# SISTEMAS DE AUTENTICAÇÃO ELETRÔNICA NA AVALIAÇÃO: CONTRIBUIÇÕES NA EDUCAÇÃO EM REDE

**Luziana Quadros da Rosa[1];**

**Lucyene Lopes da Silva [2];**

**Felipe de Matos Müller[3];**

**Márcio Vieira de Souza[4];**

***Resumo**: Os atuais modelos de avaliação online exigem novos padrões de segurança e mecanismos diferenciados contra os casos de fraudes e plágio. Os sistemas de autenticação eletrônica são recursos utilizados para identificação de usuários e legitimação de autoria, tais como os softwares antiplágio, chaves de acesso, senhas, sistemas de biometria, sistemas de localização, entre outros. Este estudo é uma revisão da literatura sobre o modo como os sistemas de autenticação eletrônica são utilizados na educação. Este estudo correlaciona os conceitos apresentados ao relato de uma experiência de educação em rede sobre o Projeto TeSLA que desenvolve tecnologias para autenticação com base na abordagem RRI. As possibilidades de se obter uma avaliação autêntica online devem considerar questões éticas, legais e de confiabilidade dos avaliados, independente do sistema eletrônico escolhido.*

Palavras-chave: *autenticação eletrônica; avaliação on-line; educação em rede; pesquisa e inovação responsáveis (RRI); TeSLA.*

***Abstract**: The current online assessment models require new security standards and differentiated mechanisms against fraud and plagiarism cases. Electronic authentication systems are resources used to identify users and legitimation of authorship, such as antiplagiarism software, access keys, passwords, biometrics systems, location systems, among others. This study is a review of the literature on way electronic authentication systems are used in education. The study correlates the concepts presented to the report of a networked education experience on the TeSLA Project that develops technologies for authentication based on the RRI approach. The possibilities of obtaining an authentic online assessment should consider ethical, legal and reliability issues of the assessed ones, independent of the electronic system chosen.*

*Keywords*: *electronic authentication; e-assessment; network education; responsible research and innovation (RRI); TeSLA.*

---

[1]Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento – Universidade Federal de Santa Catarina (UFSC) Florianópolis – Brasil. E-mail: luziana@hotmail.com

[2] Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento – UFSC - Florianópolis – Brasil. E-mail: lucyenen@gmail.com

[3] Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento – UFSC - Florianópolis – Brasil. E-mail: matos.muller@gmail.com

[4] Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento – UFSC - Florianópolis – Brasil. E-mail: marciovieiradesouza@gmail.com

## 1 CONSIDERAÇÕES INICIAIS

O uso de tecnologias da informação e comunicação propicia a disseminação do conhecimento para muitas pessoas. À medida que se torna natural à convivência humana e tecnológica mudam-se padrões culturais, sociais, biológicos e, até mesmo, os padrões físicos. Nesse contexto, como apontou uma pesquisa realizada pela University of the Sunshine Coast, localizada em Queensland, na Austrália, e que foi amplamente divulgada pela mídia no primeiro semestre de 2019 ao revelar a observação feita pelos cientistas de uma alteração óssea na cabeça de jovens que utilizam em excesso seus *smartphones* (Shahar & Sayers, 2018).

Esses aspectos supracitados caracterizam a atual geração de humanos formada pelos nativos digitais, como denominado por Marc Prensky (Palfrey & Gasser, 2011), sendo composta pelos nascidos em meio às tecnologias digitais, totalmente conectados, cuja vida provavelmente será alterada pelo envolvimento com essa tecnologia. Toda essa conexão com o mundo virtual pode levar a outros excessos que são percebidos também na busca de fontes de informação. Na educação, por exemplo, se torna relevante identificar se determinado texto foi realmente elaborado por um estudante, considerando o fácil acesso à internet e seus portais de conteúdos, em que comandos no teclado do computador, do tipo "CTRL+C" e "CTRL+V", transportam quase que instantaneamente um texto da *web* para dentro de um documento.

Este exemplo supramencionado se configura como um ato de plágio, ou seja, alguém se apropria de um conteúdo ou parte dele sem referenciar o autor da obra, como se aquele material fosse seu. No Brasil, a prática de plágio é crime, conforme descrito no Art. nº 184, do Decreto Lei nº 2.848, Código Penal (1940), que trata de Crime de Violação aos Direitos Autorais, redação dada pela Lei nº 10.695, de 1º de Julho de 2003.

Atualmente é comum encontrar a oferta de *softwares* para identificação de plágio em textos, tais como Turnitin, iThenticate, Ephorus, Plagius, Plagiarism Detect, entre outros. Através do uso de *softwares* e outros sistemas operacionais algumas instituições de ensino, privadas ou públicas, iniciam gradualmente um trabalho de identificação de autores em seus processos avaliativos por meio de sistemas de autenticação de análise textual, seja por meio dos simples detectores de plágio ou por outros sistemas mais sofisticados. Para Okada, Whitelock, Holmes e Edwards (2019a) os sistemas de autenticação eletrônica no campo da avaliação surgem para evitar plágios e fraudes, prevendo autenticação da identidade e dando suporte à identificação de autoria de seus usuários.

Nesse contexto, delimitando-se a verificar os aspectos mencionados pelos autores supracitados, todavia sem entrar na seara de privacidade de dados, especificamente referente às legislações locais e globais vigentes sobre o tema, este artigo aborda o modo como os sistemas de autenticação eletrônica são utilizados na educação. Assim, por meio desta revisão bibliográfica, são apresentados alguns dos atuais sistemas de autenticação eletrônica encontrados na literatura e suas potenciais vantagens no cenário educacional em rede.

## 2 METODOLOGIA

O presente estudo trata-se de uma revisão da literatura sobre o tema: sistemas de autenticação eletrônica na avaliação educacional. Neste contexto, apresentam-se como procedimentos metodológicos a revisão narrativa da literatura, que se mostra como uma temática mais aberta e não necessariamente estipula um protocolo (Cordeiro, Oliveira, Rentería & Guimarães, 2007).

No entanto, sem pretensão de se esgotar todas as fontes das informações, a revisão narrativa se mostra importante por tratar de um tema inovador e que possui carência de mais estudos aplicados, visto que a área de pesquisa é recente, como apontam Okada et al. (2019a). Todavia, a temática é necessária de ser investigada, pois, como apontam Pithan e Vidal (2013), as questões sobre plágio acadêmico - acrescentando-se ainda as fraudes nos sistemas *online* de avaliação - representam problemas éticos, jurídicos e pedagógicos.

Deste modo, na busca das referências teóricas foram utilizadas as bases científicas de dados Scopus, ERIC e SciELO, nas quais foram empregados os seguintes termos de busca: "electronic authentication" AND “e-assessment". Ademais, a seleção dos artigos conta com a inclusão de algumas investigações que apresentam experiências práticas de autenticação eletrônica, tais como as fundamentadas em Okada et al., em 2019.

Os conceitos teóricos apresentados a seguir contribuem para o conhecimento dos tipos de recursos de autenticação eletrônica que estão sendo utilizados atualmente, bem como exemplificam uma investigação relevante referente a um projeto fomentado pela Comissão Europeia, o projeto TeSLA.

## 3 PANORAMA DOS SISTEMAS DE AUTENTICAÇÃO ELETRÔNICA

Para Okada et al. (2019a) ocorre um aumento de fraudes nas avaliações *online*, em que os estudantes tendem a copiar ideias sem referenciar os autores ou adquirindo trabalhos prontos na internet, prejudicando a autenticidade da avaliação. Díaz Arce (2017) considera que o plágio acadêmico se observa em todos os níveis de ensino, afirmando que as melhores ferramentas utilizadas para a identificação e correção do plágio são comerciais, o que dificulta o acesso daqueles que possuem recursos limitados para aquisição destas ferramentas. Todavia, Santos (2018) apresenta como uma das possíveis ações de combate ao plágio, sendo desenvolvidas pelas bibliotecas das Universidades Federais da região nordeste do Brasil, o estímulo ao uso de *softwares* antiplágio, que podem ser realizadas por meio da indicação do uso dessas ferramentas para os estudantes, disponibilização de tutoriais e aquisição de assinaturas das versões comerciais de *softwares* detectores de plágio.

Em determinado caso, o Google Docs, ferramenta gratuita para criação de formulários *online*, é usado como instrumento de avaliação, como visto em Badi'atul, Mar'atus e Guritno (2017). Na investigação dos autores supracitados, o recurso Google Docs tem como uma limitação de seus resultados a contagem de tempo, em que o tempo de resposta dos estudantes foi cronometrado e limitado. No estudo mencionado, a estratégia de limitar o tempo é empregada como critério para evitar fraudes na coleta de dados, especificamente, no envio das respostas; no entanto, deixando frustrados os estudantes, participantes da pesquisa.

Já os autores Lilley, Meere e Barker (2016) sugerem para aprimoramento da autenticação *online*, no intuito de reduzir fraudes e trapaças, o "*remote live invigilation"*, que corresponde a um processo de chamada remota ao vivo, como forma de dar credibilidade às avaliações na educação a distância. Neste sentido, Clarke, Dowland e Furnell (2013) também investigaram um sistema de chamada remota eletrônica que denominaram de "e-Invigilator", em um processo de supervisão biométrico para avaliações eletrônicas em Ambientes Virtuais de Aprendizagem. Para Aguilar, Burlak e Lara (2010) esse tipo de sistema ajuda a identificar realmente quem está realizando determinada avaliação, entretanto, os pesquisadores utilizaram, ainda, um sistema de mineração de dados empregado ao sistema avançado de avaliação remota na avaliação de estudantes de nível superior.

No contexto de autenticação via senha alfanumérica, Enamait (2012) identifica que este é um sistema muito frágil, e sua investigação mostra que o uso do *software* de gerenciamento de senhas, juntamente com os esforços de conscientização do usuário de informações secundárias (eletrônicas e verbais), resulta em um aumento na entropia de senhas, ou seja, tornam o processo mais seguro por meio de maior aleatoriedade e

imprevisibilidade. Hoshiar et al. (2014) reconhecem a respeito da eficácia da autenticação e autenticidade do estudante no aprendizado *online,* em instituições de ensino superior comunitárias, que estas dependem de ajustes entre políticas e procedimentos institucionais, desenvolvimento e treinamento dos profissionais e de efetivos serviços de suporte tecnológico.

Outros autores trabalham com abordagem de autenticação bimodal, ou seja, referente ao uso concomitante de mais de um recurso de autenticação. Nesse contexto, Levy, Ramim, Furnell e Clarke (2011) apresentam a multibiometria que incluiu impressões digitais, reconhecimento de voz e face dos usuários. Os autores Adetunji, Zuva e Appiah (2018) trabalham em um *framework* de biometria bimodal, em um estudo de sistemas de avaliação eletrônica que integram digitação (pressionamento) de teclas e reconhecimento de face.

De acordo com Ojo, Zuva e Ngwira (2016), a biometria multimodal e a autenticação transparente aparecem como necessárias nas investigações futuras sobre os processos de autenticação. Nesse contexto, a aplicação potencial da autenticação multibiométrica contínua e dinâmica, segundo Levy et al. (2011), surge como uma abordagem justificável quando comparada com a abordagem de autenticação mais comum de identificação de usuário, por meio de senha, em diferentes tipos de exames.

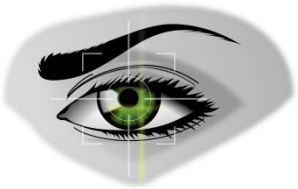
Corroborando com as tecnologias apresentadas, as técnicas desenvolvidas pelo Projeto Adaptive Trust-based e-Assessment System for Learning (TeSLA), fundada pela União Europeia, referem-se a uma parceria entre a Open University, visa investigar a autenticação e autoria de estudantes através da biometria, análise textual e segurança (Okada et al., 2019a).

No Projeto TeSLA a investigação da **biometria** se dá por meio de análise de reconhecimento facial, reconhecimento de voz e avaliação de como o usuário utiliza o teclado para digitar; a **análise textual** se dá por meio de ferramentas antiplágio que são utilizadas em comparações textuais de documentos e, também, na verificação de autoria de documentos pelo meio de técnica forense; por fim, a **assinatura digital** é usada como meio de autenticação, já o registro de data e hora para a identificação do período em um evento é registrado pelo computador (Okada et al., 2019a).

Neste contexto, uma avaliação autêntica pode ser conquistada através do uso de tecnologias da informação e comunicação (Okada et al., 2019a). A Figura 1 demonstra cinco grupos de instrumentos de autenticação eletrônica, em que os grupos conhecimento, biometria, propriedade e outros (mecanismos) foram identificados por Karim e Shukur

(2016), já o grupo *output* de aprendizado foi acrescentado por Okada et al., (2019a) com base no Projeto TeSLA.

Figura 1 – Grupos de autenticação eletrônica

| **Grupos** | **Tipo** | **Contexto em que a autenticação é baseada** |
|---|---|---|
|  | CONHECIMENTO | A autenticação é baseada no conhecimento dos estudantes. Como vantagens apresentadas aparecem à facilidade de uso e o baixo-custo, como desvantagem apresentado está o baixo nível de segurança. Os exemplos comumente usados neste grupo são: nome, senha, pergunta de segurança (Ullah, Xiao, Barker, & Lilley, 2014). |
|  | BIOMETRIA | A autenticação é baseada em características fisiológicas e comportamentais. A vantagem deste grupo é a eficácia e a precisão, já as desvantagens estão no fato que elas podem ser tecnicamente complexas e ter um dispendioso custo.<br>As características fisiológicas incluem imagens faciais (2D ou 3D), termografia facial, impressões digitais, geometria das mãos, impressões, termogramas infravermelhos, íris e retina, ouvido, pele, dentária e DNA (Gao, 2012). As características comportamentais incluem o estado da voz, andar, assinatura, movimentos com o mouse, teclado e batimentos (Levy & Ramin, 2007). |
|  | PROPRIEDADE | A autenticação é baseada em objetos privados que o avaliado possui no momento da avaliação, tais como cartões de memória, *dongles* (dispositivo para limitar o acesso de determinados programas no computador) e chaves de acesso (Hastings & Dodson, 2004). |
|  | OUTROS MECANISMOS | A autenticação é baseada em um processo, como a localização do candidato, um registro de data e hora ou de um endereço IP (Okada et al., 2019a) |

| | | |
|---|---|---|
|  | OUTPUT DE APRENDIZADO | A autenticação é baseada no que o estudante produziu em sua escrita e como ela foi estruturada, por exemplo, por meio do uso de *software* antiplágio e análise textual forense (Okada et al., 2019a) |

Fonte: Adaptado de Karim e Shukur (2016) e Okada et al., (2019a).

Todavia, existem preocupações e problemas a serem resolvidos na adoção de sistemas de autenticação eletrônica para validação de avaliações *online* para além das questões virtuais. Como previsto por Rowe (2004) os pequenos testes e os questionários de respostas curtas tendem ser realizados de maneira *online* sob o controle contra o plágio e fraude, por parte de seus avaliadores, no entanto, as avaliações presenciais ainda aparecem como modelos absolutos correspondendo sempre a maior nota de um estudante.

## 4 INOVAÇÃO PARA ALÉM DO CONTROLE DA AVALIAÇÃO

No Projeto TeSLA o processo investigativo baseou-se na abordagem de *Responsible Research and Innovation* (RRI), aqui denominada de Pesquisa e Inovação Responsáveis, que objetiva o envolvimento de pesquisadores, estudantes e tecnólogos no processo de pesquisa e inovação para alinhar as melhores práticas de seus processos e resultados de suas pesquisas com os valores, necessidades e expectativas de sociedade, como descrito no Programa Horizon 2020 (Okada et al., 2019a; European Commission, 2016).

Para Okada et al. (2019a) as descobertas de pesquisa baseada em RRI, no qual os autores verificaram as percepções dos estudantes sobre plágios e fraudes na internet, representam dados relevantes que podem ser utilizados pelos (i) desenvolvedores de tecnologia de autenticação eletrônica, (ii) as instituições de educação, sejam as que ofertam cursos a distância ou que aplicam suas avaliações por meio de tecnologias e (iii) os formuladores de políticas educacionais.

Essa pesquisa supramencionada teve relevância por realizar parcerias com instituições e universidades por intermédio da instituição The Open University (OUUK). No Brasil, por exemplo, através de uma rede de pesquisadores RRI, voluntariamente participaram da coleta de dados estudantes, professores e pesquisadores das seguintes instituições: Universidade Federal de Santa Catarina (UFSC); Universidade do Estado da Bahia (Uneb); Pontifícia Universidade Católica do Paraná (PUC-PR); Universidade Federal de Itajubá (UNIFEI);

Universidade de Santa Maria (UFSM); Pontifícia Universidade Católica de São Paulo (PUC-SP); Universidade Federal do Rio de Janeiro (UFRJ); Universidade Federal do Ceará (UFC); Universidade Federal de Juiz de Fora (UFJF); Universidade Aberta do Brasil (UAB); Universidade Estadual do Ceará (UECE).

Além destas, outras instituições também participaram da investigação por meio de seus voluntários. No período em que foi realizada (entre os meses de junho e julho de 2018), a pesquisa obteve no Brasil a participação de mais de 1000 respondentes que encaminharam seus textos de modo *online*, através do ambiente virtual, Modular Object-Oriented Dynamic Learning Environment (MOODLE), para verificação de estilo de escrita.

A ideia principal do projeto baseia-se na possível contribuição da abordagem RRI para sistemas avaliativos efetivos, indo além da disponibilização de dados para elaboração de sistemas eficientes de controle nas avaliações. Para tanto, as questões da pesquisa buscaram responder: Qual a aceitação dessas tecnologias de autenticação eletrônica para a sociedade? Quais suas vantagens e barreiras? Quais as necessidades e oportunidades de sua aplicação? Quais os requisitos de pesquisa sobre este tema?

A articulação da rede para coleta de dados por si só abriu vantagens para a disseminação do conhecimento. Nesse período de pesquisa, ocorreram possibilidades de internacionalização por meio da colaboração entre algumas instituições nacionais e a instituição internacional The Open University. Ademais, houve a utilização de ferramentas de rede, via mídias digitais, para ampliar o convite de participação voluntária, elaboração de certificados e divulgação das parcerias institucionais.

Mesmo realizado dentro de um planejamento pedagógico, os projetos que envolvem os sistemas eletrônicos de avaliação devem considerar a confiança dos usuários. Nesse sentido, as avaliações devem permitir que os estudantes desenvolvam suas habilidades e a compreensão dos diferentes domínios de conhecimento com o melhor de suas competências, como visto nos estudos de alguns pesquisadores (Okada, et al., 2019b). As vantagens apresentadas por Alsadoon (2017) na avaliação eletrônica é a percepção positiva do estudante, o *feedback* imediato do resultado da avaliação e o benefício do aprendizado.

Noguera, Guerrero-Roldán, Peytcheva-Forsyth e Yovkova (2018) verificam que os estudantes *online* estão mais habituados a este tipo de avaliação do que os estudantes presenciais, que se mostram menos confiantes quanto ao uso de um sistema de autenticação eletrônica na avaliação. Para Levy e Ramin (2007) o uso de tecnologias de autenticação contribui para vencer barreiras, tornando o ambiente *online* mais ético e, assim, eliminando opiniões daqueles opositores do ensino *online* que não confiam no método de avaliação.

# 5 CONSIDERAÇÕES FINAIS

Este trabalho buscou investigar, à luz da literatura, as possíveis contribuições dos atuais sistemas de autenticação eletrônica nos processos de avaliação que ocorrem no ambiente educacional. Nesses sistemas frequentemente são vistos ocorrências de plágio e fraude, percebido por alguns autores como aspectos problemáticos para a validação e a autenticação das avaliações.

Entre os atuais sistemas de autenticação, verificou-se um grupo de cinco tipos principais identificados por Karim e Shukur (2016) e Okada et al., (2019a). Os tipos descritos são: (1) conhecimento, aparece como o modelo mais comum e menos seguro, referente a identificações do tipo nome, senha e pergunta de segurança; (2) biometria, aparece como uma autenticação segura, porém complexa e de custo elevado, com base nas características fisiológicas e comportamentais; (3) propriedade, refere-se às autenticações com chaves-de seguranças e demais tipos de recursos de acesso, apesar de segura pode ser fraudada mais facilmente por terceiros; (4) outros mecanismos, referente à autenticação por localização, horário de acesso ou pela informação do Internet Protocol (IP) do computador; (5) *output* de aprendizado, refere-se às autenticações desenvolvidas pelo Projeto TeSLA.

O Projeto TeSLA utiliza a abordagem RRI, referente a Pesquisa e Inovação Responsáveis, para desenvolver avaliações mais autênticas, nas quais os estudantes têm participação significativa no processo avaliativo, demonstrando confiança ao método aplicado, em que são utilizadas *softwares* antiplágio e análise textual forense. Neste projeto supracitado, especificamente a autenticação eletrônica fundamenta-se na produção escrita destes estudantes.

Deste modo, torna-se relevante neste artigo registrar algumas ações feitas em rede pelo Projeto TeSLA com instituições educacionais brasileiras. Na pesquisa, estudantes de universidades públicas e privadas participaram como voluntários do Projeto TeSLA. Essas investigações em rede contribuem para o acesso à informação e ampliam o interesse de pesquisadores sobre o desenvolvimento de sistemas de autenticação eletrônica. Como contribuições do projeto, apresenta-se a possibilidade de realizar avaliações *online*, de modo mais seguro, permitindo até mesmo as substituições das atuais avaliações presenciais.

Todavia o processo de adoção de sistemas avaliativos *online* não depende somente de atributos tecnológicos a serem investidos para garantir sua segurança e efetividade. Ainda,

verifica-se a necessidade de considerar questões éticas, legais e pedagógicas na constituição de um sistema de autenticação. A cooperação em rede, na execução de projetos nessa área, apresenta-se como um fator relevante na Educação em Rede por considerar necessidades e contribuições de culturas e expertises diferentes, ou seja, dividir o conhecimento na rede é a fórmula para multiplicá-lo.

## REFERÊNCIAS


Adetunji, T. O., Zuva, T., & Appiah, M. (2018, December). A framework of bimodal biometrics for e-assessment authentication systems. In 2018 *International Conference on Intelligent and Innovative Computing Applications* (ICONIC) (pp. 1-5). IEEE.

Aguilar, J. A. H., Burlak, G., & Lara, B. (2010). Design and implementation of an advanced security remote assessment system for universities using data mining. *Computación y Sistemas*, 13(4), 463-473.

Alsadoon, H. (2017). Students' perceptions of e-assessment at Saudi Electronic University. *Turkish Online Journal of Educational Technology* - TOJET, 16 (1), 147-153.

Badi'atul, A., Mar'atus, S., & Guritno, A. (2017, July-December). The university students' perception of online examination using Google Form. *Britania Journal of English Teaching*, 1(1), 120-135.

Clarke, N. L., Dowland, P., & Furnell, S. M. (2013, June). E-invigilator: a biometric-based supervision system for e-assessments. In *International Conference on Information Society* (i-Society 2013) (pp. 238-242). IEEE.

Código Penal. *Decreto-Lei nº 2.848*. (1940). Rio de Janeiro. (Redação dada pela Lei Nº 10.695, de 1º de Julho de 2003).

Cordeiro, A. M., Oliveira, G. M., Rentería, J. M. & Guimarães, C. A. (2007). Revisão sistemática: uma revisão narrativa. *Revista do Colégio Brasileiro de Cirurgiões*, 34(6), 428-431. https://dx.doi.org/10.1590/S0100-69912007000600012

Díaz Arce, D. (2017). Evaluación del desempeño de tres herramientas antiplagio gratuitas en la detección de diferentes formas de copy-paste procedentes de internet. *Edutec. Revista Electrónica de Tecnología Educativa*, 59, a354. https://doi.org/10.21556/edutec.2017.59.812

Enamait, J. D. (2012). *The effect of password management procedures on the entropy of user selected passwords* (Doctoral dissertation). Indiana State University Terre Haute, IN, USA.

European Commission [EC]. (2016). *Responsible research and innovation*. Recuperado em https://ec.europa.eu/pro-grammes/horizon2020/en/h2020-section/responsible-research-innovation

Gao, Q. (2012). Biometric authentication to prevent e-cheating. *International Journal of Instructional Technology and Distance Learning*, 9(2), 3-14.

Hastings, N. E., & Dodson, D. F. (2004). Quantifying assurance of knowledge based authentication. In: Proceedings European Conference on Information, 3., *Warfare and Security*. London, UK: ECIW.

Hoshiar, M. et al. (2014). Examining the effectiveness of student authentication and authenticity in online learning at community colleges. *Community College Journal of Research and Practice*, v. 38, n. 4, p. 337-345.

Levy, Y. & Ramim, M. (2007). A theoretical approach for biometrics authentication of e-exams. *Nova Southeastern University*, USA, 93-101.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011). Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, 28(2), 102-113.

Lilley, M., Meere, J., & Barker, T. (2016). Remote Live Invigilation: A Pilot Study. *Journal of Interactive Media in Education*, 2016(1), 6. http://doi.org/10.5334/jime.408

Karim, N. & Shukur, Z. (2016). Proposed features of an online examination interface design and its optimal values. *Computers in Human Behavior*, 64, 414–422.

Noguera, I., Guerrero-Roldán, A., Peytcheva-Forsyth, R., & Yovkova, B. (2018, march). Perceptions of students with special educational needs and disabilities towards the use of e-assessment in online and blended education: barrier or aid? International Technology, *Education and Development Conference* (INTED2018). 818-828, http://doi: 10.21125/inted.2018.1157

Ojo, S. O., Zuva, T., & Ngwira, S. M. (2015, December). Survey of biometric authentication for e-assessment. In 2015 *International Conference on Computing, Communication and Security* (ICCCS) (pp. 1-4). IEEE.

Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2019a). E-authentication for online assessment: a mixed-method study. *British Journal of Educational Technology*, 50(2), 861-875.

Okada, A., Noguera, I., Alexieva, L., Rozeva, A., Kocdar, S., Brouns, F., ... & Guerrero-Roldán, A. E. (2019b). Pedagogical approaches for e-assessment with authentication and authorship verification in Higher Education. *British Journal of Educational Technology*. [s.l.], p.1-19, 11 fev. 2019. Wiley. http://dx.doi.org/10.1111/bjet.12733

Palfrey, J. & Gasser, U. (2011). *Nascidos na era digital*: entendendo a primeira geração de nativos digitais. Artmed.

Pithan, L.; Vidal, T. (2013, janeiro-julho). O plágio acadêmico como um problema ético, jurídico e pedagógico. *Direito & Justiça*, 39 (1), 77-82.

Rowe, N. (2004). Cheating in online student assessment: beyond plagiarism. *Online Journal of Distance Learning Administration* http://www.educause.edu/Resources/CheatinginOnlineStudentAssessm/153159

Santos, I. (2018). Ações de combate ao plágio desenvolvidas pelas bibliotecas universitárias da região Nordeste. *Revista ACB*, 23(3), 460-464. Recuperado de https://revista.acbsc.org.br/racb/article/view/1456

Shahar, D., & Sayers, M. (2018). Prominent exostosis projecting from the occipital squama more substantial and prevalent in young adult than older age groups. *Scientific reports*, 8(1), 3354. http://dx.doi.org/10.1038/s41598-018-21625-1

Ullah, A., Xiao, H., Barker, T., & Lilley, M. (2014). Evaluating Security and Usability of Profile Based Challenge Questions Authentication in Online Examinations. *Journal of Internet Services and Applications*, 5(1), [2]. https://doi.org/10.1186/1869-0238-5-2