

Desarrollo de un Videojuego Educativo Orientado a la Seguridad Informática para Niños en la Ciudad de Ocaña, Fase de Concepción.

B.A. García M, *Member, SIGLAS - UFPSO*

Abstract— The concern for the physical and psychological security of children on online social networks, in many cases even knowing about the dangers on the network, they do not know how to identify warning signs or how to protect their data from criminals. Consequently, the creation of a video game will be the ideal aims to stimulate children learning in safety concepts having a fun tool; considering that it is an effective tool that will join efforts to educate and protect children on the Internet.

Keywords— Game, education, security, social networking, children, internet.

I. INTRODUCCION

La proliferación de la tecnología informática, evidentemente ha mejorado nuestras vidas de muchas maneras, como permitir la mejora de la productividad y la eficiencia en el trabajo, la escuela y el hogar. Cualquier persona con acceso a una computadora y un módem ahora tiene oportunidades recreativas y educativas sin precedentes. [1].

La innovación tecnológica como internet de alta velocidad y dispositivos móviles con una gran variedad de aplicaciones para todos los gustos y necesidades, ha sido muy atractiva entre las personas y ha transformado las sociedades de todo el mundo. Los niños en particular, han aumentado el acceso a las TIC y en las últimas décadas, han tendido que adoptar estas tecnologías desde una edad temprana, teniendo como resultado que se conviertan en parte de sus vidas. [2]

Problema social

Por desgracia, internet tiene muchos peligros, entre ellos están los delincuentes que utiliza la tecnología moderna, para aprovecharse de las víctimas. Las computadoras y el Internet han hecho el trabajo del depredador más fácil y más anónimo, al proporcionar un espacio para buscar y preparar a niños para fines delictivos, tales como la producción y distribución pornografía infantil, contactar y acechar a niños con el propósito de participar en actos sexuales y usarlos para el

turismo sexual con fines personales y comerciales. Estas actividades de captación de víctimas históricamente se desarrollan, en lugares públicos donde los niños tienden a reunirse como en patios escolares, terrenos de juegos, y centros comerciales. Hoy en día, con tantos niños en línea, Internet proporciona una nueva estrategia donde se elimina muchos de los riesgos que los depredadores sexuales enfrentan al entrar en contacto en persona. [1]

Los niños siempre han sido vulnerables por su naturaleza confiada e ingenuidad, y hacen que sean blancos perfectos tanto de delincuentes especializados, como de otros niños o adultos que usan la internet para ridiculizarlos, hostigarlos, chantajearlos o amenazarlos.

Esfuerzos de la comunidad

En este punto es donde todos los esfuerzos de las comunidades, las familias, los gobiernos y la participación activa de los niños deben ser encaminados a la reducción del abuso infantil y el acoso tanto en redes sociales como en internet en general.

Privar a los menores del uso de Internet para de evitar riesgos como el *grooming*, *el sexting*, *el ciberbullying* y el ciberacoso es una medida drástica, ya que de manera simultánea se les niega el acceso a un conjunto de recursos de gran utilidad como la amplia información, conocimiento o entretenimiento. Y teniendo en cuenta que muchos de los problemas de seguridad se relacionan con el desconocimiento de las amenazas y formas de protección, algunos maestros brindan a sus alumnos clases tradicionales de seguridad que con frecuencia son conferencias en donde los estudiantes aprenden básicas amenazas y mecanismos de defensa sin la aplicación de ese conocimiento.

II. JUSTIFICACIÓN

Dado el crecimiento del uso de las tecnologías en los niños en su cada vez más temprana edad, es importante proyectar medidas que puedan ser utilizadas para la formación de los niños frente a los peligros que puede presentar el internet.

En busca de una medida efectiva

Se hace indispensable la creación de una herramienta eficaz que se sume a los esfuerzos por educar y proteger a los menores en internet, pero las investigaciones y técnicas preventivas sobre el uso de las tecnologías están enfocadas a los adolescentes [3], que en muchos casos cuando reciben la capacitación ya han sido víctimas en internet. Lo que hace necesario una metodología que sirva como base y active la atención de los niños en la protección de su integridad física y emocional, teniendo en cuenta que ingresan al mundo tecnológico cada vez en edades más tempranas. La solución es armarlos de herramientas, métodos e información que permitan que disfruten de la tecnología en un ambiente saludable. Que sean ellos mismos los que se cuiden e identifiquen sus propias amenazas, que logren proteger sus datos, reconocer posibles peligros y que actúen correctamente ante estas señales de alarma.

Sería ideal que siendo la tecnología tan atractiva para los niños, poder usarla como mecanismo de educación y ayudarlos en esta problemática. Teniendo en cuenta que los niños tienen grandes expectativas al usar tecnologías, dado que muestran una gran adaptabilidad intuitiva en el uso de las mismas, por lo que son comúnmente denominados “nativos digitales”, son capaces de conceptualizar sobre un amplio rango de dispositivos móviles hasta el uso de computadores [4].

Es aquí donde los videojuegos serían la clave para inculcar hábitos de seguridad informática, pues brindan la posibilidad de conectar la teoría y la práctica mediante la creación de un escenario donde el niño tiene que reaccionar a una sucesión de eventos, donde además de obtener conceptos, aplique lo aprendido y verifique los resultados a medida que avanza en el juego [5]. Además pueden ser utilizados para transmitir conceptos de seguridad y pueden ser efectivos para mejorar los cuidados en seguridad [6].

A pesar de que se pueden encontrar videojuegos que traten de estimular la seguridad en internet éstos no son aptos para edades tempranas debido a que muchos de ellos tienen una compleja solución y un bajo grado de diversión como podemos verificar algunos ejemplos en [7].

En definitiva un videojuego podría cumplir con la tarea de ser efectivo como método preventivo contra abusos a niños en la red, siempre que esté orientado a niños de edades más tempranas, que cuente con un componente divertido, sea de fácil manejo, y además utilice metodología de enseñanza que se pueda comprobar de una manera práctica.

Diseño y estrategia de enseñanza

El videojuego a desarrollar tendrá que motivar al niño a ser independiente en la web, así que se usará la analogía entre navegar en internet y navegar en el mar.

En el juego el niño se identificará con un personaje marítimo(un pez), que tendrá que elegir al inicio del juego el lugar a donde quiere emprender una aventura, ya escogido su rumbo, comienza a explorar su mundo y a darse cuenta que en el viaje van apareciendo obstáculos y peligros a los cuales tendrá que hacerle frente. Habrá personajes en los cuales podrá confiar y aceptar sus consejos y por el contrario hay otros que son depredadores y tratarán de convencerlo de dar algo que después puede ser usado para lastimarlo y de los cuales se tiene que cuidar evitando que les llegue información de su ubicación y actividades. También tendrá que tener cuidado en los sitios que frecuenta o ingresa, pues esto significaría ponerse en peligro. Al igual que caer en trampas como redes o anzuelos. Su defensa será el reconocer a los atacantes e informar a la autoridad en el mar (un enorme pez policía) haciendo que el enemigo desaparezca de su zona. El éxito de la aventura depende de las decisiones que el pez tome para poder llegar a su destino.

Con ésta historia, se busca que el niño comprenda que en toda aventura hay obstáculos y pruebas y solo sobrevive el que tiene cuidado, se trata de despertar en el niño la duda sobre la validez de la información que se encuentra en su medio. Despertar en el niño la suspicacia para protegerse y hacerle caso a sus presentimientos cuando algo anda mal. También que tome métodos de prevención y cuando ya detecte una agresión informe a quien le puede ayudar.

III. METODOLOGÍA

Entre las diversas metodologías que existen para el desarrollo de software, se pueden encontrar las que tradicionalmente se han utilizado, en donde el control riguroso del proceso de desarrollo resulta un problema constante. Y aquellas metodologías ágiles en donde se adoptan medidas para un desarrollo más realista y práctico [8].

Para el desarrollo de este proyecto se tomará como guía la metodología de desarrollo *software Extreme Programming* (XP) propuesta por Kent Beck en 1999. Partiendo en que los cambios de los requisitos sobre la marcha son acontecimientos naturales, inevitables y a veces deseables en el desarrollo de software, se determina este enfoque como el más adecuado para este proyecto pues se centra en la adaptabilidad más que en la previsibilidad, plantea que es más viable adaptarse a los cambios de requerimientos en cualquier punto del ciclo de vida del proyecto, que intentar plantear todos los requisitos desde el comienzo, generando esfuerzos para controlar los cambios.

Debido a que en el XP la respuesta ante los cambios es más importante que el seguimiento de un plan, entre sus fases: planificación, diseño y codificación deben realizarse pruebas constantes, además de contar con la participación y colaboración del cliente para garantizar su éxito [9]. Lo cual hace a esta metodología ideal para el desarrollo de videojuegos educativos en donde constantemente se busca

además del buen funcionamiento, la aceptación del público infantil de la ciudad de Ocaña.

Retos del proyecto

- Identificar las fases y herramientas a utilizar en el proyecto, para la iniciación del aprendizaje en torno al desarrollo de videojuegos educativos.

-Reconocer técnicas y metodologías para la protección de datos en internet que permita la capacitación necesaria para la difusión de esa información por medio de videojuegos.

- Aprobar el diseño del videojuego que sea divertido y con altas posibilidades de aceptación entre los niños ocañeros.

IV. CONCLUSIONES

Ciertos comportamientos están relacionados con la información sensitiva que las personas comparten en la red, que conllevan riesgos en espacios virtuales y en el mundo real. Por lo cual, deben tomarse acciones pedagógicas para mejorar los niveles de seguridad en los comportamientos cuando se interactúa en Internet

Los niños muestran comportamiento que los ponen en riesgo de robo de identidad e intrusiones no deseadas como por ejemplo a través de las redes sociales, a lo cual no le prestan mucha atención. Investigaciones han demostrado que la tecnología afecta el desarrollo de los niños. Además las investigaciones sobre el uso de las tecnologías están enfocadas en los adolescentes.

Los niños tienen grandes expectativas al usar tecnologías, dado que muestran una gran adaptabilidad intuitiva en el uso de las mismas, por lo que son comúnmente denominados “nativos digitales”. Además son capaces de conceptualizar sobre un amplio rango de dispositivos desde dispositivos móviles hasta el uso de computadores. Los videojuegos pueden ser utilizados para transmitir conceptos de seguridad y puede ser efectivos para mejorar los cuidados en seguridad.

Un videojuego será la herramienta ideal para estimular en los niños conceptos de seguridad al mismo tiempo que estimula el aprendizaje del niño mientras se divierte.

REFERENCIAS

[1] Internet Crimes Against Children, 1st ed. Washington, DC: U. S. Department of Justice, 2001.

[2] S. Malby, T. Jesrani, T. Bañuelos, A. Holterhof and M. Hahn, Study on the Effects of New Information Technologies

on the Abuse and Exploitation of Children, 1st ed. Vienna: United Nations, 2016.

[3] J. Guan and J. Huck, "Children in the digital age", Proceedings of the 2012 iConference on - iConference '12, 2012.

[4] J. Korte, L. Potter and S. Nielsen, "Great expectations", Proceedings of the 52nd ACM conference on Computers and people research - SIGSIM-CPR '14, 2014.

[5] N. Padilla Zea, C. Collazos Ordoñez, F. Gutiérrez Vela and N. Medina Medina, "Videojuegos educativos: Teorías y propuestas para el aprendizaje en grupo", Ciencia e Ingeniería Neogranadina, vol. 22, no. 1, p. 139, 2012.

[6] M. Guimaraes, H. Said and R. Austin, "Using video games to teach security", Proceedings of the 16th annual joint conference on Innovation and technology in computer science education - ITiCSE '11, 2011.

[7] "Security Awareness Games | MindfulSecurity.com – The Information Security Awareness Resource", Mindfulsecurity.com, 2016. [Online]. Available: <http://mindfulsecurity.com/2010/09/14/security-awareness-games/>. [Accessed: 03- Sep- 2016].

[8] Á. Cortes Téllez and E. Rojas, metodologías de desarrollo de videojuegos, 1st ed. Servicio Nacional de Aprendizaje (SENA), 2013.

[9] J. Rodríguez and D. Bustamante, metodología actual, metodología xp., 1st ed. universidad nacional experimental de los llanos occidentales ezequiel zamora, 2014.



Brodny Andrea García Márquez.

Estudiante de Ingeniería de Sistemas (c). Integrante Semillero de Investigación GNU/Linux and Security – SIGLAS y del Grupo de Investigación en Ingenierías Aplicadas para la Innovación, la Gestión y el Desarrollo - INGAP. Universidad Francisco de Paula Santander Ocaña.