TALENTO TECH 2024-MINTIC

FORMATO DE PRESENTACIÓN "PLAN DE PROYECTO TI"

Nota: Eliminar todo lo que está en azul y cursiva ya que son orientaciones para el diligenciamiento

Contexto específico de aplicación del proyecto *(Marque con una X)*

AGRO	EDUCACIÓN	TURISMO	GOBIERNO	FINANZAS	MARKETING	SALUD	OTRO
							x

Cohorte #: __4__ Año: ___2025__ Tutor: Felipe Andrés Escallón_____

Nombre del Proyecto (y del producto/servicio):

CIFRADO VIGENÈRE EXTENDIDO CON RED SIMULADA

Departamento de residencia del estudiante:

Cundinamarca

Municipio de residencia del estudiante:

Bogotá

Rural: (Marque con una X)

SI	**x**	**NO**	
Vereda o Corregimiento:	N/A		

Autor (es):

No.	Nombres y Apellidos	Tipo de identificación	No. identificación	Curso: Programación, Inteligencia Artificial, Análisis Datos, Block Chain, Arquitectura Nube	Nivel: Explorador, Integrador, Innovador	Modalidad: Virtual, Semipresencial o Presencial

	GABRIEL RIVERA	CC	93181670	CIBERSEGURIDAD	EXPLORADOR	VIRTUAL

Palabras clave: *(conceptos con los que se relaciona el proyecto)*

Palabra clave 1	CIFRADO RSA
Palabra clave 2	CIFRADO DE VIGENERE
Palabra clave 3	RED SIMULADA
Palabra clave 4	CONEXCION DE NODOS

Planteamiento del problema que solucionará el producto/servicio:

¿Qué sucede?
R/ En la actualidad, muchas comunicaciones digitales, como mensajes entre dispositivos, pueden ser interceptadas fácilmente si no están protegidas, especialmente en redes inseguras o públicas.
¿Por qué sucede?
R/ Esto ocurre porque gran parte de la información se transmite sin métodos de cifrado adecuados, o utilizando protocolos vulnerables, lo que permite que atacantes intercepten y accedan al contenido de los mensajes (ataques tipo *man-in-the-middle*)
¿A quiénes afecta?
R/ Este problema afecta a **usuarios, empresas, instituciones educativas, servicios públicos** y en general a **cualquier persona u organización que envíe o reciba información sensible a través de una red digital**.
¿De qué manera?
R/ La falta de seguridad puede resultar en:

Robo de datos personales o bancarios.
Suplantación de identidad.
Pérdida de confianza en los sistemas.
Costos económicos por fugas de información o ciberataques.

Pertinencia del proyecto TI:

Pertinencia:

Cómo funciona el producto/servicio a desarrollar?

R/ El proyecto simula una red de dispositivos interconectados mediante grafos. Los mensajes enviados entre nodos se cifran utilizando el algoritmo **Vigenère extendido** y la **clave se protege con RSA**. También se incluye la posibilidad de un ataque tipo **Man in the Middle (MITM)** para ilustrar vulnerabilidades. El sistema muestra visualmente cómo viaja el mensaje, qué nodo lo intercepta (si aplica) y si el mensaje mantiene su integridad al llegar.

¿En qué beneficia a los usuarios?

R/ Educación**:** Ayuda a comprender cómo funcionan los sistemas de cifrado y la seguridad en redes.
Concientización: Muestra de forma práctica la importancia del cifrado y los riesgos de no proteger la información.
Formación en TI: Apoya el aprendizaje de algoritmos criptográficos, redes y simulación de sistemas.
Demostración técnica: Puede ser usado en entornos académicos o conferencias para demostrar seguridad en redes de forma visual e interactiva.

Mercado:

¿Qué tamaño tiene el mercado y la oportunidad?

R/ **Educativo:** Universidades, bootcamps, colegios técnicos y cursos de ciberseguridad que requieren herramientas interactivas para enseñanza.
Corporativo: Empresas que capacitan a su personal en buenas prácticas de seguridad informática.
Público en general: Personas interesadas en aprender cómo proteger su información digital.
La creciente demanda de soluciones en **ciberseguridad**, **formación técnica** y **simuladores interactivos** representa una **gran oportunidad de expansión** para este tipo de herramientas, especialmente si se adapta a plataformas web o móviles.

¿Es un mercado en crecimiento?)

R/ **Sí.** La ciberseguridad y la educación tecnológica están creciendo rápidamente por estas razones:
Aumento de ciberataques a empresas, gobiernos y usuarios individuales.
Más dispositivos conectados (IoT) que requieren protección.
Mayor demanda de profesionales en ciberseguridad y formación técnica en redes y criptografía.
Educación remota y digital que necesita herramientas didácticas interactivas.
Esto abre oportunidades para proyectos como el tuyo, que combina **educación, seguridad y visualización interactiva.**
¿Cuáles son las tendencias?)
R/ **Gamificación de la educación** en seguridad informática y redes.
Simuladores interactivos que explican procesos complejos de manera visual.
Uso de inteligencia artificial y automatización para detectar vulnerabilidades.
Criptografía híbrida (simétrica + asimétrica) como la que usa tu proyecto.
Capacitación empresarial en ciberseguridad básica para empleados.
Apps educativas web o móviles enfocadas en concientización digital.
Este tipo de solución puede evolucionar en una plataforma educativa o en un recurso de entrenamiento empresarial, adaptándose a las tendencias de **educación práctica y concientización digital**

Estado del Arte de productos/servicios existentes y ventajas comparativas:

Nombre producto	Fabricante/País	Qué ventajas tiene frente a mi producto (detallar)	Qué ventaja tiene mi producto frente a este (detallar)	Es un competidor Directo o Indirecto?
Wireshark	Wireshark Foundation / EE.UU.	- Muy completo para analizar tráfico real. - Captura en tiempo real. - Usado profesionalmente.	No incluye cifrado ni simulación didáctica. - Alto nivel técnico que puede ser difícil para novatos.	indirecto
GNS3 (Graphical	GNS3 Technologies Inc. / Canadá	- Permite emular redes reales con routers y switches.	- No incluye capa de seguridad integrada por	indirecto

Network Simulator 3)		- Integración con sistemas operativos	defecto. - No simula ataques como MITM de forma visual ni educativa	
Simuladores básicos de cifrado (educativos)		- Muy simples y fáciles de usar. - Ideales para introducir conceptos.	- Mi proyecto incluye integración completa: red, cifrado simétrico y asimétrico, firma digital y visualización dinámica con Plotly.	Directo (Educativo)
Proyectos en GitHub de seguridad de red	Comunidad de desarrolladores / Global	- Algunos incluyen cifrado y análisis. - Código abierto.	Pocos integran todo en un solo simulador didáctico. - Enfocado en educación visual, interacción y explicación paso a paso.	indirecto

Marco Legal y Ético

Ley 1581 de 2012 (Colombia): *Ley de protección de datos personales. Regula el tratamiento de la información de carácter personal, exigiendo autorización expresa del titular para su uso y garantizando su privacidad y seguridad.*

Ley 1273 de 2009: *Introduce el delito informático y protege la información y los datos. Cualquier uso indebido o acceso no autorizado está penado legalmente.*

Reglamento General de Protección de Datos (GDPR - Europa): *Aunque aplica en Europa, es una referencia clave para el manejo responsable de datos personales y transparencia en el tratamiento de la información*

Principios Éticos:

Confidencialidad: La información intercambiada debe mantenerse privada y accesible solo para los participantes autorizados.

Integridad: Los datos no deben ser alterados durante el proceso de transmisión. El sistema implementado busca garantizar que la información llegue completa y sin modificaciones.
Transparencia: El sistema no oculta sus funciones a los usuarios. Se explican de forma clara los objetivos del cifrado y la simulación de red.
No maleficencia: El uso del proyecto está orientado a fines educativos y de concienciación, evitando cualquier aplicación maliciosa o ilegal
Responsabilidad del Desarrollador:
El creador del proyecto debe asegurarse de que la herramienta no sea utilizada para vulnerar derechos, robar información o ejecutar ciberataques. El enfoque debe estar en la formación, prevención y defensa digital.

ANÁLISIS DE RIESGOS:

El análisis de riesgos identifica las amenazas potenciales que podrían afectar el funcionamiento, la seguridad o la usabilidad del sistema desarrollado. Este proceso permite tomar medidas preventivas o correctivas que garanticen la continuidad y seguridad del sistema.

1. **Riesgo Potencial:** Intercepción de mensajes (MITM)
   Descripción: Un atacante podría acceder al mensaje mientras transita por la red.
   Impacto: Alto
   Probabilidad: Media
   Medidas de Mitigación: Aplicar doble cifrado (Vigenère + RSA) y validación de firma digital.
2. **Riesgo Potencial:** Uso indebido del sistema
   Descripción: El código podría utilizarse para fines no éticos o ilegales.
   Impacto: Medio
   Probabilidad: Media
   Medidas de Mitigación: Control de acceso, advertencias legales, licencias de uso.
3. **Riesgo Potencial:** Falla en el descifrado del mensaje
   Descripción: Error al desencriptar debido a clave incorrecta o mensaje alterado.
   Impacto: Medio
   Probabilidad: Baja
   Medidas de Mitigación: Integración de hash para verificar integridad y captura de errores.
4. **Riesgo Potencial:** Exposición de clave privada RSA
   Descripción: Riesgo si la clave privada no se protege adecuadamente.
   Impacto: Crítico
   Probabilidad: Baja
   Medidas de Mitigación: Almacenamiento seguro y prácticas criptográficas responsables.
5. **Riesgo Potencial:** Dificultad de uso para usuarios novatos
   Descripción: Complejidad técnica del sistema puede ser barrera para nuevos usuarios.
   Impacto: Medio

Probabilidad: Alta
Medidas de Mitigación: Diseño de interfaz amigable, instrucciones claras y guías de uso.

6. **Riesgo Potencial:** Bugs o errores en el código
   Descripción: Fallas lógicas o de programación que comprometan la funcionalidad.
   Impacto: Medio
   Probabilidad: Media
   Medidas de Mitigación: Pruebas constantes, revisión de código y mantenimiento activo del sistema.

caso	¿Qué podría suceder?	¿Cuál sería el efecto/impacto en los objetivos del proyecto?	¿Cuándo, dónde, por qué y cuál es la probabilidad de que ocurran estos riesgos (positivos o negativos)?	¿Quién puede estar involucrado o impactado?	¿Cuál puede ser la fuente del riesgo?
1. ***Intercepción de mensajes (Ataque MITM - Man in the Middle)***	*Un atacante podría interceptar el mensaje mientras se transmite entre dos nodos*	Se comprometería la confidencialidad e integridad del mensaje, debilitando la seguridad del simulador.	Media, Durante la transmisión de datos por la red simulada, Falta de cifrado fuerte o ausencia de validación de identidad del emisor/destinatario.	Usuarios finales, desarrolladores, y cualquier persona con acceso a la red.	Redes públicas, nodos comprometidos, falta de autenticación de nodos
2. **Fuga o exposición de la clave privada (RSA)**	Alguien accede indebidamente a la clave privada, lo que permite descifrar cualquier mensaje cifrado	Se pierde completamente la seguridad de los mensajes; cualquier actor podría leer los datos	Baja, Durante el almacenamiento o transferencia de claves. Almacenamiento inseguro, claves en texto plano, mala gestión	Administradores, desarrolladores, atacantes externos.	Falta de buenas prácticas criptográficas, almacenamiento compartido o expuesto.
3. ***Falla en el descifrado***	El mensaje no puede ser leído correctament	Se pierde el contenido del mensaje, afecta la	Baja, En el nodo receptor al intentar descifrar el mensaje. Clave	Usuario receptor, sistema de cifrado.	Fallos de programación, errores de

del mensaje	e por el receptor debido a un error de clave o corrupción.	usabilidad y confiabilidad del sistema.	incorrecta, mensaje alterado, errores de código.		transmisión, ataques.
4. ***Uso indebido del sistema***	El código del proyecto puede ser utilizado por terceros con fines ilegales (espionaje, ciberataques, etc.).	Afecta la reputación del desarrollador o institución educativa. Puede tener consecuencias legales.	Media, Después de que el código sea distribuido públicamente. Código abierto sin restricciones ni licencias claras.	Usuarios malintencionados, terceros.	Distribución sin protección legal, falta de advertencias éticas.

Objetivos:

General: Desarrollar un simulador de red de dispositivos que permita visualizar la transmisión segura de mensajes utilizando algoritmos de cifrado Vigenère y RSA, con el fin de enseñar y demostrar conceptos clave de criptografía, seguridad de la información y comunicación digital segura**.**

Específicos:

Implementar un sistema de cifrado simétrico (Vigenère extendido) y asimétrico (RSA) para proteger los mensajes transmitidos entre nodos de la red.

Simular una red de dispositivos con nodos distribuidos geográficamente en ciudades reales de Colombia.

Visualizar de forma gráfica e interactiva el envío, cifrado, recorrido y descifrado de mensajes en la red, incluyendo posibles ataques tipo “Man in the Middle” (MITM).

Integrar funciones de firma digital para validar la integridad del mensaje transmitido.

Facilitar la comprensión de conceptos de seguridad informática mediante una interfaz interactiva, accesible para estudiantes y usuarios no expertos.

Metodología:

Para el desarrollo del proyecto se adoptará una metodología de tipo **iterativo incremental**, propia del enfoque ágil, permitiendo realizar pruebas frecuentes y mejorar progresivamente el sistema con base en retroalimentación continua.

Etapas de la metodología:

1. **Análisis y diseño del sistema:**
    - Definición de requerimientos funcionales y no funcionales.

- Selección de librerías y tecnologías.
- Diseño lógico de red y cifrado.

2. **Desarrollo e implementación:**
   - Codificación de los módulos de cifrado Vigenère y RSA.
   - Simulación de la red de nodos con coordenadas geográficas.
   - Programación del sistema de envío y validación de mensajes.
3. **Visualización e interfaz:**
   - Desarrollo de la visualización interactiva con Plotly.
   - Implementación de simulación MITM y firma digital.
4. **Pruebas y validación:**
   - Pruebas funcionales, validación de resultados, verificación de seguridad.
5. **Documentación y presentación:**
   - Elaboración de manual de usuario, análisis de resultados, presentación del proyecto.

Propia de cada área (Revisar los documentos anexos a este documento)

Plazo: Duración del proyecto.

SEMANAS	DIAS
X	

CRONOGRAMA DE ACTIVIDADES (Diagrama de Gantt): *Detalle las actividades lo más preciso posible e indique para cada una su duración en semanas, y la secuencialidad.*

No.	Actividad	S 1	S 2	S 3	S 4	S 5	S6	Responsable
1	Análisis de requerimientos	x						Gabriel Rivera
2	Diseño de la red y arquitectura	x	x					Gabriel Rivera
3	Desarrollo de módulo Vigenère		x	x				Gabriel Rivera
4	Desarrollo de módulo RSA		x	x				Gabriel Rivera
5	Firma digital y validación de integridad			x	x			Gabriel Rivera

6	Visualización interactiva y simulación			x	x			Gabriel Rivera
7	Pruebas funcionales				x	x		Gabriel Rivera
8	Documentación y presentación					x	x	Gabriel Rivera

PRESUPUESTO: Revisar Anexo "**Plantilla Presupuesto Presupuesto Desarrollo de PROYECTO.xls**"