

ANÁLISIS DE LA NECESIDAD EDUCATIVA	
Tipo: Normativa y Sentida	La necesidad a tratar es tanto normativa como sentida debido a las leyes que protegen la información personal, a la creciente amenaza de ciberataques, y a la responsabilidad social de garantizar la seguridad de los estudiantes.
Identificación del aprendizaje ideal	
<p>Los estudiantes deben conocer e identificar:</p> <ul style="list-style-type: none"> ➤ Riesgos y amenazas en el mundo digital. ➤ Protección de datos personales. ➤ Herramientas y tecnologías de seguridad. 	
Población	Rango de edad: 13 años en adelante
	Escolaridad: Grado 8° en adelante
	Conocimiento que posee: los estudiantes deben tener conocimientos previos sobre uso básico de computadoras para navegar por internet, utilizar programas <básicos, y gestionar archivos.
	Intereses y expectativas: (Población)
	Intereses y expectativas: (Creadores)
Área de formación	Área del saber: Tecnología e Informática
	Área de contenido: Seguridad Informática
Estado actual	<p>Diagnóstico:</p> <p>Examinando las Orientaciones Curriculares de Tecnología e Informática expedido por Ministerio de Educación Nacional en el año 2022, nos dimos cuenta que a pesar de la creciente importancia de las tecnologías digitales en la educación, la Institución Educativa Camilo Torres presenta una necesidad en la formación en seguridad informática como todas las instituciones educativas Colombianas, las orientaciones para este grado en la educación dice en las competencias que se deben desarrollar en este grado “Utilizo responsablemente productos tecnológicos analógicos y digitales, valorando su pertinencia, calidad y efectos potenciales sobre la salud, privacidad y seguridad personal y colectiva”. Si bien los estudiantes hacen un uso de dispositivos y plataformas digitales, existe un desconocimiento generalizado sobre los riesgos cibernéticos y las medidas de protección necesarias. Los docentes, aunque interesados en el tema, enfrentan limitaciones en cuanto a recursos didácticos y capacitación específica. Esta situación evidencia una necesidad urgente de implementar programas de educación en seguridad informática que aborden tanto los conocimientos teóricos como las habilidades prácticas de los estudiantes, con el objetivo de formar ciudadanos digitales responsables y capaces de proteger su información personal en el entorno digital.</p>
Necesidad	La Institución Educativa Camilo Torres enfrenta una necesidad urgente de formación en seguridad informática, debido a que los estudiantes, aunque utilizan frecuentemente dispositivos y plataformas digitales, carecen de conocimientos fundamentales sobre la protección de datos personales y las amenazas cibernéticas. Este vacío educativo expone a los alumnos a riesgos

	como el robo de información y ciberataques, y se ve agravado por la falta de recursos didácticos y capacitación docente adecuados. Ante esta realidad, resulta imprescindible implementar un programa educativo especializado que aborde la seguridad digital de manera integral, para formar ciudadanos digitales responsables y capaces de navegar de forma segura en un entorno cada vez más digitalizado
Causas	<ul style="list-style-type: none"> ➤ Falta de recursos didácticos y capacitación específica ➤ Desconocimiento de los riesgos digitales ➤ Ausencia de programas educativos adecuados
Soluciones	<ul style="list-style-type: none"> ➤ Capacitación docente ➤ Implementación de programas educativos en seguridad digital ➤ Recursos y herramientas didácticas ➤ Concientización y campañas informativas
Conocimientos y habilidades que debe tener el estudiante	Preconceptos: <ul style="list-style-type: none"> ● Conocimiento básico del uso de computadoras e internet. ● Habilidad para navegar por la web y gestionar archivos. ● Familiaridad con programas comunes como procesadores de texto y navegadores web. ● Noción general sobre la privacidad y la protección de información personal.
	Precondiciones: <ul style="list-style-type: none"> ● Competencias básicas de lectura y comprensión de textos. ● Capacidad para seguir instrucciones técnicas ● Habilidades motoras suficientes para interactuar con herramientas tecnológicas. ● Disposición para aprender sobre seguridad informática y protección de datos
Justificación: Para implementar un programa de seguridad informática en la Institución Educativa Camilo Torres radica en la necesidad de preparar a los estudiantes para enfrentar los crecientes riesgos digitales a los que se exponen diariamente. Actualmente, los alumnos carecen de conocimientos sólidos sobre protección de datos personales y ciberseguridad, lo que los deja vulnerables a amenazas como el robo de información y los ciberataques. Este programa no solo dotaría a los estudiantes de herramientas para navegar de forma segura, sino que también fomentaría el uso responsable de las tecnologías digitales, alineado con las competencias requeridas en el siglo XXI. Al fortalecer tanto a estudiantes como a docentes con los recursos y la formación adecuados, se garantizaría una educación integral que no solo protege su seguridad digital, sino que también impulsa su preparación para un futuro profesional en un entorno cada vez más tecnificado	

Formato 1. Formato de Análisis de la necesidad educativa.

FORMULARIO DE REGISTROS DE TIEMPO:

<https://docs.google.com/document/d/1trF-MtmEyWtZ6ssZShFZ8OpOCBjJr6Y7/edit?usp=sharing&ouid=105402654636809518824&rtpof=true&sd=true>

DESARROLLO DE ACTIVIDADES:

https://docs.google.com/document/d/1ddEym45iXe_h8UQPcWdmKB9UQva2jJFK1y843WxTOso/edit?tab=t.0

DISEÑO DE LOS FINES EDUCATIVOS	
OBJETIVOS DE APRENDIZAJE	OBJETIVO GENERAL
	Diseñar e implementar un software educativo que apoye la obtención de conocimientos y habilidades necesarias para navegar de manera segura y responsable por el entorno digital, protegiendo la información personal y los dispositivos.
	OBJETIVOS ESPECÍFICOS
	<ul style="list-style-type: none"> ● Identificar las mayores falencias de los alumnos en cuanto a conocimiento y habilidades respecto a la seguridad informática. ● Seleccionar una herramienta didáctica multimedia e interactiva para implementar la temática. ● Implementar un modelo de diseño para construir la herramienta didáctica multimedia interactiva escogida. ● Crear la herramienta didáctica multimedia interactiva.
DIMENSIONES	<ul style="list-style-type: none"> ● Capaz de desarrollar el conocimiento sobre seguridad informática, permitiendo identificar riesgos cibernéticos, proteger datos personales y aplicar prácticas seguras en línea. ● Capaz de fomentar la interacción responsable en entornos digitales, promoviendo la cooperación y el respeto hacia los demás usuarios. ● Capaz de fomentar la confianza y seguridad emocional al navegar por internet y saber cómo protegerse frente a amenazas digitales.
VALORES	<p>El presente proyecto puede fortalecer:</p> <ol style="list-style-type: none"> 1. Uso responsable de las tecnologías, haciendo un énfasis en la gestión del tiempo y el bienestar digital. 2. Respeto a la privacidad y a los derechos de los demás. 3. Cooperación interpersonal para el apoyo mutuo en la identificación y solución de problemas de seguridad digital.

Formato 4. Formato Diseño de fines educativos.

Competencia 1	Tipo de cognitiva
Objetivos	Norma
1: Enunciado	1: Contexto
Comprender los conocimientos, habilidades y valores necesarios para actuar de manera segura y responsable en el entorno digital.	El uso cotidiano de internet y plataformas tecnológicas por parte de los estudiantes de noveno grado, tanto dentro del aula como en sus actividades personales.
	2: Recursos <ul style="list-style-type: none"> ● Computadores y dispositivos móviles ● Conexión a internet ● Software educativo interactivo ● Conocimientos previos de informática

2: Elementos	3: Evidencias
1. Identifica riesgos digitales para aplicar medidas de protección personal.	<p>1.1 El estudiante identifica correctamente ejemplos de contraseñas débiles y explica los riesgos asociados a su uso.</p> <p>1.2 El estudiante crea contraseñas con una longitud mínima de 8 caracteres, que incluyen una combinación de letras mayúsculas, minúsculas, números y símbolos especiales.</p> <p>1.3 El estudiante es capaz de mejorar contraseñas débiles, aplicando los criterios de longitud, variedad de caracteres y autenticación en dos pasos.</p>
2. Analiza buenas prácticas de privacidad y seguridad en línea	<p>2.1 El estudiante aplica configuraciones de privacidad en una simulación de perfil de redes sociales, limitando el acceso a información personal.</p> <p>2.2 reflexión escrita de cómo las buenas prácticas como la protección de datos personales y la configuración de privacidad contribuyen a una navegación segura y responsable.</p>
3. Practicar la comunicación respetuosa y ética en entornos digitales.	<p>3.1 El estudiante participa activamente en un foro o actividad en línea, utilizando un lenguaje respetuoso y fomentando el diálogo constructivo con sus compañeros.</p> <p>3.2 El estudiante reflexiona sobre ejemplos de comportamientos éticos en redes sociales y propone soluciones a situaciones problemáticas, como el ciberacoso.</p>
Conceptos	
<ul style="list-style-type: none"> ● Riesgos cibernéticos: Definición de amenazas comunes en el entorno digital, como malware, phishing, ciberacoso, y robo de identidad. ● Protección de datos personales: Concepto de privacidad en línea y medidas para proteger información personal, como contraseñas seguras, cifrado y gestión de configuraciones de privacidad. ● Prácticas seguras en línea: Buenas prácticas para navegar de forma segura en internet, incluyendo el uso de redes seguras, evitar sitios peligrosos ● Autenticación y contraseñas: Importancia de contraseñas fuertes y autenticación en dos pasos para asegurar cuentas personales y proteger información. ● Cibernética: Normas y principios éticos en el uso de internet, como el respeto por la privacidad de los demás, la honestidad en el uso de información ● Responsabilidad digital: Concepto de ciudadanía digital y cómo las acciones en línea pueden afectar tanto a uno mismo como a los demás en el entorno digital. 	

Habilidades y destrezas
<ul style="list-style-type: none"> ● Navegación por internet: Capacidad para utilizar navegadores web y acceder a diferentes sitios de forma eficiente y segura. ● Comprensión de textos técnicos: Capacidad para interpretar instrucciones y conceptos relacionados con la seguridad informática, como configuraciones de privacidad y seguridad en aplicaciones. ● Interpretación de términos tecnológicos: Familiaridad con terminología digital básica (por ejemplo, "firewall", "phishing", "contraseñas seguras"). ● Interacción en entornos virtuales: Saber cómo participar en actividades colaborativas en línea, como foros o discusiones en grupo.

Formato 5. Formato de competencias 1.

Competencia 2	Tipo Digital
Objetivos	Norma
1: enunciado	1: contexto
Demostrar el uso de prácticas seguras en línea.	<p>Cuando interactúa con dispositivos digitales y está expuesto a riesgo en línea, tomar decisiones informadas y protegerse a sí mismos y a los demás.</p>
	2: Recursos
	<ul style="list-style-type: none"> ● Software educativo de seguridad en línea. ● Equipos informáticos (computadoras, tablets, smartphones) ● Biblioteca de recursos (videos, infografías).
2: Elementos	3: Evidencias
1. Observar el comportamiento propio en línea, identificando acciones que podrían poner en riesgo su seguridad digital.	<p>1.1 Detallar las prácticas cotidianas, como el uso de contraseñas, la frecuencia de cambio de las mismas, y el uso de redes públicas.</p> <p>1.2 Describir situaciones recientes en las que haya percibido riesgos, explicando por qué ciertos comportamientos pueden ser peligrosos.</p> <p>1.3 Comprobar una lista de verificación después de observar su propio comportamiento en línea, evaluando en qué medida siguen prácticas seguras.</p>
2. Ejemplificar medidas de protección digital en escenarios simulados.	<p>2.1 Describir con ejemplos concretos y en una lista, cómo aplicar medidas de seguridad digital .</p> <p>2.2 Explicar cómo aplicaría medidas de protección en situaciones hipotéticas.</p>

3. Examinar comportamientos de riesgo en sus propias actividades en línea.	<p>3.1 Autoevaluar para identificar comportamientos de riesgo en sus actividades digitales.</p> <p>3.2 Planear para mejorar las prácticas propias en línea, incluyendo cambios específicos que harán para reducir sus riesgos.</p>
Conceptos	
<ul style="list-style-type: none"> ● Prácticas seguras en línea: Buenas prácticas para la navegación en internet de manera segura. ● Autenticación y contraseñas: Importancia de usar contraseñas fuertes y autenticación en dos pasos para la seguridad de las cuentas. ● Protección de datos personales: Conceptos básicos para asegurar la privacidad en línea. 	
Habilidades y destrezas	
<ul style="list-style-type: none"> ● Navegación segura: Capacidad para utilizar navegadores de forma segura, evitando sitios de riesgo. ● Interpretación de configuraciones de seguridad: Habilidad para comprender y configurar opciones de privacidad en diversas plataformas digitales. ● Conciencia digital: Capacidad para identificar situaciones de riesgo y aplicar prácticas de protección en tiempo real. 	

Formato 5. Formato de competencias 2.

Competencia 3	Tipo Social
Objetivos	Norma
1: enunciado	1: contexto
Demuestra una cultura de respeto, responsabilidad y ética digital.	<p>Se evidencia en el entorno digital cotidiano de los estudiantes de noveno grado, quienes usan redes sociales, foros, juegos en línea y mensajería. En estos espacios, enfrentan desafíos como el ciberacoso, el mal uso de información personal y la difusión de contenido inapropiado, debiendo tomar decisiones éticas para proteger su seguridad y la de otros.</p>
	2: Recursos
	<ul style="list-style-type: none"> ● Computadores o dispositivos móviles ● Conexión a internet ● Software educativo ● Materiales didácticos
2: Elementos	3: Evidencias
1. Identifica comportamientos éticos e inadecuados en entornos digitales.	<p>1.1 El estudiante distingue entre comportamientos éticos y no éticos en casos reales o simulados, justificando sus elecciones en un cuestionario.</p> <p>1.2 el estudiante analiza un caso de ciberacoso y señala las acciones que violan la ética digital.</p>

2.Prioriza el respeto y la responsabilidad en la interacción digital.	<p>2.1 El estudiante participa activamente en un foro, utilizando lenguaje respetuoso y fomentando un ambiente positivo y colaborativo.</p> <p>2.2 El estudiante crea un mensaje o campaña digital que promueve valores de respeto y responsabilidad en el uso de las redes sociales.</p>
3.Aplica principios éticos al uso de información en línea.	<p>3.1 Un reporte o presentación en la que el estudiante examina los casos reales, identificando los problemas éticos, los comportamientos inapropiados y las acciones correctivas.</p> <p>3.2 En un análisis de casos, el estudiante propone soluciones éticas para problemas como el plagio o la difusión de información falsa.</p> <p>3.3 Reflexión sobre cómo las decisiones tomadas en los casos reales afectaron a los involucrados y el impacto social de dichas acciones.</p>
Conceptos	
<ul style="list-style-type: none"> ● Ciberacoso: Definición, formas de ciberacoso (acoso, exclusión, suplantación) y sus efectos en las víctimas. Reconocimiento de acciones y comportamientos considerados ciberacoso. ● Ciudadanía digital: Concepto de ciudadanía en el entorno digital, que implica comportarse de manera ética y responsable, respetando a los demás y protegiendo el bienestar común en el espacio en línea. ● Identidad digital y privacidad: Comprensión de la identidad digital, su construcción, protección y la importancia de controlar la información personal compartida en internet. 	
Habilidades y destrezas	
<ul style="list-style-type: none"> ● Habilidad para identificar riesgos digitales: Reconocer comportamientos inapropiados en línea, como el ciberacoso o el intercambio de información sensible, y los riesgos asociados a estos actos. ● Toma de decisiones éticas en entornos digitales: Evaluar situaciones que presenten dilemas éticos en línea y tomar decisiones responsables, considerando el impacto en los demás y en la propia reputación digital. ● Reflexión crítica sobre el comportamiento digital: Analizar sus propias conductas y las de otros en plataformas digitales, reflexionando sobre las consecuencias y la ética de sus acciones. ● Resolución de conflictos en entornos digitales: Resolver desacuerdos de forma ética y respetuosa, utilizando estrategias de comunicación que reduzcan el conflicto y promuevan el entendimiento mutuo. ● Autogestión y autorregulación digital: Gestionar su comportamiento en línea y adoptar prácticas responsables, demostrando autonomía en la toma de decisiones seguras y éticas. 	

Formato 5. Formato de competencias 3.

Concepto	Características	Definición
Riesgos Cibernéticos	<ul style="list-style-type: none"> Incluyen amenazas comunes como malware.phishing, suplantación de identidad y ciberacoso. Se manifiestan en forma de mensajes engañosos, enlaces sospechosos y prácticas de ingeniería social. 	Riesgos cibernéticos se refieren a las amenazas digitales que ponen en peligro la seguridad y privacidad de la información personal y el bienestar del usuario en el entorno digital.
Protección de Datos Personales	<ul style="list-style-type: none"> Se centra en la gestión de contraseñas seguras, la configuración de privacidad en redes sociales, el uso de cifrado, y el manejo responsable de la información personal. Prácticas para minimizar el acceso no autorizado a los datos. 	La protección de datos personales es el conjunto de prácticas y medidas que resguardan la información privada de los usuarios, evitando su exposición y uso indebido en plataformas digitales.
Prácticas Seguras en Línea	<ul style="list-style-type: none"> Involucra el uso de redes confiables. Evita la descarga de archivos de fuentes no verificadas. Verifica la autenticidad de sitios web, y mantener actualizados los sistemas de seguridad. Incluye conductas que reducen la exposición a riesgos digitales. 	Las prácticas seguras en línea son conductas y estrategias de navegación que minimizan los riesgos digitales y protegen al usuario y sus dispositivos de amenazas cibernéticas.
Responsabilidad Digital	<ul style="list-style-type: none"> Engloba la ética y respeto en el uso de internet. Incluye la protección de la privacidad propia y de otros. Incluye la autenticidad de la información compartida, y la conciencia de los efectos de las propias acciones en línea. 	La responsabilidad digital es el compromiso de actuar de manera ética y segura en el entorno digital, respetando los derechos y privacidad de otros usuarios y promoviendo un uso positivo y consciente de las tecnologías digitales.

Formato 6. Vista parcial de la matriz del diseño de contenidos.

MODELO PEDAGÓGICO CONSTRUCTIVISTA		
Bases conceptuales		Características
El modelo constructivista se fundamenta en la concepción de que el aprendizaje es un proceso activo y significativo en el cual los estudiantes construyen su propio conocimiento a partir de sus experiencias previas y el entorno que los rodea. Este enfoque valora la interacción social y cultural, reconociendo que el contexto influye directamente en la forma en que los individuos interpretan y asimilan la información. Además, el		<ul style="list-style-type: none"> - Las actividades están diseñadas para que los estudiantes experimenten, exploren y descubran conocimientos. - Se reconocen y valoran las ideas y experiencias que los estudiantes ya tienen, usándolas como base para construir nuevos conocimientos. - Ambientes de Aprendizaje Colaborativos: Se

DISEÑO PEDAGÓGICO	<p>constructivismo promueve que el aprendizaje sea un proceso adaptativo, en el que los estudiantes desarrollen habilidades críticas y de resolución de problemas, permitiéndoles enfrentar situaciones nuevas con una mentalidad analítica y flexible. En este modelo, el estudiante es el protagonista de su propio aprendizaje, participando de manera activa en la construcción de significados, mientras explora, experimenta y establece conexiones entre sus conocimientos previos y los nuevos conceptos.</p>	<p>fomenta la cooperación entre estudiantes para desarrollar habilidades de trabajo en equipo, resolución de problemas y comunicación.</p> <p>- Docente como Facilitador: En lugar de ser el centro de la información, el docente actúa como un facilitador que guía a los estudiantes, proporcionando apoyo y herramientas, y creando un ambiente propicio para que ellos construyan su aprendizaje.</p>
	Enfoques: Social	
	<p>El aprendizaje no ocurre de forma aislada, sino que se enriquece a través de la interacción con otras personas, el conocimiento se construye en gran parte a través del diálogo, la colaboración y el intercambio de ideas, lo cual ayuda a los estudiantes a contrastar y cuestionar sus propias creencias y a ampliar su comprensión.</p> <p>Además figuras como Lev Vygotsky, explican que el aprendizaje se da en un contexto cultural y que el lenguaje y la interacción social son herramientas clave para desarrollar el pensamiento y el conocimiento. Por ello, los entornos colaborativos son esenciales, ya que permiten a los estudiantes desarrollar habilidades como la comunicación, el trabajo en equipo y la empatía, creando significados compartidos y construyendo una comprensión más profunda y contextualizada.</p>	
	Principios educativos	Metáfora educativa
	<p>- Generación de Situaciones Problemáticas para Estimular el Aprendizaje Activo Cada tema en el software debe iniciar con una situación desafiante y realista que genere un "choque cognitivo" en el estudiante. Estas situaciones, que simulan riesgos digitales comunes, motivará al estudiante a investigar y descubrir soluciones a medida que avanza en los temas de seguridad en línea.</p> <p>- Docente como Facilitador y Guía en el Proceso de Aprendizaje El rol del docente es fundamental en dos momentos clave: primero, al presentar el problema inicial y guiar las primeras reflexiones, y luego al orientar en la elaboración de productos, como el diseño de contraseñas o la simulación de escenarios seguros, ayudando al estudiante a consolidar lo aprendido.</p>	<p>A lo largo del software, el estudiante será incentivado a reflexionar sobre sus propias prácticas digitales. Los ejercicios de autoevaluación permitirán identificar fortalezas y áreas de mejora, fomentando la metacognición y la capacidad de regular sus comportamientos en línea de forma segura.</p> <p>- Colaboración como Estrategia de Construcción de Conocimiento A través de foros de discusión y actividades grupales dentro del software, los estudiantes pueden compartir sus experiencias y soluciones, lo que no solo enriquece su conocimiento, sino que también fortalece el sentido de comunidad y apoyo mutuo en el aprendizaje sobre seguridad digital</p>

Formato 7. Diseño de contenidos.

COMPETENCIA#1		
Comprender los conocimientos, habilidades y valores necesarios para actuar de manera segura y responsable en el entorno digital.		
Elementos	Aplicación modelo pedagógico	Indicadores

1. Identifica riesgos digitales para aplicar medidas de protección personal.	Estudio de Casos y Escenarios: A través de este enfoque constructivista, los estudiantes debaten y resuelven problemas de la vida real, apoyándose en su experiencia previa y en la colaboración con sus compañeros para desarrollar soluciones y criterios propios con respecto a la seguridad informática de sus datos y como evitar casos como los que se den.	1.1 Participación en clase. 1.2 Aportes a las soluciones de los casos dados. 1.3 Comportamiento y respeto al momento de participar.
Secuencia de aprendizaje		
Objetivo: Comprender la importancia de la seguridad de los datos personales en la Internet.	BARRA DE RECURSOS	
	Navegación: - Salón de clases. - Computadores. - Proyector.	
Problema: Imagina que un día recibes un mensaje en tu red social favorita de alguien que parece ser un amigo. El mensaje dice que necesita tu ayuda urgentemente para recuperar su cuenta y te pide que le envíes una clave de verificación que te llegará a tu teléfono. El mensaje también incluye un enlace, que te dice que debes abrir para restablecer la cuenta.	Documentación: - Pdf - Fotos - Videos	
Estrategia: En el Estudio de Casos y Escenarios se les plantea a los estudiantes un caso y estos debatirán como poder resolverlo y evitas, como posibles preguntas problemas se les darán las siguientes. <ul style="list-style-type: none"> • ¿Cómo sabrías si realmente es tu amigo quien envió el mensaje o si es alguien intentando engañarte? • ¿Qué señales te harían sospechar que este mensaje puede ser un intento de engaño (phishing)? • Si decides ayudar, ¿qué podrías hacer para asegurarte de que sea seguro? (Contactar directamente, evitar abrir el enlace, etc.) • ¿Qué problemas podrías enfrentar si decides enviar la clave o abrir el enlace sin verificar? • ¿Cómo puedes protegerte mejor para evitar caer en situaciones como esta en el futuro? 	Comunicación: - Correo - Chat	

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 1.

COMPETENCIA#1
Comprender los conocimientos, habilidades y valores necesarios para actuar de manera segura y responsable en el entorno digital

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 1.

COMPETENCIA#1

Comprender los conocimientos, habilidades y valores necesarios para actuar de manera segura y responsable en el entorno digital		
Elementos	Aplicación modelo pedagógico	Indicadores
3. Practicar la comunicación respetuosa y ética en entornos digitales.	<p>A través de este enfoque constructivista, los estudiantes analizan y resuelven problemas relacionados con conflictos en entornos digitales, como comentarios irrespetuosos, ciberacoso o publicaciones controvertidas en redes sociales. Apoyándose en su experiencia previa y en la colaboración con sus compañeros, los estudiantes identifican los comportamientos inadecuados, proponen soluciones éticas y desarrollan criterios propios para interactuar de manera respetuosa y ética en el entorno digital.</p> <p>La actividad se lleva a cabo en un foro virtual donde los estudiantes participan activamente, debatiendo y reflexionando sobre las mejores prácticas para resolver el conflicto presentado. Al final, comparten aprendizajes sobre cómo fomentar un ambiente digital más inclusivo y respetuoso.</p>	<ul style="list-style-type: none"> El estudiante utiliza un lenguaje adecuado, evitando expresiones ofensivas o irrespetuosas El estudiante plantea soluciones o puntos de vista que promueven la empatía, la justicia y la resolución del conflicto en línea de forma ética. El estudiante responde de manera constructiva a las publicaciones de sus compañeros
Secuencia de aprendizaje		
Objetivo: los estudiantes desarrollan la capacidad de participar en discusiones digitales utilizando un lenguaje respetuoso y ético, identificando conflictos en línea y proponiendo soluciones que fomenten un ambiente inclusivo y constructivo.	BARRA DE RECURSOS	
	Navegación: - red social -plataforma -computador -internet	
Problema: En una red social ficticia utilizada por estudiantes para compartir opiniones sobre temas académicos, surge un conflicto durante un debate sobre el uso de dispositivos en clase. Algunos usuarios publican comentarios ofensivos, atacando directamente las opiniones y características personales de otros compañeros. Esto genera un ambiente hostil en el foro, donde los afectados optan por abandonar la discusión. Además, la falta de moderación adecuada ha permitido que estos	Documentación: - pdf	

comportamientos persisten sin consecuencias, afectando la confianza en la plataforma y la participación de la comunidad.	
Estrategia: <ul style="list-style-type: none"> Los estudiantes analizan los comentarios del caso, diferenciando entre comportamientos respetuosos e irrespetuosos. Detectan las principales causas del conflicto, como el uso de lenguaje ofensivo, la falta de empatía y la ausencia de moderación adecuada. Los estudiantes redactan una respuesta al conflicto en la que aplican principios de comunicación respetuosa, proponiendo soluciones concretas como: <ul style="list-style-type: none"> Fomentar el uso de un lenguaje neutro y constructivo. Promover la empatía en las interacciones, invitando a los usuarios a considerar perspectivas ajenas. Establecer pautas claras de conducta para moderar futuras discusiones. 	Comunicación: <ul style="list-style-type: none"> - correo -chat

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 3.

COMPETENCIA#2		
Demostrar el uso de prácticas seguras en línea.		
Elementos	Aplicación modelo pedagógico	Indicadores
1. Observa el comportamiento propio en línea, identificando acciones que podrían poner en riesgo su seguridad digital.	<p>Presentamos situaciones reales o simuladas que generan un "choque cognitivo". Esto despierta el interés y motiva a investigar soluciones, en lugar de simplemente recibir la información.</p> <p>Compartir listas de prácticas y ejemplos, enriquece la comprensión mediante la comparación y el aprendizaje mutuo. Este intercambio de experiencias contribuye a la construcción del conocimiento social y refuerza el enfoque colaborativo del modelo constructivista.</p>	<p>1.1 Escribe detalladamente sus prácticas personales cotidianas en línea.</p> <p>1.2 Describe situaciones recientes de riesgo en su actividad en línea.</p> <p>1.3 Evalúa sus propias prácticas en línea mediante una lista de verificación.</p>
Secuencia de aprendizaje		
Objetivo: Observar y analizar los propios comportamientos en línea para identificar prácticas de riesgo y evaluar su nivel de seguridad digital. Esto les permitirá desarrollar conciencia sobre los hábitos seguros y realizar mejoras en su actividad en línea.	BARRA DE RECURSOS	
	Navegación: -	

<p>Problema: El aumento de amenazas digitales y el uso frecuente de plataformas en línea exponen a las personas a riesgos como el robo de información, ciberacoso y suplantación de identidad. Sin embargo, muchos no reconocen los comportamientos cotidianos que incrementan su vulnerabilidad. ¿Qué prácticas realizan que los ponen en riesgo, y cómo pueden evaluarlas para mejorar su seguridad en línea?</p>	<p>Documentación:</p> <ul style="list-style-type: none"> - Pdf - Fotos - Videos
<p>Estrategia:</p> <ul style="list-style-type: none"> - Actividad de Reflexión Inicial: Los estudiantes completarán un cuestionario de autoevaluación sobre sus prácticas diarias en línea (uso de contraseñas, frecuencia de cambio de las mismas, uso de redes públicas). Esto les ayudará a detallar y reconocer sus propias prácticas. - Análisis de Situaciones Recientes de Riesgo: A partir de ejemplos comunes de situaciones de riesgo digital, los estudiantes trabajarán en parejas o pequeños grupos para discutir y analizar sus propias experiencias. Luego, documentan ejemplos específicos donde hayan percibido riesgos, explicando cómo ciertos comportamientos pueden exponerlos a amenazas en línea. Esta actividad fomenta el diálogo y ayuda a relacionar sus experiencias con prácticas seguras. - Aplicación de Lista de Verificación de Seguridad: Con el fin de comprobar y reforzar las prácticas seguras, los estudiantes utilizarán una lista de verificación que cubra aspectos clave de seguridad digital (uso de contraseñas seguras, autenticación en dos pasos, manejo de redes públicas). Evaluarán en qué medida sus propias prácticas se alinean con estas pautas seguras y anotarán áreas de mejora. 	<p>Comunicación:</p> <ul style="list-style-type: none"> - Correo - Chat

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 2.

COMPETENCIA#2		
Demuestra el uso de prácticas seguras en línea.		
Elementos	Aplicación modelo pedagógico	Indicadores
<p>2. Da ejemplos de medidas de protección digital en escenarios simulados.</p>	<p>Presentamos situaciones reales o simuladas que generan un "choque cognitivo". Esto despierta el interés y motiva a investigar soluciones, en lugar de simplemente recibir la información.</p> <p>Los estudiantes no solo reciben información sobre prácticas seguras, sino que deben aplicarlas en situaciones simuladas y diseñar estrategias propias de protección. Esto refleja la construcción activa de conocimientos, donde el estudiante va más allá de lo teórico</p>	<p>2.1 Ejemplifica el uso de medidas de protección digital en escenarios simulados.</p> <p>2.2 Describe en forma detallada cómo aplicaría medidas de seguridad en situaciones hipotéticas.</p>

	para convertir las prácticas seguras en habilidades reales y aplicables.	
Secuencia de aprendizaje		
Objetivo: Identificar y ejemplificar el uso de medidas de protección digital, aplicándolas en escenarios simulados y situaciones hipotéticas para fortalecer la comprensión y habilidad en prácticas seguras en línea.		BARRA DE RECURSOS
		Navegación: -
Problema: Las personas frecuentemente desconocen cómo aplicar medidas de seguridad digital en situaciones de riesgo, lo que las expone a amenazas como phishing, malware o robo de información personal. ¿Cómo pueden identificar y aplicar medidas específicas de protección en diversos escenarios en línea?		Documentación: - Pdf - Fotos - Videos
Estrategia: <ul style="list-style-type: none"> - Creación de Ejemplos Concretos de Medidas de Protección Digital: Cada estudiante desarrollará una lista detallada que incluya ejemplos de medidas de seguridad digital para cada escenario de riesgo presentado, como el uso de contraseñas seguras, autenticación en dos pasos, y evitar enlaces sospechosos. Este ejercicio refuerza su habilidad para reconocer y aplicar prácticas seguras. - Simulación de situaciones hipotética: Se presentarán situaciones hipotéticas adicionales, como el uso de una red pública para realizar una transacción bancaria o recibir un mensaje de phishing en redes sociales. Los estudiantes elegirán una situación e, individualmente, escribirán un texto explicando qué medidas tomarían y cómo responderían para protegerse, justificando cada paso de acuerdo con su conocimiento de seguridad digital. 		Comunicación: - Correo - Chat

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 2.

COMPETENCIA#2		
Demuestra el uso de prácticas seguras en línea.		
Elementos	Aplicación modelo pedagógico	Indicadores
3. Examina comportamientos de riesgo en sus propias actividades en línea	<p>Presentamos situaciones reales o simuladas que generan un "choque cognitivo". Esto despierta el interés y motiva a investigar soluciones, en lugar de simplemente recibir la información.</p> <p>A lo largo del software, el estudiante será incentivado a reflexionar sobre sus propias prácticas digitales. Los ejercicios de autoevaluación permitirán</p>	<p>3.1 Realiza una autoevaluación para identificar comportamientos riesgosos en su actividad en línea.</p> <p>3.2 Elabora un plan de acción para mejorar sus prácticas en línea.</p>

	identificar fortalezas y áreas de mejora, fomentando la metacognición y la capacidad de regular sus comportamientos en línea de forma segura.	
Secuencia de aprendizaje		
Objetivo: Que los estudiantes identifiquen y analicen comportamientos de riesgo en sus actividades digitales y desarrollen un plan de acción con cambios específicos para mejorar su seguridad en línea.	BARRA DE RECURSOS	
	Navegación: -	
Problema: A pesar de la importancia de la seguridad digital, muchos estudiantes desconocen cuáles de sus comportamientos cotidianos los exponen a riesgos en línea. ¿Cómo pueden identificar sus propios comportamientos de riesgo y qué acciones pueden implementar para mejorar su seguridad en el entorno digital?	Documentación: - Pdf - Fotos - Videos	
Estrategia: <ul style="list-style-type: none"> - Introducción a Comportamientos de Riesgo: El docente presenta con ejemplos de comportamientos de riesgo comunes (ej. no cambiar contraseñas, conectarse a redes públicas sin precaución, compartir información personal en redes sociales). Los estudiantes reflexionan sobre cuáles de estos comportamientos aplican a sus propias prácticas. - Actividad de Autoevaluación: Cada estudiante completa una autoevaluación diseñada para identificar comportamientos de riesgo en sus actividades en línea. La autoevaluación incluye preguntas sobre sus hábitos digitales, como la frecuencia de actualización de contraseñas, el uso de autenticación en dos pasos, y la gestión de información personal. Al finalizar, cada estudiante identifica al menos tres comportamientos de riesgo específicos en sus prácticas actuales. - Desarrollo de un Plan de Acción: A partir de la autoevaluación y las discusiones grupales, cada estudiante elabora un plan de acción con pasos específicos para reducir los riesgos identificados en su actividad en línea. Este plan incluye al menos tres cambios concretos, como actualizar contraseñas periódicamente, usar redes seguras y habilitar la autenticación en dos pasos, con metas y fechas para implementar cada cambio. 	Comunicación: - Correo - Chat	

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 2.

COMPETENCIA#3		
Demuestra una cultura de respeto, responsabilidad y ética digital.		
Elementos	Aplicación modelo pedagógico	Indicadores
Identifica comportamientos éticos e inadecuados en entornos digitales.	Se utiliza un enfoque constructivista, fomentando el	1.1 Identificar comportamientos

	<p>aprendizaje colaborativo y la reflexión crítica. Las actividades propuestas permiten a los estudiantes analizar situaciones reales o simuladas relacionadas con la ética digital y construir soluciones basadas en valores como el respeto y la responsabilidad.</p>	<p>éticos e inadecuados en entornos digitales.</p> <p>1.2 Prioriza el respeto y la responsabilidad en la interacción digital.</p> <p>1.3 Aplicación de principios éticos al uso de información en línea.</p>
Secuencia de aprendizaje		
<p>Objetivo: Que los estudiantes desarrollen habilidades para identificar conflictos éticos en entornos digitales, reflexionar sobre sus acciones y proponer soluciones que fomenten un ambiente digital inclusivo y respetuoso.</p>	BARRA DE RECURSOS	
	<p>Navegación:</p> <ul style="list-style-type: none"> - Computadoras o dispositivos móviles. - Conexión a internet. 	
<p>Problema: En una plataforma de debate estudiantil, surge un conflicto debido a comentarios irrespetuosos y ofensivos. La falta de moderación genera un ambiente hostil, afectando la participación y confianza de los usuarios. Los estudiantes deberán analizar esta situación y proponer soluciones que fomenten el respeto y la ética en las interacciones digitales.</p>	<p>Documentación:</p> <ul style="list-style-type: none"> - Guías en PDF sobre ciberacoso y ética digital. - Vídeos educativos sobre ciudadanía digital. - Estudios de casos reales o simulados 	
<p>Estrategia: Se presentará a los estudiantes un caso práctico que ejemplifica un conflicto ético en un entorno digital, como la publicación de comentarios ofensivos en una plataforma de debate. A través de un análisis grupal, los estudiantes identificarán conductas respetuosas e irrespetuosas, reflexionando sobre las causas subyacentes del conflicto y las posibles soluciones. Posteriormente, redactarán mensajes que promuevan la empatía y el respeto, proponiendo pautas claras para moderar discusiones en el futuro.</p> <p>A continuación, los estudiantes trabajarán de forma colaborativa en la creación de una campaña digital que refuerce valores como el respeto y la responsabilidad en las interacciones en línea. Utilizando herramientas digitales, diseñarán mensajes o videos que fomenten prácticas digitales positivas. Finalmente, se organizará una sesión de retroalimentación grupal, donde los compañeros compartirán sugerencias y perspectivas</p>	<p>Comunicación:</p> <ul style="list-style-type: none"> -Foros virtuales - Correos electrónico 	

sobre las propuestas presentadas. Este proceso culminará con una reflexión personal en la que cada estudiante analizará cómo los conocimientos adquiridos pueden influir en sus comportamientos digitales futuros, fortaleciendo su compromiso con la ética digital.	
--	--

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 3.

COMPETENCIA#3		
Demuestra una cultura de respeto, responsabilidad y ética digital.		
Elementos	Aplicación modelo pedagógico	Indicadores
Prioriza el respeto y la responsabilidad en la interacción digital.	Los estudiantes participan en foros colaborativos donde practican un lenguaje respetuoso y promueven un ambiente positivo.	2.1 Utilizar un lenguaje respetuoso en discusiones en línea. 2.2 Crear mensajes o campañas digitales que fomenten el respeto y la responsabilidad en redes sociales.
Secuencia de aprendizaje		
Objetivo: Fomentar interacciones digitales respetuosas y responsables mediante estrategias colaborativas y reflexivas en un entorno virtual.	BARRA DE RECURSOS	
	Navegación: <ul style="list-style-type: none"> - Computadores o dispositivos móviles. - Conexión a internet 	
Problema: Caso de ciberacoso o lenguaje inapropiado en redes sociales que genera un ambiente hostil y afecta la dinámica grupal.	Documentación: <ul style="list-style-type: none"> - Casos prácticos en formato PDF sobre dilemas éticos y ciberacoso. - Videos educativos que explican los principios de la ética digital. 	
Estrategia: El proceso para fomentar la ética digital en estudiantes se desarrolla en cinco fases. La primera introduce un caso ficticio sobre interacción hostil en una red social educativa para sensibilizarlos y motivarlos, promoviendo la reflexión sobre comportamientos éticos e inadecuados. En la segunda fase, analizan el caso en grupos, clasifican conductas y comparten conclusiones en un debate colectivo para comprender el impacto de las acciones digitales. La tercera fase aborda la resolución colaborativa, donde diseñan respuestas éticas y lineamientos de conducta digital para prevenir conflictos. Luego, en la cuarta fase, aplique lo aprendido creando campañas digitales que promuevan respeto y responsabilidad, compartiendo sus propuestas para retroalimentación. Finalmente, en la quinta fase, reflexionan individualmente sobre la	Comunicación: -Foros o chats grupales.	

importancia de la ética digital y cómo aplicarla en su vida diaria, consolidando el aprendizaje a través del intercambio de ideas en un foro. Esta metodología integra análisis crítico, trabajo en equipo, creatividad y reflexión personal para desarrollar habilidades digitales responsables.

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 3.

COMPETENCIA#3

Demuestra una cultura de respeto, responsabilidad y ética digital.

Elementos	Aplicación modelo pedagógico	Indicadores
Aplica principios éticos al uso de información en línea.	Los estudiantes analizan situaciones donde se ha utilizado incorrectamente la información, como el plagio en trabajos académicos o la difusión de noticias falsas en redes sociales. A través de esta reflexión, se fomenta el desarrollo de soluciones éticas que puedan aplicarse en la vida cotidiana o académica. Este enfoque constructivista permite que los estudiantes construyan sus propios aprendizajes basándose en experiencias y ejemplos prácticos.	<ul style="list-style-type: none"> - Examinar casos de plagio o difusión de información falsa, proponiendo soluciones éticas. - Reflexión sobre el impacto social de las decisiones digitales.

Secuencia de aprendizaje

Objetivo: Fomentar la ética y la responsabilidad en el uso de la información digital, reflexionando sobre casos prácticos y desarrollando estrategias para prevenir malas prácticas.	BARRA DE RECURSOS
	Navegación: <ul style="list-style-type: none"> - Computadores o dispositivos móviles. - Conexión a internet
Problema: Se le da al estudiante un caso que ilustra el mal uso de la información en entornos digitales. Por ejemplo, un estudiante podría copiar contenido de internet sin citar la fuente y presentarlo como propio en un trabajo escolar, o un grupo de personas podría compartir masivamente una noticia falsa en redes sociales, generando alarma pública. Estos escenarios reflejan situaciones reales que los estudiantes podrían enfrentar, ayudándoles a reconocer las implicaciones éticas de estas acciones. A través del análisis y la reflexión, los estudiantes no solo identifican las consecuencias negativas de estos comportamientos, sino que también desarrollan estrategias prácticas y éticas para abordarlos y prevenirlos en el futuro.	Documentación: <ul style="list-style-type: none"> - Casos prácticos en formato PDF sobre dilemas éticos y ciberacoso. - Videos educativos que explican los principios de la ética digital.
Estrategia: La estrategia se centra en el análisis crítico y la aplicación práctica de principios éticos mediante el trabajo con casos simulados. Los estudiantes	Comunicación: <ul style="list-style-type: none"> - Foros

comienzan reflexionando sobre un escenario ficticio de mal uso de la información, identificando errores éticos y sus posibles consecuencias. Luego, en grupos, analizan estas problemáticas, diseñan soluciones responsables, y desarrollan proyectos como infografías, videos o campañas para promover el uso ético de la información. Estas actividades se complementan con debates en foros y reflexiones individuales, fomentando un aprendizaje integral que conecta la teoría con la práctica y fortalece la responsabilidad digital en contextos reales.	
---	--

Formato 8. Diseño de la secuencia de aprendizaje basado en la competencia 3.

PROCESO EVALUATIVO			
Competencia n° 1			
Elemento n° 1	Indicadores n° 1.1	Criterio	Actividad n° 1.1
Identifica riesgos digitales para aplicar medidas de protección personal.	<p>1.1 Identifica sitios web inseguros a través de características como ausencia de protocolos HTTPS o certificados válidos.</p> <p>1.2 Reconoce intentos de phishing en correos electrónicos mediante la identificación de enlaces sospechosos y remitentes no verificados.</p> <p>1.3 Clasifica riesgos en redes sociales como perfiles falsos o solicitudes de datos personales.</p>	<p>1: El estudiante identifica y clasifica correctamente los riesgos digitales en un estudio de caso, argumentando por qué cada elemento constituye un riesgo y cómo se podría mitigar</p> <p>2: El estudiante demuestra habilidades para proponer soluciones prácticas y preventivas frente a los riesgos identificados, explicando cómo implementarlas en la vida cotidiana.</p>	Estudio de Casos de Riesgos Digitales: Se presenta un caso ficticio en el que los estudiantes analizan un correo sospechoso y detectan elementos como enlaces fraudulentos y remitentes extraños. En pequeños grupos, los estudiantes debaten sobre las acciones correctas para protegerse. Posteriormente, generan una lista de recomendaciones para evitar ser víctimas de estos riesgos en el futuro.

Formato 9. Diseño proceso evaluativo de la competencia 1.

PROCESO EVALUATIVO			
Competencia n° 1			
Elementos n° 2	Indicadores n° 2.1	Criterio	Actividad n° 2.1
Analiza buenas prácticas de privacidad y seguridad en línea.	<p>2.1: Identifica configuraciones de privacidad en redes sociales y explica cómo optimizarlas para proteger información personal.</p> <p>2.2: Reconoce la</p>	<p>1: El estudiante analiza un caso real o ficticio para identificar los errores en la configuración de privacidad y propone al menos tres mejoras basadas en buenas prácticas.</p>	Estudio de Casos sobre Configuración de Privacidad y Seguridad: Se presenta un caso donde un usuario enfrenta problemas debido a configuraciones inadecuadas en redes

	<p>importancia de autenticación en dos pasos y describe el procedimiento para activarla en diferentes plataformas.</p> <p>2.3: Evalúa políticas de privacidad de aplicaciones y determina su nivel de confiabilidad.</p>	<p>2: Evalúa la seguridad de una aplicación o plataforma utilizando un checklist de prácticas seguras y presenta un informe con recomendaciones claras.</p>	<p>sociales. Los estudiantes, organizados en equipos, analizan los errores, proponen mejoras (como activar autenticación en dos pasos y limitar la visibilidad de datos personales), y justifican cómo estas acciones refuerzan la privacidad y la seguridad. Al final, presentan sus conclusiones en una discusión grupal.</p>
--	--	--	---

Formato 9. Diseño proceso evaluativo de la competencia 1.

PROCESO EVALUATIVO			
Competencia n° 1			
Elementos n°3	Indicadores n° 3.1	Criterio	Actividad n° 3.1
Practicar la comunicación respetuosa y ética en entornos digitales.	<p>3.1: Identifica comentarios y comportamientos inadecuados en un entorno digital y explica su impacto en la comunidad.</p> <p>3.2: Propone respuestas respetuosas y éticas ante casos de conflictos digitales, argumentando su elección.</p> <p>3.3: Participa activamente en debates grupales promoviendo el respeto y la inclusión.</p>	<p>1: El estudiante identifica al menos tres comportamientos inapropiados en un caso presentado y analiza sus consecuencias en el entorno digital.</p> <p>2: Propone soluciones éticas, basadas en la reflexión y el respeto, que podrían prevenir o resolver los conflictos.</p> <p>3: Contribuye con aportaciones en un foro virtual, demostrando respeto por las opiniones ajenas y promoviendo la colaboración para resolver conflictos.</p>	<p>Foro Virtual sobre Conflictos Digitales:</p> <p>Los estudiantes analizan un caso relacionado con un conflicto digital, como ciberacoso o comentarios irrespetuosos. Participan en un foro virtual donde:</p> <ul style="list-style-type: none"> - Identifican los problemas éticos y de comunicación en el caso. - Proponen soluciones respetuosas y argumentan cómo pueden mejorar el ambiente digital. - Reflexionan sobre cómo sus propias interacciones en línea pueden influir en un entorno digital más respetuoso e inclusivo.

Formato 9. Diseño proceso evaluativo de la competencia 1.

PROCESO EVALUATIVO
Competencia n° 2

<i>Elemento n° 1</i>	<i>Indicadores n° 1.1</i>	<i>Criterio</i>	<i>Actividad n° 1.1</i>
1. Observar el comportamiento propio en línea, identificando acciones que podrían poner en riesgo su seguridad digital.	1.1. Reconoce y detalla sus propias prácticas digitales diarias relacionadas con contraseñas, redes públicas y otros hábitos.	Completa el cuestionario con información detallada y relevante.	Actividad de Reflexión Inicial: Los estudiantes completarán un cuestionario de autoevaluación sobre sus prácticas diarias en línea (uso de contraseñas, frecuencia de cambio de las mismas, uso de redes públicas). Esto les ayudará a detallar y reconocer sus propias prácticas.
	Indicadores n° 1.2	Identifica al menos tres comportamientos de riesgo en su autoevaluación.	
	1.2. Identifica comportamientos de riesgo específicos en sus actividades diarias en línea.	Propone una posible mejora para al menos uno de sus hábitos digitales actuales.	
	Indicadores n° 1.3		
	1.3. Completa el cuestionario de autoevaluación con sinceridad y precisión.		
	Indicadores n° 1.4	Participa activamente en discusiones grupales aportando experiencias relevantes.	Análisis de Situaciones Recientes de Riesgo: A partir de ejemplos comunes de situaciones de riesgo digital, los estudiantes trabajarán en parejas o pequeños grupos para discutir y analizar sus propias experiencias. Luego, documentan ejemplos específicos donde hayan percibido riesgos, explicando cómo ciertos comportamientos pueden exponerlos a amenazas en línea. Esta actividad fomenta el diálogo y ayuda a relacionar sus experiencias con prácticas seguras.
	1.4. Analiza ejemplos de situaciones de riesgo digital y establece similitudes con sus propias experiencias.	Relaciona sus propios comportamientos con los ejemplos analizados, identificando riesgos comunes.	
	Indicadores n° 1.5	Escribe un análisis detallado que explique cómo ciertos comportamientos pueden llevar a amenazas específicas.	
	1.5. Describe las consecuencias potenciales de comportamientos de riesgo discutidos en el grupo.		
	Indicadores n° 1.6		
	1.6. Documenta experiencias personales con un análisis claro de las amenazas percibidas.		
	Indicadores n° 1.7	Responde a todos los puntos de la lista de verificación con precisión y	Aplicación de Lista de Verificación de Seguridad: Con el fin de comprobar y reforzar las prácticas seguras,
	1.7. Completa la lista de verificación		

	evaluando sus prácticas en línea frente a estándares de seguridad.	honestidad.	los estudiantes utilizarán una lista de verificación que cubra aspectos clave de seguridad digital (uso de contraseñas seguras, autenticación en dos pasos, manejo de redes públicas). Evaluarán en qué medida sus propias prácticas se alinean con estas pautas seguras y anotarán áreas de mejora.
	Indicadores n° 1.8	Identifica al menos dos debilidades en sus hábitos digitales.	
	1.8. Identifica áreas de mejora específicas basadas en la evaluación realizada.	Presenta un plan de acción con pasos concretos para mejorar al menos dos de las áreas identificadas.	
	Indicadores n° 1.9		
	1.9. Propone al menos dos cambios en sus prácticas digitales actuales para alinearlas con las pautas seguras.		

Formato 9. Diseño proceso evaluativo de la competencia 2.

PROCESO EVALUATIVO			
Competencia n° 2			
Elemento n° 2	Indicadores n° 2.1	Criterio	Actividad n° 1.1
2. Ejemplificar medidas de protección digital en escenarios simulados.	2.1 Identifica correctamente al menos tres medidas de seguridad digital relevantes para escenarios específicos.	Enumera al menos tres medidas específicas (contraseñas seguras, autenticación en dos pasos, evitar enlaces sospechosos) por escenario.	Creación de Ejemplos Concretos de Medidas de Protección Digital: Cada estudiante desarrollará una lista detallada que incluya ejemplos de medidas de seguridad digital para cada escenario de riesgo presentado, como el uso de contraseñas seguras, autenticación en dos pasos, y evitar enlaces sospechosos. Este ejercicio refuerza su habilidad para reconocer y aplicar prácticas seguras.
	Indicadores n° 2.2	Explica cómo cada medida reduce el riesgo en el escenario presentado.	
	2.2 Relaciona cada medida de protección digital con el escenario de riesgo presentado, justificando su elección.	Propone soluciones preventivas adicionales, mostrando un análisis crítico y comprensión profunda de las amenazas digitales	
	Indicadores n° 2.3		
	2.3 Propone al menos dos acciones preventivas adicionales para fortalecer la seguridad en cada caso.		

	Indicadores n° 2.4	Describe claramente el escenario hipotético y las amenazas asociadas. Detalla al menos tres medidas de protección aplicables al escenario, explicando cómo estas mitigan las amenazas. Reflexiona sobre la efectividad de sus decisiones, proponiendo al menos una mejora para futuras situaciones similares.	Simulación de situaciones hipotética: Se presentarán situaciones hipotéticas adicionales, como el uso de una red pública para realizar una transacción bancaria o recibir un mensaje de phishing en redes sociales. Los estudiantes elegirán una situación e, individualmente, escribirán un texto explicando qué medidas tomarían y cómo responderían para protegerse, justificando cada paso de acuerdo con su conocimiento de seguridad digital.
	2.4 Analiza las características del escenario hipotético, identificando las amenazas presentes (phishing, redes públicas inseguras, etc.).		
	Indicadores n° 2.5		
	2.5 Explica detalladamente las medidas de protección aplicadas en el escenario, justificando cada acción tomada.		
	Indicadores n° 2.6		
	2.6 Evalúa la eficacia de las medidas propuestas, reflexionando sobre posibles limitaciones o mejoras.		

Formato 9. Diseño proceso evaluativo de la competencia 2.

PROCESO EVALUATIVO			
Competencia n° 2			
Elemento n° 3	Indicadores n° 3.1	Criterio	Actividad n° 1.1
3. Examinar comportamientos de riesgo en sus propias actividades en línea.	3.1 Completa el cuestionario de autoevaluación detallando sus hábitos digitales actuales.	Responde a todas las preguntas de la autoevaluación con información precisa y relevante.	Actividad de Autoevaluación: Cada estudiante completa una autoevaluación diseñada para identificar comportamientos de riesgo en sus actividades en línea. La autoevaluación incluye preguntas sobre sus hábitos digitales, como la frecuencia de actualización de contraseñas, el uso de autenticación en dos pasos, y la gestión de información personal. Al finalizar, cada estudiante identifica al menos tres comportamientos de riesgo específicos en sus
	Indicadores n° 3.2	Identifica correctamente al menos tres áreas de riesgo en sus hábitos digitales actuales.	
	1.2 Identifica al menos tres comportamientos de riesgo específicos en sus prácticas digitales diarias.		
	Indicadores n° 3.3	Presenta una reflexión breve y clara sobre el impacto de los comportamientos de riesgo identificados.	
	3.3 Reflexiona sobre las posibles		

	consecuencias de los comportamientos de riesgo detectados.		prácticas actuales.
	Indicadores n° 3.4	<p>Incluye un mínimo de tres acciones concretas en su plan de acción, como actualizar contraseñas periódicamente, evitar redes públicas inseguras, o habilitar la autenticación en dos pasos.</p> <p>Las metas establecidas son claras, alcanzables y están alineadas con los riesgos detectados. Justifica cada acción propuesta con argumentos basados en la importancia de las medidas de seguridad digital.</p>	<p>Desarrollo de un Plan de Acción:</p> <p>A partir de la autoevaluación y las discusiones grupales, cada estudiante elabora un plan de acción con pasos específicos para reducir los riesgos identificados en su actividad en línea. Este plan incluye al menos tres cambios concretos, como actualizar contraseñas periódicamente, usar redes seguras y habilitar la autenticación en dos pasos, con metas y fechas para implementar cada cambio.</p>
	3.4 Define al menos tres cambios específicos en sus hábitos digitales para reducir los riesgos identificados.		
	Indicadores n° 3.5		
	3.5 Establece metas concretas y realistas con fechas específicas para implementar cada cambio.		
	Indicadores n° 3.6		
	2.3 Justifica las acciones propuestas, explicando cómo contribuirán a mejorar su seguridad en línea.		

Formato 9. Diseño proceso evaluativo de la competencia 2.

PROCESO EVALUATIVO			
Competencia n° 3			
Elemento n° 1	Indicadores n° 1.1	Criterio	Actividad n° 1.1
Identifica comportamientos éticos e inadecuados en entornos digitales.	Distingue entre comportamientos éticos y no éticos en casos reales o simulados, justificando sus elecciones.		Análisis de casos prácticos: Presenta a los estudiantes casos reales o ficticios de comportamientos éticos e inadecuados en entornos digitales (por ejemplo, ciberacoso, suplantación de identidad, plagio). Donde los estudiantes deben identificar los comportamientos presentes, analicen las consecuencias éticas y propongan alternativas responsables.
	Indicadores n° 1.2	El estudiante identifica correctamente las posibles consecuencias de las conductas inadecuadas (legales, sociales o éticas).	
	Analiza casos de ciberacoso y señala las acciones que violan la ética digital.		
	Indicadores n° 1.3	El estudiante demuestra un	

	Reconoce las consecuencias de compartir información sensible o actuar de forma inadecuada en línea.	razonamiento lógico y ético consistente al analizar situaciones relacionadas con comportamientos en línea.	
	Indicadores n° 1.4		
	Conoce y respeta los términos y condiciones de uso en plataformas digitales.		

Formato 9. Diseño proceso evaluativo de la competencia 3.

PROCESO EVALUATIVO			
Competencia n° 3			
Elemento n° 2	Indicadores n° 2.1	Criterio	Actividad n° 1.1
Prioriza el respeto y la responsabilidad en la interacción digital.	El estudiante participa activamente en un foro, utilizando lenguaje respetuoso y fomentando un ambiente positivo y colaborativo.	El estudiante evidencia respeto y responsabilidad en sus interacciones digitales al utilizar un lenguaje adecuado, compartir información verificada, cumplir con las normas de la plataforma y manejar la información de manera ética. Además, promueve un ambiente colaborativo y constructivo al resolver conflictos de forma pacífica y respetuosa.	Instrucciones: Crea un foro en la plataforma educativa o utiliza una herramienta de discusión digital (Moodle). Plantea un caso práctico relacionado con la interacción digital, por ejemplo: "Un estudiante publica un meme sobre un compañero sin su permiso en un grupo escolar. ¿Qué harías en esta situación y por qué?" Desarrollo: Cada estudiante debe responder al caso en el foro utilizando lenguaje respetuoso y argumentando su posición. Luego, deben comentar al menos dos publicaciones de compañeros, aportando ideas constructivas o alternativas al planteamiento inicial. Cierre: Revisa las interacciones en el foro junto con los estudiantes, destacando ejemplos positivos de respeto y responsabilidad.
	Indicadores n° 2.2		
	El estudiante crea un mensaje o campaña digital que promueve valores de respeto y responsabilidad en el uso de las redes sociales.		
	Indicadores n° 2.3		
	El estudiante verifica la información antes de compartirla para evitar la propagación de noticias falsas o contenido inapropiado.		
	Indicadores n° 2.4		
	El estudiante evita publicar contenido que pueda dañar la		

	privacidad o reputación de otras personas.		<p>Reflexiona con ellos sobre cómo estas habilidades pueden aplicarse en otros contextos digitales.</p> <p>Evaluación: Utiliza una rúbrica basada en indicadores como lenguaje respetuoso, argumentación clara, cumplimiento de normas y actitud constructiva en los comentarios.</p>
--	--	--	--

Formato 9. Diseño proceso evaluativo de la competencia 3.

PROCESO EVALUATIVO			
Competencia n° 3			
Elemento n° 3	Indicadores n° 3.1	Criterio	Actividad n° 1.1
Aplica principios éticos al uso de información en línea.	Un reporte o presentación en la que el estudiante examina los casos reales, identificando los problemas éticos, los comportamientos inapropiados y las acciones correctivas.	<p>El estudiante debe ser capaz de analizar casos reales relacionados con el uso de información en línea, identificando problemas éticos, comportamientos inapropiados y posibles acciones correctivas. Se valorará la habilidad para proponer soluciones éticas frente a situaciones como la información falsa, demostrando un razonamiento crítico y fundamentado.</p> <p>Además, se tomará en cuenta la reflexión sobre el impacto de las decisiones tomadas en los casos analizados, evaluando cómo estas afectaron a los involucrados y su repercusión social, evidenciando una comprensión integral de las implicaciones</p>	<p>Detectives éticos en el entorno digital:</p> <p>Objetivo: Analizar casos reales relacionados con el uso ético de la información en línea y reflexionar sobre las implicaciones sociales de las decisiones tomadas.</p> <p>Preparación: Proporciona a los estudiantes una selección de casos reales relacionados con:</p> <ul style="list-style-type: none"> -Difusión de información falsa o noticias falsas. -Violaciones de privacidad o mal uso de datos personales. <p>Trabajo en grupos: Se divide a los estudiantes en equipos pequeños (4-6) y se les asigna un caso específico. Cada equipo deberá analizar su caso y responder las siguientes preguntas:</p> <ul style="list-style-type: none"> ¿Qué problemas éticos se identifican en este caso? ¿Qué comportamientos fueron inapropiados y por qué? ¿Qué acciones correctivas se
	Indicadores n° 3.2		
	En un análisis de casos, el estudiante propone soluciones éticas para problemas como el plagio o la difusión de información falsa.		
	Indicadores n° 3.3		
	Reflexión sobre cómo las decisiones tomadas en los casos reales afectaron a los involucrados y el impacto social de dichas acciones.		

		éticas en el entorno digital.	<p>podrían haber tomado?</p> <p>Propuesta de soluciones: Cada equipo redactará una propuesta ética con soluciones específicas al problema planteado, argumentando su razonamiento.</p> <p>Presentación final: Los equipos expondrán su caso, análisis y soluciones frente al grupo, fomentando el debate y la retroalimentación.</p> <p>Evaluación: Los estudiantes serán evaluados con base en: -La profundidad y claridad del análisis de los casos. -La viabilidad y fundamentación ética de las soluciones propuestas. -La calidad y reflexión de su aporte individual. -La claridad y organización de su presentación grupal.</p>
--	--	-------------------------------	---

Formato 9. Diseño proceso evaluativo de la competencia 3.

Requerimientos no funcionales

1. Tiempo de respuesta: Las páginas y actividades del sistema deben cargarse en menos de 2 segundos bajo una carga normal de usuarios.
2. Disponibilidad: El sistema debe estar disponible el 99.9% del tiempo durante horas lectivas, con un tiempo de inactividad planificado que no supere las 2 horas por mes.
3. Seguridad y rendimiento: El sistema debe mantener medidas de seguridad efectivas (como encriptación de datos y autenticación en dos pasos) incluso durante picos de hasta 500 usuarios concurrentes.
4. Escalabilidad: El sistema debe ser capaz de manejar hasta 5.000 usuarios simultáneos sin degradar su tiempo de respuesta por encima de los 3 segundos.
5. Mantenimiento:
 - La arquitectura del sistema debe ser modular, permitiendo que actualizaciones de contenido o mejoras en la interfaz no afecten el núcleo del software.
 - Las actualizaciones críticas no deben requerir más de 4 horas de implementación.
6. Compatibilidad:
 - El sistema debe funcionar correctamente en las versiones más recientes de los navegadores Chrome , Firefox , Safari y Edge , así como en dispositivos con sistemas operativos Android e iOS .
 - Debe ser responsivo, adaptándose a pantallas de diferentes tamaños (computadoras, tabletas y teléfonos).
7. Usabilidad:
 - La interfaz debe ser intuitiva, permitiendo que usuarios con conocimientos básicos de informática puedan navegar por el sistema sin asistencia adicional.
 - Debe cumplir con las pautas de accesibilidad (WCAG 2.1 nivel AA), soportando lectores de pantalla y navegación por teclado.
8. Confiabilidad:
 - El sistema debe tener un tiempo medio entre fallos (MTBF) de al menos 6 meses.
 - En caso de fallo, debe recuperarse en menos de 30 minutos (MTTR).
9. Capacidad de Auditoria:
 - Todas las actividades importantes deben registrarse, incluidos accesos, cambios en configuración, actualizaciones de contenido y envíos de evaluaciones.
 - Los registros deben conservarse por al menos 12 meses y ser accesibles solo para el administrador autorizado.
 -
10. Interoperabilidad: El sistema debe integrarse con sistemas externos como plataformas de gestión de aprendizaje (LMS) o bases de datos escolares, permitiendo la exportación/importación de datos en formatos estándar como CSV o JSON .

11. Privacidad: Los datos personales de los usuarios deben manejarse conforme a estándares como el GDPR o regulaciones locales aplicables, asegurando la protección contra accesos no autorizados.
12. Capacidad de soporte:
 - El sistema debe incluir documentación técnica y guías de usuario claras para facilitar su uso y resolución de problemas básicos.
 - Debe contar con soporte técnico disponible durante el horario laboral, con un tiempo de respuesta de máximo 1 hora.
13. Rendimiento bajo carga: Durante las pruebas de estrés, el sistema debe mantener una tasa de errores menor al 1% y evitar caídas completas en períodos de alta concurrencia.
14. Portabilidad: El sistema debe ser implementable en entornos de nube y servidores locales sin modificaciones significativas en el código fuente.
15. Integridad de los datos: Todas las operaciones críticas (como evaluaciones, planos de acción y certificaciones) deben contar con confirmación para prevenir pérdidas accidentales de datos.

UML- (Unified Modeling Language) Diagrama de Casos de Uso

Casos de uso para un Software Educativo

Listado de casos de uso para el software educativo orientado a la seguridad digital

Listado General de Casos de Usos

1. Gestionar recursos multimedia
 - Agregar
 - Actualizar
 - Eliminar
2. Realizar actividades de aprendizaje
 - Crear escenarios de riesgo digital
 - Desarrollar contraseñas seguras
 - Autoevaluar los hábitos digitales
 - Personalizar configuraciones de privacidad
 - Desarrollar de un plan de acción personalizado
 - Participar en foros virtuales
3. Realizar evaluaciones de progreso
 - Realizar pruebas
 - Realizar cuestionarios
4. Elaborar un chequeo del progreso
 - Registrar actividades completas e incompletas
 - Actualizar el registro del progreso
5. Observar el progreso en las actividades
 - Permitir ver el progreso en las actividades
 - Eliminar el registro del progreso
6. Adaptar el contenido a diferentes estilos de aprendizaje
7. Certificar competencias en seguridad digital
8. Crear el perfil del usuario

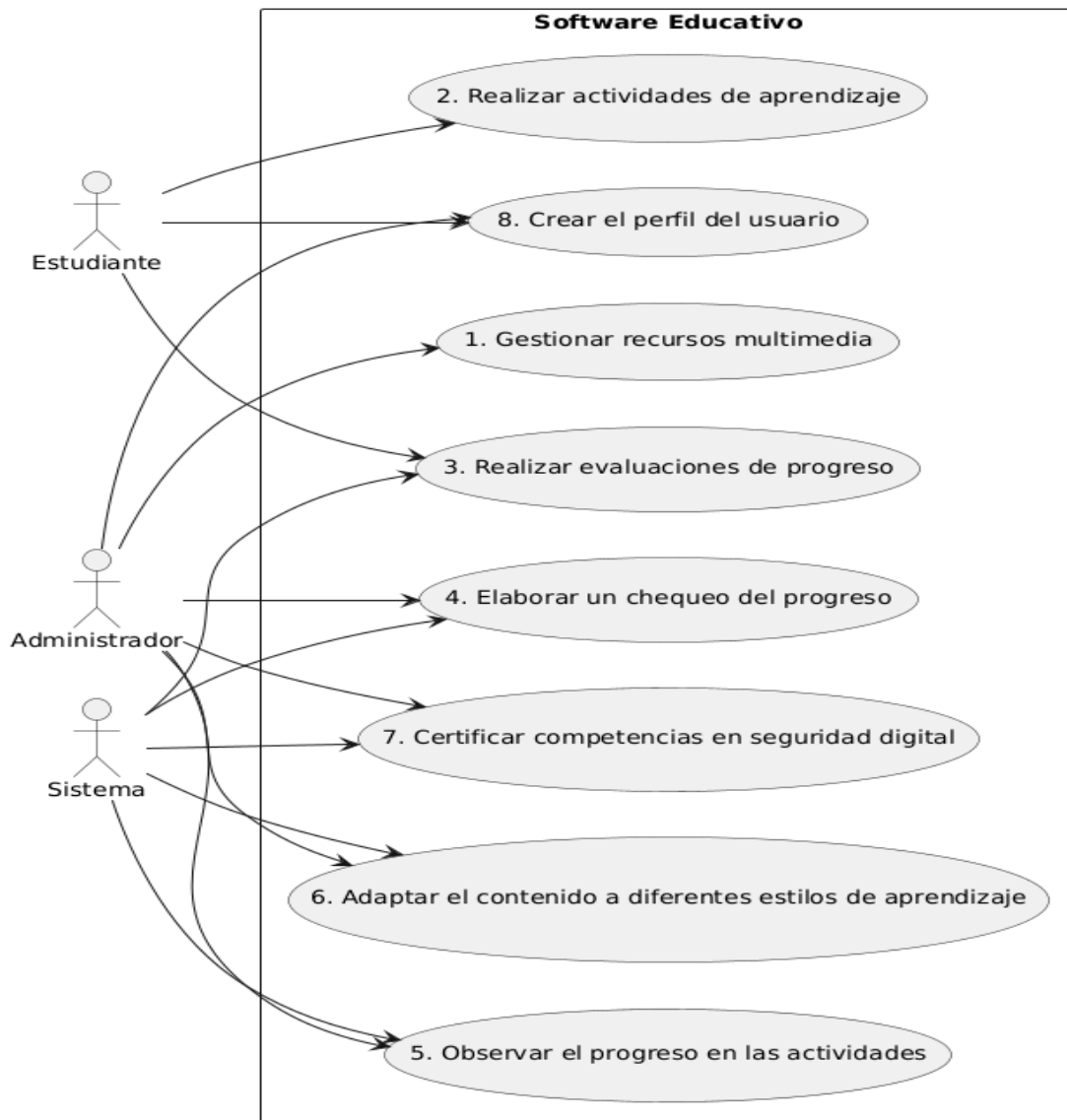


Figura 1. Diagrama de Casos de Uso.

Descripción de Casos de Uso

1. Gestionar recursos multimedia

Descripción:

Permitir al administrador agregar, actualizar y eliminar recursos multimedia como imágenes, videos, y archivos relacionados con la seguridad digital.

Actores:

Administrador

Flujo Principal:

1. El administrador selecciona la opción para gestionar recursos multimedia.
2. Elige entre agregar, actualizar o eliminar un recurso.
3. Realiza la acción correspondiente.
4. Guarda los cambios.

Juan Lopez - Fabian Gomez - Viviana Care

Precondición:

El administrador debe estar autenticado en el sistema.

Postcondición:

Los recursos multimedia son actualizados en el sistema y están disponibles para los usuarios.

2. Realizar actividades de aprendizaje

Descripción:

Permitir a los estudiantes acceder y completar actividades de aprendizaje interactivas relacionadas con la seguridad digital.

Actores:

Estudiante

Flujo Principal:

1. El estudiante inicia sesión y selecciona una actividad de aprendizaje.
2. Completa los pasos o ejercicios requeridos.
3. Envía los resultados.
4. El sistema almacena el progreso del estudiante.

Precondición:

El estudiante debe estar registrado y autenticado.

Postcondición:

El progreso del estudiante queda registrado en el sistema.

3. Realizar evaluaciones de progreso

Descripción:

Permitir al estudiante completar evaluaciones de progreso y al sistema calificar automáticamente dichas evaluaciones.

Actores:

Estudiante, Sistema

Flujo Principal:

1. El estudiante selecciona una evaluación de progreso.
2. Completa las preguntas o ejercicios.
3. El sistema califica automáticamente la evaluación.
4. Muestra los resultados al estudiante.

Precondición:

El estudiante debe haber completado las actividades previas asociadas a la evaluación.

Postcondición:

Se generan los resultados y quedan almacenados en el sistema.

4. Elaborar un chequeo del progreso

Descripción:

Permitir al administrador y al sistema crear y presentar un resumen del progreso de los estudiantes en las actividades y evaluaciones realizadas.

Juan Lopez - Fabian Gomez - Viviana Care

Actores:

Administrador, Sistema

Flujo Principal:

1. El administrador solicita un chequeo del progreso.
2. El sistema compila los datos relevantes.
3. Se genera un reporte detallado del progreso estudiantil.

Precondición:

El sistema debe contar con datos registrados de las actividades y evaluaciones de los estudiantes.

Postcondición:

Se presenta un informe actualizado del progreso de los estudiantes.

5. Observar el progreso en las actividades

Descripción:

Permitir al administrador y al sistema visualizar el progreso de los estudiantes en tiempo real.

Actores:

Administrador, Sistema

Flujo Principal:

1. El administrador accede a la sección de progreso.
2. El sistema muestra un resumen actualizado del avance de cada estudiante.
3. El administrador analiza los datos presentados.

Precondición:

El sistema debe estar actualizado con el progreso registrado de las actividades.

Postcondición:

El administrador obtiene una visión general del avance estudiantil.

6. Adaptar el contenido a diferentes estilos de aprendizaje

Descripción:

Permitir al administrador y al sistema personalizar las actividades y recursos según los estilos de aprendizaje del estudiante.

Actores:

Administrador, Sistema

Flujo Principal:

1. El administrador configura opciones de personalización.
2. El sistema ajusta automáticamente el contenido según las preferencias establecidas.
3. El estudiante accede al contenido personalizado.

Precondición:

El administrador debe estar autenticado y el sistema debe contar con las configuraciones base para personalización.

Postcondición:

El contenido adaptado se refleja en la experiencia del estudiante.

7. Certificar competencias en seguridad digital

Descripción:

Permitir al sistema generar certificaciones digitales para los estudiantes que completen los módulos requeridos y al administrador validar estas certificaciones.

Actores:

Administrador, Sistema

Flujo Principal:

1. El sistema verifica que el estudiante cumple con los requisitos para la certificación.
2. Genera el certificado automáticamente.
3. El administrador valida la certificación emitida.
4. El estudiante descargar su certificado.

Precondición:

El estudiante debe haber completado todos los módulos requeridos.

Postcondición:

El estudiante obtiene un certificado digital de sus competencias.

8. Crear el perfil del usuario

Descripción:

Permitir al estudiante y al administrador configurar y editar los perfiles de usuario con información básica.

Actores:

Estudiante, Administrador

Flujo Principal:

1. El estudiante o administrador accede a la opción de perfil.
2. Ingresa o actualiza información básica (nombre, correo, preferencias).
3. Guarda los cambios realizados.

Precondición:

El usuario debe estar autenticado.

Postcondición:

El perfil queda actualizado en el sistema.

FORMATO DE CASOS DE USO	
Nº cu – 01	Gestionar recursos multimedia
Descripción: Permitir al administrador agregar, actualizar y eliminar recursos multimedia como imágenes, videos, y archivos relacionados con la seguridad digital.	
Actor 1: Usuario	Actor 2: Sistema

Agregar recursos multimedia: El administrador selecciona archivos (imágenes, videos, documentos) desde su dispositivo y los carga al sistema, incluyendo una descripción adecuada.	Validar los formatos y tamaños de archivo: Comprueba que los archivos multimedia cargados cumplen con los requisitos establecidos (formato, tamaño, etc.).
Actualizar recursos multimedia: Edita información existente sobre un recurso multimedia, como cambiar la descripción, reemplazar el archivo o modificar su categoría.	Guardar los recursos multimedia: Almacena los archivos y sus descripciones en la base de datos, garantizando su organización y disponibilidad.
Eliminar recursos multimedia: Selecciona uno o varios recursos y confirma su eliminación del sistema.	Actualizar la información de los recursos: Refleja los cambios realizados por el administrador en tiempo real.
Buscar y filtrar recursos multimedia: Realiza búsquedas específicas utilizando palabras clave o filtros por tipo de archivo, fecha de carga o categoría.	Eliminar recursos de forma segura: Asegura que los archivos eliminados no puedan recuperarse accidentalmente y actualiza la base de datos.
Caminos de excepción	
Actor 1	Actor 2
<p>Carga de archivo no permitida: El usuario intenta subir un archivo con un formato o tamaño no admitido por el sistema (por ejemplo, un archivo mayor a 10 MB o en un formato no compatible como <code>.exe</code>).</p> <ul style="list-style-type: none"> Respuesta del sistema: Mostrar un mensaje de error indicando las restricciones de formato y tamaño, y permitir al usuario intentar nuevamente. <p>Error en la conexión a internet: Durante la carga o actualización de un recurso multimedia, la conexión del usuario se interrumpe.</p> <ul style="list-style-type: none"> Respuesta del sistema: Pausar el proceso y notificar al usuario con un mensaje que le permita reintentar la acción una vez restablecida la conexión. <p>Intento de eliminar un recurso por error: El usuario selecciona un recurso incorrecto para eliminar y lo confirma accidentalmente.</p> <ul style="list-style-type: none"> Respuesta del sistema: Proporcionar una opción de "Deshacer" que permita recuperar el recurso eliminado dentro de un tiempo limitado. <p>Recurso no encontrado al intentar actualizarlo: El usuario intenta actualizar un recurso que ha sido eliminado previamente por otro administrador.</p> <ul style="list-style-type: none"> Respuesta del sistema: Mostrar un mensaje de error indicando que el recurso ya no está 	<p>Fallo en la base de datos: El sistema no puede guardar, actualizar o eliminar un recurso debido a problemas técnicos con la base de datos.</p> <ul style="list-style-type: none"> Respuesta del sistema: Mostrar un mensaje al usuario informando que hay un error técnico y guardar un registro del problema en el sistema de logs para su posterior resolución. <p>Archivo corrupto: El archivo cargado por el usuario está dañado y no puede ser procesado por el sistema.</p> <ul style="list-style-type: none"> Respuesta del sistema: Notificar al usuario sobre el problema, solicitando que suba un archivo válido. <p>Espacio de almacenamiento insuficiente: El sistema no puede guardar un recurso multimedia porque se ha alcanzado el límite de almacenamiento.</p> <ul style="list-style-type: none"> Respuesta del sistema: Informar al usuario sobre la falta de espacio, proporcionando opciones para liberar espacio eliminando recursos innecesarios. <p>Conflicto de versión: Dos usuarios intentan actualizar o eliminar el mismo recurso al mismo tiempo, generando conflictos en la base de datos.</p> <ul style="list-style-type: none"> Respuesta del sistema: Bloquear la acción duplicada y notificar al segundo usuario que el recurso está siendo modificado por otro

disponible y ofrecer opciones para gestionar otros recursos	administrador.	
Puntos de extensión		
Autor	Requerimiento	Modificación
	<p>Requerimiento funcional: El sistema debe permitir al administrador gestionar (agregar, actualizar y eliminar) recursos multimedia, como imágenes, videos y documentos relacionados con la seguridad digital, asegurándose de validar los formatos y tamaños permitidos.</p> <p>Requerimiento no funcional: El sistema debe procesar las solicitudes de carga de archivos multimedia en un tiempo máximo de 5 segundos y garantizar la seguridad de los datos mediante protocolos de cifrado durante la transferencia.</p>	<p>Modificación en la funcionalidad: Agregar la posibilidad de etiquetar recursos multimedia con categorías específicas, permitiendo una mejor organización y búsqueda de los archivos dentro del sistema.</p> <p>Modificación en la interfaz: Rediseñar la interfaz de gestión para que sea más intuitiva, implementando funciones de arrastrar y soltar (drag-and-drop) para cargar archivos multimedia y un visor previo de los recursos cargados.</p>

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
Nº cu – 02	Realizar actividades de aprendizaje
Descripción: Permitir a los estudiantes acceder y completar actividades de aprendizaje interactivas relacionadas con la seguridad digital.	
Actor 1: Usuario	Actor 2: Sistema
Inicia sesión en la plataforma educativa para acceder al módulo de actividades interactivas.	Presenta al estudiante una lista organizada de actividades interactivas según su progreso o nivel.
Selecciona una actividad específica relacionada con la seguridad digital desde la lista disponible.	Valida las respuestas del estudiante y genera retroalimentación en tiempo real.
Resuelve preguntas o ejercicios prácticos interactivos, como simulaciones, cuestionarios o actividades de arrastrar y soltar.	Guarda el progreso del estudiante y actualiza los registros de finalización de actividades.
Envía las respuestas o completa las actividades para recibir retroalimentación inmediata.	Genera reportes detallados del desempeño del estudiante para que pueda revisar su aprendizaje.
Caminos de excepción	

Actor 1		Actor 2	
Error al iniciar sesión: <ul style="list-style-type: none">El estudiante ingresa credenciales incorrectas, lo que impide acceder a las actividades. Solución: Mostrar un mensaje de error e instrucciones para recuperar la contraseña. Actividad no cargada correctamente: <ul style="list-style-type: none">Problemas de conectividad o errores en la plataforma que impiden que la actividad se despliegue. Solución: Mostrar un mensaje indicando problemas técnicos e intentar recargar la actividad. Dudas en la comprensión de la actividad: <ul style="list-style-type: none">El estudiante no comprende las instrucciones para completar la actividad. Solución: Incluir un botón de ayuda con explicaciones detalladas o ejemplos de resolución. Progreso no guardado: <ul style="list-style-type: none">El estudiante completa parte de la actividad, pero la plataforma no guarda su avance debido a un fallo técnico. Solución: Implementar un sistema de guardado automático y permitir al estudiante reanudar desde el último punto guardado.		Fallo en la validación de respuestas: <ul style="list-style-type: none">El sistema no puede evaluar las respuestas debido a un error en los algoritmos de validación. Solución: Mostrar un mensaje de error y permitir al estudiante enviar la actividad más tarde. Datos del estudiante no actualizados: <ul style="list-style-type: none">El sistema no registra correctamente el progreso del estudiante por problemas en la base de datos. Solución: Crear copias de respaldo temporales y sincronizar datos una vez se solucione el error. Interrupción del servicio: <ul style="list-style-type: none">La plataforma educativa experimenta una caída del sistema, interrumpiendo la actividad. Solución: Notificar al estudiante sobre el incidente y garantizar la reanudación desde el último punto guardado al restaurar el servicio. Acceso a actividades bloqueado: <ul style="list-style-type: none">El sistema detecta al estudiante como no autorizado por error. Solución: Permitir una verificación manual de permisos por parte del administrador o soporte técnico.	
Puntos de extensión			
Autor	Requerimiento		Modificación
	Requerimiento funcional: <ul style="list-style-type: none">El sistema debe permitir a los estudiantes acceder a actividades interactivas relacionadas con la seguridad digital, presentando retroalimentación inmediata	Modificación de contenido: <ul style="list-style-type: none">Actualizar las actividades existentes para incluir nuevas amenazas digitales o tendencias en ciberseguridad, asegurando que los contenidos estén	

	<p>para cada respuesta.</p> <p>Requerimiento no funcional:</p> <ul style="list-style-type: none"> La plataforma debe garantizar que las actividades carguen completamente en menos de 5 segundos bajo condiciones normales de red. 	<p>alineados con las necesidades actuales.</p> <p>Modificación técnica:</p> <ul style="list-style-type: none"> Mejorar la funcionalidad del guardado automático para que almacene el progreso del estudiante cada vez que complete una pregunta o tarea parcial, minimizando la pérdida de datos ante interrupciones.
--	--	---

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
Nº cu – 03	Realizar evaluaciones de progreso
<p>Descripción: Ofrecer a los estudiantes la oportunidad de realizar evaluaciones que midan su nivel de conocimiento y aprendizaje. Estas evaluaciones son calificadas automáticamente por el sistema, lo que permite proporcionar retroalimentación inmediata y personalizada. Están diseñadas como herramientas de autoevaluación, ayudando a los estudiantes a identificar áreas de mejora y asegurando que cumplan con los objetivos establecidos en las actividades previas.</p> <p>Este caso de uso incluye todo el proceso, desde la selección de la evaluación por parte del estudiante, la resolución de preguntas o ejercicios, hasta la generación automática de calificaciones y la presentación de resultados detallados.</p>	
Actor 1: Usuario	Actor 2: Sistema
Resolver las preguntas o ejercicios proporcionados en la evaluación	Proveer las preguntas de la evaluación, registrar las respuestas del estudiante, calificar automáticamente y generar resultados.
El estudiante debe haber iniciado sesión en el sistema y haber completado todas las actividades previas relacionadas con la evaluación. Esto asegura que esté preparado para abordar el contenido evaluativo.	Debe estar programado con un algoritmo que permita calificar automáticamente las respuestas y mostrar resultados al estudiante en tiempo real.
Responder correctamente las preguntas para demostrar su conocimiento.	Procesar las respuestas y generar resultados confiables y precisos.
Caminos de excepción	
Actor 1	Actor 2

Si el estudiante no cumple con las actividades previas asociadas, no podrá acceder a la evaluación. El sistema debería mostrar un mensaje de advertencia indicando qué actividades faltan por completar. Otro caso podría ser que el estudiante abandone la evaluación a la mitad; en este escenario, el sistema debe guardar su progreso parcial y permitirle retomarla más tarde.	Si ocurre un error técnico, como una caída del sistema o un fallo al calificar automáticamente, el sistema debe registrar el problema y notificar al administrador para su solución. También debe garantizar que el estudiante pueda volver a realizar la evaluación sin pérdida de datos.	
Puntos de extensión		
Análisis detallado de resultados: Después de la evaluación, el sistema podría generar un informe completo que destaque las preguntas incorrectas y brinde explicaciones o recursos adicionales para mejorar en las áreas débiles.		
Personalización de las evaluaciones: Permitir que las preguntas se adapten al nivel de conocimiento del estudiante en tiempo real, ofreciendo una experiencia más personalizada.		
Integración con certificaciones: Relacionar el desempeño en evaluaciones con la obtención de certificaciones.		
Autor	Requerimiento	Modificación
	El estudiante debe haber completado las actividades de aprendizaje previas asociadas a la evaluación.	Implementar herramientas de análisis avanzado para que los resultados sean más informativos y detallados.
	El sistema debe contar con un módulo de calificación automática que garantice resultados precisos y rápidos.	Permitir la integración con plataformas externas de aprendizaje para mejorar la experiencia del usuario.
	El diseño del sistema debe permitir al estudiante retomar evaluaciones en caso de interrupciones.	Agregar funcionalidad para generar reportes personalizados de progreso.

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
N° cu – 04	Elaborar un chequeo del progreso
<p>Descripción: El propósito de este caso de uso es permitir al administrador y al sistema generar un informe detallado sobre el progreso de los estudiantes. Este informe incluye datos sobre actividades completadas, evaluaciones realizadas, resultados obtenidos y áreas de mejora. El administrador utiliza este informe para analizar el desempeño general y tomar decisiones informadas sobre estrategias de enseñanza.</p> <p>Este caso cubre desde la solicitud del informe por parte del administrador hasta la compilación de los datos y la presentación del reporte en un formato claro y comprensible.</p>	
Actor 1: Usuario	Actor 2: Sistema
Solicitar un informe que detalle el progreso de los	Generar el informe basado en los datos disponibles

estudiantes en las actividades y evaluaciones realizadas.	sobre el desempeño de los estudiantes.	
Debe estar autenticado en el sistema y contar con los permisos necesarios para acceder a la información de los estudiantes.	El sistema debe contar con una base de datos actualizada que incluya información completa y precisa sobre las actividades y evaluaciones realizadas.	
Analizar los informes generados para identificar áreas de mejora o destacar logros específicos.	Garantizar la generación de un informe confiable y fácilmente comprensible para el administrador.	
Caminos de excepción		
Actor 1	Actor 2	
Si el administrador solicita un informe, pero no existen suficientes datos registrados en el sistema, este debe notificar al administrador sobre la falta de información y sugerir posibles soluciones, como completar más actividades.	Si ocurre un error durante la compilación de datos (por ejemplo, problemas de conexión con la base de datos), el sistema debe registrar el error, notificar al administrador y permitir la generación del informe una vez solucionado.	
Puntos de extensión		
<p>Gráficos dinámicos y visuales: Incorporar gráficos interactivos para que el administrador visualice patrones y tendencias de progreso.</p> <p>Exportación de datos: Permitir la descarga del informe en diferentes formatos, como PDF o Excel, para facilitar el análisis externo.</p> <p>Alertas personalizadas: Generar notificaciones automáticas cuando se detecten estudiantes con bajo desempeño o quienes no estén completando las actividades.</p>		
Autor	Requerimiento	Modificación
	<p>Una base de datos completa y actualizada con información sobre el progreso de los estudiantes.</p> <p>Herramientas dentro del sistema para procesar y presentar datos de manera clara y visual.</p> <p>Permisos de acceso para que el administrador pueda consultar esta información.</p>	<p>Añadir opciones de personalización en los informes para adaptarlos a necesidades específicas del administrador.</p> <p>Implementar inteligencia artificial para identificar patrones en los datos y sugerir mejoras en las estrategias educativas.</p>

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
Nº cu – 05	Observar el progreso en las actividades

Descripción:El monitorear y registrar el avance de los estudiantes en las actividades educativas de manera sistemática. Permite generar reportes automáticos sobre la participación, el tiempo invertido, las tareas completadas y las áreas donde el estudiante enfrenta mayores dificultades. Además, incluye herramientas de autoevaluación y retroalimentación en tiempo real para que los estudiantes puedan reflexionar sobre su aprendizaje.		
Actor 1: Usuario		Actor 2: Sistema
Monitoreo de los avances de las actividades de los estudiantes.		Funcionalidad de alertas para actividades pendientes o atrasadas.
El encargado debe estar autenticado como docente.		Indicadores visuales de progreso (gráficos, barras de avance, estadísticas).
Analizar las actividades y calificar actividades		Indicadores visuales de progreso (gráficos, barras de avance, estadísticas).
		Indicadores visuales de progreso (gráficos, barras de avance, estadísticas).
Caminos de excepción		
Actor 1		Actor 2
Si el administrador solicita un informe, pero no existen suficientes datos registrados en el sistema, este debe notificar al administrador sobre la falta de información y sugerir posibles soluciones, como completar más actividades.		Si ocurre un error durante la compilación de datos (por ejemplo, problemas de conexión con la base de datos), el sistema debe registrar el error, notificar al administrador y permitir la generación del informe una vez solucionado.
Puntos de extensión		
Los estudiantes pueden observar su avance en tiempo real a través de gráficas y barras de progreso, lo que los motiva a completar las actividades pendientes. Además, reciben alertas personalizadas que los ayudan a priorizar tareas.		
Algunos usuarios pueden sentirse abrumados si ven retrasos acumulados en su progreso; sin embargo, la retroalimentación positiva ayuda a mejorar su confianza.		
Autor	Requerimiento	Modificación
	Generar reportes automáticos sobre el avance de los estudiantes. Permitir la visualización de indicadores como tareas completadas, porcentaje de avance y calificaciones. Alertar a los usuarios sobre actividades pendientes o próximas a vencer. Exportar reportes en formatos estándar (PDF, Excel). Ofrecer filtros por estudiante, grupo,	Análisis predictivo: Integrar herramientas de inteligencia artificial (IA) para prever posibles dificultades o áreas de mejora de los estudiantes. Gamificación: Incorporar insignias, logros o recompensas virtuales basadas en el progreso para motivar a los usuarios. Reportes avanzados: Permitir a los docentes generar reportes personalizados con comparativas

	<p>actividad o tiempo.</p> <p>Sistema de base de datos robusto para almacenar registros de actividades.</p> <p>Integración con sistemas LMS (Learning Management System) existentes.</p> <p>Infraestructura para soportar múltiples usuarios concurrentes.</p>	<p>históricas y tendencias de aprendizaje.</p> <p>Interoperabilidad: Hacer compatible el sistema con nuevos LMS o herramientas de análisis externo.</p>
--	--	--

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
Nº cu – 06	Adaptar el contenido a diferentes estilos de aprendizaje
<p>Descripción: Busca proporcionar recursos educativos diseñados para atender la diversidad de estilos de aprendizaje de los estudiantes. Ofrece materiales interactivos, como simulaciones, videos, textos enriquecidos y actividades prácticas, adaptados a los estilos visual, auditivo y kinestésico. También incluye opciones de personalización del contenido según las preferencias del usuario.</p>	
Actor 1: Usuario	Actor 2: Sistema
Realizar Estudio para saber los tipos de aprendizaje más comunes en la población.	Proveer una biblioteca multimedia con recursos en distintos formatos (videos, audios, textos interactivos).
Diseño de Material educativo para los estudiantes de forma que abarque diferentes tipos de aprendizaje	Evaluar el estilo de aprendizaje del usuario mediante un cuestionario inicial.
Acceso a los materiales en todo momento para fomentar el trabajo independiente	Permitir la personalización de las actividades según el estilo de aprendizaje. Habilitar una opción para descargar materiales educativos.
Caminos de excepción	
Actor 1	Actor 2
Si el estudiante no cumple con las actividades previas asociadas, no podrá acceder a la evaluación. El sistema debería mostrar un mensaje de advertencia indicando qué actividades faltan por completar. Otro caso podría ser que el estudiante abandone la evaluación a la mitad; en este escenario, el sistema debe guardar su progreso parcial y permitirle retomarla más tarde.	Si ocurre un error técnico, como una caída del sistema o un fallo al calificar automáticamente, el sistema debe registrar el problema y notificar al administrador para su solución. También debe garantizar que el estudiante pueda volver a realizar la evaluación sin pérdida de datos.

Puntos de extensión		
<p>Los usuarios se sienten más comprometidos porque pueden acceder a materiales que se adaptan a su forma preferida de aprender (videos para visuales, audios para auditivos, simulaciones para kinestésicos).</p> <p>Los docentes pueden diseñar actividades variadas que sean atractivas para toda la clase, fomentando una mejor comprensión de los temas.</p> <p>La necesidad de probar diferentes formatos antes de encontrar el que mejor se adapte a su estilo puede ser algo confusa inicialmente.</p> <p>Crear o seleccionar recursos específicos para todos los estilos puede tomar tiempo adicional durante la planificación.</p>		
Autor	Requerimiento	Modificación
	<p>Gamificación: Integrar elementos de juego, como insignias o puntos, para aumentar la motivación en todos los módulos.</p> <p>Tutoriales iniciales: Asegurar que tanto docentes como estudiantes reciban una guía clara para navegar por los módulos.</p> <p>Soporte técnico: Ofrecer asistencia en tiempo real para resolver problemas durante el uso de la plataforma.</p>	<p>Proveer una biblioteca multimedia con recursos en distintos formatos (videos, audios, textos interactivos).</p> <p>Evaluar el estilo de aprendizaje del usuario mediante un cuestionario inicial.</p> <p>Permitir la personalización de las actividades según el estilo de aprendizaje.</p> <p>Habilitar una opción para descargar materiales educativos.</p>

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO	
Nº cu – 07	Certificar competencias en seguridad digital
<p>Descripción: Está diseñado para evaluar y validar las competencias adquiridas por los estudiantes en temas de ciberseguridad. Incluye evaluaciones prácticas, simulaciones y cuestionarios basados en rúbricas previamente definidas. Al final del proceso, los estudiantes reciben una certificación digital que valida su conocimiento y habilidades en seguridad informática.</p>	
Actor 1: Usuario	Actor 2: Sistema
Los estudiantes pueden observar su avance en tiempo real a través de gráficas y barras de progreso, lo que los motiva a completar las actividades pendientes. Además, reciben alertas personalizadas que los ayudan a priorizar tareas.	Garantizar que las Actividades sean Realizadas correctamente y relevantes puede requerir ajustes técnicos periódicos.

Los docentes tienen acceso a informes claros que les permiten identificar qué estudiantes necesitan apoyo adicional, optimizando el tiempo de intervención.	El sistema debe permitir validar el aprendizaje de manera objetiva, facilitando la evaluación de competencias individuales y grupales.	
Caminos de excepción		
Actor 1	Actor 2	
Obtener una certificación digital les proporciona una sensación de logro y les motiva a completar el programa. Las simulaciones les permiten aplicar conocimientos en escenarios prácticos, haciéndolos sentir más seguros en el entorno digital.	El sistema permite validar el aprendizaje de manera objetiva, facilitando la evaluación de competencias individuales y grupales. Garantizar que las simulaciones sean realistas y relevantes puede requerir ajustes técnicos periódicos.	
Puntos de extensión		
Certificación avanzada: Añadir un módulo que permita la emisión de micro certificaciones específicas, como "Dominio de contraseñas seguras" o "Protección en redes públicas."		
Marketplace de certificaciones: Conectar con plataformas de empleo o aprendizaje como LinkedIn, permitiendo a los usuarios mostrar sus logros automáticamente.		
Verificación de certificaciones: Integrar un sistema blockchain o similar para que las certificaciones sean seguras y rastreables.		
Autor	Requerimiento	Modificación
	Escalabilidad: Capacidad de soportar un número creciente de usuarios. Mantenimiento: Procedimientos claros para actualizaciones y resolución de problemas. Interoperabilidad: Integración con otros sistemas educativos y plataformas digitales. Seguridad: Cumplimiento de normativas de protección de datos y prevención de acceso no autorizado.	Certificados verificables: Implementar tecnología blockchain para que las certificaciones sean seguras y verificables globalmente. Microcertificaciones: Ofrecer certificaciones específicas para competencias individuales, como contraseñas seguras o configuración de privacidad. Pruebas dinámicas: Crear bancos de preguntas y escenarios de simulación que se actualicen periódicamente para mantenerse relevantes.

		Integración profesional: como LinkedIn o portafolios digitales para aumentar su valor en el mercado laboral. Vincular los certificados con plataformas
--	--	---

Formato 17. Formato de casos de uso.

FORMATO DE CASOS DE USO		
Nº cu – 08		Crear el perfil del usuario
Descripción: Recopilar y analizar datos personales, académicos y de aprendizaje para crear un perfil único de cada usuario. La información recolectada se utiliza para personalizar la experiencia educativa, adaptar el contenido a sus necesidades y hacer recomendaciones específicas para mejorar el aprendizaje. También permite a los docentes entender mejor las características y necesidades de sus estudiantes.		
Actor 1: Usuario		Actor 2: Sistema
Debe diligenciar los formularios a conciencia y de forma clara para facilitar y mejorar la experiencia tanto del usuario como del encargado del sistema.		Deben crear formatos perfiles detallados proporcionando una mejor comprensión de sus estudiantes, ayudándoles a diseñar estrategias personalizadas de enseñanza.
Notificar los cambios de información relevante con los datos requeridos tales como Cambio de domicilio, número de contacto o correo electrónico.		Completar el formulario inicial de perfil puede parecerles tedioso, aunque se simplifica con una interfaz intuitiva.
Caminos de excepción		
Actor 1		Actor 2
En caso de que no se pueda crear un usuario debe comunicarse con el soporte		En caso de recibir un ticket de petición digital se debe responder con el menor tiempo posible para garantizar una buena experiencia del usuario.
Puntos de extensión		
Se sienten reconocidos y valorados al ver que el sistema adapta el contenido a sus características y progreso personal. Esto fomenta la confianza y el sentido de pertenencia.		
Se sienten reconocidos y valorados al ver que el sistema adapta el contenido a sus características y progreso personal. Esto fomenta la confianza y el sentido de pertenencia.		
Autor	Requerimiento	Modificación

	<p>Formulario inicial de registro y evaluación diagnóstica.</p> <p>Creación de perfiles dinámicos que se actualizan según el progreso y las preferencias.</p> <p>Integración de análisis de datos para personalización de contenidos y actividades.</p> <p>Visualización del perfil del usuario con gráficos e informes detallados.</p>	<p>Interfaz amigable e intuitiva para facilitar el acceso a los datos.</p> <p>Tiempo de respuesta menor a 2 segundos al consultar reportes.</p> <p>Acceso multiplataforma (computadoras, tablets, smartphones).</p> <p>Protección de datos según normativas de seguridad y privacidad (GDPR o Ley 1581 en Colombia).</p>
--	---	--

Formato 17. Formato de casos de uso.

Matriz de prioridad para los casos de uso

Desde el análisis de los requisitos, funcionalidades y el proceso de design thinking, se ha desarrollado una matriz de prioridades para los casos de usos. Esta matriz utiliza una escala con valores específicos para interpretar y asignar importancia a cada caso de uso.

La escala se utiliza como un marco de referencia para evaluar y clasificar la prioridad de cada caso de uso en función de su relevancia y contribución al éxito general del proyecto.

		Urgencia				
Esfuerzo		1- Baja	2- Menor	3- Moderada	4- Alta	5- Obligatoria
	5-Muy alto	5	10	15	20	25
					CU-6	
	4-Alto	4	8	12	16	20
						CU-2 CU-3 CU-7
	3-Medio	3	6	9	12	15
				CU-4	CU-1	
	2-Bajo	2	4	6	8	10
				CU-5		CU-8
	1-Muy bajo	1	2	3	4	5

Matriz de prioridad para los casos de uso

Construcción del diagrama de clases:

1. Qué clases para la gestión de la persistencia de los datos:

1. Clase *Usuario*

Esta clase representa información general para todos los usuarios, incluidos estudiantes y administradores.

Atributos:

- *idUsuario*(int): Identificador único del usuario.
- *nombre*(Cadena): Nombre completo del usuario.
- *correo*(Cadena): Correo electrónico del usuario.
- *contraseña*(Cadena): Contraseña cifrada.
- *rol*(Cadena): Rol del usuario (puede ser "Estudiante" o "Administrador").

Métodos:

- *registrarUsuario*(): Crea un nuevo usuario en el sistema.
- *actualizarUsuario*(): Actualiza la información del usuario.
- *eliminarUsuario*(): Elimina al usuario del sistema.
- *autenticar*(correo: String, contraseña: String): boolean: Verifica las credenciales del usuario.

2. Clase *Estudiante* (heredado de *Usuario*)

Representa a los estudiantes registrados en el sistema.

Atributos (heredados de usuario):

- *progresoGeneral*(flotante): Porcentaje del progreso en las actividades y evaluaciones.

Métodos:

- *consultarProgreso*(): Devuelve el estado general del progreso del estudiante.
- *actualizarProgreso*(actividadCompletada: int): Actualiza el progreso basado en actividades o evaluaciones realizadas.

3. Clase *Administrador* (hereda de *Usuario*)

Representa a los administradores del sistema que gestionan contenido y usuarios.

Métodos adicionales:

- *gestionarRecursosMultimedia*(recurso: *RecursoMultimedia*): Permite al administrador agregar, editar o eliminar recursos.
- *revisarProgresoGeneral*(estudiante: *Estudiante*): Consulta y supervisa el progreso de los estudiantes.
- *generarCertificado*(estudiante: *Estudiante*): Emite un certificado basado en las competencias alcanzadas.

4. Clase *RecursoMultimedia*

Representa los recursos multimedia del sistema.

Atributos:

- *idRecurso(int): Identificador único del recurso.*
- *titulo(Cadena): Título del recurso multimedia.*
- *tipo(Cadena): Tipo de recurso (video, imagen, documento, etc.).*
- *url(Cadena): Ruta o enlace del recurso.*
- *descripcion(Cadena): Detalles del recurso.*

Métodos:

- *crearRecurso(): Permite agregar un recurso nuevo.*
- *actualizarRecurso(): Actualiza un recurso existente.*
- *eliminarRecurso(): Eliminar un recurso.*
- *buscarRecurso(palabraClave: String): List<RecursoMultimedia>: Busca recursos relacionados por palabras clave.*

5. ClaseActividad

Representa actividades de aprendizaje para los estudiantes.

Atributos:

- *idActividad(int): Identificador único de la actividad.*
- *titulo(Cadena): Nombre de la actividad.*
- *descripcion(Cadena): Detalles de la actividad.*
- *idRecurso(int): Referencia al recurso multimedia asociado.*
- *estado(Cadena): Estado de la actividad (completada, pendiente, etc.).*

Métodos:

- *crearActividad(): Crea una nueva actividad.*
- *actualizarActividad(): Permite modificar una actividad existente.*
- *completarActividad(estudiante: Estudiante): Marca la actividad como completada para el estudiante.*

6. ClaseEvaluacion

Representa las evaluaciones asociadas a actividades o módulos.

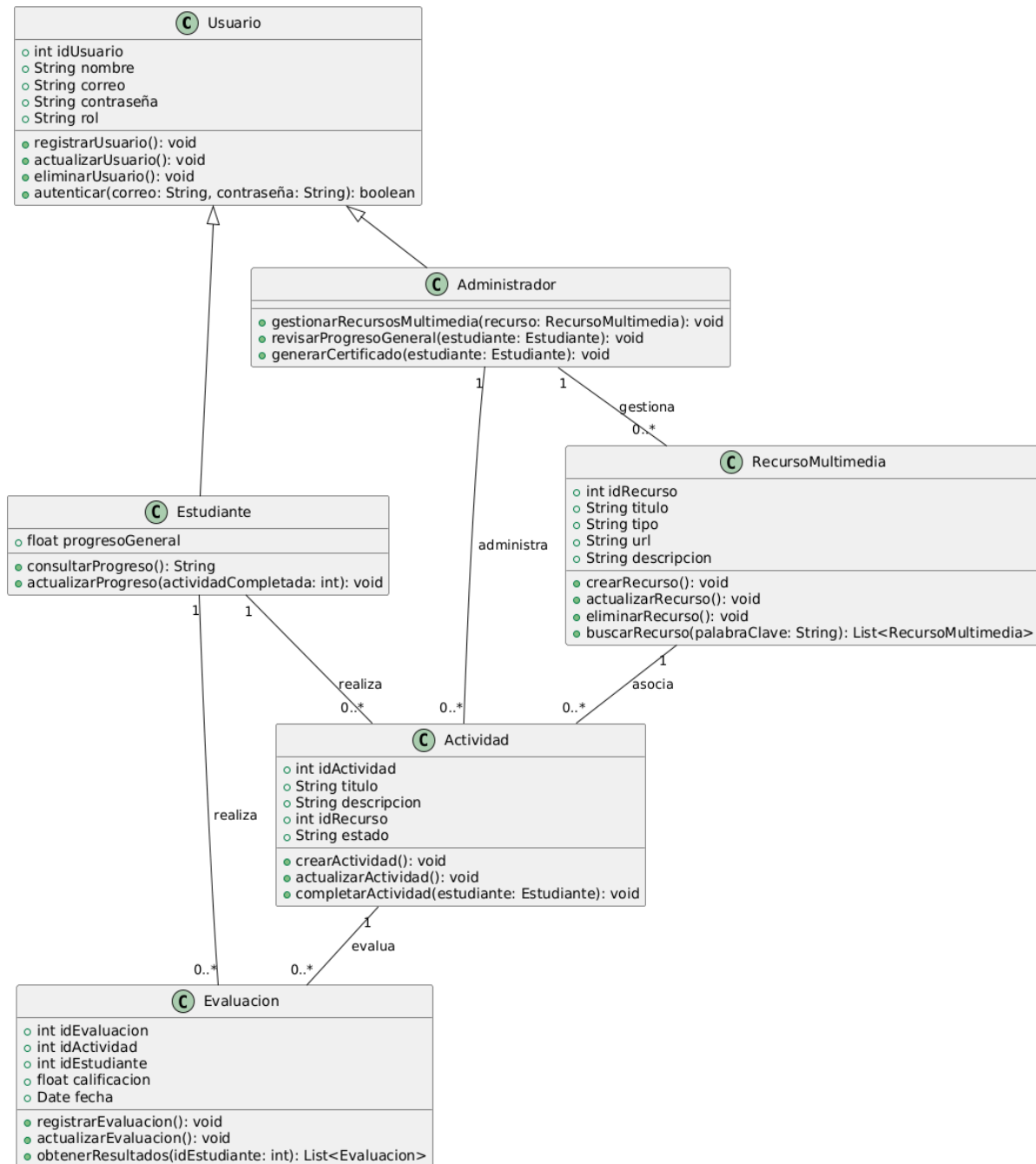
Atributos:

- *idEvaluacion(int): Identificador único de la evaluación.*
- *idActividad(int): Actividad asociada a la evaluación.*
- *idEstudiante(int): Estudiante que realizó la evaluación.*
- *calificacion(float): Calificación obtenida en la evaluación.*
- *fecha(Fecha): Fecha en que se realizó.*

Métodos:

- *registrarEvaluacion(): Crea una nueva evaluación.*
- *actualizarEvaluacion(): Modifica los resultados de una evaluación.*
- *obtenerResultados(idEstudiante: int): List<Evaluacion>: Devuelve las evaluaciones realizadas por un estudiante.*

2: diagrama de clases y sus relaciones:



*

Figura 2. Diagrama de clases.

Entidades:

Usuarios

- ID_Usuario
- Primer_nombre
- Segundo_nombre
- Primer_apellido
- Segundo_apellido
- Correo
- Contraseña
- Última_modificación_contraseña
- Fecha_registro
- Última_fecha_inicioSesión
- Estado
- Rol

Evaluación

- ID_Evaluacion
- Calificación
- Fecha_finalización
- Hora_finalización
- Intentos_realizados
- Fecha_inicio
- Hora_inicio

Archivos

- ID_Archivo
- Fecha_publicación
- Nombre
- Formato
- Ancho
- Alto
- Descripción
- Ruta
- Peso
- Tipo

Entrega

- ID_Entrega
- Fecha
- Hora
- Nota
- Adjunto
- Comentario

Módulos

- ID_Modulo
- Nombre
- Descripción
- Fecha_creación
- Estado

Tareas

- ID_Tarea
- Nombre
- Descripción
- Fecha_publicación
- Hora_publicación
- Adjunto
- Estado

Quices

- ID_Quiz
- Nombre
- Descripción
- Fecha
- Tiempo
- Número_intentos
- Orden
- Fecha_inicio
- Hora_inicio
- Fecha_finalización
- Hora_finalización

Foros

- ID_Foro
- Nombre
- Descripción
- Fecha_apertura
- Fecha_cierre
- Fecha_respuesta
- Hora_respuesta

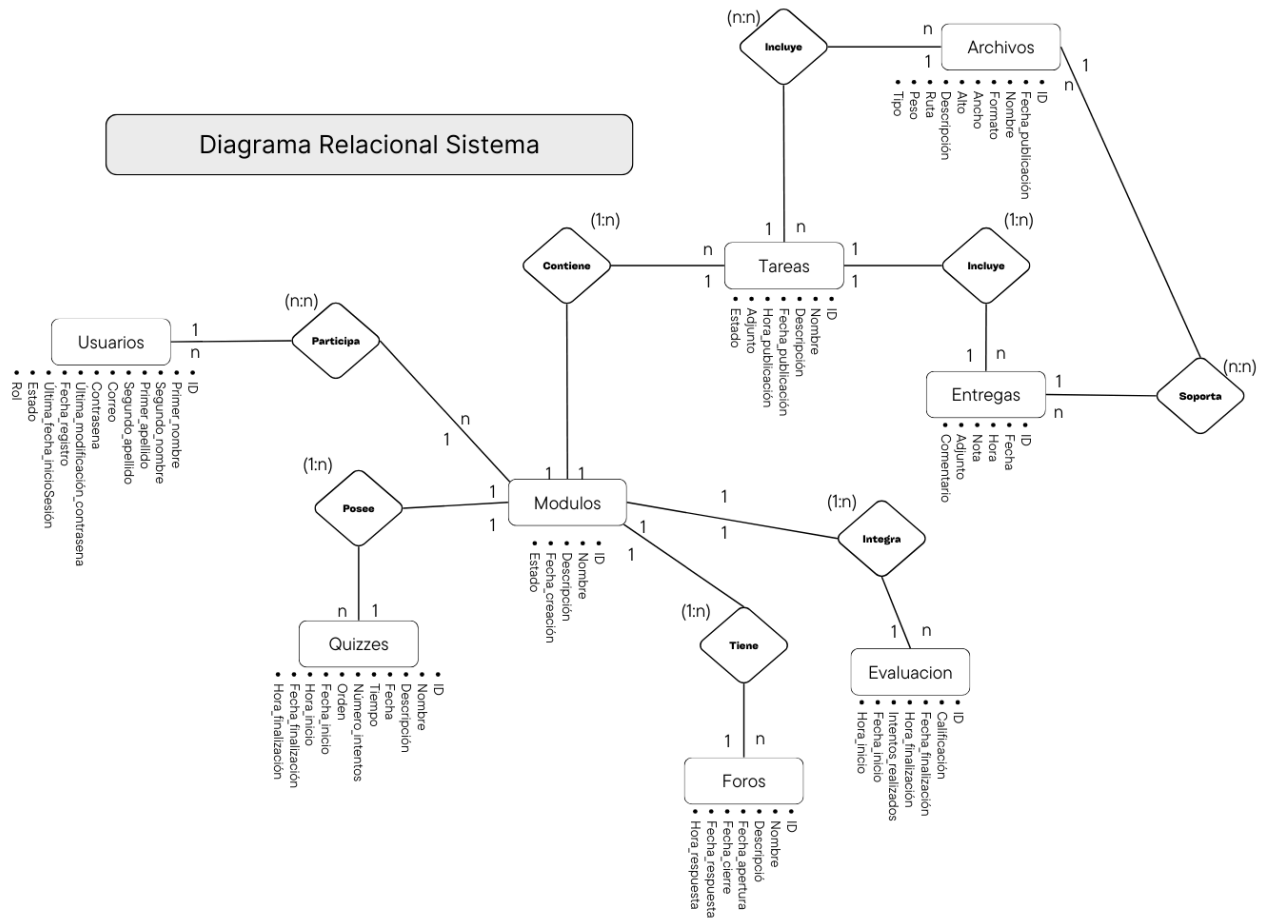


Figura 3. Diagrama entidad relación

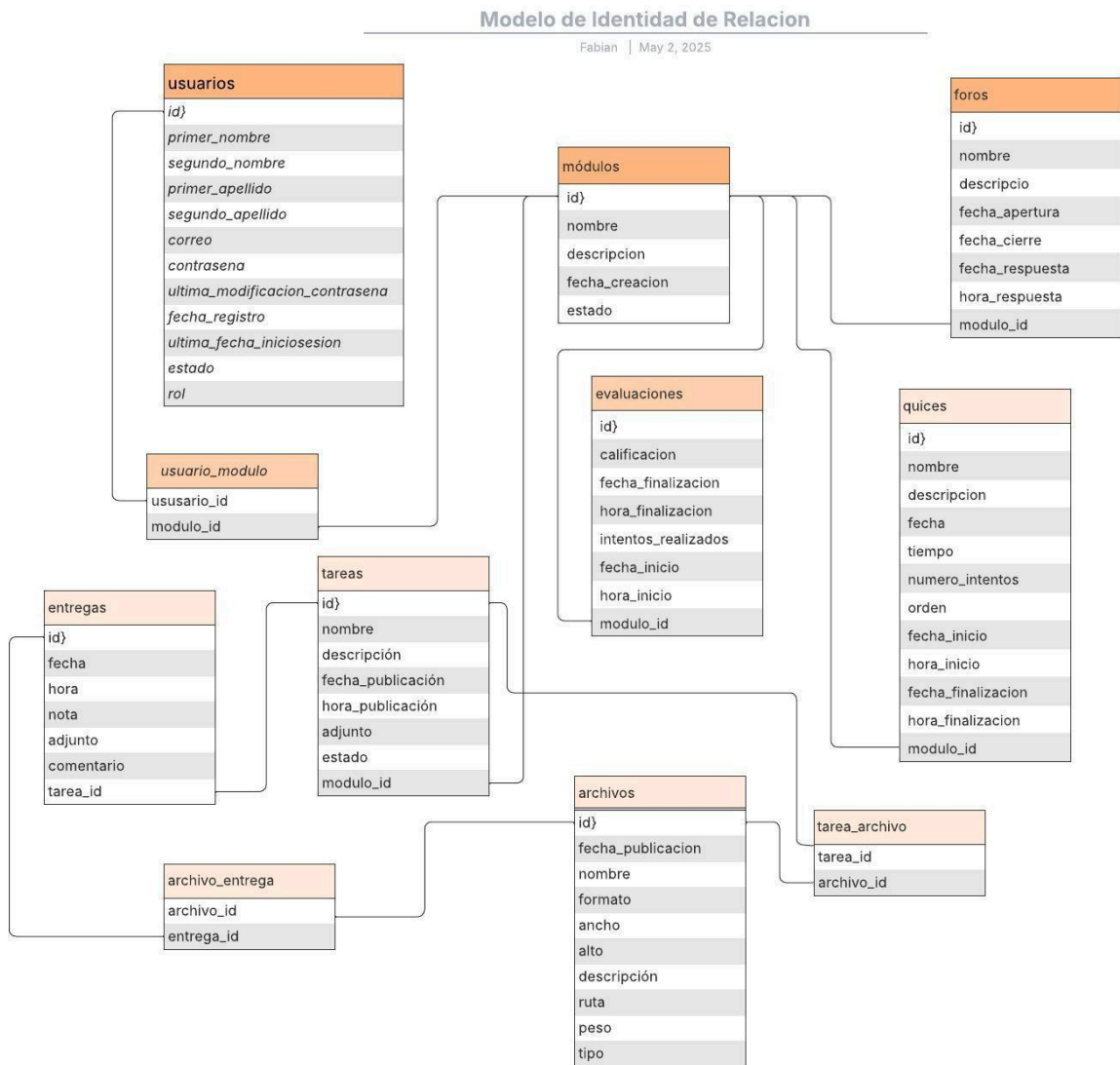
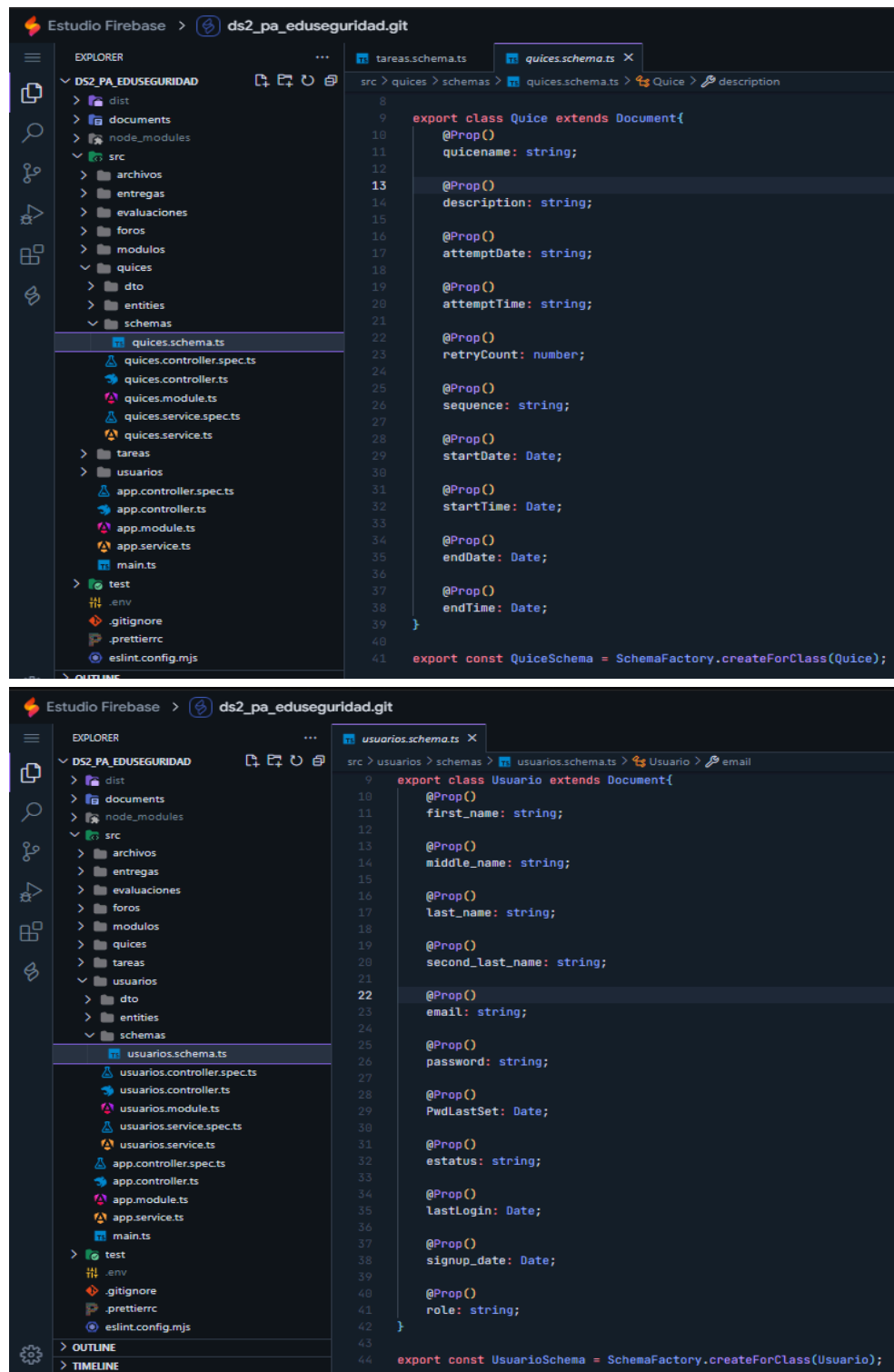
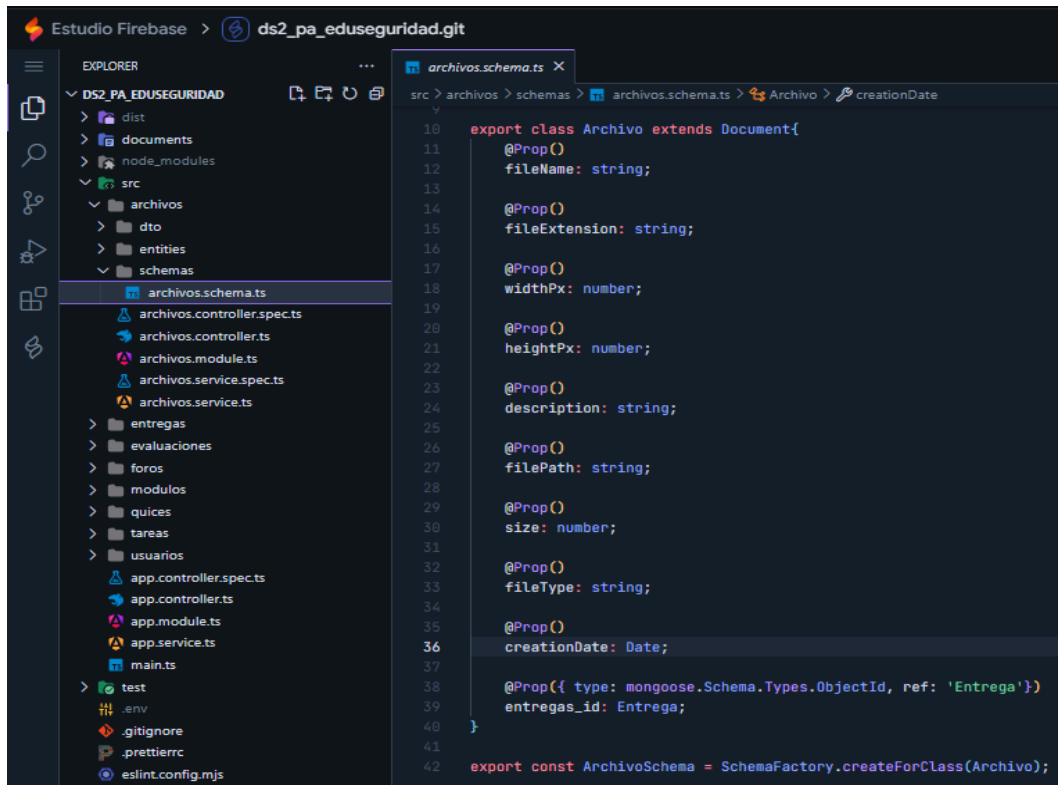


Figura 4. Modelo Entidad Relación





Estudio Firebase > ds2_pa_eduseguridad.git

EXPLORER

- DS2_PA_EDUSEGURIDAD
 - dist
 - documents
 - node_modules
 - src
 - archivos
 - dto
 - entities
 - schemas
 - archivos.schema.ts
 - archivos.controller.spec.ts
 - archivos.controller.ts
 - archivos.module.ts
 - archivos.service.spec.ts
 - archivos.service.ts
 - entregas
 - evaluaciones
 - foros
 - modulos
 - quices
 - tareas
 - usuarios
 - app.controller.spec.ts
 - app.controller.ts
 - app.module.ts
 - app.service.ts
 - main.ts
 - test
 - .env
 - .gitignore
 - .prettierrc
 - eslint.config.mjs

src > archivos > schemas > archivos.schema.ts > Archivo > creationDate

```
18 export class Archivo extends Document{
19   @Prop()
20   fileName: string;
21   @Prop()
22   fileExtension: string;
23   @Prop()
24   widthPx: number;
25   @Prop()
26   heightPx: number;
27   @Prop()
28   description: string;
29   @Prop()
30   filePath: string;
31   @Prop()
32   size: number;
33   @Prop()
34   fileType: string;
35   @Prop()
36   creationDate: Date;
37
38   @Prop({ type: mongoose.Schema.Types.ObjectId, ref: 'Entrega'})
39   entregas_id: Entrega;
40 }
41
42 export const ArchivoSchema = SchemaFactory.createClass(Archivo);
```