Ciberseguridad y educación: Uso de videojuegos como estrategia pedagógica para adolescentes de Colombia sobre los riesgos en redes sociales

Santiago Eduardo Muñoz Castillo, Estudiante Universidad Santo Tomas, Seccional Tunja.

Resumen – El área de la ciberseguridad ha tomado fuerza en los últimos años debido al aumento progresivo de la población y de los dispositivos que tienen acceso a internet, abonado a ello las estrategias que los delincuentes aplican para vulnerar la seguridad, robar, secuestrar o dañar la información que en ellos reposa, ha mutado de generación en generación convirtiéndose en una problemática que trasciende en el tiempo.

Las redes sociales también son una ventana que los ciberdelincuentes utilizan para acceder a la información, ya que el objetivo de éstas es mostrar a las personas en una vitrina digital y permitirles comunicarse con cualquier usuario de la misma red social sin importar el género, la edad o la ubicación geográfica. Esto genera preocupación ya que los usuarios que más frecuentan las redes sociales son los adolescentes y ellos, al estar en una etapa de aprendizaje de la vida, pueden desconocer las técnicas de ciberseguridad para asegurarse que su información está protegida. Por esta razón, este documento pretende explicar mediante la revisión de literatura, los tipos de ataques cibernéticos que pueden ejecutarse a través de las redes sociales para sugerir una estrategia educativa que ilustre a los jóvenes sobre los ciber ataques para que puedan protegerse a sí mismos.

Índice de Términos - Adolescentes, ciberseguridad, educación, videojuegos.

Abstract **- The area of cybersecurity has gained strength in recent years due to the progressive increase in the population and devices that have access to the internet, subscribed to it strategies that criminals apply to breach security, stealing, kidnapping or damaging the information that lies in them, has mutated from generation to generation becoming a problem that transcends time.**

Social networks are also a window that cybercriminals use to access the information, since the aim of these is to show people in a digital showcase and allow them to communicate with any user of the same social network regardless of gender, age or geographical location. This is a cause for concern as the most frequent users of social networks are teenagers and they, being in a life learning stage, may be unaware of cybersecurity techniques to ensure that their information is protected. For this reason, this document aims to explain by reviewing literature, the types of cyber-attacks that can be run through social media to suggest an educational strategy that will illustrate young people about cyber-attacks so that they can protect themselves.

Index - Adolescents, cybersecurity, education, video games.

I. INTRODUCCIÓN

Colombia, un país en constante evolución y desarrollo, a lo largo de su historia ha experimentado una notable revolución tecnológica en la que los cambios no han pasado desapercibidos. Como resultado, ha surgido la necesidad de actualizar los sistemas informáticos utilizados tanto por el gobierno, las empresas como por las personas. Esto se debe a que el software debe ser compatible con los últimos sistemas operativos disponibles en el mercado, los cuales a su vez garantizan fiabilidad y seguridad en su utilización [1]. Así pues, los cambios tecnológicos ocasionaron que la delincuencia creara y empleara estrategias para vulnerar los nuevos sistemas informáticos, en los que se busca atacar a la víctima con el fin de quebrantar su privacidad, para luego obtener algún tipo de beneficio económico a cambio de la información usurpada[2], esta práctica se conoce como ciberdelincuencia.

Los datos personales e información en general que se encuentre en una base de datos o repositorio digital (Computadoras, celulares, archivos locales) es codiciada por los ciberdelincuentes, por esto se requiere mantener medidas de seguridad en el caso de un ciberataque[3]. En el último año, algunas entidades gubernamentales de Colombia han sido víctimas de ataques cibernéticos en numerosas ocasiones, sin embargo, estas fueron detectadas y detenidas sin que la información se viera comprometida[4].

La inversión en recursos que ayuden a evitar los ciberataques es bastante alta y es empleada cuando una empresa u organización ha sido víctima, ya que este delito se traduce en millonarias pérdidas para las empresas u organizaciones como se observa en la Fig 1 y TABLA 1.

Teniendo en cuenta que no sólo el gobierno y las empresas son las únicas que emplean sistemas informáticos y que desde una etapa temprana es necesario conocer las prácticas en ciberseguridad, la población del común también es susceptible a sufrir un ataque cibernético debido a la falta de información sobre ciberseguridad[5], [6], ya que este puede efectuarse en

cualquier dispositivo que almacene información y se conecte a internet.

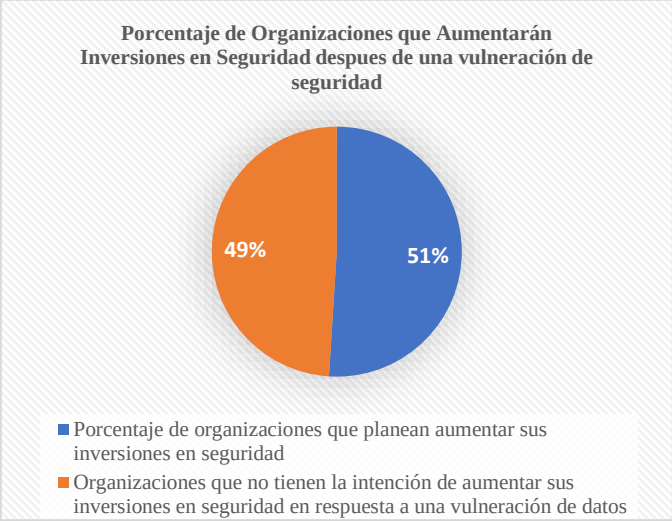

Fig 1. Empresas que planean aumentar su inversión en seguridad después de una vulneración de seguridad. Adaptación propia con referencia tomada de https://www.ibm.com/es-es/reports/data-breach[7]

También, hay que tener en cuenta que los ataques cibernéticos no sólo consisten en la implantación de un virus en el dispositivo electrónico, sino que existen prácticas en las que el robo de información no corresponde a un ataque de fuerza bruta[6], en cambio, este se efectúa cuando el usuario permite de forma indirecta al ciber atacante acceder a su información[8].

Indicador/Estadística	Valor	Detalles
Costo promedio de una vulneración de datos en 2023 a nivel global	$4,45 millones	Aumento del 15% desde el 2020.
Porcentaje de organizaciones que aumentarán inversiones	$2,26 millones un aproximado del 51%	Inversión para respuesta a amenazas.
Ahorro promedio para organizaciones que usan IA y automatización	$1,76 millones	En comparación con organizaciones que no emplean estas tecnologías de seguridad.

TABLA 1.
COSTOS POR VULNERACIONES E INVERSIONES
Adaptación propia con referencia de https://www.ibm.com/es-es/reports/data-breach[7]

La ciberseguridad se rige como un pilar fundamental para conservar la privacidad, la integridad y la confidencialidad de la información personal[9].

Como parte de la evolución tecnológica y el propósito de eliminar la barrera de comunicación, las redes sociales (Facebook, Instagram, Tiktok, Twitter, WhatsApp) se han convertido en la herramienta preferida en el contexto del entretenimiento de las personas[10], [11], éstas permiten al usuario compartir con el mundo su día a día por medio de publicaciones en las que se incluye contenido como: texto, imágenes, videos, enlaces, ubicación geográfica, estado de ánimo e información sensible (nombre completo, fecha de nacimiento, estado civil, contraseñas). Además, brindan la posibilidad del intercambio de mensajes a nivel global, es decir, entrar en contacto con algún usuario de la red social que se encuentre en cualquier lugar del mundo y entablar conversaciones que incluyen la transferencia de imágenes y videos[12].

La simplicidad y los bajos requisitos para crear una cuenta o perfil en cualquier red social junto con la accesibilidad a sus plataformas han promovido la diversidad que compone el mundo digital actual. La rápida propagación de ideas a través de las redes sociales ha revolucionado la forma en que nos comunicamos, informamos y colaboramos dentro de la sociedad moderna. Por esta razón, las redes sociales se han convertido en una fuente de información pública de gran volumen, con alcance global e impacto significativo en el estilo de vida de sus usuarios[13].

Los adolescentes constituyen la población más activa en el uso diario de las redes sociales, ya que dedican una significativa cantidad de tiempo a aprovechar las diversas funciones que estas plataformas ofrecen[14]. Esta situación se debe en gran parte a la afinidad que tienen con las redes sociales, debido a que el público objetivo se centra en esta población, por lo que las mismas redes se encargan de que sus usuarios publiquen contenido que llame la atención de los adolescentes[15], llegando a remunerar dichas publicaciones para obtener cada vez más y más usuarios[16]. En términos generales, los adolescentes utilizan estas plataformas principalmente para dos propósitos: Primero la comunicación a través de servicios de mensajería y segundo la publicación de contenido[17].

La adolescencia, al ser una etapa crítica en el desarrollo de la personalidad[18], convierte a esta población en un blanco para los ciber atacantes ya que puede ser considerada como ingenua, sin embargo, esto es sólo una creencia[19]. La problemática de la seguridad de los adolescentes en las redes sociales radica en la falta de información y educación, convirtiendo al individuo en impresionable y crédulo, propenso a dejarse convencer por anuncios o propaganda sin detenerse a analizar la veracidad del contenido[20]. La concienciación, la educación y la adopción de medidas preventivas se vuelven imperativas para mitigar los riesgos inherentes al uso de redes sociales.

La evolución de la tecnología, si bien ha proporcionado innumerables beneficios, también ha generado nuevas vulnerabilidades que son explotadas por los ciber atacantes; ellos aprovechan las funciones de las redes sociales y se beneficia con cada una de ellas[21], ya que buscan la manera de interceptar la información de los usuarios[22] en un mundo cada vez más interconectado y dependiente de la tecnología.

Por esta razón, comprender la naturaleza cambiante de las amenazas cibernéticas y promover prácticas de seguridad sólidas se convierten en un desafío y una responsabilidad colectiva, tanto a nivel gubernamental como a nivel individual, en aras de proteger el mundo digital y garantizar un entorno seguro para todos.

II. Metodología

Este artículo se desarrolló con un enfoque descriptivo[23] que pretende realizar una investigación exhaustiva de literatura en bases de datos académicas como Scopus, IEEE Explorer y Google Académico con el fin de responder la pregunta ¿Cuáles

son las formas más efectivas de incorporar los videojuegos como herramienta pedagógica para facilitar la enseñanza a los adolescentes sobre la identificación y prevención de ataques cibernéticos a través de las redes sociales?

Con la contextualización de los ciber ataques y la manera de identificarlos, se plantea principalmente el uso de videojuegos serios como una alternativa lúdica e innovadora que puede ser usada dentro de las aulas de clase o ámbitos académicos como una estrategia pedagógica para concientizar a los estudiantes adolescentes sobre los riesgos que pueden presentarse en las redes sociales. A demás se proponen otras estrategias donde el principal objetivo es incentivar al estudiante a que participe activamente de su propia formación, generando experiencias que le ayuden a construir su propio concepto y motivando al continuo aprendizaje sobre el tema.

III. Resultados

A. Definición de ciberseguridad y generalidades.

Las acciones donde se busca que la información personal o empresarial permanezca segura ante personas u organizaciones inescrupulosas que buscan dañar, robar o secuestrar datos que se encuentren almacenados en cualquier medio electrónico o estén siendo transmitidos a través de las redes de comunicación, como el internet, se denominan prácticas de ciberseguridad. La ciberseguridad está presente en el momento que se requiere manipular información a través de medios electrónicos o redes de transmisión de datos para prevenir que, por algún tipo de descuido o brecha de seguridad, la información se vea afectada[24].

En el ámbito empresarial, la familia de normas de calidad como la ISO 27000 pretenden establecer las medidas que la empresa debe adoptar en pro de proteger la información de sus clientes[25] y brindarles la tranquilidad de que está segura ante cualquier amenaza cibernética, manteniendo la confidencialidad, donde los datos sensibles de los usuarios o clientes es guardada de manera segura y su divulgación es restringida únicamente a personal autorizado; disponibilidad, en donde la información esté disponible para su consulta únicamente a personal autorizado y que dicha información no sea restringida a causa de un ataque que la encripte; integridad, donde se espera que la información no sea modificada o malograda y cada dato sea verídico[26].

La confianza que dicha empresa le genere a sus clientes juega un papel muy importante para que ellos estén tranquilos de que su información está en buenas manos y no está siendo vendida o usada para obtener remuneraciones económicas a cambio de ella.

Si nos enfocamos en el ámbito personal, podemos realizarnos la siguiente pregunta: ¿Qué tan importante es la información que poseo en mis dispositivos?

Si la respuesta a la pregunta fuera NO es importante, podríamos pensar en que no conocemos el alcance de los ciber ataques, debido a que van más allá de lo que se espera o incluso creemos que otro ser humano no “gastara” su tiempo intentando realizar dichas acciones o, por otro lado, que nuestros datos no tienen información comprometedora. La cantidad de datos que recopila un dispositivo es bastante amplia y la lista de variables es extensa. Por ejemplo: una foto capturada mediante un celular almacena datos como la ubicación donde ésta fue tomada y al mismo tiempo, al recibir una foto, esta también es un archivo que podría llegar a tener un software malicioso escondido en una capa inferior, es decir, no detectable a simple vista.

La información que cada persona posee en su dispositivo también es vista como lucrativa en el momento que un ciber atacante pueda acceder a ella. El secuestro de información y estafa mediante la suplantación de identidad son ciberataques comunes, pero no por eso son de difícil detección. Cada ciberataque se compone de características y similitudes que permiten identificar la táctica que el ciber atacante está utilizando para robar la información.

B. Tipos de ataques cibernéticos a través de las redes sociales.

La prevención de ataques cibernéticos a través de las redes sociales es una responsabilidad independiente (actividad autónoma), sin embargo, es de gran ayuda tener el asesoramiento de un experto en el tema, además de las herramientas necesarias para superar el desafío más grande a la hora de ser un posible objetivo o directamente la víctima del ciberataque. La importancia de entender el riesgo nos prepara y alerta sobre la manera en que manejamos las redes sociales, para identificar si directamente nuestro perfil cumple con las medidas de seguridad necesarias para que nuestra información solo sea compartida con personas de confianza y no brindemos datos que pueden ser usados en nuestra contra, como la dirección donde vivimos o nuestra rutina diaria.

En los servicios que ofrecen las redes sociales, como el servicio de mensajería o publicaciones de contenido, podemos identificar los ataques cibernéticos que pueden ser efectuados a través de éstos:

1) Ingeniería social

Este tipo de ciber ataque involucra un conjunto de técnicas psicológicas en las que el atacante interactúa con la víctima, le genera incertidumbre y angustia con el pretexto de una situación que afecta o amenaza directamente a la persona[27]. Un ejemplo que esta fuera del contexto informático pero que pertenece a este conjunto de prácticas psicológicas es el de la llamada de un familiar que tiene un problema y que para solucionarlo necesita enviar dinero a un desconocido o que se le brinde algún tipo de información. Dentro de la ingeniería social en línea podemos identificar componentes como: el pretexto, que es la creación de un escenario inventado, en donde la victima presenta un problema y para solucionarlo deberá dar información sensible como sus contraseñas, números de tarjeta de crédito o códigos de verificación enviados por mensaje de texto (MSM); el suplantador, que corresponde a la suplantación de una persona, marca o empresa; el contexto, que es la situación problema que el atacante plantea para que la víctima reacciones, este evento amerita una respuesta inmediata, según el atacante; la oportunidad, es la situación que plantea el atacante para obtener la información que necesita[28]. Estos componentes pueden ayudar a identificar el ciber ataque, por lo que, si la víctima no sabe reconocer este tipo de prácticas psicológicas, podrá sentirse bajo presión y brindar la información que el atacante necesita. Aunque la mayoría de los casos involucran la interacción con un atacante, existen practicas donde éste realiza una investigación del contenido

público en el perfil de la víctima, para así obtener información valiosa que pueda usar para cualquier tipo de estafa, suplantación, etc.
Bajo esta modalidad de ataque existen distintas variantes:

a) Suplantación de identidad

Esta técnica consiste en hacerse pasar por otra persona, entidad o servicio con el objetivo de obtener acceso a información confidencial o realizar actividades maliciosas en nombre de la persona o entidad imitada. Junto con el phishing, esta práctica puede llevarse a cabo para que una vez obtenidos los datos de la víctima a través de un correo y pagina web falsa, otra suplante su identidad.
En el contexto de las redes sociales esta práctica podría vulnerar la identidad de una persona o marca, permitiendo que el atacante solicite información, dinero o favores a los contactos, aprovechado de la confianza que éstos tengan con la persona suplantada[29].
Lamentablemente, en el mundo de las redes sociales, es necesario mantener un nivel de desconfianza hacia el entorno, por esta razón, siempre que exista la más mínima duda de veracidad hacia un perfil o cuenta que nos contacte, encontrar la manera de verificar que la persona detrás de la pantalla sea quien dice ser.

b) Phishing

Este término se refiere a la suplantación de identidad mediante correos electrónicos. El ciber atacante realiza un envío masivo de correos bajo el nombre e identidad grafica de una marca o persona reconocida, que viene acompañado con enlace a un sitio fraudulento, es decir, aparenta ser legitimo pero que es controlado por alguien ajeno a la marca o empresa. En esta práctica se espera que al menos una persona de clic e ingrese sus datos en la página fraudulenta[30]. Al estar imitando una página real, el usuario puede ingresar sus datos de inicio de sesión y de esta manera el atacante tendrá acceso a la cuenta. Por ejemplo, en el caso de una tienda en línea (ejemplo: mercado libre), podrá hacer compras con la tarjeta de la víctima, que previamente pudo haber registrado.
Enfocándonos en el contexto de las redes sociales, este ataque puede efectuarse cuando la víctima recibe un correo o mensaje expresando la necesidad de que inicie sesión nuevamente debido a que ha ocurrido algún evento que requiere de su atención inmediata, esto genera en el usuario angustia por evitar perder su cuenta o que algo malo pase. Al hacer clic, el mismo correo le proporciona el enlace a una página que tiene la misma apariencia de la red social, pero al ingresar los datos estos se capturaran y enviaran al atacante, obteniendo así la información necesaria para acceder a la cuenta. Luego de eso, podemos pensar que pueden clonar la cuenta o hacer estafas sin que el usuario se percate de lo sucedido.

c) Ataques de cebo

Mediante esta táctica, el atacante ofrece a la(s) victima(s) algún tipo de recompensa o incentivo si confirma datos confidenciales o realiza alguna tarea que involucre replicar la estafa o acciones que sean perjudiciales para sí mismo[31].
Dentro de las redes sociales, este ataque puede presentarse como mensaje en el que una marca reconocida solicita ingresar a una página y registrarse para obtener los beneficios ofrecidos, sin embargo, lo que podría causar sería la divulgación de información personal o implantación de un virus.
Existen casos recientes, donde paginas fraudulentas con la identidad de un comercio mayorista de alto prestigio celebran un aniversario u otro tipo de eventos e indican a las personas que han ganado un premio[32]. Al ingresar datos como teléfono, correo electrónico, dirección, etc. podrán reclamar los supuestos beneficios, sin embargo, no hay ninguna recompensa y los datos están siendo enviados a un ciber atacante. Estas páginas están hechas cuidando los detalles para que su apariencia sea lo suficientemente creíble. Por esta razón, es importante desconfiar de cualquier publicidad que indique que ha recibido premios o recompensas, ya que este tipo de almacenes de cadena tienen sus propios dominios web y publicidad previa sobre premiaciones a clientes que hacen públicas a través de sus redes oficiales, nunca a través de mensajes privados o enlaces a páginas. Estar al tanto de las noticias es la manera más rápida de conocer si estos eventos se tratan de una estafa o son oficiales.

2) Programa maligno

El programa maligno o malware consiste en un software cuyo objetivo es dañar o destruir sistemas y/o robar información. Generalmente, el malware esta creado por ciberdelincuentes. Este es el termino global que incluye virus, ransomware, troyanos, spyware, etc. donde cada uno puede propagarse a través de archivos, anuncios, instalación de software falso, dispositivos de almacenamiento o aplicaciones infectadas[33].
En las redes sociales también es posible ser víctima de un virus ya que existen plataformas con servicio de mensajería y transmisión de documentos, por lo que es posible descargar un archivo infectado que sea capaz de espiarnos, robar información o incluso encriptarla, como es el caso del ransomware.
Para prevenir este tipo de ataques se debe desconfiar de mensajes de personas que no pertenecen a nuestra lista de contactos, en el caso de envío de documentos o enlaces. En ocasiones, los enlaces contienen un virus que al abrirlo se propaga de forma inadvertida o sin el conocimiento del usuario ya que este se replica de forma automática sin que haya rastro de él.

3) Fuerza bruta

El ataque de fuerza bruta es aquel en el que los ciber atacantes intentan descifrar el nombre de usuario, contraseñas, etc. con el objetivo de que los métodos acierten con en el dato correcto[34].
La creación de contraseñas seguras es un ítem fundamental cuando se habla de seguridad en internet, ya que éstas son el método más común para validar nuestra identidad al ingresar a un servicio que cuenta con perfiles. Las contraseñas se componen de caracteres, por lo que éstas pueden llegar a ser descifradas. Una buena práctica es la de crear contraseñas seguras, que combinen caracteres alfanuméricos y símbolos, con una longitud de al menos 8 caracteres, también evitar usar

nombres propios, fechas de nacimiento y contraseñas simples o comunes, como 1234.
En redes sociales, estos ataques son usados para robar cuentas y cometer otro tipo de ciberataques como la ingeniería social, la estafa y la divulgación de noticias falsas.

C. Redes sociales, adolescentes y ciberataques

Hoy en día, el internet es el recurso más usado para conectarnos con cualquier persona, sin importar su ubicación en el mundo, lo que brinda a la humanidad infinitas posibilidades para que la comunicación se preste de formas más sencillas. La evolución, en el contexto de la comunicación, ha puesto las herramientas necesarias al alcance de las personas y hasta el día de hoy seguimos explotando las funciones que nos brindan y desarrollando nuevas. Dentro de las herramientas que nos brinda el internet para comunicarnos existen las redes sociales, las cuales brindan servicios de mensajería y publicación de contenido idóneo para el entretenimiento. La población en general utiliza este tipo de redes para expresarse, comunicarse, informarse o incluso como el medio para aprender algo de forma gratuita, así como una gran población de personas tienen cuentas en estas redes, el contenido que se puede encontrar es bastante amplio. En términos de usuarios, los adolescentes entre los 13 y 17 años son los que más usan las redes sociales. Más allá de pensar en lo que afecta el uso de cualquier red a esta edad, es importante enfocarnos en los peligros que se presentan debido a la cantidad de ciberataques a los que pueden estar expuestos por el desconocimiento de las medidas básicas de ciber seguridad. La educación de los adolescentes empieza desde casa, sin embargo, ellos mismos se encargan de ocultar contenido a sus padres, tutores o acompañantes, cerrando la posibilidad de entablar conversaciones sobre temas apropiados sobre la ciberseguridad en redes sociales[35].
Las estafas que son aplicadas a los adolescentes consisten en la vulneración de la privacidad, haciendo uso del contenido publicado, para que el ciber atacante emplee cualquier técnica mencionada anteriormente para obtener información confidencial. Teniendo en cuenta los tipos de ataques y el impacto social que puede generar en un individuo, es importante resaltar el correcto uso de redes sociales en adolescentes para que no se conviertan en víctimas directas del robo de información y estafa en línea. Mediante el conocimiento, los adolescentes deben adoptar una postura responsable durante el uso de redes sociales que incluyan la apertura e interés por concientizarse sobre las practicas que los ciberdelincuentes pueden usar y las características que permitan detectar cualquier técnica de ciberataque.
Según el estudio realizado por el grupo de investigación Comunicación y Estudios Culturales de la Universidad EAFIT y la empresa Tigo Une, los niños pasan en promedio 3 horas 31 minutos en el internet por día[36]. Según el DANE (Departamento administrativo nacional de estadísticas), en Colombia más de 9.2 millones de hogares obtuvieron acceso a internet en el 2020 y el aumento en el uso del internet de jóvenes entre los 12 y 24 años fue del 84.1% [35].

D. Estrategias educativas sugerida para el conocimiento de los ciberataques a través de redes sociales.

En la educación, juegan papeles muy importantes para que un estudiante, o en este caso, el adolescente, capte la información de una manera que sea amena y que la comunicación sea asertiva. Por esta razón, se plantea usar el enfoque constructivista, el cual enfatiza en el papel activo del estudiante y en su propio proceso de aprendizaje[37]. El enfoque constructivista se centra en la idea de que el conocimiento se construye activamente mediante interacciones y experiencias previas[38], es decir, con un evento que sea familiar y pueda ser asociado de manera rápida, con la expectativa de que sea más intuitivo el aprendizaje para que el estudiante se motive a experimentar, explorar y resolver problemas autónomamente, ya que se alienta a conectar nuevos conocimientos con situaciones del mundo real[39].
Dos figuras clave en el desarrollo del constructivismo fueron Jean Piaget y Lev Vygotsky. Ambos coincidían en la idea de que todos los seres humanos son discípulos activos que cuentan con la capacidad de desarrollar conocimientos por sí solos. No obstante, ambos tenían perspectivas distintas, Vygotsky se enfocaba en comprender como el entorno social impacta en la formación interna de las personas, mientras que Piaget se enfocó en explorar como las personas construyen sus conocimientos a partir de su interacción en un entorno real[40].
Para lograr el correcto entendimiento de la ciberseguridad en redes sociales, existen diferentes tipos de estrategias y dinámicas en donde la participación del estudiante incita a que él mismo genere sus conceptos y opiniones.
La importancia de la interacción entre el estudiante y el tema de manera habitual será clave para que los conceptos teóricos que se requieren abordar sean de fácil comprensión y retentiva. Al ser el propio estudiante el que encamina la manera en que capta los conceptos, convierte esta estrategia educativa en participativa, ya que no solo el docente realiza el esfuerzo de transmitir la información al estudiante, sino que el mismo crea conceptos y relaciona términos con fenómenos del mundo real, siendo estos la experiencia previa que requiere el enfoque constructivista.
Para lograr un aprendizaje significativo, es necesario que el docente y el estudiante estén involucrados en el proceso de enseñanza-aprendizaje, el cual es un proceso bidireccional en el cual se facilita por parte del docente la adquisición de conocimiento, habilidades, actitudes y hasta valores en otro individuo, en este caso, el estudiante. El proceso de enseñanza-aprendizaje es dinámico y puede variar en factores, como el estilo de enseñanza del docente, el entorno educativo, las capacidades individuales de cada estudiante y las estrategias pedagógicas utilizadas. Idealmente este proceso busca crear un entorno en el que el estudiante no solo reciba información, sino que también participe en su formación. Como parte del proceso evaluativo y para evidenciar la correcta comprensión de la temática tratada, la evaluación formativa brinda las herramientas para recopilar información continuamente durante el proceso de enseñanza-aprendizaje y para comprender el progreso de los estudiantes en pro de mejorar su educación. La evaluación formativa se lleva a cabo de manera continua para identificar áreas de mejora y adaptar la enseñanza en consecuencia.

Como parte de la implementación de este modelo y en pro de ser fiel a la técnica enseñanza-aprendizaje, se proponen las siguientes estrategias pedagógicas para enseñar a los adolescentes los conceptos necesarios para que puedan aplicarlos a su vida en redes sociales.

1) Videojuegos

Para acercar al estudiante a una experiencia previa que resulte más familiar, se propone el uso de videojuegos. Las características de un videojuego permiten disfrutar de la experiencia de entretenimiento mediante la gamificación de elementos que principalmente no lo son. También conocidos como videojuegos educativos, su propósito, más allá de entretener, es educar, informar, capacitar y sobre todo modelar situaciones del mundo real para acercar al usuario a una experiencia más allegada a la realidad. Los juegos educativos pueden abarcar una amplia gama de temas, desde matemáticas, lenguaje, programación, etc. y su beneficio es el aprendizaje del estudiante ante temas que sean de difícil comprensión, generando una perspectiva completamente nueva al enfoque que el docente o educador este implementando en sus clases magistrales[41].

La variedad de juegos que podrían emplearse para la gamificación de conceptos de ciberseguridad y vulnerabilidades en redes sociales es amplia. Grandes empresas como Google se han preocupado por transmitir información de carácter popular y tradicional a través de internet de manera entretenida, es por eso por lo que en el año 1998 fue publicado el primer Doodle[42], que es una alteración del logo principal de Google para conmemorar o celebrar algún evento importante del mundo. Cada Doodle tiene como objetivo explicarnos el contexto del evento mediante contenido multimedia e incluso mediante actividades dinámicas como juegos. Este ejemplo es claro para entender cómo funciona la gamificación, donde se modelan fenómenos del mundo a través de la interacción con un juego.

Un juego que podemos tomar como ejemplo de los antecedentes del uso de video juegos para fomentar la enseñanza de un tema específico es el juego *Interland* creado por Google como parte de la estrategia "Se genial en internet"[43]. El juego está enfocado en los niños y pretende presentarles las situaciones incomodas que pueden generar los hostigadores en línea, mostrándolos como enemigos y planteando la estrategia de como colaborar dentro del internet para evitar que los demás usuarios se vean afectados por las molestias del hostigador. El juego pertenece a los juegos de plataformas, donde el jugador toma el control de un robot que reparte emociones positivas y protege a los demás de los abusos.

De acuerdo con lo anterior, debemos comprender que las mecánicas de otros juegos existentes pueden ser empleadas para que la experiencia del jugador (en este caso, estudiante) sea percibida como algo conocido e incluso, si el estudiante conoce de los video juegos, acepte la dinámica con propiedad.

El mundo de los videojuegos incluye contenidos como juegos de aventura, de rol, casuales, en realidad virtual, de plataformas, de lógica, de carreras, de mundo abierto, de supervivencia, multijugador, etc. Esta amplia gama de opciones nos permite emplear sus dinámicas, por ejemplo, podríamos proponer la creación de un video juego de realidad virtual completamente nuevo, que le permita al usuario interactuar en un entorno creado por computador, pero con las características de ser lo suficientemente inmersivo para centrar toda la atención en el mundo virtual. Para emplear este tipo de videojuegos se requiere la creación desde cero del ambiente que se va a tratar y la configuración de los periféricos necesarios (controles, micrófonos, lentes de realidad virtual), el guion que seguirá el juego y los problemas o enemigos a los que el usuario se deberá enfrentar. Para continuar con la propuesta de crear un video juego de realidad virtual, podemos plantear el escenario de un videojuego de lógica, en el que el tutorial corresponde a los conceptos de ciberseguridad y el personaje se encuentra en un laberinto lleno de enemigos, cada vez que uno de ellos intenta atacar al jugador, este podrá vencerlo respondiendo preguntas (en voz alta o por medio de selección múltiple) correspondientes a la ciberseguridad en redes sociales, detectando las características de un ataque cibernético, configurando las medidas de seguridad aprendidas en conceptos anteriores, etc.

De esta forma, se da paso a aplicar la evaluación formativa comprobando si los conocimientos fueron comprendidos por el jugador, que es en este caso, el estudiante.

El uso de plataformas existentes también es una opción válida para implementar esta estrategia para educar a los adolescentes, como el uso de plataformas en línea gratuitas que permiten la interacción en una sala virtual, donde el docente instructor define preguntas y los participantes responden de acuerdo su consideración, premiando las respuestas acertadas y que fueron respondidas en el menor tiempo en comparación a los demás.

La participación del estudiante en este caso corresponderá al interés y dedicación que pueda ofrecer hacia la dinámica. El objetivo del juego será generar experiencias diferentes y con ello enfatizar en la participación del estudiante para generar sus propios conceptos y relacionar el fenómeno gamificado con la realidad

2) Charlas con expertos

Como se menciona anteriormente, existe personal capacitado en este tema, el cual puede compartir su experiencia y transmitir datos y consejos útiles para que los adolescentes adopten los conceptos y los apliquen en su vida diaria.

Para que las conferencias sean dinámicas y los adolescentes puedan participar activamente, se proponen diferentes tipos de conversatorios, como paneles, tertulias, simposios, etc. donde el objetivo sea que cada persona forje su concepto y opinión a través de los distintos modelos de comunicación que estas charlas nos pueden brindar. De esta manera, el estudiante podrá poner en práctica su capacidad comunicativa para generar su propio argumento y definición a la hora de hablar ante un público o defender un punto de vista.

3) Actividades lúdicas dirigidas

Por lo general, el salón de clase es el espacio donde los estudiantes o adolescentes reciben la mayoría de sus clases, sin embargo, existen otros espacios en los que también es posible transmitir conocimiento, incluso, este cambio genera motivación en el estudiante y convierte la experiencia en algo significativo. Como propuesta a un método de enseñanza más interactivo, emplear juegos tradicionales (yoyo, bolo criollo, etc.), balones, globos de agua, pesca de objetos, dibujos,

crucigramas, etc. para crear actividades enfocadas a la comprensión de los conceptos de ciberseguridad mediante el juego al aire libre, donde exista material didáctico que permita a los estudiantes asociar los conceptos. Por ejemplo, un circuito de bases en donde cada una tiene la temática de un ciber ataque y cada reto que ésta proponga aporte a las respuestas correctas mediante una actividad, así de esta manera, verificamos si el concepto está comprendido. En el caso de que la respuesta sea errónea, que el castigo no sea visto como un fracaso sino la oportunidad de entender que no es el camino correcto y debe cambiar la manera de ver la pregunta.

IV. Recomendaciones generales

En el rol de educadores o tutores, es necesario brindar las herramientas necesarias para que los estudiantes (que a partir de los 12 años son adolescentes) adquieran los conocimientos necesarios para afrontar los retos y adquirir la responsabilidad que requiere la interacción dentro del internet. A demás de eso y como aspecto adicional, la ética juega un rol importante, ya que el mismo adolescente puede convertirse en el victimario. En consecuencia, la sociedad en general debe aportar a la educación en internet debido a la gran dependencia que se tiene hacia las herramientas y espacios cibernéticos a los que podemos acceder desde dispositivos móviles o de cómputo.

La búsqueda de estrategias educativas no puede detenerse, esto debido a que al mismo tiempo que la tecnología avanza, los delincuentes inventan estrategias con el fin de vulnerar los sistemas informáticos y donde las redes sociales son la ventana a la información de los usuarios.

V. Conclusión

Como parte de la investigación realizada sobre los tipos de ataques cibernéticos que pueden ser ejecutados a través de las redes sociales, se despierta la preocupación por la cantidad de adolescentes que poseen una cuenta y desconocen completamente los riesgos a los que se exponen cuando no adoptan las medidas de ciberseguridad que requiere un perfil en la red social de su preferencia y uso frecuente. De acuerdo con las características de los ataques por medio de las redes sociales, podemos entender que la protección que nos brindamos a nosotros mismos es la más eficiente, pero al mismo tiempo requiere que el usuario sea experto en el tema, adquiriendo la habilidad de detectar cuando un ciber atacante pretenda ejecutar alguna técnica en un perfil. El componente educativo cumple un papel fundamental en los adolescentes, ya que debe ser capaz de transmitir los conocimientos necesarios para que éste se prepare para identificar un ataque cibernético. Por esta razón, la opción que más se profundizó en este artículo fue la implementación de un videojuego serio, ya que esté brinda entretenimiento y la experiencia del estudiante será aún más significativa al generar diversión a la hora de aprender y teniendo en cuenta que la participación activa del estudiante se verá incentivada por la parte llamativa del juego, sin contar la cantidad de opciones que un video juego brinda a sus desarrolladores para establecer la gamificación de este fenómeno de la ciberseguridad.

Referencias

[1] D. Jayasuriya, V. Terragni, J. Dietrich, S. Ou, and K. Blincoe, “Understanding Breaking Changes in the Wild,” in *ISSTA 2023 - Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis*, J. R. and F. F., Eds., Association for Computing Machinery, Inc, 2023, pp. 1433 – 1444. doi: 10.1145/3597926.3598147.

[2] H. Suryotrisongko and Y. Musashi, “Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective,” in *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*, 2019, pp. 162–167. doi: 10.1109/SOCA.2019.00031.

[3] M. E. Oka and M. Hromada, “Analysis of Current Preventive Approaches in the Context of Cybersecurity,” in *Proceedings - International Carnahan Conference on Security Technology*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICCST52959.2022.9896499.

[4] M. C. Botero, “Ciberataque a IFX Networks: la amenaza que golpea a Colombia.” Accessed: Oct. 28, 2023. [Online]. Available: https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

[5] B. Sloane, *Cybersecurity Behavior and Behavioral Interventions*. CRC Press, 2023. doi: 10.1201/9781003415060-14.

[6] G. R. K. Rao, V. V. Battu, V. Anupama, A. Allada, S. V. R. Krishna, and C. Hema, “Modern Progressive Pitfalls of Cyber Attacks on the Digital World,” in *Proceedings of the 2nd International Conference on Edge Computing and Applications, ICECAA 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 244 – 248. doi: 10.1109/ICECAA58104.2023.10212303.

[7] “Coste de la vulneración de datos 2023 | IBM.” Accessed: Nov. 02, 2023. [Online]. Available: https://www.ibm.com/es-es/reports/data-breach

[8] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, “Social engineering in social networking sites: Affect-based model,” in *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, Dec. 2013, pp. 508–515. doi: 10.1109/ICITST.2013.6750253.

[9] R. Sen, “Challenges to cybersecurity: Current state of affairs,” *Communications of the Association for Information Systems*, vol. 43, no. 1, pp. 22 – 44, 2018, doi: 10.17705/1CAIS.04302.

[10] N. Q.-R. argentina de estudios de juventud and undefined 2020, “TikTok: La aplicación favorita durante el aislamiento,” *perio.unlp.edu.ar*, doi: 10.24215/18524907e044.

[11] S. Anzano-Oto, S. Vázquez-Toledo, and C. Latorre-Cosculluela, “Digital reality in Compulsary Secondary Education: uses, purposes and profiles in social networks,” *New Review of Information Networking*, 2023, doi: 10.1080/13614576.2023.2219244.

[12] I. Ahmadi, A. Waltenrath, and C. Janze, “Congruency and Users’ Sharing on Social Media Platforms: A Novel Approach for Analyzing Content,” *J Advert*, vol. 52, no. 3, pp. 369 – 386, 2023, doi: 10.1080/00913367.2022.2055683.

[13] F. Yus, “La construcción de la identidad en las redes sociales,” *Guía Práctica de Pragmática del Español*, pp. 219–229, Aug. 2019, doi: 10.4324/9781351109239-21/LA-CONSTRUCCI.

[14] R. T.-R. P. Social and undefined 2020, “¿ Por qué los y las jóvenes están en las redes sociales? Un análisis de sus motivaciones a partir de la teoría de usos y gratificaciones,” *revistaprismasocial.es*, Accessed: Oct. 29, 2023. [Online]. Available: https://revistaprismasocial.es/article/view/3558

[15] M. C.- de Imagen, A. y E. C. y Social, and undefined 2022, “Identidad y adolescencia: la educación artística, visual y audiovisual frente a la influencia de redes sociales y publicidad,” *revistascientificas.us.es*, Accessed: Oct. 30, 2023. [Online]. Available: https://revistascientificas.us.es/index.php/Communiars/article/view/22259

[16] M. O.-P. Clave and undefined 2022, “‘Me encanta mi trabajo, pero es un trabajo’: creadores de contenido en redes sociales e imaginarios laborales,” *scielo.org.co*, Accessed: Oct. 30, 2023. [Online]. Available: http://www.scielo.org.co/scielo.php?pid=S0122-82852022000402544&script=sci_arttext

[17] M. Lemus, “Exposición regulada: prácticas de jóvenes en instagram,” *Astrolabio*, no. 26, pp. 312–342, Jan. 2021, doi: 10.55441/1668.7515.N26.25144.

[18] X. Palacios, “Adolescencia: ¿una etapa problemática del desarrollo humano?,” *Revista Ciencias de la Salud*, vol. 17, no. 1, pp. 5–7, Feb. 2019, doi: 10.12804/REVISTAS.UROSARIO.EDU.CO/REVSALUD/A.7587.

[19] J. Protzko and J. W. Schooler, “Kids these days: Why the youth of today seem lacking,” *Sci Adv*, vol. 5, no. 10, 2019, doi: 10.1126/sciadv.aav5916.

[20] H. S. Berry, “Survey of the Challenges and Solutions in Cybersecurity Awareness Among College Students,” in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 2023, pp. 1–6. doi: 10.1109/ISDFS58141.2023.10131851.

[21] A. DE Revisión, M. Chérrez, W. I. Eduardo, Á. Pesantez, and D. I. Fernando I, “Ciberseguridad en las redes sociales: una revisión teórica,” *dialnet.unirioja.es*, Accessed: Oct. 30, 2023. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8298208

[22] N. Shinde and P. Kulkarni, “Cyber incident response and planning: a flexible approach,” *Computer Fraud and Security*, vol. 2021, no. 1, pp. 14 – 19, 2021, doi: 10.1016/S1361-3723(21)00009-9.

[23] G. Patricia Guevara Alban, A. Eduardo Verdesoto Arguello, and N. Esther Castro Molina, “Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción),” *recimundo.com*, no. 3, pp. 163–173, doi: 10.26820/recimundo/4.(3).julio.2020.163-173.

[24] M. Cazares, W. Fuertes, R. Andrade, I. Ortiz-Garcés, and M. S. Rubio, “Protective Factors for Developing Cognitive Skills against Cyberattacks,” *Electronics (Switzerland)*, vol. 12, no. 19, 2023, doi: 10.3390/electronics12194007.

[25] “ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.” Accessed: Nov. 04, 2023. [Online]. Available: https://www.iso.org/standard/73906.html

[26] E. L.-D. e informática: algunos aspectos and undefined 2007, “Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos,” *academia.edu*, Accessed: Nov. 04, 2023. [Online]. Available: https://www.academia.edu/download/59779491/2007-Delitos_informaticos20190618-52109-6fm00r.pdf#page=85

[27] C. E. L. Grande and R. S. Guadrón, “Ingeniería social : el ataque silencioso,” 2015, Accessed: Nov. 04, 2023. [Online]. Available: http://redicces.org.sv/jspui/handle/10972/2910

[28] T. De Fin and D. E. Grado, “Estudio de las técnicas de la ingeniería social usadas en ataques de ciberseguridad y análisis sociológico,” 2015, Accessed: Dec. 04, 2023. [Online]. Available: https://oa.upm.es/id/eprint/37773

[29] C. Stalin *et al.*, “Análisis del uso de las técnicas de ingeniería social caso de estudio: Instituto Superior Tecnológico Huaquillas-Ecuador,” *ciencialatina.org*, vol. 1, no. 7, p. 11471, 2023, doi: 10.37811/cl_rcm.v7i2.5696.

[30] E. Benavides, W. Fuertes, … S. S.-C. y, and undefined 2020, “Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura,” *revistas.uteq.edu.ec*, doi: 10.18779/cyt.v13i1.357.

[31] • Autor and J. Alzas Hernandez, “Estudio de fraudes basados en la técnica de Ingeniería Social,” Jun. 2023, Accessed: Nov. 04, 2023. [Online]. Available: https://openaccess.uoc.edu/handle/10609/148147

[32] “D1 alerta sobre estafa a clientes - Empresas - Economía - ELTIEMPO.COM.” Accessed: Nov. 04, 2023. [Online]. Available: https://www.eltiempo.com/economia/empresas/d1-alerta-sobre-estafa-a-clientes-617262

[33] H. Rodriguez-Bazan, G. Sidorov, and J. Escamilla-Ambrosio, “Revisión del estado del arte en técnicas de procesamiento de lenguaje natural para análisis de malware.,” *rcs.cic.ipn.mx*, vol. 149, no. 8, pp. 2020–1105, Accessed: Nov. 04, 2023. [Online]. Available: https://rcs.cic.ipn.mx/2020_149_8/Revision%20del%20estado%20del%20arte%20en%20tecnicas%20de%20procesamiento%20de%20lenguaje%20natural%20para%20analisis%20de%20malware.pdf

[34] J. M. Conforme Tomala *et al.*, “Medios de ataques a los sistemas de seguridad de la información,” *revistas.unesum.edu.ec*, doi: 10.47230/Journal.TechInnovation.v2.n1.2023.72-78.

[35] “Colombia avanza en su meta de estar conectada en un 70 % en 2022: DANE.” Accessed: Nov. 05, 2023. [Online]. Available: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/182108:Colombia-avanza-en-su-meta-de-estar-conectada-en-un-70-en-2022-DANE

[36] “55 % de los menores de edad en Colombia contactan con desconocidos por internet - Portal de Noticias - Uninorte.” Accessed: Nov. 05, 2023. [Online]. Available: https://www.uninorte.edu.co/es/web/grupo-prensa/w/55-de-los-menores-de-edad-en-colombia-contactan-con-desconocidos-por-internet

[37] J. Aulestia *et al.*, “Contribución del enfoque constructivista al trabajo colaborativo en la educación superior,” *revistaespacios.com*, vol. 40, p. 41, Accessed: Nov. 02, 2023. [Online]. Available: https://www.revistaespacios.com/a19v40n41/a19v40n41p04.pdf

[38] A. Pérez, A. Rámoz, … C. M.-… científica: R., and undefined 2020, “Aplicación de la tecnología en las aulas de educación superior desde el enfoque constructivista,” *repositorio.umecit.edu.pa*, Accessed: Nov. 02, 2023. [Online]. Available: https://repositorio.umecit.edu.pa/handle/001/4756

[39] G. V. Gomez, “Propuesta de un modelo de formación de mentores bajo enfoque constructivista para fortalecer la enseñanza-aprendizaje de los estudiantes de pregrado de,” 2020, Accessed: Nov. 02, 2023. [Online]. Available: https://repositorio.ucv.edu.pe/handle/20.500.12692/61817

[40] L. G.- Milenaria, C. y arte, and undefined 2021, “EL CONSTRUCTIVISMO;: posibilidades en el aula universitaria,” *milenaria.umich.mx*, vol. 8, no. 1, p. 1, 2021, Accessed: Nov. 04, 2023. [Online]. Available: http://www.milenaria.umich.mx/ojs/index.php/milenaria/article/view/131

[41] I. Cruz-García, J. Antonio Martín-García, D. Pérez-Marín, and C. Pizarro, “Propuesta de didáctica de la Programación en Educación Primaria basada en la gamificación usando videojuegos educativos,” *revistas.usal.es*, 2021, doi: 10.14201/eks.26130.

[42] “12 cosas que no sabías sobre los Doodles de Google.” Accessed: Dec. 03, 2023. [Online]. Available: https://blog.google/intl/es-419/actualizaciones-de-producto/12-cosas-que-no-sabias-sobre-los-doodles-de-google/

[43] “Acerca de Sé genial en Internet.” Accessed: Dec. 04, 2023. [Online]. Available: https://beinternetawesome.withgoogle.com/es-419_all/