Maestría en
EDUCACIÓN
CON MENCIÓN EN GESTIÓN DEL APRENDIZAJE MEDIADO POR TIC

Trabajo de titulación previa a la obtención de título de Magister en Educación mención Gestión del Aprendizaje mediado por TIC.

AUTORES:
Erik Joel Chasi Sandoval
Tamya Alejandra Oña Pillajo
Fabiola Maribel Hachi Toapanta
María Angeles Jácome Razo
Kevin Alexander Jiménez Hurtado

TUTORES:
Adriana Romero
Jesús Sánchez
Luis Guerrero
Noelia Salvador
Teresa Campaña

Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera

Quito, noviembre 2023

Autoría del Trabajo de Titulación

Yo, ***Erik Joel Chasi Sandoval,*** declaro bajo juramento que el trabajo de titulación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera*** es de mi autoría y exclusiva responsabilidad legal y académica; que no ha sido presentado anteriormente para ningún grado o calificación profesional, habiéndose citado las fuentes correspondientes y respetando las disposiciones legales que protegen los derechos de autor vigentes.

Erik Joel Chasi Sandoval

Correo electrónico: erik.chasi@outlook.com

Yo, ***Tamya Alejandra Oña Pillajo,*** declaro bajo juramento que el trabajo de titulación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera*** es de mi autoría y exclusiva responsabilidad legal y académica; que no ha sido presentado anteriormente para ningún grado o calificación profesional, habiéndose citado las fuentes correspondientes y respetando las disposiciones legales que protegen los derechos de autor vigentes.

Tamya Alejandra Oña Pillajo

Correo electrónico: ale-ale07@hotmail.com

Autoría del Trabajo de Titulación

Yo, ***Fabiola Maribel Hachi Toapanta***, declaro bajo juramento que el trabajo de titulación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera*** es de mi autoría y exclusiva responsabilidad legal y académica; que no ha sido presentado anteriormente para ningún grado o calificación profesional, habiéndose citado las fuentes correspondientes y respetando las disposiciones legales que protegen los derechos de autor vigentes.

_____

Fabiola Maribel Hachi Toapanta
Correo electrónico: elimaris1621@gmail.com

Yo, ***María Angeles Jácome Razo***, declaro bajo juramento que el trabajo de titulación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera*** es de mi autoría y exclusiva responsabilidad legal y académica; que no ha sido presentado anteriormente para ningún grado o calificación profesional, habiéndose citado las fuentes correspondientes y respetando las disposiciones legales que protegen los derechos de autor vigentes.

_____

María Angeles Jácome Razo
Correo electrónico: maangelesjacome@gmail.com

Autoría del Trabajo de Titulación

Yo, ***Kevin Alexander Jiménez Hurtado***, declaro bajo juramento que el trabajo de titulación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera*** es de mi autoría y exclusiva responsabilidad legal y académica; que no ha sido presentado anteriormente para ningún grado o calificación profesional, habiéndose citado las fuentes correspondientes y respetando las disposiciones legales que protegen los derechos de autor vigentes.

Kevin Alexander Jiménez Hurtado
Correo electrónico: kevjimal24@gmail.com

Autorización de Derechos de Propiedad Intelectual

Yo, ***Erik Joel Chasi Sandoval***, en calidad de autor del trabajo de investigación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera***, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Noviembre 2023

_____

Erik Joel Chasi Sandoval

Correo electrónico: erik.chasi@outlook.com

Yo, ***Tamya Alejandra Oña Pillajo***, en calidad de autor del trabajo de investigación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera***, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Noviembre 2023

_____

Tamya Alejandra Oña Pillajo

Correos electrónicos: ale-ale07@hotmail.com

Autorización de Derechos de Propiedad Intelectual

Yo, ***Fabiola Maribel Hachi Toapanta***, en calidad de autor del trabajo de investigación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera***, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Noviembre 2023

_____

Fabiola Maribel Hachi Toapanta

Correo electrónico: elimaris1621@gmail.com

Yo, ***María Angeles Jácome Razo***, en calidad de autor del trabajo de investigación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera***, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Noviembre 2023

_____

María Angeles Jácome Razo

Correo electrónico: Maangelesjacome@gmail.com

Autorización de Derechos de Propiedad Intelectual

Yo, ***Kevin Alexander Jiménez Hurtado***, en calidad de autor del trabajo de investigación titulado ***Escudo digital: Un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera***, autorizo a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autor me corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Noviembre 2023

_____

Kevin Alexander Jiménez Hurtado

Correo electrónico: kevjimal24@gmail.com

DEDICATORIA

El presente proyecto de titulación va dedicado a Dios y a mis padres por ser mi guía y apoyo constante en cada paso de mi vida.

Erik

A mi buen Dios siempre por estar mi vida, a mis padres por ser mi apoyo incondicional, a mis queridos hermanos quienes son mi inspiración y mi ejemplo.

Tamya

Al ser supremo que siempre me acompaña, a mi familia por su apoyo incondicional y a mis compañeros quienes me dieron la oportunidad de tener nuevas aventuras.

Maribel

Quiero dedicar este logro a Dios, a mi Abuelita y madre por ser pilares fundamentales, mis consejeras, por demostrarme ese amor incondicional y saber guiarnos por el camino correcto.

María Angeles

Este proyecto va dedicado a mí y a las personas que hicieron que me guste mi vida, quienes me guiaron y apoyaron hasta este punto. Especialmente a Blanca, Luis, Lastenia y Byron.

Kevin

AGRADECIMIENTO

Agradecemos de manera especial a la Universidad Internacional del Ecuador (UIDE) y a la Escuela Internacional de Gerencia (EIG) por brindarnos la oportunidad de cursar el programa de maestría y a todo su cuerpo docente quienes supieron guiarnos y transmitir su conocimiento para formarnos y permitirnos alcanzar esta nueva meta en nuestra formación profesional.

Los autores

TABLA DE CONTENIDO

CAPÍTULO II

CAPÍTULO III

INDICE DE FIGURAS

RESUMEN

Los MOOCS son una modalidad de aprendizaje en línea, que está teniendo auge a nivel mundial que está evolucionando y formando parte de la actividad escolar. Para el presente proyecto de titulación se realizó una propuesta de un MOOC de ciberseguridad para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera que se planteó para un grupo de estudiantes de décimo año de educación básica en primera instancia como grupo de prueba, para los cuales se identificó que pueden enfrentar múltiples problemas de ciberseguridad debido a que no cuentan con una cátedra direccionada a la capacitación y utilización de las herramientas tecnológicas con el fin de prevenir y precautelar a los estudiantes. La herramienta tecnológica MOOC en cuanto a la educación se ha constituido en un método lúdico y creativo para la enseñanza de los temas de ciberseguridad, siendo el único recurso indispensable el acceso a internet.

PALABRAS CLAVE: MOOC, Ciberseguridad, Ciberdelitos, Educación.

ABSTRAC

MOOCs (Massive Open Online Courses) are a form of online learning that is gaining worldwide popularity and becoming an integral part of academic activities. For this graduation project, a proposal was developed for a cybersecurity MOOC to enhance the online protection and awareness of students at the Isaac Jesús Barrera Educational Unit. Initially designed as a pilot program for a group of tenth-grade students, it was identified that these students may face multiple cybersecurity challenges due to the lack of a specific curriculum focused on training and using technological tools to prevent and safeguard students. The MOOC technology, in terms of education, has evolved into a playful and creative method for teaching cybersecurity topics, with internet access being the only essential requirement.

KEY WORDS: MOOC, Cybersecurity, Cybercrime, Education.

INTRODUCCIÓN

En la actualidad, vivimos en un mundo cada vez más conectado digitalmente. Internet nos ofrece una gran cantidad de oportunidades y beneficios, pero también presenta riesgos y amenazas que constantemente están buscando formas de infiltrarse en nuestros dispositivos y redes, robar nuestra información personal, realizar fraudes o causar daño a nuestras vidas digitales. Es por eso que es crucial y recomendable que todos tengamos un conocimiento básico de ciberseguridad y sepamos cómo protegernos. El MOOC (Massive Open Online Course) de ciberseguridad para los estudiantes de la Unidad Educativa Isaac Jesús Barrera es un curso en línea que brindará a los estudiantes los conocimientos y habilidades necesarios para protegerse en línea y navegar de manera segura en el mundo digital. El curso está disponible de forma gratuita para todos los estudiantes y consta de una serie de módulos que abordan diferentes aspectos de la ciberseguridad. El curso de ciberseguridad ofrecerá una información completa en la protección y seguridad en línea. Desde los conceptos básicos hasta temas más específicos, los estudiantes aprenderán sobre amenazas comunes, protección de datos personales, seguridad en redes sociales y dispositivos móviles. A través de recursos educativos interactivos como videos, ejercicios prácticos y evaluaciones, los estudiantes adquirirán conocimientos prácticos y estarán preparados para identificar y evitar riesgos en línea. El MOOC de ciberseguridad para los estudiantes de la Unidad Educativa Isaac Jesús Barrera es una oportunidad invaluable para adquirir los conocimientos y habilidades necesarios para protegerse en línea. A través de este curso, los estudiantes aprenderán a proteger su información personal, evitar ataques cibernéticos y navegar de manera segura en el mundo digital. Al promover la conciencia y la educación en ciberseguridad, se busca crear una comunidad estudiantil empoderada y protegida en línea.

CAPÍTULO I

1. DIAGNÓSTICO DEL PROBLEMA

1.1. Definición del problema o reto

La ciberseguridad a nivel mundial es un tema de mucho interés para toda la sociedad, en vista que la información facilitada por todo ciudadano cuando realiza una actividad en una institución sea pública o privada se encuentra almacenado dentro de la herramienta del ciberespacio, lo cual pone en un riesgo latente los datos obtenidos, por parte de personas que se especializan en temas de informática avanzada, lo que les permite acceder a determinados dispositivos electrónicos y sustraer información que en la mayoría de los casos es utilizada para realizar actividades ilegales.

La tecnología es un medio muy útil en la sociedad actual para el desarrollo en todos los ámbitos, pero que al mismo tiempo es una bomba a punto de explotar pues lamentablemente las personas no están en la capacidad de discernir páginas reales y confiables, es así que dentro de las víctimas por parte de estos delitos virtuales, tenemos a los niños y adolescentes que por su naturaleza y curiosidad pueden ser un blanco fácil, a su vez son los nativos digitales que en su mayor parte pasan cerca de un equipo tecnológico.

Es importante señalar que el Ecuador posee una legislación muy amplia, contra los ciberdelitos a su vez cuenta con instituciones gubernamentales como Consejo de la Judicatura, Fiscalía y Policía Nacional quienes realizan diligencias preventivas e investigativas con la finalidad de disminuir el aumento de víctimas por este delito, que abarca una amplia gama de infracciones como el uso malicioso de datos personales, ciberbullying, suplantación de identidad, aprovechan los datos obtenidos para proceder a la extorsión en la cual solicitan una fuerte cantidad de dinero, incluso existen casos

que los adolescentes y niños son víctimas del delito del siglo XXI que es la trata de personas y todos sus fines. (Arregui & Lasso Ruiz, 2021, págs. 56-57)

Por tal circunstancia la Unidad Educativa Isaac Jesús Barrera, ubicada en la provincia de Imbabura cantón Otavalo, así como las demás instituciones educativas está propensa a enfrentar múltiples problemas de ciberseguridad, pues tenemos que dentro de la malla curricular no se cuenta con alguna materia direccionada a la capacitación y utilización de estas herramientas tecnológicas, por tal circunstancias a fin de prevenir y precautelar el interés superior de los estudiantes, se espera proponer un MOOC (Massive Open Online Course) de capacitación sobre temas de ciberseguridad para los estudiantes del décimo año de educación básica, en una primera fase. El MOOC se desarrollará con materiales educativos digitales interactivos y accesibles, que aborden temas como prevención en ser víctima de delitos cibernéticos, tipos de delitos y acciones que se debe ejecutar cuando algún estudiante sea víctima o a su vez conozca del hecho. Por lo cual en función de la definición del problema o reto se ha planteado la siguiente pregunta de investigación ¿Cómo desarrollar un MOOC de capacitación sobre temas de ciberseguridad mediante el diseño de materiales educativos digitales para ayudar a fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera?

1.2. Justificación del proyecto

1.2.1. Necesidad del proyecto

Actualmente en un mundo digitalizado que se desarrolla a pasos agigantados, se puede constatar que las personas se encuentran sumergidas en el mundo tecnológico y que su necesidad de estar conectadas a las diversas redes sociales ha crecido aceleradamente en los últimos años, en la mayoría de personas en especial los adolescentes se observa una tendencia marcada por destacar ante los demás en redes

sociales siendo usuarios de por lo menos una cuenta en alguna de estas como son Facebook, tik tok, Messenger, YouTube, Instagram, entre otras y que para su creación solicitan información personal del usuario que va desde la fecha de nacimiento hasta los datos personales que pueden ser sensibles.

Esta información es procesada y guardada en el ciberespacio y en ocasiones es vulnerable a que sea atacada por profesionales con malicia como son los hackers o piratas informáticos, quienes al obtener datos confidenciales proceden a manipular mediante engaños a los adolescentes a realizar actos ilegales o a su vez realizan extorsiones o amenazas a fin de obtener un beneficio económico o personal, vulnerando de esta manera el interés superior de los niños y adolescentes que es garantizado por el Estado.

1.2.2. Finalidad del proyecto

La ciberseguridad constituye una herramienta que protege la información sensible de las personas resguardando sus datos personales, además de brindar una serie de recomendaciones y protecciones para prevenir peligros y situaciones de vulnerabilidad. Un ciberataque puede provocar que los datos confidenciales lleguen a manos peligrosas que pueden usar esta información para extorsión y estafas causando daños significativos en las victimas que puede llegar a generar suicidios en algunos casos.

El curso estará diseñado para proporcionar una comprensión de los ataques cibernéticos y cómo protegerse contra ellos con diferentes temas los cuáles serán de gran utilidad para las personas interesadas, el curso brindará un entendimiento sólido de las amenazas cibernéticas**.**

1.2.3. ¿Qué problemática resuelve?

El tema de la ciberseguridad tiene un protagonismo importante y actual frente a las nuevas generaciones de nativos digitales que manejan con facilidad y destreza las herramientas tecnológicas, navegan en internet, realizan compras online y se conectan en línea con el mundo a través de sus redes sociales. Los estudiantes de nuestro grupo de prueba pertenecientes a la Unidad Educativa Isaac Jesús Barrera no son la excepción, están conectados con las tecnologías digitales durante todo el día y es pertinente que la institución educativa les brinde una efectiva y eficaz capacitación sobre los temas que les permiten vincularse con el mundo de la ciberseguridad para protegerlos, prevenirlos, precautelar su bienestar y que no se sientan vulnerables frente a los peligros y situaciones de riesgo a las que pueden estar expuestos.

La unidad educativa actualmente no cuenta con un programa de capacitación sobre temas de ciberseguridad y dentro de su malla curricular no existe una materia direccionada a vincular al estudiante con estos temas, por tal motivo se desarrollará un MOOC (Massive Open Online Course) de capacitación sobre temas de ciberseguridad que en primera instancia y como grupo de prueba será entregado a un grupo de estudiantes del décimo año de educación básica de esta institución.

1.2.4. Exigencias del proyecto

- **Diseño de Contenido:** se desarrollarán módulos de aprendizaje en línea, formato SCORM respetando los parámetros que este formato nos pide, los módulos abordarán conceptos clave de ciberseguridad de manera accesible y atractiva para adolescentes. El contenido incluirá animaciones, ejemplos prácticos y recursos interactivos.

- **Plataforma de Aprendizaje:** se utilizará una plataforma de aprendizaje en línea que permita a los estudiantes acceder a los módulos de aprendizaje,

realizar seguimiento de su progreso y participar en actividades interactivas.

- **Contenido Actualizado:** el contenido se mantendrá actualizado para reflejar las últimas amenazas y tendencias en ciberseguridad.

- **Interacción Instructor - Estudiante:** se fomentará la interacción entre instructor (docentes responsables de la Unidad Educativa) y estudiantes a través de foros de discusión.

- **Evaluación:** se proporcionarán cuestionarios y evaluaciones en línea para medir el conocimiento y aprendizaje de los estudiantes.

- **Accesibilidad y Privacidad:** se asegurará la accesibilidad, también se enfocará en la privacidad y seguridad de los datos del estudiante. Este proyecto MOOC abordará de manera efectiva las exigencias educativas al proporcionar una educación sólida en ciberseguridad, empoderando a los adolescentes para protegerse en línea y promoviendo una cultura de seguridad digital.

1.3. Naturaleza o tipo de proyecto

La naturaleza o tipo de proyecto, es una propuesta centrada en la problemática alrededor del tema de la ciberseguridad y los peligros que combate de la cual se encuentran siendo víctimas muchos adolescentes, pues este grupo etario desconocen los peligros a los cuales pueden estar expuestos por el abuso en la utilización del internet. Por tal circunstancia la propuesta del proyecto es el diseño y elaboración de un MOOC (Massive Open Online Course), mismo que será entregado a la Unidad Educativa Isaac Jesús Barrera. Si a futuro se precisa la investigación del impacto de esta propuesta se podría abordar la investigación con un enfoque mixto (cuantitativo / cualitativo).

Cualitativo, se podría basar en los análisis subjetivos que los estudiantes den a los contenidos que son presentado mediante las herramientas digítales, así como también la valoración crítica durante el desarrollo y culminación del curso.

Cuantitativo, en la culminación del MOOC los participantes deben aprobar una evaluación con puntuación dentro del MOOC, misma que podría servir para evaluar los conocimientos adquiridos.

1.4. Presentación de la institución

La Unidad Educativa "Isaac Jesús Barrera", comenzó con el proceso de fusión de 5 instituciones, el 13 de febrero del 2013, por el MINEDUC – Zona 1 – Distrito 10D02, precedida por la rectora Msc. Teresa Sánchez como primera autoridad, junto a su equipo trabajada apegada a la normativa legal, al cumplimiento de la identidad institucional plasmado en la visión, misión e ideario, buscando la calidad educativa gracias a los adecuados procesos de enseñanza-aprendizaje de los docentes, promoviendo un alto nivel de respeto entre autoridades, maestros, estudiantes y padres de familia.

En el 27 de abril del 2015 y bajo decreto ministerial de Resolución N° 00230, art 1 , resuelven: Autorizar la fusión de cinco Unidades Educativas para formar un solo establecimiento con el nombre de: UNIDAD EDUCATIVA ISAAC JESÚS BARRERA, perteneciente a la parroquia San Luis, cantón Otavalo, provincia de Imbabura, que oferta el servicio educativo de Educación General Básica, Bachillerato General Unificado en Ciencias y Bachillerato, con código AMIE 10h00443, régimen sierra, sostenimiento fiscal, jornada matutina, vespertina y nocturna. El número de estudiantes matriculados son 2.445, con 80 paralelos, para cubrir esta gran demanda estudiantil se cuenta con 85 docentes, 7 autoridades, 2 miembros del DECE, 1 apoyo pedagógico, 2 secretarias y 2 conserjes. Para el eficaz y eficiente trabajo de la Unidad

Educativa se ha realizado la planificación estratégica institucional con el apoyo de la comunidad educativa teniendo al día el PEI, PCI, Código de Convivencia.

El reto que tiene la Unidad Educativa además de mejorar el mantenimiento de la infraestructura es reducir la falta de información sobre la protección online en los estudiantes. Para abordar esta necesidad, se propone desarrollar un MOOC como herramienta de capacitación, incentivando la investigación y la obtención de información por parte de los estudiantes. (Tabi, 2019, págs. 12-13)

1.4.1. Misión de la institución

La Unidad Educativa Isaac Jesús Barrera es una Institución Educativa que desarrolla en los estudiantes habilidades, actitudes, aptitudes e intereses; preparándolos para construir su proyecto de vida con capacidad, creatividad, fortaleza y responsabilidad; mediante el diseño, implementación y aplicación de estrategias de aprendizaje socio- constructivista, logrando en ellos una formación integral en el ámbito académico, científico, técnico y ambiental, conscientes de su desempeño social, cultural y económico como parte activa de la sociedad. (Tabi, 2019, pág. 3)

1.4.2. Visión de la institución

Ser una comunidad educativa de excelencia en el cantón y la provincia; con un elevado nivel de aprendizajes significativos con enfoque socio- constructivista, que desarrolle habilidades, destrezas, competencias y valores, garantizando calidad educativa y aplicación del buen vivir (sumak kawsay); con docentes y padres de familia participativos en la formación de estudiantes preparados para el futuro en el campo científico y técnico en la industria de la confección, uso de las Tic´s, conciencia ambiental, espíritu ético, solidario y reflexivo, como parte de una sociedad dinámica. (Tabi, 2019, pág. 3)

1.4.3. Valores de la institución

Estos son los valores fundamentales que se promueven en la Unidad Educativa Isaac Jesús Barrera:

- **Justicia:** En la Unidad Educativa se busca la justicia al garantizar igualdad de oportunidades para todos los estudiantes, sin importar su origen socioeconómico u otras diferencias, y se resuelven los conflictos de manera justa.
- **Solidaridad:** La solidaridad es un valor importante en la Unidad Educativa, donde se fomenta el apoyo mutuo y la colaboración entre estudiantes, docentes y personal administrativo a través de actividades solidarias.
- **Responsabilidad:** Se enseña a los estudiantes la importancia de asumir responsabilidad por sus acciones y decisiones, cumpliendo con sus deberes académicos, siendo puntuales y cuidando el entorno escolar, además de participar en proyectos comunitarios.
- **Cooperativa:** Se valora la cooperación en la Unidad Educativa, promoviendo la colaboración entre estudiantes en proyectos académicos y extracurriculares para desarrollar habilidades de comunicación y resolución de problemas.
- **Tolerancia:** Se promueve la tolerancia, respetando las diferencias individuales y culturales, fomentando el diálogo abierto y el respeto hacia las opiniones y creencias de los demás para promover una convivencia pacífica.

- **Amor:** Se promueve el amor como base de las relaciones humanas en la Unidad Educativa, fomentando el afecto y el cuidado mutuo entre estudiantes y docentes para crear un ambiente acogedor y seguro.

- **Respeto:** El respeto es fundamental en la Unidad Educativa, enseñando a los estudiantes a respetar a sus compañeros, docentes, personal administrativo y al entorno escolar, así como valorar la diversidad de ideas y opiniones.

- **Honestidad:** La honestidad es un valor primordial en la Unidad Educativa. Se promueve la integridad académica, animando a los estudiantes a realizar su trabajo de manera honesta y a reconocer sus errores.

Estos valores se inculcan para fomentar un ambiente de convivencia armoniosa y formar a los estudiantes como ciudadanos íntegros y comprometidos con la sociedad.

1.5. Objetivos

1.5.1. Objetivo general

Desarrollar un MOOC de capacitación sobre temas de ciberseguridad mediante el diseño de materiales educativos digitales para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera.

1.5.2. Objetivos específicos

- Analizar diversos conceptos acerca de la ciberseguridad mediante la recopilación bibliográfica de información en repositorios académicos y fuentes confiables para establecer medidas de protección enfocadas a capacitar y concientizar a los estudiantes de la Unidad Educativa Isaac Jesús Barrera.

- Establecer los requerimientos del curso definiendo los parámetros y unidades de aprendizaje para satisfacer las necesidades de capacitación en temas de ciberseguridad de los estudiantes de la Unidad Educativa Isaac Jesús Barrera.
- Diseñar la estructura y seleccionar el contenido del MOOC de capacitación mediante la elaboración de material multimedia y la utilización de softwares de desarrollo de cursos virtuales para satisfacer los requerimientos establecidos.

CAPÍTULO II

2. DISEÑO DE MATERIALES EDUCATIVOS DIGITALES

1.1. Propuesta del proyecto

2.1.1. Contextualización

El grupo de prueba que se tomó en cuenta en el presente proyecto son adolescentes de 15 a 16 años, de ambos sexos, pertenecientes a décimo año de educación básica de la Unidad Educativa Isaac Jesús Barrera, del cantón Otavalo, en la cual trabajaremos con dicho segmento que no cuenta con acceso a dispositivos tecnológicos por motivo al reglamento interno de la institución por lo cual se utilizará las salas de computación que posee la institución educativa.

Esta investigación aporta conocimientos extracurriculares para el alumnado garantizando la prevención de amenazas cibernéticas, mediante la creación de MOOC (Massive Open Online Course), con temas relevantes a la ciberseguridad para fortalecer la protección y conciencia online. Dentro del proyecto se van a desarrollar los siguientes temas como base para elaborar el contenido del MOOC:

- "Conceptos fundamentales de la ciberseguridad".
- "Peligros y situaciones de vulnerabilidad".
- "Medidas y recomendaciones de protección".

2.1.2. Justificación curricular

Una estructura inicial como punto de partida para estructurar el MOOC consiste en desarrollar el tema principal a través de tres unidades distribuidas como sesiones, las cuales se detallan a continuación:

Unidad 1 (Sesión 1): "Conceptos fundamentales de la ciberseguridad"

Objetivos

Comprender los conceptos fundamentales de la ciberseguridad para fortalecer la capacidad de protección y tomar decisiones seguras en el entorno digital.

Contenidos

- Definición de ciberseguridad ***(Conceptual)***.
- Conceptos básicos como confidencialidad, integridad y disponibilidad de la información ***(Conceptual)***.
- Tipos de amenazas y ataques cibernéticos ***(Conceptual)***.
- Importancia de las contraseñas seguras ***(Actitudinal)***.

Criterios de evaluación

- Comprender los conceptos clave de la ciberseguridad.
- Comprender y explicar correctamente los conceptos de confidencialidad, integridad y disponibilidad de la información.
- Identificar correctamente los diferentes tipos de amenazas y ataques cibernéticos.
- Aplicación de medidas de seguridad básicas, como el uso de contraseñas seguras.

Unidad 2 (Sesión 2): "Peligros y situaciones de vulnerabilidad"

Objetivos

Identificar los peligros y situaciones de vulnerabilidad en el entorno digital, para tomar medidas de precaución y adoptar comportamientos seguros que minimicen los riesgos en línea.

Contenidos

- Riesgos de compartir información personal en línea ***(Conceptual)***.

- Riesgos y situaciones de vulnerabilidad ***(Conceptual)***.
- El ciberacoso, grooming, sextorsión, entre otros ***(Conceptual)***.

Criterios evaluación

- Identificar y explicar correctamente los diferentes peligros y riesgos en línea.
- Demostrar comprensión sobre detección de situaciones de vulnerabilidad en el entorno digital.
- Demostrar habilidades para buscar ayuda y actuar de manera adecuada en caso de ser víctima de una situación de vulnerabilidad en línea.

Unidad 3 (Sesión 3): "Medidas y recomendaciones de protección"

Objetivos

Adquirir conocimientos sobre las medidas y recomendaciones de protección en el entorno digital, para poder aplicar de manera efectiva tomar decisiones seguras en línea.

Contenidos

- Protección a los datos personales en línea, como el uso de contraseñas seguras y la autenticación de dos factores ***(Procedimental)***.
- Cómo prevenir el phishing y los engaños ***(Procedimental)***.
- Cómo evitar la descarga de software malicioso ***(Procedimental)***.
- Estrategias para protegerse del ciberacoso, el grooming y otros riesgos en línea ***(Procedimental)***.
- La importancia de la educación sobre ciberseguridad en la prevención de amenazas cibernéticas ***(Actitudinal)***.

Criterios evaluación

- Identificar y aplicar correctamente las medidas de protección para la privacidad y los datos personales en línea.

- Reconocer y evitar los engaños y amenazas en línea, como el phishing y el software malicioso.
- Demostrar habilidades para prevenir situaciones de riesgo en línea, como el ciberacoso o el grooming.
- Reflexionar sobre la importancia de la educación en ciberseguridad y su impacto en la prevención de amenazas cibernéticas.

2.1.3. Recursos digitales educativos

A continuación, se lista un serie de recursos digitales educativos que pueden ser tomados como punto de partida para la creación del MOOC de capacitación estudiantil sobre seguridad y prevención, utilizando Storyline 360 como plataforma de desarrollo y Photoshop para generar recursos multimedia:

- **Videos explicativos:** Los vídeos pueden mostrar situaciones reales y escenarios de seguridad, proporcionando ejemplos visuales de medidas preventivas. Seleccionamos esta opción porque el formato de video es altamente efectivo para la comprensión visual y la retención de información.

- **Infografías interactivas:** Las infografías pueden destacar datos clave, estadísticas y consejos importantes de manera visualmente atractiva. Al ser interactivas, los estudiantes pueden explorar contenido específico de acuerdo con sus necesidades, lo que favorece la adaptación individual.

- **Simulaciones interactivas:** Mediante Storyline 360, puedes crear simulaciones que permitan a los estudiantes tomar decisiones en escenarios de seguridad. Esto promueve la toma de decisiones informadas y la comprensión de las consecuencias de sus elecciones.

- **Cuestionarios y pruebas:** Incorporar cuestionarios después de cada sección o módulo ayuda a evaluar la comprensión y retención del material. Esto fomenta la participación activa y brinda retroalimentación inmediata.

- **Recursos descargables:** Ofrecer material descargable, como folletos informativos o listas de verificación de seguridad, permite a los estudiantes acceder al contenido fuera de la plataforma y aplicarlo en situaciones cotidianas.

- **Historias de casos:** Presentar estudios de casos reales sobre incidentes de seguridad y su resolución ayuda a contextualizar la información y a mostrar cómo se aplican las medidas preventivas en la vida real.

- **GIFs explicativos:** Los GIFs pueden ilustrar procesos, procedimientos o acciones de manera breve y animada. Son útiles para demostrar acciones específicas de seguridad y prevención de manera concisa.

Se considera que estos recursos son idóneos para un enfoque educativo, ya que fomentan la comprensión profunda, la aplicación práctica y la participación activa de los estudiantes en la temática de seguridad y prevención.

2.1.4. Preguntas de reflexión

Es de interés plantear interrogantes que nos permitan reflexionar sobre varios ejes antes, durante y después de la ejecución del proyecto, para realizar una evaluación y retroalimentación que permita mejorar, actualizar, adaptar o ajustar el proyecto con base a los objetivos planteados, con esta finalidad y buscando cumplir los principios básicos y finalidades de los recursos educativos digitales de este proyecto se han planteado las siguientes preguntas de reflexión en base a dos ejes fundamentales:

a) Contenido y relevancia del tema

¿El proyecto está enfocado a resolver o mejorar alguna problemática social de interés para la comunidad educativa?

En esta interrogante es importante que nos preguntemos si:

- El proyecto responde a dejar algún mensaje de concientización.
- El tema planteado es de relevancia actual para la educación.
- El proyecto brinda alguna oportunidad para mejorar algún problema social en el alumnado.

¿El contenido educativo seleccionado se adapta a los principios básicos para lograr un aprendizaje en el alumnado?

En esta pregunta es interesante reflexionar si el contenido seleccionado:

- Cumple con los objetivos de aprendizaje planteados.
- Permite realizar una evaluación del aprendizaje.
- Fomenta la motivación del alumnado.
- Brinda posibilidades de retroalimentación de los temas.

¿El contenido presentado es entretenido e informativo para captar la atención del alumnado?

Aquí es importante pensar si el contenido:

- Presenta temas de relevancia e interesantes para el alumnado.
- Fue seleccionado y adaptado para las edades del alumnado.
- Proviene de fuentes confiables y brinda un aprendizaje significativo.

b) Criterios para el diseño

¿El diseño es interactivo despertando interés y motivando la participación del alumnado?

Para esta pregunta es importante cuestionarnos si en el diseño:

- El contenido permite despertar curiosidad por investigar más en el tema.
- El contenido fomenta una reflexión del alumnado sobre el tema.
- Los elementos de aprendizaje presentan un reto interesante que motive al alumnado.

¿El diseño está pensado para adaptarse a las necesidades de interacción del alumnado y es accesible para todos los usuarios?

En esta cuestión es importante que analicemos si en el diseño:

- Los títulos y textos son adaptables en tamaño.
- Existen elementos o herramientas que permitan ajustar la interfaz haciéndola dinámica y adaptable a tamaños y orientaciones.
- El diseño presenta recursos de audio y video ajustables a las necesidades de los usuarios.

¿Existe un equilibrio en el diseño dotándolo de sencillez y simplicidad para su uso?

Para esta pregunta es importante que reflexionemos si el diseño:

- Mantiene un equilibrio en el uso del color.
- Existe un uso adecuado de tipografías o fuentes.
- El contenido está estructurado de forma ordenada siguiendo una jerarquía en los elementos de texto para una mejor comprensión.
- El tamaño de los elementos gráficos y multimedia es proporcional para una correcta visión del contenido.
- La navegación por el contenido es simple para no confundir a los usuarios.

¿El diseño me permite brindar una retroalimentación para reforzar el aprendizaje del alumnado?

Para responder esta interrogante es importante reflexionar si en el diseño:

- Existen elementos que posibiliten la autoevaluación del alumnado.
- Existen elementos para reforzar el aprendizaje de los contenidos.
- Existe diversidad en los mecanismos de “evaluación” para consolidar el aprendizaje y estos cuentan con elementos para brindar una retroalimentación.

2.2. Diseño del material educativo audiovisual

2.2.1. Contextualización

El grupo de prueba que se tomó en cuenta como base para este proyecto se identifica como multiétnica entre mestizos e indígena dado principalmente su ubicación geo-étnica los mismos que en su gran mayoría cuentan con acceso a la tecnología desde temprana edad que les permite el acceso a redes sociales principalmente Tik-Tok, YouTube, Facebook, así mismo es utilizan juegos en línea como: call of duty, free fire, zooba y minecraft. Sin dejar de lado el tema educativo ya que estos tienen un gran acceso a plataformas que les aportan a sus conocimientos educativos es por eso que se desarrollará el MOOC para aprovechar el tiempo de uso tecnológico que dan los estudiantes diariamente.

2.2.2. Preguntas de reflexión

¿Qué?

Un contenido que busca educar a los adolescentes sobre la ciberseguridad y la importancia de su uso responsable, utilizando diferentes herramientas tecnológicas, tales como Audacity, TTSMAKER, Pixabay, Photoshop, Qrita, Pinterest y Adobe Express. El proyecto incluirá la creación de un guión multimedia que abordará esta temática.

¿Para quién?

Este contenido va dirigido a un grupo de estudiantes adolescentes de 15 a 16 años, del paralelo “A” conformado de: 15 hombres y 24 mujeres, dando un total de 39

participantes pertenecientes al décimo año de educación básica, de la Unidad Educativa Isaac Jesús Barrera. Está dirigido a adolescentes, ya que es una edad en la que prefieren los encuentros digitales y están mucho más familiarizados con la tecnología. Por esta razón, es importante educarlos sobre la importancia de la ciberseguridad y proporcionarles información básica para que puedan navegar de manera segura en línea.

¿Para qué?

Este contenido se realiza con el objetivo de concienciar y educar a los adolescentes sobre la importancia de la ciberseguridad, así como brindarles conocimientos y recursos prácticos de mucho interés para el estudiante para protegerse de amenazas en línea y promover un uso responsable de las redes sociales y plataformas virtuales con herramientas atractivas para el usuario.

¿Cómo?

Se proyecta el uso de herramientas tecnológicas como Audacity, TTSMAKER, Pixabay, Photoshop, Qrita, Pinterest y Adobe Express. Se creará un guión multimedia que incluirá elementos visuales, de audio y texto para transmitir información sobre ciberseguridad de manera clara y atractiva. También se fomenta la participación activa de los estudiantes en este curso para fortalecer su comprensión y aplicación práctica de la temática.

2.2.3. Manifiesto y herramientas

En los últimos años la sociedad ha sido testigo de las evoluciones tecnológicas, por lo cual también aparecieron nuevas amenazas cibernéticas, los adolescentes participantes al ser nativos digitales usan mucho la tecnología pero al mismo tiempo se convierten en personas vulnerables a ser posibles víctimas de delitos cibernéticos, por lo cual dentro de este acápite hemos seleccionado un tema extracurricular pero de vital

importancia para que los adolescentes estén en la capacidad de manejar correctamente sus redes sociales y demás espacios virtuales.

Los recursos a ser utilizados son de diversos formatos tales como textos, videos, imágenes, audios, que son idóneos para un enfoque educativo y ayudarán a que exista una conexión de los estudiantes con la realidad de la utilización de las redes sociales y la ciberseguridad, a su vez motiva a que los adolescentes sean más participativos durante el desarrollo del curso online en el cual se fomentará la comprensión profunda, la aplicación práctica y activa de los estudiantes en la temática de ciberseguridad.

Para la elaboración del MOOC se utilizarán diferentes herramientas digitales las cuales ayudarán a que el presente curso sea más sencillo y de fácil comprensión para los estudiantes inmersos, pues a base de diferentes actividades creativas y lúdicas se explicará los temas de la ciberseguridad.

- **AUDACITY:** Este es un potente editor y grabador multipista de audio que nos permite, entre otras funciones realizar grabaciones desde diferentes fuentes sonoras: micrófono, entrada de línea de la PC, placas de audio externas por USB. Es un software gratuito que se utiliza para realizar las grabaciones y edición de audio con los temas relacionados a la ciberseguridad.
- **PIXABAY:** Este es un sitio web internacional para el intercambio de fotos de alta calidad esta herramienta sirve para el intercambio de fotos y audios de auditoría propio, este facilita la combinación de estos elementos para producir fotografías de muy buena calidad.
- **PHOTOSHOP:** Es una herramienta utilizada para la edición de fotografías, es decir retoques a las imágenes ya se en color, tamaño entre otras.

- **KRITA:** Es un programa profesional de pintura digital, gratuito y hecho con código libre, ha sido creado por artistas estas nos servirá para la creación del robot el cual será el protagonista dentro del MOOC.
- **PINTEREST:** Esta herramienta permite descubrimiento visual de distintas temáticas es así como dentro del MOOC se va a utilizar para las gráficas que hay dentro de este.
- **ADOBE EXPRESS:** Es una aplicación de diseño online y para dispositivos móviles, con esta aplicación se podrás crear fácilmente impresionantes imágenes.
- **ARTICULATE:** encuentre bibliotecas para crear elementos interactivos, evaluaciones didácticas y una interfaz para diseñar y crear su curso lo que nos permitió realizar el diseño de nuestro personaje principal denominado ByteBot quien nos ayudará a aplicar el contenido del curso virtual a los estudiantes.

2.2.4. Guion multimedia de los principales recursos audiovisuales

a) Material educativo Audiovisual 1

Título: Creación de personaje.

Descriptivo: generación de un personaje para el MOOC.

Base didáctica: contenido visual, de carácter interactivo que busca mejorar la recepción de información en el usuario además de volverlas más digerible y amigable para el mismo, lo cual ayuda a mejorar la percepción del tema.

Tipo de recurso o actividad: ilustración digital y articulación de personaje para animación.

Parametrización:

Nombre: ByteBot.

Descripción: ByteBot es un robot creado para ayudar a los estudiantes a comprender los conceptos de ciberseguridad de manera única y memorable. Toma forma humanoide para presentarse familiar con el usuario, ByteBot se manifiesta como una entidad digital con una personalidad divertida y amigable.

Apariencia:

- ByteBot está ilustrado en estilo cartoon, utilizando patrones de colores 8 bits que evocan un aspecto tecnológico y clásico.
- Su "rostro" está compuesto por una estructura humanoide de colores que pueden cambiar para expresar diferentes emociones, como ojos felices, cejas levantadas o una boca sonriente. Para mejorar la Ux de los usuarios y crear empatía con el personaje.

Características distintivas:

- Tiene una voz amigable y animada que utiliza para guiar a los estudiantes a través del MOOC.
- Su estructura corporal es simple, lo cual lo vuelve fácil de recordar.

Rol en el MOOC:

- ByteBot es el mentor digital que presenta los conceptos de ciberseguridad a los estudiantes de manera entretenida.
- Guía a los estudiantes a través de ejercicios prácticos y simulaciones virtuales.

Objetivo del personaje:

- ByteBot busca hacer que los conceptos de ciberseguridad sean accesibles y atractivos para los estudiantes adolescentes.
- A través de su estilo lúdico y su enfoque interactivo, ByteBot pretende promover una mayor conciencia sobre la importancia de la ciberseguridad y empoderar a los estudiantes para proteger sus identidades digitales.

Este personaje no humano, ByteBot, está diseñado para captar la atención y el interés de los estudiantes adolescentes al abordar la ciberseguridad de manera innovadora y visualmente atractiva.

Archivador:

- adobe express.
- adobe after effects.

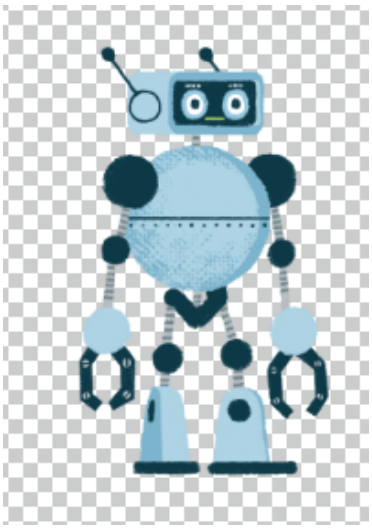

Figura 1: Creación del personaje MOOC.

b) Material educativo Audiovisual 2

Título: Generación de background.

Descriptivo: crear el fondo de la escena que acompañará a nuestro personaje ByteBot, creado anteriormente.

Base didáctica: contenido visual, de carácter interactivo que busca mejorar la recepción de información en el usuario además de volverlas más digerible y amigable para el mismo, lo cual ayuda a mejorar la percepción del tema.

Tipo de recurso o actividad: ilustración digital.

Parametrización: ilustración digital de 1920x1080 que funcione de background para el personaje de tal manera que sus estilos gráficos se adapten y brinden una experiencia satisfactoria al usuario.

Archivador:

- adobe express
- qrita

Figura 2: Background 1 del MOOC.

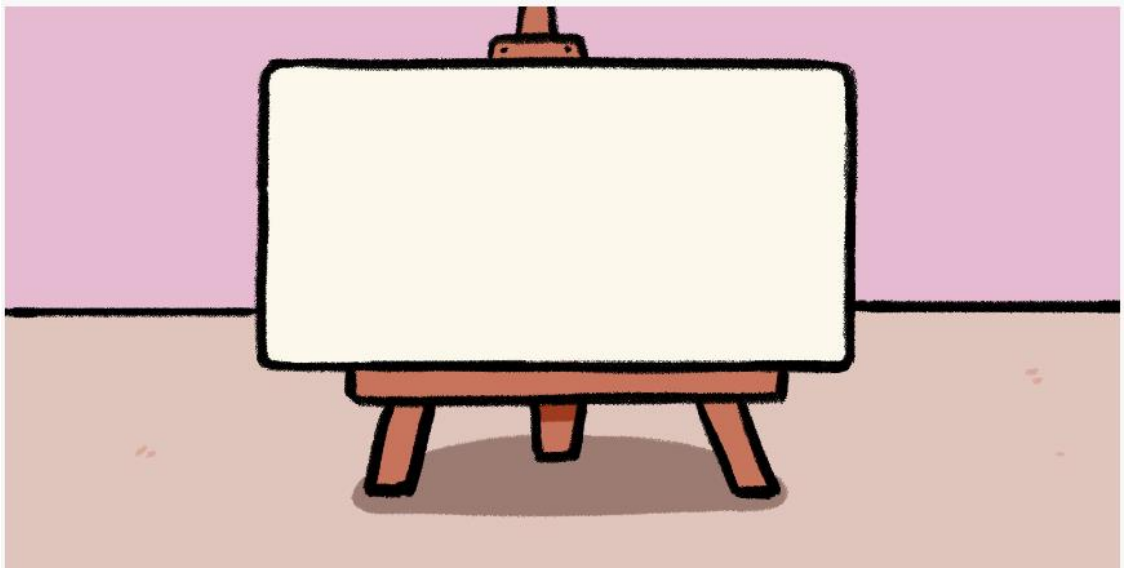

Figura 3: Background 2 del MOOC.

c) Material educativo Audiovisual 3

Título: Bienvenida y conceptos fundamentales de la ciberseguridad.

Descriptivo: en este recurso se abordan dos aspectos del curso general, el primero da la bienvenida a los estudiantes donde se menciona el nombre, los principales contenidos y aspectos introductorios del curso. El segundo aspecto está enfocado a responder las preguntas ¿Qué es ciberseguridad? - ¿Por qué es importante?, el recurso será de carácter narrativo por medio de una animación donde se conjugará el recurso 1 con el 2, generando un nuevo recurso multimedia para abordar estos aspectos.

Base didáctica: contenido conceptual de carácter narrativo que brinda una introducción al curso y pretende brindar al estudiante información acerca del concepto de ciberseguridad y su importancia, bajo el objetivo de que el estudiante pueda comprender los conceptos fundamentales de la ciberseguridad para fortalecer la capacidad de protección y tomar decisiones seguras en el entorno digital.

Tipo de recurso: animación digital 2d.

Parametrización: el recurso audiovisual se compone de 3 subrecursos, en el primero se presenta la bienvenida a los estudiantes, el segundo responde a la pregunta ¿Qué es ciberseguridad? el mismo que se piensa desplegar a través de un botón, finalmente en el tercero se aborda la pregunta ¿Por qué es importante? de igual manera se accede a través de un botón solo habiendo finalizado el recurso 2, la herramienta seleccionada para elaborar el recurso será Adobe Express, ayudado de Audacity con TTSMAKER y "Pixabay" para complementar la experiencia auditiva. Adicional se adjunta el texto empleado en la elaboración del audio narrativo, el mismo que fue adaptado a nuestro target en función del perfil de personaje expuesto anteriormente.

Archivador:

- Texto – Bienvenida

¡Hola y bienvenidos al curso online "Escudo Digital" Soy ByteBot, su guía y compañero en este emocionante viaje hacia el mundo de la ciberseguridad. Estoy aquí para asegurarme de que estén preparados para navegar por el ciberespacio de manera segura y protegida.

Fuente: Autoría propia grupal.

- Texto – Narración ¿Qué es ciberseguridad?

La ciberseguridad o seguridad informática es la suma de procesos y herramientas que se emplean para proteger anticipadamente o defender de ciberataques a dispositivos, sistemas electrónicos, servidores de redes y programas, de posibles ataques digitales (UNIR - Universidad Internacional de La Rioja, 2021, pág. 1).

BYTEBOT: “¡Hola nuevamente, exploradores digitales! ? ¿Qué es la ciberseguridad? Imaginen que la ciberseguridad es como el escudo que protege sus mundos digitales, sus datos personales y sus dispositivos. ¿Recuerdan cómo cerramos las puertas y ventanas de nuestras casas para mantener a salvo nuestras pertenencias? Bueno, la ciberseguridad hace algo similar en el mundo virtual. Desde contraseñas hasta transacciones, todo está en línea. Y mantenerlo seguro es clave.”

- Texto – Narración ¿Por qué es importante?

Con la educación en ciberseguridad, podemos aprender a reconocer y evitar amenazas, proteger nuestros datos personales y financieros, conocer las mejores prácticas de ciberseguridad para la navegación en internet, aumentar la protección y privacidad online (Impulso 06, 2020, pág. 1).

BYTEBOT: “Ahora bien, ¿por qué es tan importante? Bueno, nuestras vidas están cada vez más conectadas a la tecnología. Desde nuestras redes sociales hasta nuestras transacciones bancarias, gran parte de nuestra información y actividades se realizan en línea. Eso significa que debemos asegurarnos de que nuestras acciones digitales estén protegidas.”

2.3. Desarrollo del MOOC y digitalización del contenido (SCORM 1.2)

2.3.1. Objetivo del material didáctico generado

Desarrollar un material didáctico interactivo y atractivo que proporcione a los estudiantes de la Unidad Educativa Isaac Jesús Barrera conocimientos sólidos prácticos sobre ciberseguridad, promoviendo la conciencia de los riesgos en línea y brindando estrategias efectivas para proteger su privacidad, datos personales y mantener una conducta responsable en el entorno digital.

2.3.2. Estructura del MOOC y distribución de los contenidos

El contenido del curso se organizará a través de pantallas dentro del MOOC las mismas que respetan una línea gráfica que mantiene un equilibrio del uso de colores y fuentes, abordan tópicos de relevancia y de fácil comprensión para los estudiantes respecto a ciberseguridad y ofrecen un entorno dinámico, intuitivo e interactivo captando la atención y motivando al estudiante a seguir avanzando en el contenido.

El MOOC introduce un personaje animado de nombre “Bytebot” creado por los autores del proyecto, que es una ilustración de un robot diseñada con la finalidad de captar la atención de los estudiantes y motivar su interés por continuar avanzando en los contenidos, Bytebot es el encargado de guiar a los estudiantes a través del MOOC y presentarles cada uno de los temas contemplados en el curso ofreciéndoles una mejor experiencia.

A continuación, se presentan los tópicos y actividades que conforman el contenido a tratar en cada una de las pantallas del MOOC:

Título: "Escudo Digital: Un MOOC sobre Ciberseguridad para Adolescentes"

PANTALLA 1: Introducción

¡Hola y bienvenidos al curso online "Escudo Digital"! Soy ByteBot, su guía y compañero en este emocionante viaje hacia el mundo de la ciberseguridad. Estoy aquí para asegurarme de que estén preparados para navegar por el ciberespacio de manera segura y protegida.

PANTALLA 2: ¿Qué es la Ciberseguridad?

¡Hola nuevamente, exploradores digitales! qué es la ciberseguridad Imaginen que la ciberseguridad es como el escudo que protege sus mundos digitales, sus datos personales y sus dispositivos. ¿Recuerdan cómo cerramos las puertas y ventanas de nuestras casas para mantener a salvo nuestras pertenencias? Bueno, la ciberseguridad

hace algo similar en el mundo virtual. Desde contraseñas hasta transacciones, todo está en línea. Y Mantenerlo seguro es clave.

PANTALLA 3: ¿Por qué es Importante la Ciberseguridad?

Ahora bien, ¿por qué es tan importante? Bueno, nuestras vidas están cada vez más conectadas a la tecnología. Desde nuestras redes sociales hasta nuestras transacciones bancarias, gran parte de nuestra información y actividades se realizan en línea. Eso significa que debemos asegurarnos de que nuestras acciones digitales estén protegidas.

PANTALLA 4: Navegación Segura en Línea

Diálogo sobre Navegación Segura en Línea - Pantalla 4:

ByteBot (en pantalla): ¡Hola de nuevo, hoy vamos a adentrarnos en el emocionante mundo de la navegación segura en línea. Aquí aprenderemos dos cosas cruciales: cómo identificar sitios web seguros y cómo reconocer posibles amenazas en línea.

Diapositiva 1: Cómo Identificar Sitios Web Seguros.

ByteBot (en pantalla): Primero, hablemos de cómo saber si un sitio web es seguro. Un sitio seguro es como una puerta con cerradura en el mundo digital, y aquí hay algunas señales que debes buscar:

Imágenes de candados o "https://" en la barra de direcciones. Cuando veas un candado junto a la URL o "https://" en lugar de "http://", es una buena señal de que la conexión es segura.

Comprobar el certificado del sitio. Puedes hacer clic en el candado o en el icono de seguridad en la barra de direcciones para ver el certificado del sitio. Asegúrate de que el nombre del sitio coincida con lo que esperabas.

Diapositiva 2: Cómo Reconocer Posibles Amenazas en Línea.

ByteBot (en pantalla): Ahora, hablemos de cómo reconocer posibles amenazas en línea. Desafortunadamente, el mundo digital está lleno de peligros, pero puedes protegerte. Aquí tienes algunos consejos:

Ten cuidado con los correos electrónicos sospechosos. No hagas clic en enlaces ni descargues archivos adjuntos en correos electrónicos de remitentes desconocidos.

No compartas información personal. Nunca compartas contraseñas, números de tarjeta de crédito ni información sensible en línea.

Vigila las estafas en línea. Sé escéptico ante ofertas que parecen demasiado buenas para ser verdad y no compartas información personal con sitios sospechosos.

Diapositiva 3: Práctica y Seguridad.

ByteBot (en pantalla): La práctica hace al maestro, y la seguridad en línea no es la excepción. Ahora te animo a que practiques lo que has aprendido. Navega por la web, verifica la seguridad de los sitios y mantente alerta ante posibles amenazas.

ByteBot hace un gesto de ánimo.

ByteBot (en pantalla): En la siguiente lección, profundizaremos aún más en cómo proteger tus dispositivos y datos en línea. Recuerda, la ciberseguridad es como un escudo que tú mismo construyes. ¡Hasta la próxima lección!

La pantalla se desvanece, dejando a los estudiantes con conocimientos sobre cómo navegar de manera segura en línea y cómo identificar amenazas potenciales.

PANTALLA 5: Cómo Crear Contraseñas Fuertes

- Consejos para crear contraseñas seguras.
- Ejemplos de contraseñas débiles y fuertes.

Diálogo sobre Cómo Crear Contraseñas Fuertes - Pantalla 5:

ByteBot (en pantalla): ¡Continuamos en nuestro emocionante viaje de ciberseguridad! Ahora nos adentraremos en el fascinante mundo de las contraseñas seguras. Aprenderemos cómo crear contraseñas fuertes y veremos ejemplos de contraseñas débiles y fuertes. ¡Vamos a ello!

Diapositiva 1: Consejos para Crear Contraseñas Seguras.

ByteBot (en pantalla): Una contraseña segura es como un fuerte muro de protección para tu información en línea. Aquí tienes algunos consejos clave para crear contraseñas seguras:

Longitud: Cuanto más larga, mejor. Apunta a al menos 12 caracteres.

Combinación de letras, números y símbolos: Mezcla mayúsculas y minúsculas, números y símbolos para aumentar la complejidad.

Evita información personal: No uses datos personales como nombres o fechas de nacimiento.

No utilices palabras del diccionario: Las contraseñas de una sola palabra son fáciles de adivinar. En cambio, crea frases o combinaciones de palabras.

Cambia tus contraseñas regularmente: Renueva tus contraseñas periódicamente.

Diapositiva 2: Ejemplos de Contraseñas Débiles y Fuertes.

ByteBot (en pantalla): Ahora, vamos a ver ejemplos de contraseñas débiles y fuertes. Esto te dará una idea de lo que debes evitar y lo que debes buscar en una contraseña segura.

Ejemplo de Contraseña Débil: "password" (muy común y fácil de adivinar).

Ejemplo de Contraseña Fuerte: "Tr@bajo_En_Linea_2023" (larga, con combinación de caracteres).

Diapositiva 3: Práctica y Seguridad.

ByteBot (en pantalla): práctica y aplica lo aprendido, creando contraseñas seguras y fuertes para tus cuentas en línea. ¡Es un paso esencial para proteger tu información!

ByteBot hace un gesto de ánimo.

ByteBot (en pantalla): En la próxima lección, continuaremos nuestra exploración de la ciberseguridad y aprenderemos sobre la navegación segura en línea. ¡Recuerda, tu seguridad en línea está en tus manos! ¡Hasta la próxima lección!

La pantalla se desvanece, dejando a los estudiantes con conocimientos sobre cómo crear contraseñas seguras y la importancia de mantener sus cuentas seguras en línea.

PANTALLA 6: Protegiendo tus Dispositivos

- Medidas para proteger teléfonos, computadoras y otros dispositivos.
- Importancia de las actualizaciones de seguridad.

PANTALLA 7: Cuidado con el Phishing y el Correo Electrónico No Deseado

- Qué es el phishing y cómo detectarlo.
- Cómo manejar correos electrónicos sospechosos.

PANTALLA 8: Redes Sociales Responsables

- Consejos para usar redes sociales de manera segura.
- Compartir información personal de manera responsable.

PANTALLA 9: Conclusiones y Próximos Pasos

- Resumen de los conceptos clave de ciberseguridad.
- Invitación a continuar con el MOOC y explorar más temas.

PANTALLA 10: Evaluación

- Espacio para preguntas a los estudiantes.
- Desarrollo de cuestionario interactivo.

PANTALLA 11: Despedida

- Agradecimiento a los estudiantes por su participación.
- Recordatorio de la importancia de la ciberseguridad.

Figura 4: Pantalla contraseñas fuertes del MOOC.

Figura 5: Pantalla navegación segura del MOOC.

CAPÍTULO III

3. PLATAFORMAS DE GESTIÓN EN ENTORNOS VIRTUALES

3.1. Aspectos previos

3.1.1. Componentes del proceso educativo

- **¿Quiénes serán los estudiantes o asistentes a esta formación?**

Teniendo en cuenta que el MOOC es un curso a distancia, accesible para cualquier persona sin límite de participantes. Se creó un MOOC sobre ciberseguridad el cual es accesible para las personas interesadas en el tema, sin embargo, se escogió un grupo de prueba lo cual sirve como apoyo para la prueba del funcionamiento y acogida del proyecto. Se tomará en cuenta 39 alumnos que conforman el décimo año de educación básica paralelo "A" pertenecientes a la Unidad Educativa Isaac Jesús Barrera.

La elección de este grupo específico se debe a que la adolescencia es una etapa en la que los jóvenes tienen un mayor interés y familiaridad con el entorno digital y la tecnología.

- **¿Quiénes serán los docentes?**

Los diseñadores de este MOOC son estudiantes de la maestría en Educación con mención gestión del aprendizaje mediado por TIC, de la Universidad Internacional de Ecuador (UIDE), en convenio con EIG, Escuela Internacional de Gerencia, los mismos que se encargarán de diseñar y entregar la herramienta tecnológica a la institución para su uso y ellos a su vez darán a conocer su aplicación a los estudiantes de una manera responsable.

- **¿Dónde se producirá la acción educativa?**

La acción educativa se llevará a cabo en las salas de computación que posee la Unidad “Educativa Isaac Jesús Barrera” con los estudiantes que se tomó la muestra de prueba.

El presente curso se ejecutará online, en donde se creará un MOOC de capacitación estudiantil sobre ciberseguridad, utilizando Storyline 360 como plataforma de desarrollo y Photoshop para generar recursos multimedia, teniendo una comunicación más interactiva y entretenida con los estudiantes. Para la fase de prueba el recurso MOOC podrá ser visualizado y ejecutado en primera instancia a través SCORM Cloud una plataforma online que permite subir, visualizar y probar el MOOC.

3.1.2. Cuestiones pedagógicas

Las cuestiones académicas para considerar son: la identificación de los objetivos de aprendizaje específicos como la adquisición de conocimientos básicos de la ciberseguridad para fortalecer la capacidad de protección y tomar decisiones seguras , identificar los peligros y situaciones de vulnerabilidad en el entorno digital, tomar medidas de precaución y adoptar comportamientos seguros que minimicen los riesgos en línea, el desarrollo de habilidades fomentando actitudes y valores en los estudiantes.

En el curso se tratarán conceptos fundamentales de la ciberseguridad como: ¿Qué es la ciberseguridad?, ¿Por qué es importante la ciberseguridad?, Navegación Segura en Línea, Cómo Crear Contraseñas Fuertes, además identificaremos los peligros, vulnerabilidades, medidas y recomendaciones de protección a base de temas como: Protegiendo tus dispositivos, cuidado con el phishing y el correo electrónico no deseado, redes sociales responsables.

Así mismo en cuestiones pedagógicas se plantea dentro del curso el estudio de casos prácticos relacionados a la ciberseguridad, realización de debates,

retroalimentación, e inclusión de actividades evaluativas formativas para monitorear el progreso de los estudiantes que se lo realizará a base de cuestionarios con preguntas relacionadas a los contenidos aprendidos, con su respectiva revisión y retroalimentación que permitan afianzar el conocimiento de los participantes.

3.1.3. Uso del entorno

Las actividades o acciones que se llevaran a cabo para la utilización del entorno de aprendizaje se fundamentan en cuatro pilares básicos y describen a continuación:

- **Información**

Para este pilar se plantea realizar en la plataforma una guía para explicar a los estudiantes la organización del curso donde se mostrarán los contenidos como: conceptos fundamentales de la ciberseguridad como: ¿Qué es la ciberseguridad?, ¿Por qué es importante la ciberseguridad?, Navegación Segura en Línea, Cómo Crear Contraseñas Fuertes, además identificaremos los peligros, vulnerabilidades, medidas y recomendaciones de protección a base de temas como: Protegiendo tus dispositivos, cuidado con el phishing y el correo electrónico no deseado, redes sociales responsables, así mismo actividades a realizar tales como cuestionarios interactivos en cada sesión, también evaluaciones en las dos sesiones que al culminarlas poder evaluar el conocimiento del estudiante.

- **Comunicación**

Dentro del espacio MOOC el curso está pensado para utilizar una comunicación en una sola vía en primera instancia, la misma que será evaluada en función de los resultados de la evaluación obtenidos por los estudiantes al finalizar el MOOC validando de esta manera la efectividad de la comunicación al impartir el curso. Sin embargo, también se tendrá un espacio para una comunicación bidireccional a través de

la plataforma LMS donde el recurso MOOC sea cargado a través de foros de debates donde todos los participantes de la acción educativa puedan participar.

- **Cooperación**

En primera instancia el espacio MOOC del curso será tomado de manera individual, sin embargo, el aspecto de cooperación se aborda al compartir los resultados obtenidos por cada estudiante en clase con el resto de sus compañeros existiendo un intercambio de experiencias y conocimiento entre todos los participantes, así como también a través de los foros abiertos de opinión donde los participantes complementan y construyen su conocimiento.

- **Administración**

El aspecto de administración del curso se ve limitada a los criterios de los diseñadores y se centra en aspectos de organización de los contenidos tomando en cuenta la jerarquización, establecer un entorno intuitivo y de fácil comprensión, finalmente el criterio estético de las imágenes, colores y fuentes a utilizar.

3.1.4. Recursos de apoyo

Teniendo en cuenta que los recursos pedagógicos son instrumentos formadores para facilitar a los alumnos que lleguen al objetivo de aprendizaje. Hemos tomado en cuenta 4 recursos qué será de gran utilidad dentro de la investigación:

Recursos de apoyo: son los medios que facilitan el proceso de enseñanza aprendizaje en estos podemos encontrar:

- Software de aprendizaje este recurso principalmente es el MOOC el cual nos permitirá la interacción estudiante/ tecnología.

Recurso metodológico: son elementos del currículo qué incluye principios de intervención educativa y las fórmulas y estratégicas en las áreas de educación. Dentro de estas podemos encontrar:

- La elaboración de estrategias de resolución de problemas a partir de causas principales y secundarias las cuales no llevarán a la solución del núcleo del problema.
- La planificación conjunta del aprendizaje siguiendo los pasos principales como planificar, hacer, verificar, actuar para llevar un correcto control del proyecto.

Recursos informativos: estos permiten adquirir, ampliar o comunicar datos y conocimientos, con el fin de resolver una necesidad de información o conocimiento. Dentro de estas podemos encontrar:

- Documentos instructivos de ser necesarios para el uso correcto y asertivo del MOOC.

Recursos relacionales: estos permiten generar una interacción entre los diferentes recursos los cuales se relacionan mediante el uso de tecnología tales como:

- Plataformas virtuales se interrelacionan con el MOOC con una mayor participación estudiante/ tecnología.

3.2. Estructura de la plataforma (LMS)

Dentro de la plataforma de BrightSpace se ha planteado la siguiente estructura en función de los contenidos abordados en el MOOC de ciberseguridad:

a) Bienvenida

En este video de bienvenida, queremos presentarles el MOOC "Escudo Digital" y resaltar su importancia en la protección en línea. Les explicaremos cómo funcionará el curso, incluyendo debates interactivos y actividades de retroalimentación.
También les daremos un vistazo a las dos sesiones fundamentales del curso y la forma en que evaluaremos su progreso, la valoración de sus opiniones y la realización de la encuesta de satisfacción al finalizar el curso. Esto nos ayudará a mejorar y adaptar

futuros cursos, asegurando que cumplan con las expectativas y necesidades de los participantes.

b) Debate de apertura

Dentro de esta sección se pretende plantear un debate inicial entre los participantes del curso con el tópico central “Hablemos de ciberseguridad: lo que sabemos actualmente” que contempla dos preguntas principales:

¿Conoces algo acerca de ciberseguridad?

¿Has escuchado hablar de los peligros/ataques cibernéticos o has sufrido alguno?

El objetivo de este debate es que cada uno de los participantes pueda dar respuestas a estas interrogantes y establecer un punto de partida que nos permita conocer si los participantes tienen algún conocimiento inicial en el tema de ciberseguridad, además de promover un espacio de confianza donde todos puedan interactuar.

c) Sesión MOOC: escudo digital

Esta sección está destinada a la ejecución del MOOC y el desarrollo de sus contenidos. La estructura del MOOC se detalló previamente y su ejecución y visualización podrá realizarse a través de un enlace que conduce a SCORM Cloud, que es un espacio virtual gratuito para la ejecución y prueba de este tipo de recursos.

d) Sesión evaluación general y discusión del curso

- **Test de evaluación**

Una vez culminado el curso virtual MOOC de ciberseguridad, el cual se divide en 11 pantallas que contiene información relevante sobre ciberseguridad y cómo promover un espacio de confianza dentro del mundo digital, se pretende conocer si el estudiante afianzó conocimientos claves e importantes para evitar que sean posibles víctimas del ciberdelito.

El cuestionario formulado para este proceso estará conformado de 10 (diez), preguntas las cuales están divididas 05 preguntas cerradas y 05 preguntas abiertas, con un valor de 01 punto por cada pregunta contestada de manera asertiva, en el caso que no sepa o dude de la respuesta de alguna pregunta, el participante tiene la opción de pasar a la siguiente pregunta, a su vez antes de enviar el cuestionario, puede regresar a revisar y contestar las preguntas que haya tenido alguna duda.

Los cursantes tendrán 30 minutos de duración para el desarrollo del cuestionario, así también dos intentos para solucionar, en donde la nota más alta obtenida será la que se tomará en cuenta como resultado de la evaluación

- **Debate de opinión**

En esta sección se pretende brindar a los participantes una última retroalimentación acerca del curso, mediante la participación colaborativa para construir y consolidar el conocimiento mediante un debate de opinión con el tópico central "Ciberseguridad: lo que hemos aprendido hasta ahora" que contempla dos preguntas principales:

¿Podrías compartirnos alguna recomendación que aprendiste durante el curso para protegernos de los peligros a los que podemos estar expuestos?

¿Puedes aportar algo más que conozcas sobre ciberseguridad?

El objetivo de este debate es cerrar el curso con una última aportación personal de los participantes y conocer el impacto que el curso ha tenido sobre su conocimiento en temas de ciberseguridad tomando como un punto de contraste el conocimiento inicial que los participantes mostraron al iniciar el curso con el primer debate.

- **Encuesta de satisfacción**

Una encuesta de satisfacción es una serie de preguntas la cuales ayudan a conocer las fortalezas y debilidades del proyecto, las cuales servirán de ayuda para el

mejoramiento del mismo. Esta encuesta está dirigida a los participantes del curso y será ejecutada posterior a su participación en el debate de opinión.

e) Despedida

En un mundo cada vez más conectado, la ciberseguridad se ha convertido en una preocupación fundamental. La creciente amenaza de ataques cibernéticos y la vulnerabilidad de nuestros datos personales nos obligan a tomar medidas para protegernos.

La creación de este video de despedida es para resaltar la importancia de adquirir conocimientos básicos sobre ciberseguridad en nuestra era digital. A lo largo del curso, hemos proporcionado herramientas necesarias para comprender los peligros y desafíos de la ciberseguridad, así como las medidas y recomendaciones de protección que les permitirán navegar de manera segura en el mundo virtual, debates interactivos y actividades de retroalimentación para fortalecer su comprensión. Nuestro objetivo ha sido brindar herramientas y conocimientos para protegerse en línea.

3.3. Ampliando horizontes

El curso plateado en el MOOC ejecuta un programa de dos partes al final de cada una de ellas se contempla la realización de una evaluación que permita determinar el progreso y la compresión de los estudiantes sobre los temas tratados, a pesar de que se brinda una retroalimentación sobre las evaluaciones realizadas consideramos pertinente ampliar el horizonte y contar con un plan B, en nuestro caso para seguir con la línea de la experiencia interactiva que motiva al estudiante a ser un miembro activo de su proceso de aprendizaje planteamos la ejecución de experiencias basadas en RPG (Role Playing Game) que colocan al estudiante en el mundo virtual a través de una experiencia basada en videojuegos con una aplicación pedagógica donde el estudiante se convierte en protagonista de su historia y se enfrenta a retos con escenarios que le

permiten comprender los peligros y acciones de protección en el tema de ciberseguridad, de esta manera se brinda una retroalimentación que despierta la atención de los participantes y los mantiene motivados. Para abordar esta propuesta hallamos nuestro respaldo para su posible ejecución en la herramienta web gratuita *RPG Playground*, un instrumento que permite al docente generar de manera rápida y sencilla videojuegos con estética 32 bits para crear sus propias aventuras, adaptar contenidos y realizar pequeñas gamificaciones.

CAPÍTULO IV

4. RESPONSABILIDAD SOCIAL, ÉTICA Y COMUNICACIÓN EDUCATIVA EN ENTORNOS VIRTUALES

4.1. Código ético

4.1.1. Justificación del código ético

La Constitución de la República del Ecuador en su sección quinta en el artículo 26 señala que "la educación es un derecho de las personas a lo largo de su vida y un deber ineludible e inexcusable del Estado" (Asamblea Constituyente República del Ecuador, 2008, pág. 32), en virtud de lo mencionado se debe trabajar en la creación de políticas públicas que garanticen la igualdad e inclusión social de todos los agentes implicados en este proceso como son alumnado, familias, instituciones educativas, claustro docente y sociedad garantizando el derecho y responsabilidad que tienen de participar en el proceso educativo.

El proceso educativo tiene como objetivo la búsqueda de una formación integral que brinde conocimientos y herramientas para desarrollar destrezas y habilidades intelectuales, sociales, culturales y emocionales existiendo de esta manera una inserción responsable y ética con la sociedad pero también permitiendo adquirir un sentido de responsabilidad que está ligado a la adquisición de compromisos y deberes para cada uno de los agentes implicados en el proceso educativo como se menciona en la sección primera, artículo 347, numeral 11 de la Constitución de la República del Ecuador donde se señala que será responsabilidad el Estado promover y "garantizar la participación activa de estudiantes, familias y docentes en los procesos educativos" (Asamblea Constituyente República del Ecuador, 2008, pág. 161).

Es importante estructurar y construir un código de ética que vincule a todos los agentes implicados en el proceso educativo que recoja los ideales formativos e institucionales expresado en valores para el cumplimento de la misión y visión y los propósitos generales de la acción educativa acatando los valores y principios de ética y conducta (Donoso Rosero, 2015, págs. 20-21).

4.1.2. Compromisos y deberes del código ético

4.1.2.1. Compromisos y deberes en relación con el alumnado

Los compromisos y deberes en relación con el alumnado pueden incluir:

- Participar activa y colaborativamente en el proceso educativo para garantizar una formación integral.
- Demostrar honestidad y responsabilidad en el cumplimiento de todas las actividades a desarrollarse en el proceso educativo.
- Respetar las normas de convivencia que forman parte del proceso educativo, así como el respeto a las diferencias e individualidad de los demás participantes.
- Participar en actividades que promuevan el desarrollo de habilidades y destrezas para su formación.

4.1.2.2. Compromisos y deberes en relación con las familias y los tutores del alumnado

Los compromisos y deberes en relaciones con las familias y los tutores del alumnado, se basa especialmente en la Constitución del Ecuador, seguida por diversas leyes, reglamentos y códigos que regulan el buen comportamiento de cada uno de los

participantes en la educación y el buen vivir de todos los que conforman la familia (Asamblea Constituyente República del Ecuador, 2008).

- Respetar los derechos de la comunidad educativa sin discriminación de cualquier índole, que afecte a la integridad física, psicológica y sexual.

- Compartir entre padres de familia o tutores información confiable y verificada en canales oficiales del tema de ciberseguridad.

- El artículo 39 del Código de la Niñez y Adolescencia numeral 3 menciona "Participar activamente en el desarrollo de los procesos educativos" (Código de la niñez y adolescencia, 2003, pág. 09).

- El artículo 39 del Código de la Niñez y Adolescencia numeral 4 menciona "Controlar la asistencia de sus hijos, hijas o representados a los planteles educativos" (Código de la niñez y adolescencia, 2003, pág. 10).

- Colaborar con el plantel educativo en el cumplimiento de los protocolos existentes cuando exista el conocimiento de alguna novedad de vulnerabilidad hacia los estudiantes, en virtud que es una responsabilidad compartida del docente y el tutor.

- Realizar el seguimiento y apoyo incondicional a los estudiantes que tengan algún problema sea este familiar o estudiantil.

- El artículo 12 de la Ley Orgánica de Educación Intercultural (LOEI) literal a menciona "Escoger, con observancia al Interés Superior del Niño, el tipo de institución educativa que consideren conveniente para sus representados, acorde a sus creencias, principios y su realidad cultural y lingüística" (Ministerio de Eduación Ecuador, 2011, pág. 23).

- El artículo 13 de la Ley Orgánica de Educación Intercultural (LOEI) literal f menciona “Propiciar un ambiente de aprendizaje adecuado en su hogar, organizando espacios dedicados a las obligaciones escolares y a la recreación y esparcimiento, en el marco de un uso adecuado del tiempo” (Ministerio de Eduación Ecuador, 2011, pág. 24).

- Impartir valores tanto éticos y morales a los estudiantes a fin de que no sean posibles víctimas de vulneración de sus derechos.

4.1.2.3. Compromisos y deberes en relación con la institución educativa

Los compromisos y deberes en relación con la institución educativa pueden incluir

- Cumplir con los horarios que la institución educativa establece al personal docente, estudiantes, personal de la institución, promoviendo un ambiente de orden y disciplina para un buen desarrollo académico.
- Participar activamente en las actividades de aprendizaje, mostrando interés y compromiso en el proceso educativo.
- Utilizar adecuadamente los recursos y materiales proporcionados por la institución, cuidando el mobiliario, equipos y materiales de estudio.
- Cumplir con las normas de conducta establecidas por la institución, evitando comportamientos disruptivos o perjudiciales para el ambiente educativo.
- Contribuir al ambiente de respeto y tolerancia, fomentando la inclusión y la diversidad dentro de la comunidad educativa.
- Mantener una comunicación fluida con los profesores y el personal de la institución, buscando resolver dudas o inquietudes de manera oportuna.
- Mantener un buen rendimiento académico, cumpliendo con las evaluaciones

y trabajos asignados y buscando mejorar constantemente.

- Representar a la institución educativa de manera positiva dentro y fuera del entorno escolar.

Estos compromisos y deberes son fundamentales para garantizar un ambiente propicio para el aprendizaje y el desarrollo integral de los estudiantes.

4.1.2.4. Compromisos y deberes en relación con los compañeros

Los compromisos y deberes en relación con los compañeros pueden incluir:

- Respetar la diversidad y las opiniones de los compañeros, promoviendo un ambiente de tolerancia y aceptación.
- Tratar a los compañeros con amabilidad y cortesía, evitando cualquier forma de acoso o discriminación.
- Colaborar y trabajar en equipo, compartiendo conocimientos y apoyando a los compañeros en su aprendizaje.
- Ser empático y solidario, ofreciendo ayuda a los compañeros que lo necesiten.
- Mantener la confidencialidad de la información personal de los compañeros.
- Resolver conflictos de manera pacífica y respetuosa, buscando el diálogo y la negociación como vías de solución.
- Evitar difundir rumores o participar en conductas que puedan perjudicar la reputación o el bienestar emocional de los compañeros.
- Promover un ambiente de estudio y trabajo colaborativo, respetando los espacios comunes y manteniendo un nivel adecuado de concentración.

- Participar en actividades extracurriculares o proyectos conjuntos que fortalezcan el compañerismo y la cooperación entre los estudiantes.
- Brindar apoyo moral y emocional a los compañeros en momentos difíciles o de necesidad.
- Mantener una mesa de diálogo para verificar el aprendizaje, asimismo proponer nuevas estrategias de enseñanza.

Estos compromisos y deberes contribuyen a crear un ambiente escolar armonioso, donde se fomenta el respeto mutuo, la solidaridad y la colaboración entre los compañeros.

4.1.2.5. Compromisos y deberes en relación con la profesión

Compromisos y deberes en relación con la profesión docente:

- Desarrollar la labor docente con profesionalidad, vocación y compromiso ético.
- Mantener actualizados los conocimientos disciplinares y las competencias didácticas.
- Respetar la dignidad de los estudiantes y promover su aprendizaje y desarrollo integral.
- Evaluar con justicia el rendimiento académico sin discriminación alguna.
- Cumplir responsablemente con los deberes y obligaciones propias de la función docente.
- Velar por la calidad de la educación y la mejora de la enseñanza.

Compromisos y deberes en relación con los estudiantes:

- Respetar la individualidad y circunstancias particulares de cada estudiante.
- Procurar un trato justo y sin favoritismos hacia los estudiantes.
- Orientar a los estudiantes en su proceso formativo con dedicación.
- Ser un modelo ético para seguir para los estudiantes.
- Velar por la integridad física, psicológica y moral de los estudiantes.

Compromisos y deberes en relación con los padres y familias:

- Mantener comunicación fluida con las familias sobre el proceso educativo.
- Respetar las convicciones y opiniones de los padres sobre la educación.
- Informar con veracidad sobre el desempeño y conducta de los estudiantes.
- Cumplir los acuerdos establecidos con los padres que favorezcan la educación.
- Promover la cooperación de las familias en las actividades educativas.

4.1.2.6. Compromisos y deberes en relación con la sociedad

Los compromisos y deberes en relación con la sociedad pueden incluir:

- Respeto y responsabilidad por el cuidado y la promoción de la salud.
- Respeto y cuidado del medio ambiente.
- Respeto y cuidado responsable de los recursos materiales.
- Libertad con responsabilidad y participación democrática.
- Respeto a la Diversidad.
- Asumir con responsabilidad los deberes de ciudadanía actuando con bien

ante la sociedad.

- Colaborar activamente en programas socioculturales lo cuales fomenten la diversidad.
- Promover y practicar la solidaridad por el bien de la comunidad.
- Fomentar el respeto y la igualdad dentro y fuera de la sociedad y el entorno en el cual se encuentre.

Estos compromiso y deberes son de gran importancia para mantener una buena comunicación con la sociedad y el entorno, es así que para ellos se deben empezar por uno mismo para poder enseñar al resto y llegar en conjunto al objetivo planteado.

4.2. Guía de buenas prácticas en la comunicación en entornos virtuales de aprendizaje

4.2.1. Justificación de la guía de buenas prácticas

La educación es un proceso que involucra la participación y colaboración de diversos actores como lo son docentes, estudiantes, padres de familia, instituciones educativas, estado y sociedad. La guía para la buena práctica del docente del Ministerio de Educación de Ecuador hace énfasis en que el rol docente no se limita únicamente a enseñar lo que está en el currículo, su presencia contribuye a formar en hábitos ayudando a los estudiantes a desarrollar destrezas para la vida, respetar su entorno, la naturaleza y los demás seres que lo rodean (Higgins Bejarano, 2013, pág. 15).

La Constitución de la República del Ecuador en su sección primera referente a la educación artículo 343 señala que “el sistema nacional de educación tendrá como finalidad el desarrollo de capacidades y potencialidades individuales y colectivas de la población, que posibiliten el aprendizaje, y la generación y utilización de

conocimientos, técnicas, saberes, artes y cultura" (Asamblea Constituyente República del Ecuador, 2008, pág. 160).

Los objetivos de desarrollo sostenible (ODS) contemplados en la agenda de 2030 reconocen el rápido crecimiento de las TIC (Tecnologías de la información y la comunicación) y el gran impacto que pueden tener en la reducción de la brecha digital permitiendo el progreso y desarrollo de la sociedad del conocimiento. El marco de competencias de los docentes en materia de TIC elaborado por la UNESCO señala que "la integración efectiva de las TIC en las escuelas y las aulas puede transformar la pedagogía y empoderar a los alumnos" (UNESCO, 2019, pág. 1).

En virtud de lo mencionado se reconoce la importancia de las TIC en el proceso educativo, así como cada una de las herramientas que ésta nos brinda para el desarrollo de competencias digitales en el aula permitiendo el desarrollo de nuevas destrezas y habilidades en los estudiantes, por lo que se considera necesario y existe la motivación para la incorporación de una guía de buenas prácticas en la comunicación de entornos virtuales de aprendizaje que constituyen los espacios de comunicación digital y aprendizaje entre estudiantes, docentes y la institución educativa.

4.2.2. Componentes de la guía de buenas prácticas

La guía de buenas prácticas en la comunicación en entornos virtuales de aprendizaje aplicado al contexto del MOOC de ciberseguridad elaborado para el presente proyecto se desarrolla en función de los aspectos para tener en cuenta en los siguientes puntos que son los recursos base para el desarrollo del proyecto.

4.2.2.1. Componente entorno virtual de aprendizaje (LMS)

Este sistema de gestión de aprendizaje es una plataforma tecnológica que brinda herramientas para cursos como contenidos, seguimientos del progreso de estudiantes, interacción y evaluación.

Este Entorno virtual de aprendizaje brinda al estudiante acceso a los contenidos del curso y materiales de estudio, además de permitir su participación en actividades que promueven una experiencia de aprendizaje positiva. Con el fin de promover un buen uso de la plataforma es necesario tener en cuenta lo siguiente:

- Mantenerse organizado con la información, fechas, tiempo, actividades del curso.
- Participar activamente, compartir ideas, esto fomenta la participación activa.
- Revisar regularmente la información, contenidos como lecturas, videos, materiales complementarios, pues esto ayuda a mantenerse al día con la información.
- Utilizar al máximo las herramientas disponibles brindadas, esto ayuda a mejorar la comprensión y facilita el aprendizaje.

Prácticas para evitar:

- Evitar compartir contraseñas, pues puede exponer la seguridad de la cuenta y la privacidad de la información personal.
- Evitar crear contraseñas fáciles o usar las mismas contraseñas para todas las cuentas.
- No revisar regularmente los contenidos expuestos en la plataforma.
- No usar adecuadamente las herramientas proporcionadas por la plataforma.
- Evitar usar un lenguaje irrespetuoso en las interacciones entre estudiantes y profesores.
- Evitar la deshonestidad de las evaluaciones en línea como la copia. Es importante que el estudiante lo haga de manera honesta y ética.

El uso adecuado y eficaz del LMS permite al estudiante una experiencia positiva de aprendizaje en línea, con pautas claras y útiles de esta herramienta, dando resultados positivos, maximizando su potencial.

4.2.2.2. Componente massive open online course (MOOC)

El MOOC es una herramienta tecnológica que apareció por el principio del año 2000, sus siglas en inglés significan *Massive open online course y traducido al español se denomina* "curso en línea masivo y abierto" que permite al usuario a acceder a varios cursos de manera virtual, dejando a libre decisión de los estudiantes el tiempo y horario que utilizará para la culminación de algún curso seleccionado.

Para que sea un MOOC, interactivo con la comunidad educativa debe tener algunos lineamientos tales como:

- Organizar el tiempo acorde a la disponibilidad del estudiante.
- Revisar y cumplir con todas las actividades que se encuentran en el curso virtual.
- Respetar los comentarios en las diferentes actividades que realizan los demás participantes.
- Verificar y revisar la información en la plataforma las veces que sea necesario para mejor entendimiento.
- Si obtienen más información de otras fuentes, colocar la bibliografía de la fuente obtenida de esta manera evitaremos el cometimiento del delito de plagio.

Que no hacer y colocar dentro del MOOC

- No la utilización de emoticonos en las respuestas.
- No utilizar palabras ambiguas que pueden llegar a confundir a los demás participantes.

- No dar respuestas despectivas hacia el criterio de los demás participantes.
- No intentar modificar los contenidos que se encuentran subidos en la plataforma.

4.2.2.3. Componente foros de opinión y discusión

Las plataformas educativas nos ofrecen hoy en día una amplia gama de herramientas tecnológicas que, bien planificadas y aplicadas en nuestro currículo, brindan oportunidades de aprendizaje realmente útiles.

Desde que se inició la incorporación de las TIC en la educación, los foros virtuales ha sido una de las actividades favoritas de los docentes es por esto que es de gran importancia tener en cuenta como manipular esta herramienta.

Qué hacer y colocar en un foro

- Ajusta el contenido del mensaje al tema planteado, si quieres debatir sobre otro tema abre un nuevo hilo.
- Plantear argumentos y preguntas de forma clara y concisa.
- Respeta las normas de ortografía y signos de puntuación.
- Cuando reproduzcas información de otras webs, cita la fuente de dónde has sacado la información y pon un enlace a la misma.

Que no hacer y colocar dentro del foro

- No redactar mensajes que contengan críticas a webs o personas concretas.
- No utilizar el foro para enviar spam al resto de los usuarios por mail o por mensajes privados.
- No insertes publicidad.
- No escribas en mayúsculas a no ser que sea necesario. En internet, escribir en mayúsculas equivale a gritar.

4.2.2.4. Componente internet

- Ser prudente con la información personal que se comparte. No proporcionar datos sensibles que puedan ser usados indebidamente.
- Evitar las distracciones durante las clases y actividades en línea. Silenciar dispositivos y cerrar pestañas no relacionadas con la actividad.
- Consultar dudas cuando no se ha entendido algo, tanto al docente como a compañeros. Es importante clarificar para poder avanzar.
- Utilizar un lenguaje respetuoso y cordial en los mensajes y comunicaciones. Evitar expresiones irrespetuosas u ofensivas. El objetivo es generar un ambiente de aprendizaje positivo.
- Leer comprensivamente los mensajes antes de responder. Evitar respuestas apresuradas que puedan generar malentendidos. Tomarse el tiempo necesario para entender lo que el interlocutor quiere transmitir.
- Expresar las ideas y opiniones de forma clara y coherente. Estructurar el mensaje para facilitar su comprensión.
- Respetar los turnos de participación en chats y foros. No monopolizar las conversaciones para dar espacio a todos.
- Cuidar la ortografía y la gramática en las comunicaciones escritas. Un texto cuidado refleja respeto al lector.
- Citar adecuadamente las fuentes de información consultadas y evitar el plagio. Es fundamental respetar la propiedad intelectual.

CONCLUSIONES

- Que, mediante la propuesta del proyecto que se encuentra realizado a base de la herramienta MOOC, se establecerá los requerimientos del curso, definiendo los parámetros y unidades de aprendizaje para satisfacer las necesidades de capacitación en temas de ciberseguridad de los estudiantes de la Unidad Educativa Isaac Jesús Barrera.
- Que, la herramienta tecnológica MOOC contiene parámetros muy flexibles y de fácil manejo para todas los estudiantes que deseen participar en el proyecto, permitiendo analizar diversos contenidos en línea sobre la ciberseguridad, medidas de protección con los estudiantes de la Unidad Educativa Isaac Jesús Barrera.
- Que, el diseño la estructura y selección del contenido del MOOC de la capacitación sobre la ciberseguridad se ejecutará mediante la elaboración de materiales multimedia y la utilización de softwares de desarrollo de cursos virtuales para satisfacer los requerimientos establecidos.
- Que, la herramienta tecnológica MOOC en cuanto a la educación se ha constituido en un método lúdico y creativo para la enseñanza de los temas de ciberseguridad, siendo el único recurso indispensable el acceso a internet.

RECOMENDACIONES

- Es un trabajo que requiere el compromiso de todos los que se encuentran inmersos en el ambiente de educación y desarrollo de los adolescentes, por ende, es necesario estar en constantes capacitaciones, charlas, cursos virtuales y presenciales sobre la ciberseguridad a fin de evitar que los estudiantes sean futuras víctimas de algún delito.
- Se recomienda que el presento proyecto que se encuentra elaborado en la herramienta MOOC, que son cursos masivos se ejecute no solamente dentro de la unidad educativa Unidad Educativa Isaac Jesús Barrera, sino se expanda a nivel nacional en todas las instituciones educativas, en virtud que contiene información importante sobre la ciberseguridad en un lenguaje claro y de fácil comprensión.
- Promover la elaboración, creación y ejecución de más proyectos dentro de las unidades educativas, que contengan información relevante sobre los diversos problemas sociales del país.
- En caso de no tener acceso al internet en las instituciones educativas se recomienda gestionar con las diversas autoridades gubernamentales pues el único requisito para estos cursos masivos es el internet.

BIBLIOGRAFÍA

Arregui, L. M., & Lasso Ruiz, A. (2021). CIBERDELITOS. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad,*, 56-57.

Asamblea Constituyente República del Ecuador. (2008). *Constitución de la República del Ecuador.* Ecuador: Publicada en el Registro Oficial No. 449.

Canelos, R. (2010). *Formulación y Evaluación de un Plan Negocio.* Quito, Ecuador: Universidad Internacional del Ecuador. doi:978-9942-03-111-2

Código de la niñez y adolescencia. (03 de Enero de 2003). *Código de la niñez y adolescencia.* Obtenido de Biblioteca Defensoria Pública: https://biblioteca.defensoria.gob.ec/bitstream/37000/3365/1/C%c3%b3digo%20de%20la%20Ni%c3%b1ez%20y%20Adolescencia%20%2817-01-2022%29.pdf

Donoso Rosero, B. (2015). *Código de Ética.* Ecuador: MInisterio de Eduación - Dirección Nacional de Auditoría a la Gestión Educativa.

Higgins Bejarano, A. (2013). *Guía para la buena práctica del docente de Educación General Básica - Ministerio de Educación Ecuador.* Quito: Editogran S.A.

Impulso 06. (2020). *La importancia de la educación en ciberseguridad*. Obtenido de Impulso Formación y Futuro: https://impulso06.com/la-importancia-de-la-educacion-en-ciberseguridad/#:~:text=Proteger%20datos%20personales%20y%20financieros,evitar%20compartir%20informaci%C3%B3n%20sensible%20online.

Ministerio de Eduación Ecuador. (31 de Marzo de 2011). *Ley Orgánica de Educación Intercultural.* Obtenido de https://educacion.gob.ec/wp-content/uploads/downloads/2017/02/Ley_Organica_de_Educacion_Intercultural_LOEI_codificado.pdf

Richard, T. (2019). ISAAC JESUS BARREA REVISTA INSTITUCIONAL. *ISAAC JESUS BARREA REVISTA INSTITUCIONAL*, 12-13.

Richard, T. (2029). ISAAC JESUS BARRERA REVISTA INSTITUCIONAL. *ISAAC JESUS BARRERA REVISTA INSTITUCIONAL*, 12-13.

Tabi, R. (2019). ISAAC JESUS BARRERA REVISTA INSTITUCIONAL. *ISAAC JESUS BARRERA REVISTA INSTITUCIONAL*, 5.

UNESCO. (2019). *Marco de competencias de los docentes en materia de TIC - UNESCO.* París: UNESCO.

UNIR - Universidad Internacional de La Rioja. (2021). *¿Qué es la ciberseguridad?* Obtenido de UNIR : https://colombia.unir.net/actualidad-unir/que-es-ciberseguridad/#:~:text=La%20ciberseguridad%20o%20seguridad%20inform%C3%A1tica,programas%2C%20de%20posibles%20ataques%20digitales.

ANEXOS

Otavalo, 15 de agosto de 2023

Msc. Teresa Sánchez
RECTORA DE LA UNIDAD EDUCATIVA ISAAC JESUS BARRERA

Presente. -

Estimada Rectora, es un gusto dirigirme a usted muy respetuosamente, con la finalidad de solicitar su consentimiento para llevar a cabo nuestro proyecto de grado de la Universidad Internacional del Ecuador - UIDE.

El tema de nuestro proyecto se titula: "Escudo digital: Un MOOC de ciberseguridad, para fortalecer la protección y conciencia online de los estudiantes de la Unidad Educativa Isaac Jesús Barrera". Este proyecto tiene como objetivo principal, brindar herramientas y conocimientos, en ciberseguridad a nuestros estudiantes, buscando fortalecer su protección y conciencia en línea.

Las personas involucradas en este proyecto son las siguientes:

- Hachi Toapanta Fabiola Maribel, con número de cédula 1803871456.
- Jácome Razo María Angeles, con número de cédula 0502887227
- Tamya Alejandra Oña Pillajo, con número de cédula 1003673942.
- Chasi Sandoval Erik Joel, con número de cédula 1805329867
- Jimenez Hurtado Kevin Alexander, con número de cédula 0503439259

Nos comprometemos a realizar el proyecto de manera responsable, respetando los lineamientos establecidos por la institución y garantizando la participación activa de los estudiantes, que estarán involucrados en este proyecto.

Agradecemos de antemano su atención y consideración hacia nuestra solicitud, y quedamos a disposición para cualquier consulta o información adicional que se requiera.

Atentamente,

Ing. Tamya Alejandra Oña Pillajo
Estudiante y Representante del proyecto

UNIDAD EDUCATIVA "ISAAC J. BARRERA"
OTAVALO
RECIBIDO
Fecha: 15-08-23 Hora: 10:17