Revista
EDaPECi
EDUCAÇÃO A DISTÂNCIA E PRÁTICAS EDUCATIVAS COMUNICACIOANIS E INTERCULTURAIS

ISSN: 2176-171X

Revista EDaPECI
São Cristóvão (SE)
v.22. n. 3, p. 63-77
set./dez. 2022

DOI: http://dx.doi.org/10.29276/redapeci.2022.22.3182471.63-77

Perceptions on gamification towards cybersecurity literacy: social sustainability of educative projects

----

Percepções sobre a gamificação para a alfabetização ciber-segurança: sustentabilidade social de projectos educativos

----

Percepciones sobre la gamificación hacia la alfabetización en ciberseguridad: sostenibilidad social de los proyectos educativos

José Morais[1]
Jorge Simões[2]
Justino Lourenço[3]
Sérgio Sargo Lopes[4]

Resumo: Covid19 pandemic has stimulated both the discussion on the use of IT related teaching tools and the exposure of the student population to vulnerabilities linked to cybersecurity literacy. The study presented is based on the assumption that the use of gamification as an element or tool that promotes learning within digital environments may be feasible, and more specifically may function as a teaching element on issues related to cybersecurity for students, especially for higher education students. In order to quantify the openness of students to such a tool path, quantitative methodology was used, and a survey was carried out in two Polytechnic Institutions (PI), achieving a sample of 95 students, and seeking perceptions on positive impacts resulting from the creation of a game scenario for better learning. The statistical analysis conducted tested hypotheses regarding representations and practices about gamification and cybersecurity. Results show that students, regardless of their higher education course, clearly understand what Gamification is and its goals, and also that students adopt good cybersecurity practices according to their higher education course. This last result goes accordingly with the supposition that gamification can and should be used in cybersecurity literacy.

Palavras-chave: *Cybersecurity. Covid19. Gamification learning environments. Higher education.*

***Abstract**: A pandemia de Covid19 estimulou tanto a discussão sobre a utilização de ferramentas de ensino relacionadas com as TI como a exposição da população estudantil a vulnerabilidades ligadas à alfabetização em matéria de cibersegurança. O estudo apresentado baseia-se no pressuposto de que o uso da gamificação como elemento ou ferramenta que promove a aprendizagem em ambientes digitais pode ser viável, e mais especificamente pode funcionar como elemento de ensino sobre questões relacionadas com a cibersegurança para estudantes, especialmente para estudantes do ensino superior. A fim de quantificar a abertura dos estudantes a tal caminho de ferramenta, foi utilizada metodologia quantitativa, e foi realizado um inquérito*

[1] Doutor em Sociologia, Professor Coordenador no Instituto Superior Politécnico Gaya (ISPGAYA), Portugal, Investigador no CEOS.PP, Portugal.

[2] Doutorado em Engenharia Telemática, Professor Coordenador no Instituto Superior Politécnico Gaya (ISPGAYA), Portugal, Investigador no INESC-TEC.

[3] Mestre em Telecomunicações, Professor no Instituto Superior Politécnico Gaya (ISPGAYA), Portugal.

[4] PhD em Ciências da Informação, Professor no Instituto Superior Politécnico Gaya (ISPGAYA), investigador no Distance Education and E-learning Laboratory - LE@D - Universidade Aberta, Portugal.

em duas Instituições Politécnicas (PI), obtendo uma amostra de 95 estudantes, e procurando perceções sobre os impactos positivos resultantes da criação de um cenário de jogo para uma melhor aprendizagem. A análise estatística realizada testou hipóteses relativas a representações e práticas sobre gamificação e cibersegurança. Os resultados mostram que os estudantes, independentemente do seu curso superior, compreendem claramente o que é a gamificação e os seus objectivos, e também que os estudantes adoptam boas práticas de cibersegurança de acordo com o seu curso superior. Este último resultado vai de acordo com a suposição de que a gamificação pode e deve ser utilizada na alfabetização em cibersegurança.

Keywords*: Ambientes de aprendizagem da gamificação. Cibersegurança. Covid19. Ensino superior.*

Resumen*: La pandemia de Covid19 ha estimulado tanto el debate sobre el uso de herramientas de enseñanza relacionadas con las TI como la exposición de la población estudiantil a las vulnerabilidades relacionadas con la alfabetización en ciberseguridad. El estudio que se presenta parte de la base de que el uso de la gamificación como elemento o herramienta que promueve el aprendizaje dentro de los entornos digitales puede ser factible, y más concretamente puede funcionar como elemento didáctico sobre temas relacionados con la ciberseguridad para los estudiantes, especialmente para los de educación superior. Para cuantificar la apertura de los estudiantes a tal vía de herramienta, se utilizó una metodología cuantitativa, y se realizó una encuesta en dos Instituciones Politécnicas (IP), logrando una muestra de 95 estudiantes, y buscando las percepciones sobre los impactos positivos resultantes de la creación de un escenario de juego para un mejor aprendizaje. El análisis estadístico realizado puso a prueba las hipótesis relativas a las representaciones y prácticas sobre la gamificación y la ciberseguridad. Los resultados muestran que los estudiantes, independientemente de su curso de educación superior, entienden claramente lo que es la gamificación y sus objetivos, y también que los estudiantes adoptan buenas prácticas de ciberseguridad según su curso de educación superior. Este último resultado concuerda con la suposición de que la gamificación puede y debe ser utilizada en la alfabetización en ciberseguridad.*

Palabras clave: *Educación superior. Ciberseguridad. Covid19. Entornos de aprendizaje con gamificación.*

1 INTRODUÇÃO

The pandemic stress caused by COVID19 required a sudden change in daily work routines and especially in teaching. The college's traditional classrooms had to be quickly converted from ordinary face-to-face sessions to remote sessions using videoconferencing software. This sudden change had to be made within a short period of time. It happened perhaps without the proper preparation of all involved in terms of best practices related to the use of communications software and the full range of cybersecurity issues that went along with those practices.

At the same time, and even after pandemic constraints have been minimised, it is clear that the remote communication solutions employed will remain relevant as enablers of work and classroom efficiency. This new thinking in the learning environment could be enriched with the leverage of gamification. Several relevant state-of-the-art articles have shown the clear relevance of new technologies and processes in increasing the efficiency of the learning ecosystem (LOURENÇO et al., 2022; MORAIS et al., 2022; KINH, 2004; PEARSHOUSE, & SHARPLES, 2000).

If we can link the issue of cybersecurity to that of sustainability by minimizing the costs associated with cyberthreats (SADIK et al., 2020), starting from a financial perspective, the two issues are brought together when cybersecurity is linked to the notion of insecurity or uncertainty (LEWALLEN, 2021) that characterize contemporary societies. The promotion of sustainability in its different meanings should be integrated in the governance strategy of the educational, scientific and cultural projects of higher education institutions, according to the Institutional Evaluation Manual of the Portuguese Higher Education Evaluation Agency A3ES (2022). In this study, we follow an approach of engagement of the institutions involved in the sense of sustainability also in social terms, as a way of institutional strategy that contributes to a social general access to knowledge in the field of cybersecurity literacy and places the topic on the horizon of the curricular content offered to students. The purpose of this study is to answer the questions: a) are students aware of issues such as gamification or cybersecurity? b) are students aware of the potential that lies in replicating gamification for cybersecurity literacy purposes?

2 GAMIFICATION: CONCEPTS AND TECHNOLOGIES

The strategic introduction of a game scenario into a non-game environment, implemented through solutions such as websites, online communities, learning management systems, or corporate intranets, aims to increase the motivation of participants and promote the efficiency of the process (GONZÁLEZ, HERNÁNDEZ-MUÑOZ et al., 2021; Y. LU et al, 2021; ROOSTA et al, 2016; TRINIDAD GARCÍA et al, 2021; VANDUHE, et al, 2020).

Gamification, a concept known since 2010 (DICHEV, DICHEVA, 2017; KRATH SCHUERMANN, VON KORFLESCH, 2021), is usually defined as the use of game design elements in non-game contexts (DETERDING et al, 2011). Gamification uses the features of digital games such as narrative, feedback, reward systems, conflict, cooperation, competition, clear goals, experience points, levels, progressive disclosure of content, and more. Studies on gamification have focused on how these game features can be used in other contexts not directly related to games (KHALEEL et al, 2016; SAILER et al, 2017).

Education is one of the most important contexts of gamification research that do not involve games (BOZKURT, DURAK, 2018; SAILER, HOMNER, 2020; TRINIDAD, RUIZ, CALDERÓN, 2021). It can be seen as the use of game features in learning environments. These learning environments are often supported by digital platforms and tools. The purpose of gamified learning environments is to enhance student motivation and engagement by changing their behavior toward learning activities, especially those that may not otherwise be engaging. Gamification in education should not be confused with game-based learning and the use of serious games. Although these approaches share common elements, gamification does not use full-fledged games, but only elements and techniques extracted from games.

Recent literature reviews (MANZANO--LEÓN et al., 2021; TRINIDAD, RUIZ ,CALDERÓN, 2021) have shown that gamification has been used in different learning environments and at different levels of learning. Gamification proved to be a valid learning strategy at different educational levels with positive effects on students' academic performance, engagement, and motivation. A meta-analysis conducted by Sailer and Homner (2020) also found that gamified learning can be an effective approach, but which factors contribute most to the success of gamification is still unclear. The academic community is trying to establish gamification as a scientific research discipline, with contributions from other fields of knowledge such as psychology, education, and information and communication technologies (TRINIDAD et al, 2021).

The popularity of gamification has increased in recent years, promoting its use in a variety of application areas such as health, business, society, tourism and especially education. On the other hand, this gamification push brought a number of theatrical, empirical, and technological challenges that need to be addressed. Regarding the technological challenges, there is an urgent need for appropriate software tools and new technological approaches to support and promote new gamification tools that provide flexibility, adequate gamification design support and activity monitoring, and expand the range of game elements besides the traditional points, badges and leaderboards. All these topics have one main goal: faster and more efficient development tools to support rich immersive teaching environments (TRINIDAD et al, 2021). Next, new and trendy technological approaches to the (expected) technological gamification evolution are presented.

A gaming solution that could dynamically adapt to a student's particular learning curve would promote more effective gamification application in a learning scenario. One example is its use as a tool for an Artificial Intelligence (AI) course (DRASKOVIC, 2019; REYES et al, 2020). A tool that could generate a personalized gamified learning system in an automated way. A bibliographic source refers to the relevance of the following concepts in gamification: fun, motivation, autonomy, progressivity, feedback, fault tolerance, experimentation, creativity, and adaptation to the specific case (LLORENS-LARGO et al, 2016). The adaptive play cycle concept is also applied in supporting mobile health applications by encouraging user engagement (LLORENS-LARGO et al, 2016). Another approach relies on an ontological structure to represent gamified collaborative learning scenarios (CL) and demonstrates the utility of this approach in generating personalized conceptual models for gamification of CL scenarios based on students' needs and individual characteristics (CHALLCO et al., 2015).

It is of great importance to develop a rich learning environment that truly engages the student in an immersive learning experience. To this end, augmented reality (AR) and virtual reality (VR) resources can be key to success (JIANG , ZENG, 2019). A much richer experience with a gamified platform could be achieved through gesture recognition (GR), as proposed in Ekneling et al. (2018), which enables the improvement of data collection and annotation through gamification. The article describes a hand tracking and a GR with the support of a AR and VR application. On the other hand, Google's game Ingress (AR) can serve as a basis for developing learning from games (SHENG, 2013). Support from AR, VR and immersive 3D projections can enrich students' museum visit (PANTILE et al, 2016). In some science fields, being able to almost physically feel a shape or even an object will enrich the learning experience: astronomical concepts are a possible example (Patricio, 2019), an electrochemistry course can also be an application example (CHEN, LIAO, 2015), or teaching mobile X-ray imaging (SÜNCKSEN, 2018). Learning new languages will also benefit from the use of AR technologies (ZHENMING, 2017). Finally, all of these VR and AR will make important contributions to learners with disabilities in the context of gamification (BOZGEYIKLI, 2014; MAIDENBAUM, AMEDI, 2015).

Blockchain (BC) technology is a new trend and is growing in popularity. The popularity of BC has expanded its application beyond a digital currency: from finance, medicine, digital marketplaces, pharmaceuticals, and government agencies. Their relevance is underpinned by trust, transparency, and integrity, without the need for a third party to support them (PARIZI, DEHGHANTANHA, 2018). One approach presented enables Da Vinci discovery through a novel AR, which combines BC with experiential learning to engage participants in an interactive discovery of Leonardo da Vinci's work (SUVAJDZIC, 2020).

The Internet-of-Things (IoT) approach makes it possible to efficiently build a multitude of ordinary devices that can be connected to each other. Any object relevant to the learning process can be used as a sensor or an actuator. In addition to the immersive visual experiences described in the previous sections, the IoT allows all objects in the classroom to be used to measure or directly influence the learning experience.

2.1 CYBERSECURITY CONCERNS

A gamified system as a learning tool has great potential, as described in the previous sections. At the same time, all information flow, processing, and storage should maintain integrity and take all measures to protect the user's privacy. Thus, a gamification solution should consider the cybersecurity risks (YONEMURA, 2017; SHARIF, AMEEN, 2020). On the other hand, gamification is a tool for teaching security awareness (DIAKOUMAKOS, 2021; MARTIN et al, 2019; YONEMURA ET AL, 2018; YONEMURA et al, 2018; KUMAR, 2017; NGUYEN, PHAM, 2020; RAVAL et al, 2018).

The following theoretical construct describes some general problems related to the security of a gamified system. First, we refer to the problem of login and password security. Authentication via a login and password is the most common method for accessing a gamified tool. Unless good security practices are implemented, this first process is a major failure point. A combination of an unsecured password without a proper aging mechanism, or even sharing the credentials with a colleague, pose a serious security risk. Also of great concern is the risk of remote access without the support of a secure connection such as a Virtual Private Network (VPN). Multi-level authentication is an important step in circumventing these security vulnerabilities. Several solutions have been proposed to overcome the described vulnerabilities. These include support for machine learning techniques (DJOSIC, et al., 2020; MISBAHUDDIN et a.l, 2017), secure login solutions (WAHEED, 2016), or support for BC technology (BISWAS, 2021).

About software vulnerabilities and updates, we can state that the layer of software is also of extreme relevance. All the data input, processing and output in a usable interface are the result of a secure code execution. Any coding flaw may be the open door for a security issue, and it is an important point of research (IANNONE et al., 2022). In particular, over the communication management software module – where all the information flows from and into the communication path: wired or wireless, each of it with its particular vulnerabilities.

There are several proposed solutions: the development of a software vulnerability prediction model. This solution allows predicting whether a software module is vulnerable or not, promoting a relevant tool for security improvement (SHAMAL, 2017). Automatic vulnerability detection is also a proposal. In a new approach, a compressed experimental setup is created for accessing the methodology and reporting the vulnerabilities found (GHOSH, 1998; VISALLI, 2019). Static code analysis (SCA) also has a good detection rate and is the key technique to improve the effectiveness of vulnerability detection (PEREIRA, 2020). Finally, the last bibliographic reference is the support of machine learning solutions as a relevant tool for software vulnerability analysis (PEERZADA & KUMAR, 2021). A good security policy, which includes the constant updating of software, is also a simple way to improve software productivity and reduce the threat of software vulnerabilities.

3 METHODOLOGY

This study adopts a predominantly quantitative methodological approach through the use of a questionnaire survey as a research tool with a series of questions related to two different areas, i- learning through gamification in online environments and ii- cybersecurity practices, in a sample composed of college students from different academic knowledge areas. The study aims to understand students' perceptions of active methods, in the specific case of gamification in digital learning environments, and students' resulting attitudes towards cybersecurity practices in the same digital environments.

3.1. STATISTICAL ANALYSIS

Statistical analysis included descriptive statistical measures (absolute and relative frequencies, means and their standard deviations) and inferential statistical measures. The significance level for rejecting the null hypothesis was set at (α) ≤ 0.05. Exploratory factor analysis (EFS), Cronbach's coefficient for internal consistency alpha, Pearson's correlation coefficient, and Kruskal-Wallis test were used. The normality of the distribution of the variables was analyzed with the Shapiro-Wilk test and the homogeneity of the variances with the Levene test. Statistical analysis was performed using SPSS (Statistical Package for the Social Sciences) software version 28.

Ninety-five college students from two Portuguese universities participated in the study (see Table 1). Most of the students are male (87.4%) and have a high school academic degree (82.1%). The average age is 23.3 years (SD = 6.6 years) and ranges from a minimum of 18 years to a maximum of 49 years. A significant proportion of students major in HEI to science, math, and computer science (57.9%) and engineering, manufacturing, and construction (30.5%).

Table 1- Sample characterization

	N	%
Age (Mean; Std. Deviation)	23,6	6,6
Gender		
Male	83	87,4
Female	11	11,5
Other	1	1,1
Academic degree		
High School	78	82,1
Undergraduate	16	16,8
Specialist	1	1,1
Undergraduate degree in progress		
Higher Professional Course (CTeSP)	33	34,7
Undergraduate	56	58,9
Master's degree	6	6,4
Knowledge area		
Sciences, Mathematics, and Informatics	55	57,9
Engineering, Manufacturing, and Construction	29	30,5
Social Sciences, Business, and Law	11	11,6

Source: Elaborated by the author (2022).

3.2. RESULTS

In Table 2, we can review students' responses to questions about their experiences with gamification (items 1 through 8) and cybersecurity practises. We highlight the most frequent responses in grey. The responses that resulted in higher agreement were, "In the virtual learning environments or systems (HEI), I always use a password for my student account a password that has uppercase and lowercase letters, numbers, and symbols." (M = 3.61) and "I consider important to implement different teaching methodologies in digital learning environments, e.g., Gamification." (M = 3,40). During the online, because of the pandemic, I took classes in which the teacher used Gamification techniques." (M = 2.11) and "I have already been reading (even partially) the General Data Protection Regulation (GDPR) and I understand everything I read." (M = 2,21).

Table 2- Gamification and cybersecurity practices

Subtitle: 1 - Totally disagree (%); 2 - Partly disagree (%); 3 - Partially agree (%); 4 - Totally agree (%) M - Mean SD - Std. Deviation	1	2	3	4	M	SD
1. I have a full understanding, in general terms, of what lessons with Gamification techniques are.	10,5	15,8	49,5	24,2	2,87	0,90
2. I can identify when the teacher implements gamification techniques in class.	10,5	17,9	47,4	24,2	2,85	0,91
3. During the online class period, because of the COVID-19 pandemic, I took classes in which the teacher used Gamification techniques.	35,8	25,3	30,5	8,4	2,11	0,99
4. I have already had classroom lessons in which the teacher used Gamification techniques.	25,3	24,2	34,7	15,8	2,41	1,03
5. Lessons conducted with Gamification techniques are more interesting and motivating than traditional lecture classes.	7,4	3,2	47,4	42,1	3,24	0,83
6. I consider it important to implement different teaching methodologies in digital learning environments, e.g., Gamification.	5,3	3,2	37,9	53,7	3,40	0,79
7. When I use of networked (Internet), gamified, or other digital teaching and learning resources, I check the system's origin and its digital certificates.	13,7	25,3	46,3	14,7	2,62	0,90
8. In the virtual learning environments or systems of my Higher Education Institution (HEI), I always use in my student account, a password that has uppercase and lowercase letters, numbers, and symbols.	1,1	4,2	27,4	67,4	3,61	0,62
9. I am in the habit of periodically changing the passwords for the systems I use.	26,3	31,6	24,2	17,9	2,34	1,06
10. I only remember to change the password when a particular system makes such a request.	15,8	21,1	37,9	25,3	2,73	1,01
11. I try to inform myself about the security procedures used in the systems and applications I use in my HEI.	13,7	30,5	44,2	11,6	2,53	0,87
12. I only use free antivirus systems (among other protection systems) on my personal computer for study and work.	16,8	16,8	26,3	40	2,89	1,11
13. I frequently check that the computer's antivirus is up to date and functional.	7,4	18,9	31,6	42,1	3,08	0,95
14. I periodically check that my computer's firewall is up to date and functional.	9,5	22,1	32,6	35,8	2,94	0,98
15. I try to be informed about the best information security practices to adopt when using the Internet.	3,2	13,7	50,5	32,6	3,13	0,76
16. I have already been reading (even partially) the General Data Protection Regulation (GDPR) and I understand everything I read.	32,6	25,3	30,5	11,6	2,21	1,03

Source: Elaborated by the author (2022).

The questionnaire concluded by asking students if they had already been the victim of a cyberattack that caused tail damage, and if so, what the cyberattack was. In Table 3, we see that almost all students indicated that they had never been a victim of an attack in a digital environment. However, the few students who indicated they had ever been a victim of an attack primarily indicated phishing attacks and ransomware, and some could not provide any information.

Table 3- Cyberattacks suffered by students

		N	%
17. Have you ever been the victim of a cyberattack that caused you any personal, academic, and/or professional harm? If yes, what was the attack, and in what context?	**Yes**	9	9,5
	No	86	90,5

Source: authors (2022).

The analysis of the relational structure of the items of the scale about students' experiences with gamification was done by an exploratory factor analysis of the correlation matrix with extraction of the factors by the principal components method followed by varimax rotation. The common factors retained were those with a higher eigenvalue of 1. The validity of the factor analysis was checked using the KMO test (0.656- gamification and 0.751- cybersecurity) and Bartlett's test (significant in both sets of questions), indicating acceptable values for continuing the analyses. The factor analysis resulted in a solution with three principal components in the Gamification question complex explaining 74.3% and three components in the Cybersecurity question complex explaining 61.4% of the total variance (see Table 4 and Table 5). The components showed good internal consistency when the internal coefficients were analyzed by the Cronbach Alpha test.

Table 4- Variance explained (Gamification)

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2,859	40,848	40,848	2,859	40,848	40,848
2	1,279	18,277	59,125	1,279	18,277	59,125
3	1,064	15,205	74,330	1,064	15,205	**74,330**
4	,664	9,486	83,817			
5	,556	7,945	91,762			
6	,368	5,253	97,015			
7	,209	2,985	100,000			

Source: Elaborated by the author (2022).

Table 5. Variance explained (Cybersecurity)

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3,275	36,389	36,389	3,275	36,389	36,389
2	1,209	13,434	49,823	1,209	13,434	49,823
3	1,046	11,618	61,441	1,046	11,618	**61,441**
4	,823	9,145	70,586			
5	,800	8,884	79,470			
6	,640	7,109	86,579			
7	,468	5,200	91,779			
8	,420	4,672	96,451			
9	,319	3,549	100,000			

Source: Elaborated by the author (2022).

In the rotated matrix, only elements that had a saturation level > 0.40 were considered. The components generated from the gamification question set were labeled as follows: i- "knows gamification," ii- "uses gamification," and iii- "importance gamification." The components generated from the cybersecurity question set were labeled as follows: i- "best practices IS personal" (IS means Information Security), ii- "best practices IS password", and iii- "best practices IS HEI".

3.3. HYPOTHESES

For this study and in the context of the research questions posed, two hypotheses were formulated, one related to gamification and the other to cybersecurity. Statistical analysis was performed through the Krus-kal-Wallis test between the correlation of the components generated in the factor analysis and the independent groups, as shown below.

H1 - Students, regardless of their higher education course, clearly understand what Gamification is and its goals. We found no statistically significant differences between students' majors and their understanding of gamification, as we can see in Table 6.

Table 6- Hypothesis test (Gamification)

	Hypothesis Test Summary Null Hypothesis	Test	Sig.
1	The distribution of C1 - Knows_Gamification is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,391
2	The distribution of C2 - Uses_Gamification is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,496
3	The distribution of C3 - Importance_Gamification is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,713

Source: Elaborated by the author (2022)

H2 - Students regardless of their higher education course, adopt good cybersecurity practices. As shown in Table 7, there is a significant difference in the adoption of personal information security best practices between the groups. Thus, we found that the difference between the master's degree group and the other course groups is relevant. We found that the group with master's degree (median = 0.897) adopts as many good information security practices compared to the undergraduates (median = -0.020) and the higher professional courses-CTeSP (median =-0.030).

Table 7- Hypothesis test (Cybersecurity)

	Hypothesis Test Summary Null Hypothesis	Test	Sig.
1	The distribution of C1 - Best_practices_IS_personal is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,034
2	The distribution of C2 - Best_practices_IS_password is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,899
3	The distribution of C3 - Best_practices_IS_HEI is the same across categories of current_course_degree.	Independent-Samples Kruskal-Wallis Test	0,875

Source: Elaborated by the author (2022).

The results of the survey and the tests of the hypotheses tend to show that the students' level of maturity is significant in cybersecurity practices and consequently in the use of gamified educational computer resources. In this case, there may be some influence on life and professional experience on the significance presented in the scope of master's degree students compared to other educational groups. However, we stress that a number of factors can affect this trend because, specifically, students can adopt different cybersecurity behaviors and in the use of gamification resources. This does not imply, however, that they will fully adopt good cybersecurity practices and use of information in virtual learning environments, which is something that can be generally verified in the survey conducted for this study.

4 - CONCLUSIONS

The pandemic problem had a profound effect on civilization in the twenty-first century. For the lecturing sector in particular, an immediate response was required. The COVID19 pandemic presented an opportunity for a number of novel techniques and technology, as previously discussed in the sections, to be the required lever for the introduction of innovative practises. The research's bibliography unequivocally points to gamification, IoT, AI, or blockchain as cutting-edge and pertinent educational techniques. The lecture players are pushed to their connected gadgets and into faraway parts as a direct result of the crisis' physical remoteness. The additional security issues that teachers and students now face are also covered in this article.

The methodology used was a survey and in-depth statistical analysis. Among the main conclusions: Most participants partially agreed that they could understand and identify with gamification in the context of a classroom. On the other hand, the majority did not have an idea of how a classroom would work with the gamification tool. The majority also agree that it is important to use different teaching methods such as gamification in digital learning environments. Gamification is a tool that needs to be researched, and its implementation has failed in the pandemic period

Under the research topic of security vulnerabilities and user knowledge, there were most positive responses for the good practice of using strong passwords, regular concern for updating the virus list, and the general state of the firewall.

Some negative points are the following: there is no practice of a regular password change, the majority uses free antivirus solutions and there is little knowledge about the principles, implications, and advantages of the GDPR.

Finally, the statistical process of hypothesis testing clearly show that there is no correlation between students' degree and the understanding of the goals and the definition of gamification. On the contrary, students with more literacy adopt better security practices. Results show that gamification can be used to achieve cybersecurity literacy objectives, and HEIs should integrate these objectives in their content, in an effort to establish best practices.

REFERENCES

A3ES. **Manual de Avaliação Institucional**. 2022. Disponível em: https://www.a3es.pt/sites/default/files/Manual_de_avaliacao_institucional_A3ES_Consulta_publica.pdf

BISWAS, B. N.; BHITKAR, S. D.; PUNDKAR, S. N. **Secure Login: A Blockchain based web application for Identity Access Management System**. 2021 2nd International Conference for Emerging Technology (INCET). Anais...IEEE, 2021. https://doi.org/10.1109/INCET51464.2021.9456352

BOZGEYIKLI, E. et al. **Poster: Design and development of a virtual reality system for vocational rehabilitation of individuals with disabilities. 2014 IEEE Symposium on 3D User Interfaces** (3DUI). **Anais**... IEEE, 2014. Disponível em: https://doi.org/10.1109/3DUI.2014.6798877

BOZKURT, A.; DURAK, G. A systematic review of gamification research: In pursuit of homo ludens. **International journal of game-based learning**, v. 8, n. 3, p. 15–33, 2018. http://doi.org/10.4018/IJGBL.2018070102

C. CHALLCO, G. et al. Personalization of gamification in collaborative learning contexts using ontologies. **IEEE Latin America Transactions**, v. 13, n. 6, p. 1995–2002, 2015. Disponível em: https://doi.org/doi.org/ 10.1109/TLA.2015.7164227

CHEN, M.-P.; LIAO, B.-C. **Augmented reality laboratory for high school electrochemistry course**. 2015 IEEE 15th International Conference on Advanced Learning Technologies. **Anais**...IEEE, 2015. Disponível em: https://doi.org/doi.org/ 10.1109/ICALT.2015.105

DETERDING, S. et al. **From game design elements to gamefulness**: Defining "gamification." Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments - MindTrek '11. Anais...New York, New York, USA: ACM Press, 2011. Disponível em: https://doi.org/10.1145/2181037.2181040

DIAKOUMAKOS, J. et al. **Cyber-range federation and cyber-security games**: A gamification scoring model. 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Anais...IEEE, 2021. Disponível em: https://doi.org/ 10.1109/CSR51186.2021.9527972

DICHEV, C.; DICHEVA, D. Gamifying education: what is known, what is believed and what remains uncertain: a critical review. **International journal of educational technology in higher education**, v. 14, n. 1, 2017. Disponível em: https://doi.org/10.1186/s41239-017-0042-5

DJOSIC, N.; NOKOVIC, B.; SHARIEH, S. **Machine learning in action: Securing IAM API by risk authentication decision engine**. 2020 IEEE Conference on Communications and Network Security (CNS). **Anais**...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/CNS48642.2020.9162317

DRASKOVIC, D. **Development of intelligent systems and application of gamification in artificial intelligent learning**. 2019 27th Telecommunications Forum (TELFOR). **Anais**... IEEE, 2019. Disponível em: https://doi.org/10.1109/TELFOR48224.2019.8971360.

EKNELING, S. et al. **Magestro: Gamification of the data collection process for development of the Hand gesture recognition technology**. 2018 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct). Anais...IEEE, 2018. Disponível em: https://doi.org/ 10.1109/ISMAR-Adjunct.2018.00124

GHOSH, A. K.; O'CONNOR, T.; MCGRAW, G. **An automated approach for identifying potential vulnerabilities in software**. Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186). Anais...IEEE Comput. Soc, 2002. Disponível em: https://doi.org/ 10.1109/SECPRI.1998.674827

MADERO GONZALEZ, C. M.; HERNANDEZ-MUNOZ, G. M.; GUTIERREZ LEYTON, A. E. **The effect of gamification on motivation in a virtual classroom**. 2021 XI International Conference on Virtual Campus (JICV). Anais...IEEE, 2021. Disponível em: https://doi.org/ 10.1109/ JICV53222.2021.9600324

IANNONE, E. et al. The secret life of software vulnerabilities: A large-scale empirical study. **IEEE transactions on software engineering**, p. 1–1, 2022. Disponível em: https://doi.org/ 10.1109/TSE.2022.3140868

JIANG, J.; ZENG, L. **Research on the application of virtual reality technology in the teaching model**. 2019 14th International Conference on Computer Science & Education (ICCSE). Anais...IEEE, 2019. Disponível em: https://doi.org/ 10.1109/ICCSE.2019.8845411

KHALEEL, F. L. et al. Gamification Elements for Learning Applications. **International journal on advanced science**, engineering and information technology, v. 6, n. 6, p. 868, 2016. Disponível em: https://media.neliti.com/media/publications/103628-EN-gamification-elements-for-learning-appli.pdf

KING, V. **Technology-facilitated online and distance learning student support**. IEEE International Conference on Advanced Learning Technologies, 2004. Proceedings. **Anais**... IEEE, 2004. Disponível em: https://doi.org/ 10.1109/ICALT.2004.1357662

KRATH, J.; SCHÜRMANN, L.; VON KORFLESCH, H. F. O. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. **Computers in human behavior**, v. 125, n. 106963, p. 106963, 2021. Disponível em: https://doi.org/10.1016/j.chb.2021.106963

KUMAR, S. A. et al. **Gamification of internet security by next generation CAPTCHAs**. 2017 International Conference on Computer Communication and Informatics (ICCCI). Anais... IEEE, 2017. Disponível em: https://doi.org/ 10.1109/ICCCI.2017.8117754

LEWALLEN, J. Emerging technologies and problem definition uncertainty: The case of cybersecurity. **Regulation & governance**, v. 15, n. 4, p. 1035–1052, 2021. Disponível em: https://doi.org/10.1111/rego.12341

LLORENS-LARGO, F. et al. Gamification of the learning process: Lessons learned. **IEEE Revista Iberoamericana de Tecnologias del Aprendizaje**, v. 11, n. 4, p. 227–234, 2016. Disponível em: https://doi.org/ 10.1109/ RITA.2016.2619138

LOURENÇO, J. et al. **Conceptions on higher education students about use of technologies in the learning process**: A comparative study. INTED2022 Proceedings. Anais...IATED, 2022. Disponível em: https://library.iated.org/download/INTED2022TOC

MAIDENBAUM, S.; AMEDI, A. Blind in a virtual world: **Mobility-training virtual reality games for users who are blind.** 2015 IEEE Virtual Reality (VR). **Anais**...IEEE, 2015. Disponível em: https://doi.org/ 10.1109/VR.2015.7223435

MANZANO-LEÓN, A. et al. Between level up and game over: A systematic literature review of gamification in education. **Sustainability**, v. 13, n. 4, p. 2247, 2021. Disponível em: https://doi.org/10.3390/su13042247

MARTIN, S. et al. **Increasing engagement in a network security management course through gamification**. 2019 IEEE Global Engineering Education Conference (EDUCON). **Anais**...IEEE, 2019. Disponível em: https://doi.org/ 10.1109/EDUCON.2019.8725071

MISBAHUDDIN, M.; BINDHUMADHAVA, B. S.; DHEEPTHA, B. **Design of a risk based authentication system using machine learning techniques**. 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). **Anais**...IEEE, 2017. Disponível em: https://doi.org/ 10.1109/UIC-ATC.2017.8397628

MORAIS, J. et al. **Conceptions on higher education professors about use of technologies in the learning process**: A comparative study. INTED2022 Proceedings. Anais...IATED, 2022. Disponível em: https://library.iated.org/download/INTED2022TOC

NGUYEN, T. A.; PHAM, H. **A design theory-based gamification approach for information security training**. 2020 RIVF International Conference on Computing and Communication Technologies (RIVF). Anais...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/ RIVF48685.2020.9140730

PANTILE, D. et al. **New technologies and tools for immersive and engaging visitor experiences in museums**: The evolution of the visit-actor in next-generation storytelling, through augmented and virtual reality, and immersive 3D projections. 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). **Anais**...IEEE, 2016. Disponível em: https://doi.org/ 10.1109/SITIS.2016.78

M. PARIZI, R.; DEHGHANTANHA, A. **On the understanding of gamification in blockchain systems**. 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). **Anais**...IEEE, 2018. Disponível em: https://doi.org/ 10.1109/W-FiCloud.2018.00041

PATRICIO, J. M.; COSTA, M. C.; MANSO, A. **A gamified mobile augmented reality system for the teaching of astronomical concepts**. 2019 14th Iberian Conference on Information Systems and Technologies (CISTI). **Anais**... IEEE, 2019. Disponível em: https://doi.org/ 10.23919/CISTI.2019.8760658

PEARSHOUSE, I.; SHARPLES, M. **CETADL: a research and development facility for e-learning**. Proceedings International Workshop on Advanced Learning Technologies. IWALT 2000. Advanced Learning Technology: Design and Development Issues. **Anais**...IEEE Comput. Soc, 2002. Disponível em: https://doi.org/ 10.1109/IWALT.2000.890602

PEERZADA, B.; KUMAR, D. **Analyzing software vulnerabilities using machine learning**. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). **Anais**...IEEE, 2021. Disponível em: https://doi.org/ 10.1109/IWALT.2000.890602

PEREIRA, J. D. **Techniques and tools for advanced software vulnerability detection**. 2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). **Anais**...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/ISSREW51248.2020.00049

RAVAL, R. et al. **Competitive learning environment for cyber-physical system security experimentation**. 2018 1st International Conference on Data Intelligence and Security (ICDIS). **Anais**...IEEE, 2018. Disponível em: https://doi.org/ 10.1109/ICDIS.2018.00042

REYES, A. A. et al. **A preliminary work on visualization-based education tool for high school machine learning education**. 2020 IEEE Integrated STEM Education Conference (ISEC). **Anais**...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/ISEC49744.2020.9280629

ROOSTA, F.; TAGHIYAREH, F.; MOSHARRAF, M. **Personalization of gamification-elements in an e-learning environment based on learners' motivation**. 2016 8th International Symposium on Telecommunications (IST). **Anais**... IEEE, 2016. Disponível em: https://doi.org/ 10.1109/ISTEL.2016.7881899

SADIK, S. et al. Toward a sustainable cybersecurity ecosystem. **Computers**, v. 9, n. 3, p. 74, 2020. Disponível em: https://doi.org/10.3390/ computers9030074

SAILER, M.; HOMNER, L. The gamification of learning: A meta-analysis. **Educational psychology review**, v. 32, n. 1, p. 77–112, 2020. Disponível em: https://doi.org/10.1007/ s10648-019-09498-w

SAILER, M. et al. How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. **Computers in human behavior**, v. 69, p. 371–380, 2017. Disponível em: https:// doi.org/10.1016/j.chb.2016.12.033

SHAMAL, P. K.; RAHAMATHULLA, K.; AKBAR, A. **A study on software vulnerability prediction model**. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). **Anais**...IEEE, 2017. Disponível em: https://doi.org/ 10.1109/ WiSPNET.2017.8299852

SHARIF, K. H.; AMEEN, S. Y. **A review of security awareness approaches with special emphasis on gamification**. 2020 International Conference on Advanced Science and Engineering (ICOASE). **Anais**...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/ICOASE51841.2020.9436595

SHENG, L. Y. **Modelling learning from Ingress** (Google's augmented reality social game). 2013 IEEE 63rd Annual Conference International Council for Education Media (ICEM). **Anais**...IEEE, 2013. Disponível em: https://doi.org/ 10.1109/CICEM.2013.6820152

SUNCKSEN, M. et al. **Gamification and virtual reality for teaching mobile x-ray imaging**. 2018 IEEE 6th International Conference on Serious Games and Applications for Health (SeGAH). **Anais**...IEEE, 2018. Disponível em: https://doi.org/ 10.1109/SeGAH.2018.8401364

SUVAJDZIC, M. et al. Discover DaVinci – **A Gamified Blockchain Learning App**. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). **Anais**...IEEE, 2020. Disponível em: https://doi.org/ 10.1109/ SeGAH.2018.8401364

TRINIDAD, M.; CALDERON, A.; RUIZ, M. GoRace: A multi-context and narrative-based gamification suite to overcome gamification technological challenges. **IEEE access: practical innovations, open solutions**, v. 9, p. 65882–65905, 2021. Disponível em: https://doi.org/ 10.1109/ACCESS.2021.3076291

TRINIDAD, M.; RUIZ, M.; CALDERON, A. A Bibliometric Analysis of Gamification Research. **IEEE access: practical innovations, open solutions**, v. 9, p. 46505–46544, 2021. Disponível em: https://doi.org/ 10.1109/ACCESS.2021.3063986

VANDUHE, V. Z.; NAT, M.; HASAN, H. F. Continuance intentions to use gamification for training in higher education: Integrating the technology acceptance model (TAM), social motivation, and task technology fit (TTF). **IEEE access: practical innovations**, open solutions, v. 8, p. 21473–21484, 2020. Disponível em: https://doi.org/ 10.1109/ACCESS.2020.2966179

VISALLI, N. et al. **Towards automated security vulnerability and software defect localization**. 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA). **Anais**...IEEE, 2019. Disponível em: https://doi.org/ 10.1109/SERA.2019.8886795

LU, Y. et al. Motivation under gamification: An empirical study of developers' motivations and contributions in stack overflow. **IEEE transactions on software engineering**, p. 1–1, 2021. Disponível em: https://doi.org/ 10.1109/TSE.2021.3130088

YONEMURA, K. et al. **Effect of security education using KIPS and gamification theory at KOSEN**. 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). Anais...IEEE, 2018. Disponível em: https://doi.org/ 10.1109/ISCAIE.2018.8405480

YONEMURA, K. et al. **Security education using gamification theory**. 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST). **Anais**...IEEE, 2018b. Disponível em: https://doi.org/ 10.1109/ICEAST.2018.8434432

YONEMURA, K. et al. **Practical security education on operational technology using gamification method**. 2017 7th IEEE International Conference on Control System, Computing and Engineering (ICCSCE). **Anais**...IEEE, 2017. Disponível em: https://doi.org/ 10.1109/ICCSCE.2017.8284420

ZHENMING, B. et al. **Development of an english words learning system utilizes 3D markers with augmented reality technology**. 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE). **Anais**...IEEE, 2017. Disponível em: https://doi.org/ 10.1109/GCCE.2017.8229353

Recebido em 14 de julho de 2022
Aceito em 15 de novembro de 2022