design inseguro – nova categoria inserida com foco nos riscos relacionados a falhas de design, caracterizada por ser ampla e representar diferentes pontos fracos. É importante pontuar que um design inseguro não pode ser corrigido após uma implementação perfeita, visto que os controles de segurança necessários nunca foram criados. Essa categoria apresenta, também, a relevância de uso de modelagem de ameaças, padrões e princípios de design seguro e arquiteturas de referência.

Configuração incorreta de segurança – categoria que subiu uma posição, é derivada de elementos como mais mudanças em softwares altamente configuráveis, listando vulnerabilidades providas de falta de proteção apropriada, permissões configuradas de forma incorreta em serviços em nuvem, ou mesmo onde as contas padrões que possuem senhas ativas em que alterações não foram feitas.

Componentes vulneráveis e desatualizados – por meio de análise de dados, essa categoria foi dada como um dos dez principais riscos. É a única categoria que não possui Exposições Comuns, mas possui elementos que podem caracterizar vulnerabilidades providas de um sistema que não realiza varreduras regularmente,

ou no qual correções e atualizações não são realizadas na plataforma, estruturas e dependências subjacentes, aumentando os riscos.

Quebra de identificação e autenticação – componente que era conhecido como "autenticação quebrada", está relacionado a falhas de identificação, tais como a permissão de ataques automatizados ou mesmo a permissão de senhas padrão, fracas ou conhecidas.

Falhas de software e integridade de dados – essa categoria foi expandida para incluir mais tipos de falhas. As falhas em questão estão diretamente relacionadas ao código e à infraestrutura que não possuem mecanismos de proteção contra violações de integridade.

Falhas de registro e monitoramento de segurança – anteriormente nomeada como "registro e monitoramento insuficientes", essa categoria foi reformulada a fim de abranger uma quantidade maior de tipos de falhas. Destina-se a detectar, escalar e responder às violações ativas. Em elementos como monitoramento e registro, violações não podem ser detectadas.

Server-Side Request Forgery – as falhas de SSRF ocorrem sempre que um aplicativo da web busca um recurso remoto sem validar a URL (*Uniform Resource Locator)* fornecida pelo usuário, e a gravidade dessa falha tem tomado maiores proporções devido aos serviços de nuvem e à complexidade das arquiteturas.

4.2 Mecanismos de segurança e métodos de prevenção

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. De acordo com Reis (2010), tais mecanismos são fragmentados em vários métodos específicos que visam falhas singulares, e que constituem dois grandes grupos onde o suporte para recomendações de segurança é pontuado:

Controles físicos: são estabelecidos por barreiras responsáveis por delimitar contato e acesso referente às informações ou à infraestrutura (responsável pela existência da informação). Alguns exemplos de mecanismos que apoiam os controles físicos são: portas, trancas, paredes, blindagem e guardas.

Controles lógicos: são barreiras responsáveis por restringir ou delimitar o acesso à informação que está em um ambiente que possui controle, geralmente eletrônico, e que poderia estar exposto à alteração não autorizada proveniente de um elemento mal-intencionado.

No que concerne aos elementos de prevenção, e utilizando como base de pesquisa os métodos preconizados pelo OWASP (2013), pontuando apenas alguns dos elementos responsáveis por compor cada categoria dos dez principais riscos de segurança, temos:

A necessidade de possuir um servidor confiável, ou API sem servidor para que o controle de acesso seja eficaz, é um dos elementos característicos de prevenção para que não ocorra nenhum tipo de modificação referente a verificação de controle de acesso. Levando-se também em consideração a implementação de mecanismos de controle de acesso ao invés de realizar a reutilização dos mesmos em todo aplicativo, dando ênfase na minimização do uso de *Cross-Origin Resource Sharing* (CORS). Outro ponto importante abordado pela categoria, e que possui fácil aplicabilidade, é o registro de falhas de controle de acessos, reportando-as aos administradores quando for apropriado.

As falhas criptográficas caracterizam-se por uma listagem com vários elementos; contudo, os métodos citados não compõem todos os métodos necessários para que haja um cenário que garanta total segurança. É necessário que haja verificação de que os algoritmos, protocolos e chaves de padrão forte e atualizadas estejam presentes dentre as características que compõem o aplicativo em questão, além de se levar em conta o não armazenamento de dados confidenciais desnecessariamente, considerando que dados que não são retidos não podem ser roubados.

Em relação à injeção, é importante pontuar elementos como a utilização de API segura, que visam a fornecer uma interface parametrizada, em paralelo com validação de entrada positiva do lado do servidor. Além disso, é importante pontuar que esses elementos não constituem uma defesa completa, partindo do princípio de que muitos aplicativos necessitam de caracteres especiais.

No que diz respeito aos elementos que constituem a categoria de design inseguro, é perceptível a importância empreendida no ciclo de via de desenvolvimento seguro, já que, posteriormente, esse será um fator primordial que se faz presente em todos os tópicos que pontuam os elementos necessários para que os princípios de um design seguro sejam aplicados. É importante considerar algumas questões, tais como: estabelecer e usar uma biblioteca constituída de padrões de projetos seguros ou o uso de estradas pavimentadas prontas para usar componentes, optando também, por delimitar o consumo de recursos por usuário ou serviço.

A vulnerabilidade é pertinente em aplicações web devido a alguns dos fatores pontuados na categoria de configuração incorreta de segurança. A esse respeito, dentre os meios de prevenção estão listados aspectos que são relativos à remoção ou não instalação de recursos e estruturas não utilizados, assim como o envio de diretivas de segurança para os clientes.

É importante pontuar também elementos como a remoção de dependências não utilizadas, recursos, arquivos, componentes e documentações desnecessárias, que fazem parte da categoria de componentes vulneráveis e desatualizados, bem como realizar o monitoramento de bibliotecas e componentes que não possuem manutenção ou que não cria *patches* de segurança visando versões anteriores.

Evidenciando a relação direta com o usuário, e visando à prevenção de possíveis erros, a identificação e a falha de autenticação, prioriza-se a aplicação de princípios de como evitar a implementação de credenciais padrões, especialmente para usuários administradores. Sempre que viável, realizar a implementação da autenticação de multifator, evitando, assim, o preenchimento automatizado de

credenciais, força bruta e ataques derivados da reutilização de credenciais roubadas. Por fim, porém não pontuando todos os métodos de prevenção abordados, está a implementação de verificação de senhas fracas, como realizar os testes que englobem as senhas novas ou alteradas que estão dentre as conceituadas como as 10.000 piores senhas.

Em falhas de software e integridade de dados, a prevenção pode se dar com o uso de assinaturas digitais a fim de verificar se o software é realmente proveniente de uma fonte esperada e não sofreu nenhum tipo de alteração, bem como manter atualizada a verificação referente ao processo de revisão que abrange as alterações de código e configurações, visando diminuir as chances de que um código malicioso seja introduzido em seu pipeline de software.

Em relação às falhas de integridade de software e dados, são levantados fatores como a certificação de todas as falhas provenientes do *login*, validação de entrada do lado do servidor e controle de acesso que fornecem registros suficientes para que contas maliciosas sejam identificadas e retiradas, assim como a adoção de um plano de respostas e recuperação de acidentes, como o Instituto Nacional de Padrões e Tecnologia (NIST) 800-61r2.

Abordando o SSRF, tal programa caracteriza-se por possuir uma segmentação da camada de rede e da camada de aplicativo. Como elementos constitutivos da primeira camada, é possível citar a imposição de políticas de *firewall* “negar por padrão” ou mesmo regras que delimitem o controle de acesso à rede para bloquear todo o tráfego de internet, a não ser o que é dado como essencial. Na segunda camada, fatores como limpar e validar todos os dados de entrada fornecidos pelo cliente, bem como não enviar respostas brutas aos clientes são conceituadas como primordiais.

5. Considerações Finais

O presente trabalho discorreu acerca da importância da aplicabilidade de vertentes da segurança da informação no cenário virtual, destacando as fragilidades e demandas dos ambientes virtuais de aprendizagem. Dentre os aspectos que poderiam ser abordados no presente artigo, priorizou-se a empregabilidade da segurança da informação, evidenciando elementos primordiais para uma abordagem significativa e fundamentada, haja vista a relevância do tema. Para melhor entendimento por parte do leitor, o tema foi fragmentado em alguns tópicos, considerando-se a necessidade de conhecimento a respeito do assunto, seja por livre escolha, ou pela imposição estabelecida perante o cenário emergencial apresentado.

Mediante a discussão proposta, concluiu-se que os ambientes virtuais de aprendizagem necessitam de uma série de abordagens providas 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.

Referências

ALVES, Luiz Gustavo. PAES, Ricyellen Oliveira. MARTINS, Henrique Pachioni.

TÉCNICAS DE SEGURANÇA EM AMBIENTE VIRTUAL DE APRENDIZAGEM.

Disponível em: http://www.fatecbauru.edu.br/mtg/source/T%C3%A9cnicas%20de%20seguran%C3%A7a%20em%20ambientes%20virtuais%20de%20aprendizagem.pdf. Acesso em: 02 de dez. de 2021.

CABRAL, Julia Leal. FAGUNDES, Thaisi dos Santos. LUX, Beatriz. FROZZA, Rejane. ANÁLISE BIBLIOMÉTRICA DOS TEMAS USABILIDADE, AMBIENTES VIRTUAIS DE APRENDIZAGEM E PESSOAS COM DEFICIÊNCIA. Revista Jovens Pesquisadores. 2016. Disponível em: https://online.unisc.br/seer/index.php/jovenspesquisadores/article/view/7298. Acesso em: 02 de dez. de 2021.

CAZELATTO, Caio Eduardo Costa. SEGATTO, Antonio Carlos. DOS CRIMES INFORMÁTICOS SOB A ÓTICA DO MEIO AMBIENTE DIGITAL CONSTITUCIONALIZADO E DA SEGURANÇA DA INFORMAÇÃO. Revista Jurídica Cesumar. 2014. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/3713/2469. Acesso em: 16 de jan. de 2022.

CONSTANTINO, Paulo Roberto Prado. POLETINE, Márcia Regina de Oliveira. EMPREGO DOS AMBIENTES VIRTUAIS DE APRENDIZAGEM NA EDUCAÇÃO PROFISSIONAL: um relato de experiências de blended learning. Revista Eletrônica Gestão & Saúde. 2013. Disponível em: https://periodicos.unb.br/index.php/rgs/article/view/309/296. Acesso em: 16 de jan. de 2022.

FERNANDES, Nélia Oliveira Campo. SEGURANÇA DA INFORMAÇÃO. Rede e-

Tec Brasil. 2013. Disponível em: http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y. Acesso em: 14 de fev. de 2022.

KOEHLER, Cristiane. AMBIENTES VIRTUAIS DE APRENDIZAGEM. Secretaria de Tecnologia Educacional Universidade Federal do Mato Grosso. 2020. Disponível em: https://setec.ufmt.br/ri/bitstream/1/88/1/FASCICULO_Ambientes_Virtuais_AprendizaApr.pdf. Acesso em: 14 de fev. de 2022.

OWASP. BEM-VINDO AO TOP 10 DA OWASP – 2021. Disponível em: http://owasp.org/Top10/.

SEGINFO. OWASP TOP 10 LIBERADAS AS VULNERABILIDADES PRINCIPAIS DE 2021. Disponível em: https://seginfo.com.br/2021/09/16/owasp-top-10-liberadasas-vulnerabilidades-principais-de-2021/. Acesso em: 14 de fev. de 2022.

REIS, Hugo Toffalini Esteves dos. 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.

SILVA, Denise Ranghetti Pilar da. STEIN, Lilian Milnitsky. SEGURANÇA DA INFORMAÇÃO: uma reflexão sobre o componente humano. Ciências & Cognição. 2007. Disponível em: http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410. Acesso em: 14 de fev. de 2022.

TERTULINO, Rodrigo. LIMA, Rommel. MAIA, Cicília. VULNERABILIDADES DE SEGURANÇA NO MOODLE. Anais de VII Escola de Computação e suas Aplicações – EPOCA. 2014. Disponível em: https://www.researchgate.net/profile/Marcos-Cintra-2/publication/341625567_Proposta_de_Classificador_de_Lesoes_de_Pele_Utilizando_Caracteristicas_de_Forma_Cor_e_Textura/links/5ecc757ba6fdcc90d69999cc/Proposta-de-Classificador-de-Lesoes-de-Pele-Utilizando-Caracteristicas-de-FormaCor-e-Textura.pdf#page=12. Acesso em: 14 de fev. de 2022.

VASCONCELOS, Cristiane Regina Dourado. JESUS, Ana Lucia Paranhos. SANTOS, Carine de Miranda. AMBIENTE VIRTUAL DE APRENDIZAGEM (AVA) NA EDUCAÇÃO A DISTÂNCIA (EAD): UM ESTUDO SOBRE O MOODLE. Brazilian Journal of Development. 2020. Disponível em: https://www.brazilianjournals.com/index.php/BRJD/article/view/8165. Acesso em: 14 de fev. de 2022.