CyberKids: video game for raising cyber security awareness in children

Juan Perez
Engineering Faculty
Andres Bello University
Vina del Mar, Chile
j.perezveas@uandresbello.edu

Roman Torres
Engineering Faculty
Andres Bello University
Vina del Mar, Chile
romina.torres@unab.cl

Sven von Brand
Engineering Faculty
Andres Bello University
Vina del Mar, Chile
svbrand@gmail.com

Abstract—In most countries, a large percentage of children between the ages of eight and thirteen have access to a mobile device at home, where monitoring and supervision by a trusted adult is not enough, so statistics on children victimized by bullying and damage to the integrity of their personal data have been increasing considerably.

In this work, we design and develop a serious game, a playful application that integrates and delivers educational content on cybersecurity to users aged 8 to 12 years, allowing them to have basic ideas about the responsibilities that the use of current technologies entails. The contents raise awareness about the use of strong passwords and vulnerabilities identification through gamification techniques to ensure both learning and entertainment.

Index Terms—Gamification, cybersecurity, vulnerabilities, ed ucational, learning

I. INTRODUCCION´

The use of technologies has been present in the new generations that are experiencing some of the evolutionary changes of recent years, so the number of underage users connected has risen (even more).

during the pandemic) and thus the risks. Risks such as: publication of sensitive information, being a victim of Phishing or scams in general, being a victim of online peer bullying or cyber predators downloading malicious content, including others. Each of these risks could damage personal integrity, as well as the devices they use.

Despite the existence of information for parents, guardians and educators regarding the dangers of the Internet, cases continue to increase. The reasons can be multiple: passive mode of learning around the subject; the way to measure if the learning was assimilated by the

students in a theoretical way (memorizing concepts) rather than by solving practical problems or fictitious situations; unattractive material or classified as

bored; among others.

In this sense, there is extensive literature on gamification techniques and serious games that have been successful in authentic teaching and learning of students in a wide range of age and subject matter [1]. In the field of cybersecurity, it has been widely used [2]. In school during specialized camps study before high two, good results are described on the 200 students intervened [3]. A systematic study on serious games in cybersecurity categorizes them into being alert, security in the network and on the web, cryptography and secure software development [4]. A recent study identifies more than 181 games related to the cybersecurity area, which are "played" for an hour and characterized [5].

Therefore, this work aims to increase children the level of awareness about the importance of the security of their information, about the existing threats and about how to learn to use technologies in a positive way in order to avoid risks. The following objectives

learning have been considered:

- They must be able to understand and learn about the cybersecurity concept.
- They must be able to learn to qualify the different types of emails in informative or malicious emails.
- They must be able to quickly recognize vulnerabilities or threats in networks.
- They must be able to understand that what you would not do in real life you wouldn't do it on social networks.
- They must be able to protect their data and media profiles. to secure keys.

In this work we propose the creation of an application of video game type in order to teach in a playful way the dangers of the Internet, generating awareness in cybersecurity[1] implicitly. The tips will be displayed as the child progresses through the game which

It will have animated scenarios set in 3D. This is a work in progress, therefore it has an incipient validation that has served to improve future versions of the game.

In the rest of the document, Section II presents Materials and Methods, Section III presents the results, Section ' IV describes the validation process, Section V compares cyberkids with other video games, and Section VI presents the conclusions and future work.

978-1-7281-8328-2/20/$31.00 ©2020 IEEE

[1] https://es.wikipedia.org/wiki/Seguridad informatica

II. MATERIALS AND METHODS

This section will describe the methods used to deliver educational content on cybersecurity 3 and some gamification techniques will also be detailed. the[2] which were applied for the construction of an application game type.

A. CyberKids Design Objective and Description

The main objective is to design an entertaining game that allows children to become aware while playing about basic cybersecurity topics through six pillars:

- Learning: Basic educational topics of cybersecurity through 3D and 2D scenarios where the user will have the experience of controlling a modified character which you must identify to solve some of the objectives that appear in the course of the levels which are set in a way friendly.
- Interaction: be So that the whole learning process more interesting, small systems were implemented ˜ integrated that allow the user to earn rewards, interact with characters within the game, receive advice, follow instructions that help you solve some of the objectives that are reflected through a simple and friendly interface.
- Achievements: The learning obtained can be shared through social networks, allowing others to raise awareness about some key points of cybersecurity, so that it is known about the Importance of private data.
- Based on Real Cases: The technique consists of integrating several real cases that are visualized in a way abstract and that lead the user to resolve instructive all kinds of objective. For this we use 4 gamification techniques and design in order to integrate a variety of windows or pop up with instructions that indicate some of the steps to follow, for example, to solve some objectives, while at the same Some content will be shown that will provide key information on how to protect yourself.
- Content: Information and key advice do not always have to be read, since they can also be heard.
- User Expectations: The ratings on the satisfaction experienced in this game will be reflected in the future in the Play Store, where the game can be downloaded for free for Android devices.

Since it had to set up networks that users can use often, it is considered to work with templates of mail, facebook[5], Whatsapp, Discord[6]. Tik Tok[7], Instagram[8]. among others, which are integrated at different levels in order to meet the objective of presenting real cases in a more playful and fun way in a 3D animated setting. To encourage quick recognition of vulnerabilities or threats [6], rewards are considered.

B. Characteristics of the game

The player must:

- Recognize what cybersecurity means and how to use it in the real world.
- Apply knowledge of what to do with safe and/or malicious emails.
- Distinguish the different possible threats in networks.
- Relate game situations to those in real life when using technologies.
- Identify safe ways to create accounts, keys etc

Complementing this with:

- Customize an Avatar: Use a character completely adjustable and modifiable which can be controlled at some point.
- Adaptable Scenarios: There are customized and modified scenarios tailored to a child from 8 to 12 years old.
- Different Challenges: There are different challenges with which the player will find as he goes participating within the application. ´ There is the possibility
- Awarding: of rewarding the player so that it can gratify the gameplay.
- Integration with different Systems: Avatar personalization systems, dialogue systems, scoring systems, quiz systems with a timer included and other functionalities that will allow you to have control of the application in a way that will allow you to achieve the objectives.
- Mini Practical Tutorials: There is the possibility of viewing basic and practical tutorials as a help method when playing.
- Share Achievements: And the most important thing is that there is the possibility of sharing achievements through social networks, especially Instagram, so that this can motivate to add other players in some way.

C. Technical Implementation

Fig. 1 shows the product solution scheme with the tools used to create a game-type application which is capable of delivering basic cybersecurity content to children from 8 to 12 years old.

us.

an attractive and massive game, it is decided to use the tool Unity3D must[9]. 3DS Max 10, Blender 11, Visual Studio 12, donde create a complete scenario that allows to emulate

[2] https://en.wikipedia.org/wiki/Computer security
[3] https://www.iebschool.com/blog/gamification-innovacion/
[4] https://www.iebschool.com/blog/gamification-innovacion/
[5] https://www.facebook.com/
[6] https://discord.com/
[7] https://www.tiktok.com/es/
[8] https://www.instagram.com/
[9] https://unity.com/es
[10] https://www.autodesk.com/products/3ds-max/overview
[11] https://www.blender.org/
[12] https://visualstudio.microsoft.com/es/

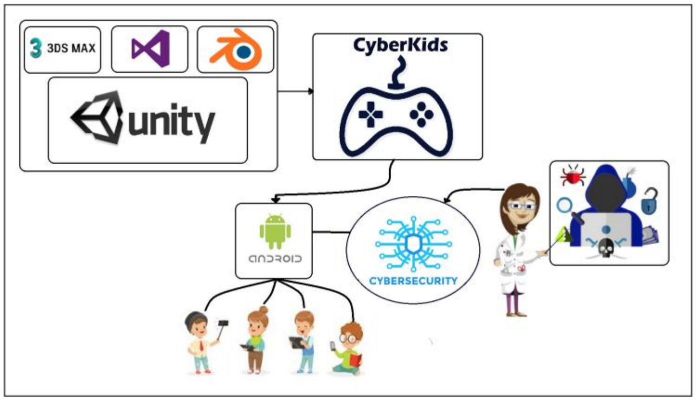


Fig. 1. Scheme of Proposed Solution

fun way a world which will be traversed by a modifiable character.

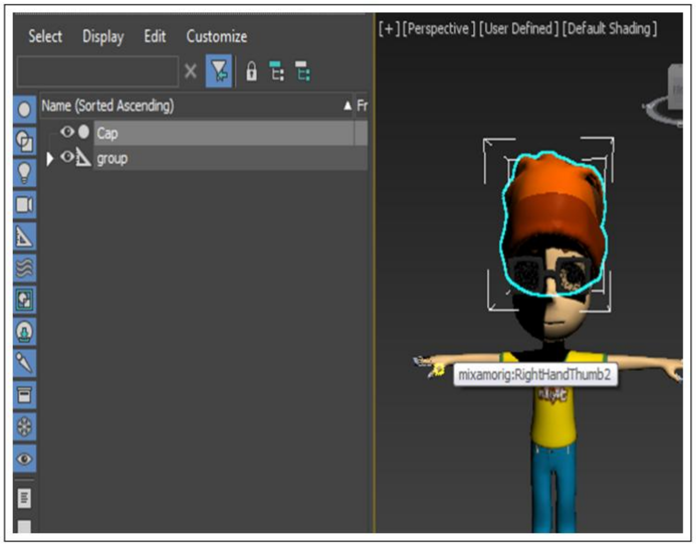

Select Display Edit Customize
[+] [Perspective] [User Defined] [Default Shading]
Name (Sorted Ascending)
Cap
group
mixamorig:RightHandThumb2

Fig. 2. Complement a character with an item in 3DS MAX

In Fig. 2 you can see how in 3ds Max[13] it is adjusted a small element tailored to the main character of CyberKids, thus allowing this element to be integrated easily in the options of modifying a character within the game.

- Gameplay: Gameplay consists of interacting both with the scenarios as interface. Users can Create your character who will be introduced in the different scenarios to go through them, look for objectives and solve them, earning the expected score. The user will go to encountering small minigames as we can see in Fig. 8.
- User Interface: The user interface is quite simple, and it has a minimum number of icons, since the main focus is on the graphics and gameplay. The game is considered to have multiple functionalities which are mainly focused on educate on the same topic, but in different ways.
- Creation of Character Items: Tools such as Blender[14] and 3ds Max[15] were used to add ˜ some customization items for the avatar. In Fig. 2 we can see how an element is integrated into the main character, so that they were made the necessary settings to export the item to your respective format to be imported into Unity[16]

In Section III you can see the icons being used to appreciate the amount of score obtained; amount of goals achieved; elements such as buttons that meet certain function when pressing them; practical aid capsules; among others.

III. RESULTS

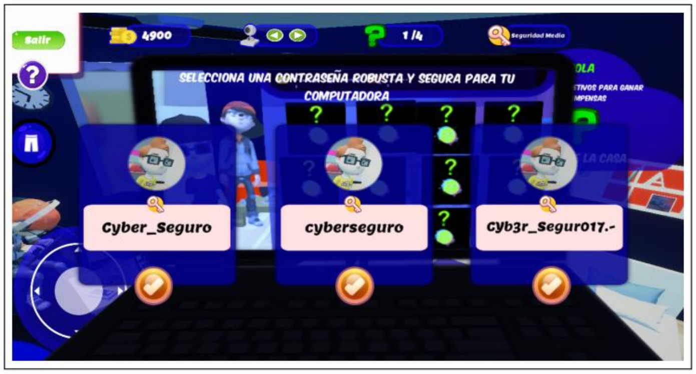


Fig. 3. Objective on security through strong passwords

In Fig. 3 you can see the game objective "identify and select strong passwords for a device". The user has the option to select between a natural password a low security password, a medium security password, and a high security password.

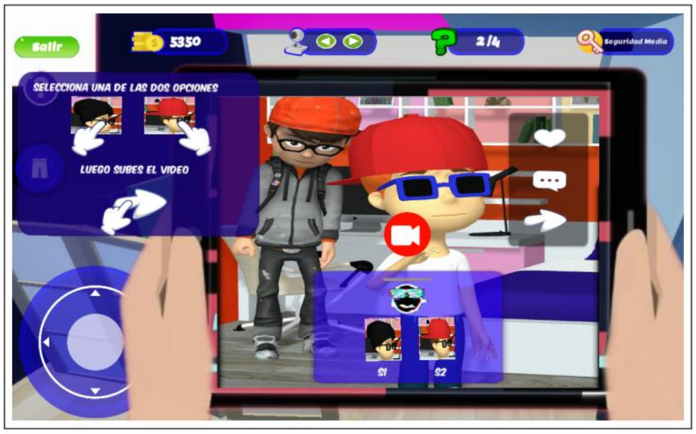


Fig. 4. Simulation of interaction on socialnetworks

[13] https://www.autodesk.com/products/3ds-max/overview

[14] https://www.blender.org/

[15] https://www.autodesk.com/products/3ds-max/overview

[16] https://unity.com/es

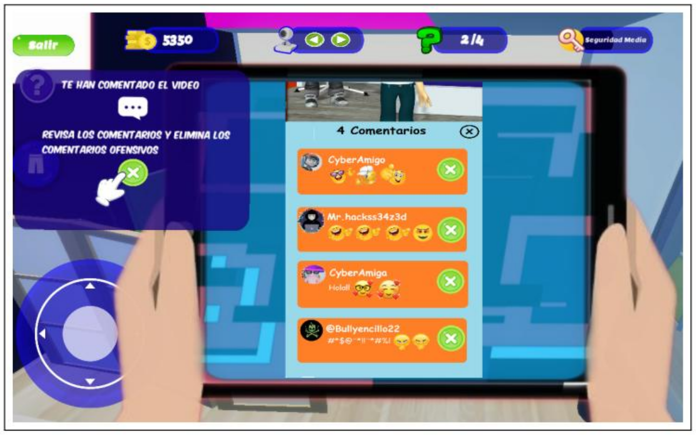


Fig. 5. Simulation of interaction on social networks - comments

Figures Fig. 4 and Fig. 5 show how the user is put to the test and will have to make decisions with quick feedback - winning or losing points. In Fig. 4 you can see a small simulation of Tik Tok where the player must be able to interact[17] with some basic options such as sharing a video through your device. If the player is not able to recognize some of With these basic options, you will have some help capsules that will allow you to quickly advance your objective. In Fig. 5 you can see a list of comments published in a video from a Tik Tok account and the player[18] must be able to to identify some of the malicious comments made by unknown users through this little na˜ simulation

Some game levels aim to raise awareness on the importance of protecting personal data in the face of any open vulnerability or any massive attack coming from unsafe locations or directions. To make more awareness on the subject, CyberKids allows players interact with a more complex level as can be seen in Fig. 6 and Fig. 7. In Fig. 6 can appreciate a level of play which consists of making use of protective shields against massive attacks caused by[19] cybercriminals who want to obtain the private data of the students. In Fig. 7 you can see some ads malicious which are activated because of the different attacks mass received.

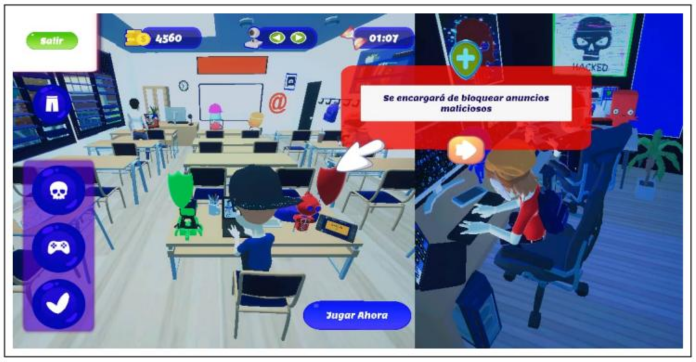


Fig. 6. Use of Protective Shields - Tutorial

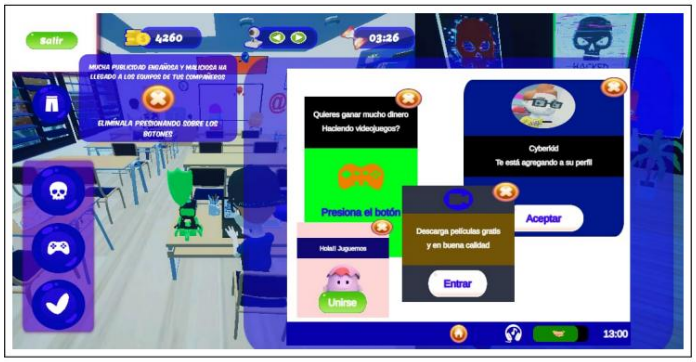

Salir
4260
03:26
MUCHA PUBLICIDAD ENGAÑOSA Y MALICIOSA HA LLEGADO A LOS EQUIPOS DE TUS COMPAÑEROS
ELIMÍNALA PRESIONANDO SOBRE LOS BOTONES
Quieres ganar mucho dinero Haciendo videojuegos?
Presiona el botón
Cyberkid
Te está agregando a su perfil
Aceptar
Descarga películas gratis y en buena calidad
Entrar
Hola!! Juguemos
Unirse
13:00

Fig. 7. Use of Protective Shields - Malicious Ads

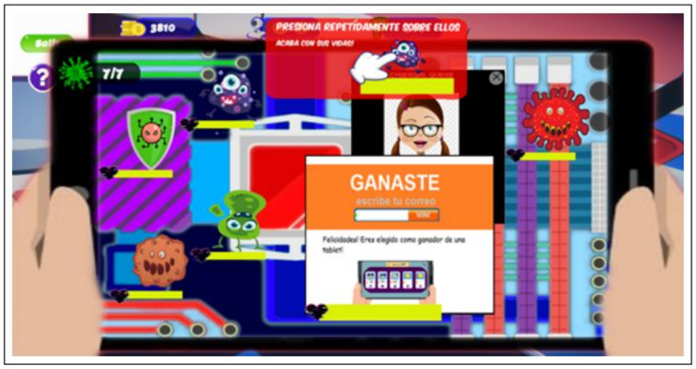

3810
PRESIONA REPETIDAMENTE SOBRE ELLOS
ACABA CON SUS VIDAS!
7/7
GANASTE
escribe tu correo
Felicidades! Eres elegido como ganador de una tablet!

Fig. 8. Mini game

In Fig. 8 you can see a small game which consists of eliminating some malicious elements through repeated keystrokes.

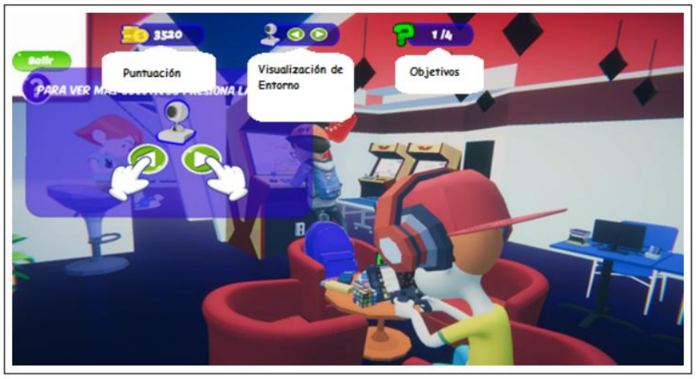


Fig. 9. ´Icons and Main Elements I

Fig. 9 and Fig. 10 show the level at which the player interacts with an animated and eye-catching environment.

[17] https://www.tiktok.com/es/

[18] https://www.tiktok.com/es/

[19] https://www.osi.es/es/campanas/los-cybercriminals-who-are

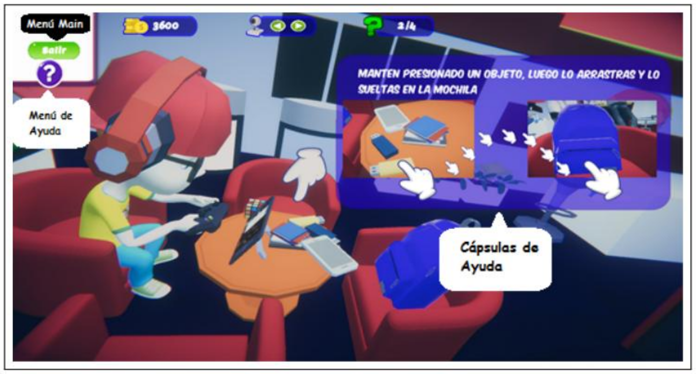

Menú Main
Salir
3600
2/4
MANTEN PRESIONADO UN OBJETO, LUEGO LO ARRASTRAS Y LO SUELTAS EN LA MOCHILA
Menú de Ayuda
Cápsulas de Ayuda

Fig. 10. ´Icons and Main Elements II

Like any game, the player can modify his character at any game level as we can see in Fig. 11.

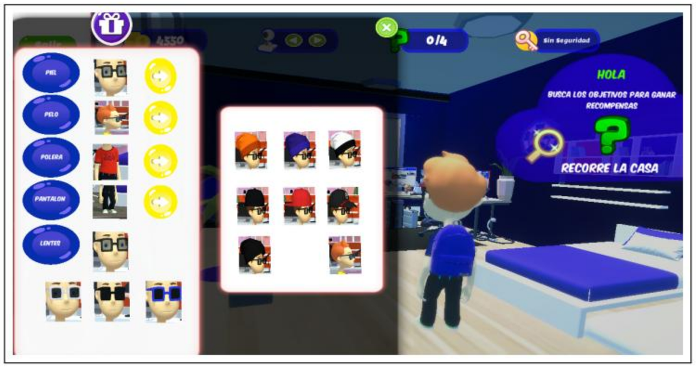


Fig. 11. Customize an Avatar

IV. DISCUSSION OF THE RESULTS

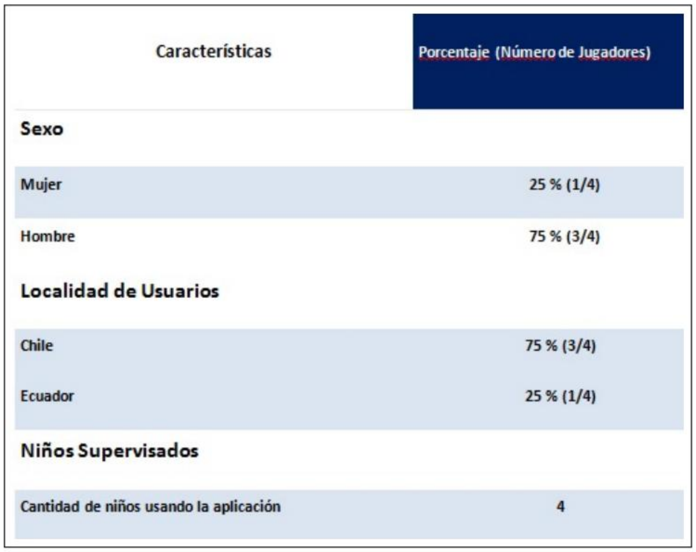
The validation presented in this work is incipient but it is a work in progress. To measure the impact of product with respect to the expected learning, we have worked with a very small sample of volunteers, fathers or mothers of children in the age range of 8 and 12 to us.

Table I shows the number of users supervisors and target users who used the application.

Regarding the gaming experience, the users who supervised the gameplay considered that the product in general is a good experience for target users (Children ˜ from 8 to 12 years), qualifying the product from a scale of 1 to 10, where 1 is a bad experience and 10 is a good experience. You can see the rating in Fig. 12

Table II shows the number of comments and recommendations on possible improvements to consider within the product in general, making it clear that the product can be improved based on the needs of Players.

TABLE I
BASIC CHARACTERISTICS OF USERS



Características	Porcentaje (Número de Jugadores)
Sexo	
Mujer	25 % (1/4)
Hombre	75 % (3/4)
Localidad de Usuarios	
Chile	75 % (3/4)
Ecuador	25 % (1/4)
Niños Supervisados	
Cantidad de niños usando la aplicación	4

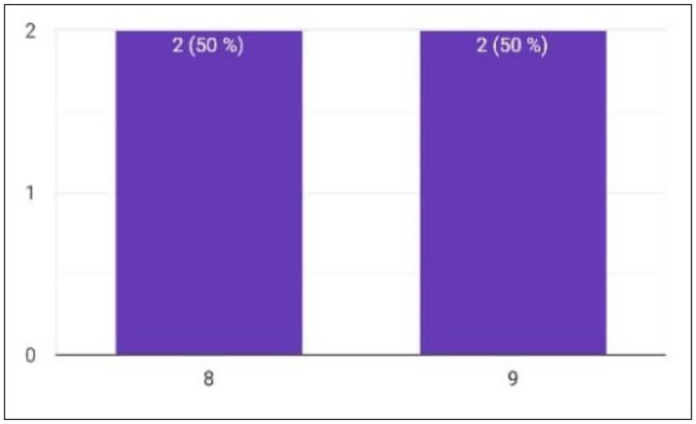


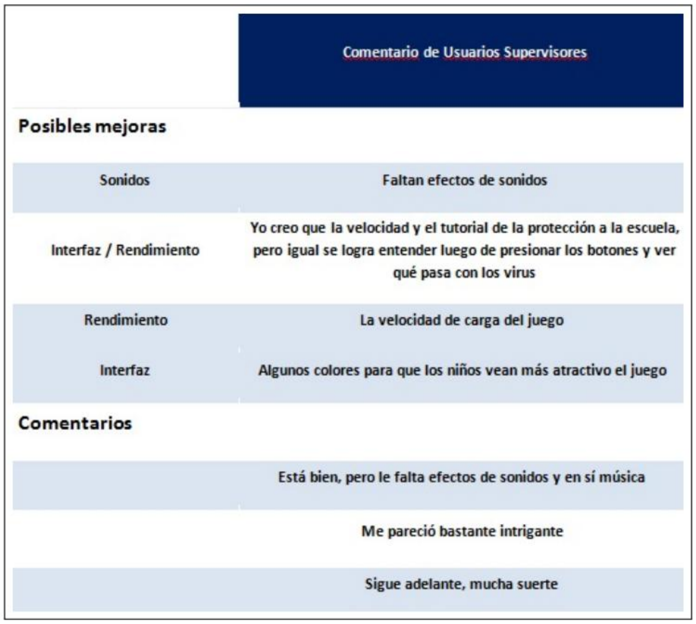
Fig. 12. Rating Scale´

An evaluation form was designed [20] of the product to evaluate the expected learning that allowed to evaluate the following aspects:

- The ease of entering the different levels of play
- Learning about the importance of personal data chosen
- Learning about the use of social networks
- Learning about sharing and caring for the integrity of personal data
- Learning about the use of patterns and passwords robust security
- The difficulty in general and the ability that the objective users to overcome challenges
- The ability of target users to recognize the educational content delivered
- The ability of targeted users to recognize malicious elements

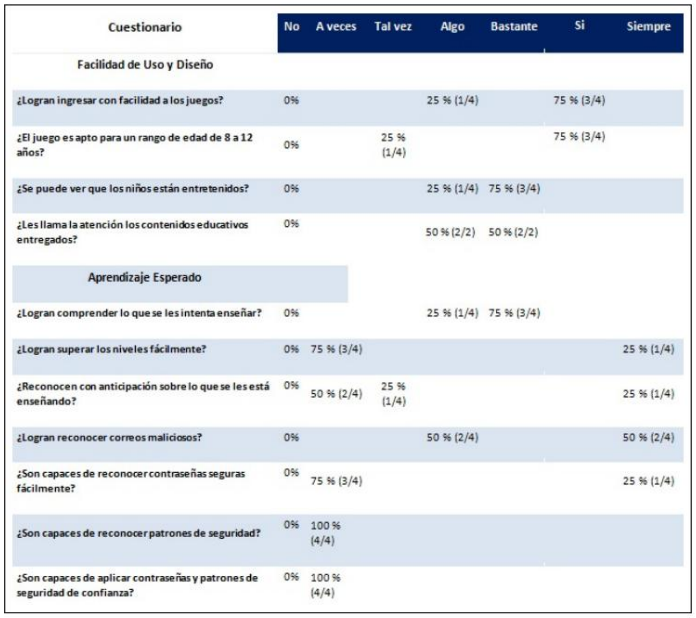
[20] https://tinyurl.com/yy9gcgf3

TABLE II
COMMENTS AND RECOMMENDATIONS



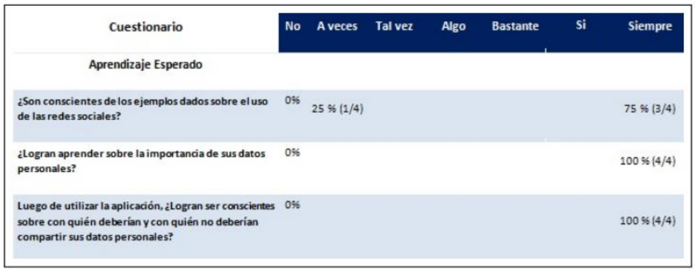
	Comentario de Usuarios Supervisores
Posibles mejoras	
Sonidos	Faltan efectos de sonidos
Interfaz / Rendimiento	Yo creo que la velocidad y el tutorial de la protección a la escuela, pero igual se logra entender luego de presionar los botones y ver qué pasa con los virus
Rendimiento	La velocidad de carga del juego
Interfaz	Algunos colores para que los niños vean más atractivo el juego
Comentarios	
	Está bien, pero le falta efectos de sonidos y en sí música
	Me pareció bastante intrigante
	Sigue adelante, mucha suerte

TABLE III
EXPECTED RESULTS



Cuestionario	No	A veces	Tal vez	Algo	Bastante	Si	Siempre
Facilidad de Uso y Diseño							
¿Logran ingresar con facilidad a los juegos?	0%			25 % (1/4)		75 % (3/4)	
¿El juego es apto para un rango de edad de 8 a 12 años?	0%		25 % (1/4)			75 % (3/4)	
¿Se puede ver que los niños están entretenidos?	0%			25 % (1/4)	75 % (3/4)		
¿Les llama la atención los contenidos educativos entregados?	0%			50 % (2/2)	50 % (2/2)		
Aprendizaje Esperado							
¿Logran comprender lo que se les intenta enseñar?	0%			25 % (1/4)	75 % (3/4)		
¿Logran superar los niveles fácilmente?	0%	75 % (3/4)					25 % (1/4)
¿Reconocen con anticipación sobre lo que se les está enseñando?	0%	50 % (2/4)	25 % (1/4)				25 % (1/4)
¿Logran reconocer correos maliciosos?	0%			50 % (2/4)			50 % (2/4)
¿Son capaces de reconocer contraseñas seguras fácilmente?	0%	75 % (3/4)					25 % (1/4)
¿Son capaces de reconocer patrones de seguridad?	0%	100 % (4/4)					
¿Son capaces de aplicar contraseñas y patrones de seguridad de confianza?	0%	100 % (4/4)					

TABLE IV
EXPECTED RESULTS 2



Cuestionario	No	A veces	Tal vez	Algo	Bastante	Si	Siempre
Aprendizaje Esperado							
¿Son conscientes de los ejemplos dados sobre el uso de las redes sociales?	0%	25 % (1/4)					75 % (3/4)
¿Logran aprender sobre la importancia de sus datos personales?	0%						100 % (4/4)
Luego de utilizar la aplicación, ¿Logran ser conscientes sobre con quién deberían y con quién no deberían compartir sus datos personales?	0%						100 % (4/4)

- The ability of target users to recognize patterns and strong security passwords • The ability of target users to recognize

cer each delivered content

- The ability of target users to recognize the educational content delivered
- The quality of the content delivered, so that

be eye-catching to target users

- The quality of the challenges, design, atmosphere, music, etc, so that the target users are able to

keep busy and entertained during the experience.

In table III and table IV important results can be seen for the continuous improvement of the game with respect to to the ease of use, the design and the expected learning of the product, considering that until now all the users manage to learn as much about the importance of personal data as can be seen in Fig. 13, as well as as they also manage to be aware of with whom they should and with whom they should not share your personal data such as can be seen in Fig. 14 In addition, it can

be seen that the ease of use and the ˜ CyberKids design allows most users to can easily access the different levels of play; Allows users to be entertained using the application; It allows it to be striking in terms of educational content and it is also considered to be a totally suitable game for a child in an age range of 8 to 12 years. Regarding the expected learning, according to the supervisory users, the objective users (children from 8 to 12 years old) ˜

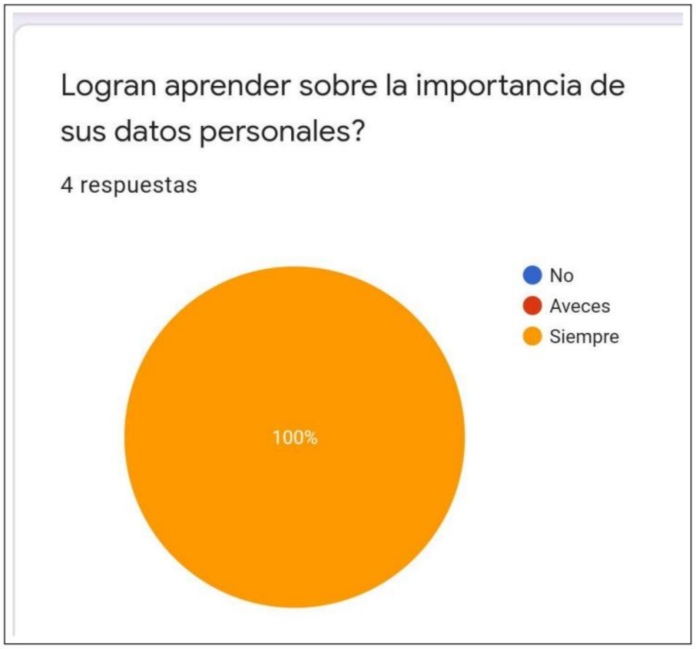
obtained the following results:

- **They manage** to understand about the teaching delivered; **It** **great** progress in the different levels; **They manage** to recognize some malicious emails; **They** become aware of the use of social networks; **They** fully achieve learning about the importance of your personal data; **They manage** to be fully aware of the correct sharing of your personal data.
- They are **rarely** able to recognize strong passwords; **few sometimes** they manage to recognize security patterns; **few Sometimes** they are able to apply passwords and security patterns based on what they have learned;
- **Sometimes they manage to** be able to recognize in advance´ about the delivered content;

V. RELATED WORK

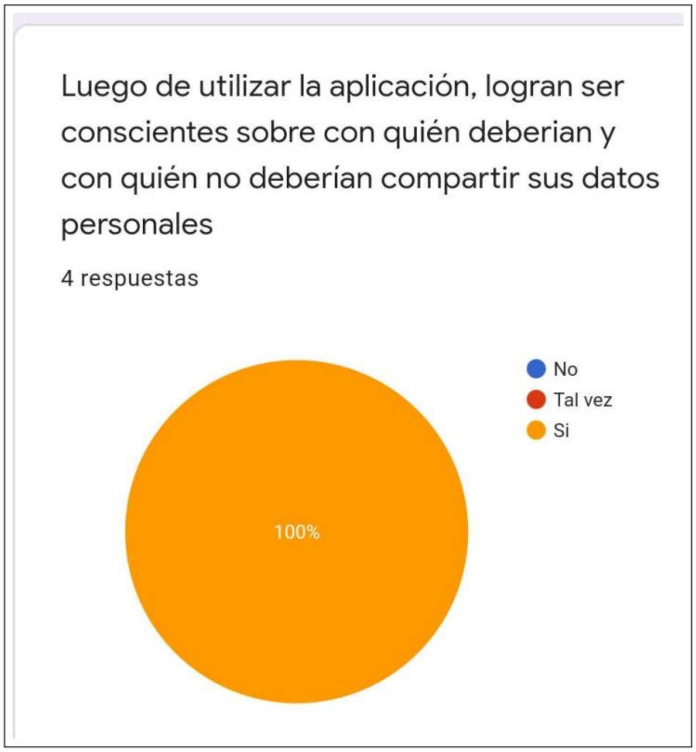
There are many other solutions on the market [7], the which were studied and analyzed as for example Hackers vs CyberCrook 21, which is a game that combines fun and learning in matters related to the

21https://www.osi.es/es/actualidad/blog/2017/12/27/ hackers-vs-cybercrook-a-fun-game-that-will-test-your


Logran aprender sobre la importancia de sus datos personales?

4 respuestas

Fig. 13. Learning about the importance of personal data


Luego de utilizar la aplicación, logran ser conscientes sobre con quién deberian y con quién no deberían compartir sus datos personales

4 respuestas

Fig. 14. Learning about personal data sharing

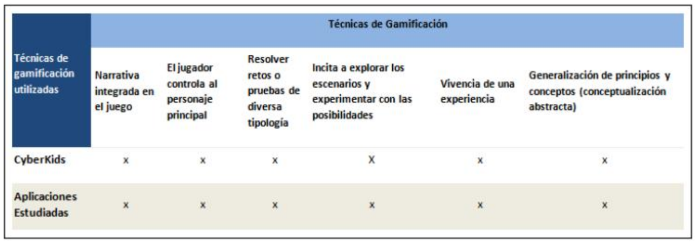
cybersecurity where a character must protect his house of cybercrook attacks and to prevent these attacks the character will go on different missions. The relationship thing CyberCrook has with CyberKids is that both games test knowledge and in both games you have control of a character, but the only difference is that CyberKids gameplay is simpler and more harmonious. In addition, CyberKids is not related to highly complex objectives, providing an adequate environment for children and pre-adolescents.

Hackend is another similar application for all ages, 22, where the user must control his character to identify some cybersecurity gaps in the company the one that belongs.

Hacking Hero – Cyber Adventure Clicker 23, a game that allows the user to interact with malicious elements which They must be removed with a click. Similar to CyberKids, both try to educate about cybersecurity issues and both they use the click to rule out vulnerabilities.

CyberScouts[24] also turns out to be another game very similar to CyberKids, where it is possible to make a variety of of knowledge tests through multiple objectives integrated into a small experience which tries to deliver educational information on cybersecurity, but in a fun and playful way. Both games share messages, advice and results at the end of each objective, so that both meet the objective of educating through their content.

These are examples of existing applications in the market, but unlike CyberKids, they are going to integrate multiple methods that will allow addressing important issues based on studies carried out on experiences lived in the today, so that the studies carried out are capable of to be integrated, thus allowing variety in terms of gaming experience.



Técnicas de gamificación utilizadas	Técnicas de Gamificación					
	Narrativa integrada en el juego	El jugador controla al personaje principal	Resolver retos o pruebas de diversa tipología	Incita a explorar los escenarios y experimentar con las posibilidades	Vivencia de una experiencia	Generalización de principios y conceptos (conceptualización abstracta)
CyberKids	x	x	x	X	x	x
Aplicaciones Estudiadas	x	x	x	x	x	x

Fig. 15. Similarities of CyberKids with the Applications Studied

SAW. CONCLUSION AND FUTURE WORK

Despite having an incipient validation, we believe that the results are encouraging because they allow us to visualize that CyberKids is a video game that allows learning of a relevant topic such as cybersecurity in an environment playful Clearly, this lack of interaction with end users has made it difficult to quickly achieve a final product through an iterative, scrum-like approach, for example. In the future it is expected to be able to use the application to train children and pre-adolescents with the respective permissions of the ethics committee. This will allow to solve the greater risk of the project allowing to adapt the product quickly to

22https://www.incibe.es/protege-tu-empresa/hackend
23https://hacking-hero.es.aptoide.com/app
24https://www.is4k.es/de-utilidad/cyberscouts

maximize the achievement of learning outcomes while the kids are having fun.

THANKS

The work of Romina Torres was partially supported by the internal project UNAB DI-02-19/R.

REFERENCES

[1] B. P. Bergeron, Developing serious games. Charles River Media, 2006.

[2] J.-N. Tioh, M. Mina, and D. W. Jacobson, “Cyber security training a survey of serious games in cyber security,” in 2017 IEEE Frontiers in Education Conference (FIE). IEEE, 2017, pp. 1–5.

[3] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, “Evaluation of game-based learning in cybersecurity edu cation for high school students,” Journal of Education and Learning (EduLearn), vol. 12, no. 1, pp. 150–158, 2018.

[4] W. A. Hill Jr, M. Fanuel, X. Yuan, J. Zhang, and S. Sajad, “A survey of serious games for cybersecurity education and training,” 2020.

[5] M. Coenraad, A. Pellicone, DJ Ketelhut, M. Cukier, J. Plane, and D. Weintrop, “Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games,” Simulation & Gaming, vol. 51, no. 5, pp. 586–611, 2020.

[6] P. Lee, J.; Ceyhan, “Greenify: A real-world action game for climate change education,” 2012. [Online]. Available: http://tcgameslab.org/wp-content/uploads/2013/02/Lee-et-al.-Greenify-Simulationand-Gaming-2013.pdf

[7] Eduka2, “Cybersecurity for children.” ˜ to [Online]. Available: http://eduka2.es/cybersecurity-for-kids-some-educational-games/