EVALUACIÓN PARA PROPUESTAS DE TRABAJO TERMINAL

NO. DE REGISTRO DEL TT: 2024-A003

TÍTULO DEL TT: PROTOTIPO WEB DE UNA CALCULADORA PASO A PASO DEL ALGORITMO AES PARA EL APOYO DEL APRENDIZAJE Y EVALUACIÓNDE ESTUDIANTES DE CRIPTOGRAFÍA

FECHA DE EVALUACIÓN: LUNES 22 DE MAYO DE 2023

NO. DE VERSIÓN 1a. X 2a.

PREGUNTA	SI	NO	OBSERVACIONES
1. Título del TT. ¿El título corresponde al producto esperado?	X	—	Ninguno.
2. Resumen. ¿El resumen expresa claramente la propuesta del TT, su importancia y aplicación?	X	—	Atender el comentario 2.
3. Palabras clave. ¿Las palabras clave han sido clasificadas adecuadamente?	—	X	Atender el comentario 22.
4. Introducción. ¿La presentación del problema a resolver es comprensible?	—	X	Atender los comentarios 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 y 19.
5. Objetivo. ¿El objetivo es preciso y relevante?	—	X	Atender los comentarios 15, 16 y 17.
6. Planteamiento. ¿El planteamiento del problema y la tentativa solución descrita son claros?	—	X	Atender comentario 20.
7. Justificación. ¿Sus contribuciones o beneficios están completamente justificados? Originalidad, vinculación con población usuaria potencial, utilidad de los resultados, complejidad en su elaboración a nivel ingeniería, mejoramiento de lo existente, etc.	—	X	Atender los comentarios 20 y 21.
8. Resultados o productos esperados. ¿Su viabilidad es adecuada? Tiempos, recursos humanos y materiales, alcances, costos y otros puntos que puedan impedir la culminación exitosa del trabajo.	—	X	Atender comentario 18.
9. Metodología. ¿La propuesta metodológica es pertinente?	X	—	Ninguno.
10. Cronograma. ¿El calendario de actividades por estudiante es adecuado?	X	—	Ninguno.

DICTAMEN

APROBADO	NO APROBADO
—	X

RECOMENDACIONES DETALLADAS:

COMENTARIO 1.
La propuesta de proyecto es interesante desde una perspectiva pedagógica, pues es evidente que se requiere invertir más recursos y más esfuerzos en la creación y mejora de instrumentos de apoyo al aprendizaje en casi todas las áreas de conocimiento, particularmente, en nuestros planes de estudio.

COMENTARIO 2.
La redacción actual podría mejorar con el uso correcto de **acrónimos** y siglas. Generalmente, estos se introducen en el texto con su significado y, posteriormente, son referidas para simplificar la lectura.

Ejemplo 2.1: A lo largo del texto se suele citar a la "Escuela Superior de Cómputo", se menciona por primera vez en el resumen, sin embargo, nunca se hace uso de sus siglas. Se vuelve a hacer referencia en las páginas 1, 2, 4 y 6.

Ejemplo 2.2: En contraste con el Ejemplo 2.1, el acrónimo "AES" nunca es descrito. Si bien cualquier lector cercano a la teoría de criptografía o incluso de números enteros con alta probabilidad lo conoce, también es cierto que una mejor redacción consideraría la definición de todo acrónimo.

COMENTARIO 3.
Uso incorrecto de **mayúsculas**.
Es indispensable revisar el texto, identificar los casos de uso incorrecto y corregirlos. Sugiero estudiar alguna referencia especializada, por ejemplo [1].

Ejemplo 3.1: En el título y en el resumen, se encuentra "Prototipo Web". Es válido "Prototipo" en el título al ser la primera palabra, pero no en la primera línea del resumen. En cambio, en ninguno de estos casos "Web" es correcto.

Ejemplo 3.2: En el séptimo párrafo de la primera sección (página 2), se encuentra “Plan de Estudios”. Podría ser válido como un nombre propio, que sería la causa más frecuente, pero no es el caso.

Un caso similar se encuentra en el décimo cuarto párrafo de la primera sección (página 3). Ahí “Estado del Arte” podría ser válido si alguna sección tuviera ese nombre, como cuando se hace referencia a una “Figura” o una “Tabla” o algún elemento en un documento, más aún si tienen alguna etiqueta ordinal.

COMENTARIO 4.
Uso incorrecto de las **comas**.
También es indispensable revisar el texto, identificar los casos de uso incorrecto y corregirlos. Sugiero estudiar alguna referencia especializada, por ejemplo [2].

Ejemplo 4.1: En la cuarta línea del tercer párrafo de la primera sección, se encuentra “…temas de estudio y, ser una alternativa…”.

Ejemplo 4.2: En el inicio del tercer párrafo de la primera sección, se encuentra “En la era moderna los estilos de aprendizaje…”. Faltó una coma en “En la era moderna, los…”. Otro caso similar está en al inicio del cuarto párrafo de la primera sección: “Según Mariela Viñas en su artículo [3], las plataformas…”.

COMENTARIO 5.
El uso incorrecto de **números**.

Ejemplo 5.1: En la segunda línea del séptimo párrafo de la primera sección, se encuentra “…Computacional 4 optativas…”. Más adelante en esa misma línea, se encuentra “…escoger 4 unidades…”.

COMENTARIO 6.
Se realizan declaraciones sin **sustento** adecuado.

Ejemplo 6.1: En el último enunciado del séptimo párrafo de la primera sección, se encuentra *“Una de las unidades de aprendizaje más demandadas es la criptografía.”*. Esta es una declaración que realiza el autor del texto, pero no aporta sustento de su declaración. Si acaso no fuera del autor, entonces podría ser de algún tercero y debería ser referenciada.

Ejemplo 6.2: En el último enunciado del segundo párrafo de la primera sección, se encuentra *“Estos estilos son: El aprendizaje visual, el aprendizaje auditivo, el aprendizaje verbal y el aprendizaje kinestésico.”*, sin embargo, en el artículo citado por la referencia 2 no menciona los enlistados como *“estilos de aprendizaje”*. De hecho, en la sección *“D. Estilos de aprendizaje”*, se identifican como: acomodador, divergente, asimilador y convergente.

Ejemplo 6.3: En la tercera línea del tercer párrafo, se encuentra *“esto ha hecho que muchos educadores y empresas creen las llamadas plataformas educativas”*. Desde la perspectiva de la pedagogía, un *“educador”* es una persona que acompaña a otra persona en su proceso de desarrollo llamado *“educación”* (que no *“capacitación”*). El ejemplo clásico es el legado de los trabajos de María Montessori. Por otro lado, las empresas son instituciones que su naturaleza es de lucro, por lo tanto, son casi contrarias a la educación, pero sí son partidarias de la capacitación de su mano de obra. Así entonces, *“educadores”* y *“empresas”* son figuras antagonistas que no pueden ponerse en la misma categoría. Finalmente, sugiero definir *“plataformas de educativas”* (aun cuando se menciona en el cuarto párrafo, se cita en el tercero), pues comúnmente puede entender como los sistemas de cómputo destinados a impartir *“cursos”* o *“talleres”*, pero esto difícilmente se puede calificar como *“educación”*. Sugiero revisar textos del mexicano Pablo Latapi Sarre o el brasileño Paulo Freire.
Sugiero optar por consultar una publicación con más información a la referencia 3, pues su *“Referente teórico”* es menudo y el resto del artículo se limita a enlistar *“plataformas”*.

Ejemplo 6.4: En sexto párrafo de la primera sección, se encuentran declaraciones muy cuestionables. Por ejemplo: *“el uso de plataformas educativas aumenta la motivación y el compromiso de los estudiantes… aprender a su propio ritmo”*. La motivación y el compromiso de los estudiantes no tienen como factor determinante el acceso a recursos. De forma simplificada, la motivación está relacionada con una meta de la persona y el compromiso con las razones por las que recorre un camino de adversidades para cumplir una meta.

Ejemplo 6.5: En el segundo enunciado del cuatro párrafo de la tercera sección, se encuentra *“…convertir esta calculadora en una API, beneficia…”*. Sugiero mencionen explícitamente los beneficios directos a los que refieren, considerando a sus beneficiarios principales: *“los estudiantes”*, pues más adelante agregan “empresas”, “usuarios finales”, etc., los cuales no están considerados como los beneficiarios principales.

COMENTARIO 7.
Acentuación faltante o incorrecta.

Ejemplo 7.1: En la cuarta línea del primer párrafo de la primera sección, se encuentra *“…generalizo…”*.

COMENTARIO 8.
Se realizan **referencias** incorrectas.

Ejemplo 8.1: Al final del primer párrafo de la primera sección, se cita a Meza: *“El aprendizaje se puede definir… en situaciones futuras.”* y se hace cita la referencia 1. Busqué esa definición, pero no la encontré. Si acaso estuviera, de antemano pido disculpa por mi error.

Ejemplo 8.2: La referencia 2 del texto apunta a un documento en Scribd. Este sitio restringe la lectura a sus documentos. Consideren que el fin último de las referencias es permitir al lector remitirse a las fuentes del texto; no obstaculizarlo. Así entonces, lo lógico sería citar la fuente primaria de publicación [4] en la Revista EIDOS.

Ejemplo 8.3: Continuando con la referencia 2, el texto nos refiere a los trabajos de Elena Mosquera, particularmente de los estilos de aprendizaje. Pueden mejorar sus referencias haciéndolo con mayor precisión al fragmento citado. Así en lugar de citar *“[2]”*, podría citar *“[2, pag. 6]”* o *“[2, pag. 6-10]”*, que son las que hacen referencia a este tema.

COMENTARIO 9.
Se cometieron **errores menores** (como “errores de dedo”).

Ejemplo 9.1: En la cuarta línea del tercer párrafo de la primera sección, se encuentra *“…alternativa a estudio…”*.

Ejemplo 9.2: En la cuarta línea del octavo párrafo de la primera sección, se encuentra *“…técnica y formas en inglés.”*.

COMENTARIO 10.

Se presenta una redacción poco simplificada. Si bien, en el español es frecuente encontrar enunciados largos o rebosantes de información, este estilo de redacción requiere un cuidado crítico para lograr el entendimiento de las ideas y que el lector no pierda todas las ideas que se le pide acumular en su memoria. Sugiero opten por una redacción de enunciados más cortos en los que la conjunción de esos enunciados simples y concisos construyan una idea más clara.

Ejemplo 10.1: En el tercer párrafo de la primera sección, se encuentra *"En la era moderna… en las instituciones educativas"*. Este enunciado, que se extiende a lo largo de cuatro de las seis líneas del párrafo, expresa muchas ideas que podrían ser expresadas con mayor claridad si se segmenta en enunciados o frases más cortas. La lectura es incluso difícil pues las comas usadas están colocadas incorrectamente (lo que se relaciona con el Comentario 4).

COMENTARIO 11.
El texto no menciona cómo es que los distintos tipos de aprendizajes, referidos de los trabajos de Elena Mosquera, serán atendidos por el prototipo que se propone. Esta propuesta se enriquecería si se agregaran formas para medir los beneficios que este prototipo se pueda plantear como objetivo para las personas con diferentes tipos de aprendizaje.

COMENTARIO 12.
El texto menciona la situación problemática en la que la documentación de varios algoritmos está expresada en forma técnica y en inglés. En principio que su redacción sea técnica no debería ser un obstáculo, pues la redacción técnica tiene el propósito de describir con precisión. Que sea un obstáculo, nos debería llamar a reflexionar a los académicos sobre las posibles deficiencias o carencias con las que nuestros estudiantes están ingresando a cursos. Por otro lado, que la documentación esté en inglés creo que sí es un obstáculo razonable. Considerando que esta propuesta se centrará en el algoritmo AES y esto implica que los estudiantes realicen un estudio adecuadamente profundo para comprenderlo con cierta plenitud, bien puede plantearse como objetivo o bien la traducción de esa documentación que será revisada o la realización de notas de esa documentación. Así este proyecto, puede dejar como aportación académica esos textos para otros estudiantes.

COMENTARIO 13.
Sugiero mencionar en la propuesta cuál es el nivel de detalle que se busca con el que los estudiantes estudien el AES y, por ende, el nivel de detalle que este prototipo debe atender. Si el estudio del AES en este curso es profundo, entonces la documentación técnica debe ser estudiada y comprendida a plenitud, y calculadoras como las de la referencia 7 y 8 resultan insustanciales. Incluso la calculadora de la referencia 10, sería insuficiente pues no hace fácil seguir la traza de los bits, aunque permite ver los detalles de cada ronda.

COMENTARIO 14.
Hacen referencia a la *"programación modular"* pero no dan detalle de sus implicaciones, así entonces, no aporta información.

COMENTARIO 15.
Si bien mencionan en el segundo objetivo específico que usarán un solo bloque, sugiero agreguen la información correspondiente al modo de operación para que quede explícito.

COMENTARIO 16.
En el primer párrafo de la tercera sección, mencionan que el objetivo es *"al sector educativo en el área de informática"*; algo completamente ambiguo. Sugiero especificar quien o quienes son las personas beneficiadas, que por el contexto podría suponer que son *"los estudiantes del curso de Criptografía de la Escuela Superior de Cómputo"*, aunque podría no ser y tener más beneficiarios. Este dato sólo se confirma hasta el primer párrafo de la tercera sección.

COMENTARIO 17.
Especificar los objetivos y hacer referencia a ellos en el texto.

Ejemplo 17.1: En el primer párrafo de la tercera sección, refieren al *"primordial objetivo"* y al *"objetivo principal"*, cada uno expresando ideas distintas. Sugiero especifiquen claramente sus objetivos y sólo hagan referencia a ellos. Bien pueden usar una enumeración al definirlos y hacer referencia a ellos.

COMENTARIO 18.
Publicación del código fuente del proyecto.
Dentro de los productos esperados no se incluyó la publicación del código fuente del proyecto, tampoco se expresó explícitamente que se use un repositorio como medio de control de versiones del código fuente del proyecto. A la par, tampoco da sustento del porqué el código lo mantienen reservado.

COMENTARIO 19:
Comentar las diferencias de implementación de acuerdo con el estándar FIPS 197 y las que no siguen este estándar.
En varias partes del texto hablan de estas diferencias de implementación. Por la naturaleza de los cifradores de bloque, se podría pensar alguna variación mínima en la implementación, tiene como resultado que un mensaje en claro tenga diferentes salidas, en este caso por seguir o no el FIPS 197, así entonces, el AES no sería funcional porque induciría que un mensaje cifrado con una implementación no podría descifrarse con otra implementación. Este detalle no se menciona en la introducción.

COMENTARIO 20.
Usar categorías de **justificación**.
Con frecuencia observo confusión entre *"motivación del proyecto"*, *"planteamiento del problema"* y *"justificación"*. Les sugiero agregar la descripción clara de estos tres temas relacionados con el proyecto, quizá los primeros dos como parte de la *"Introducción"* y el tercer ya tiene su propia sección.
Particularmente en la justificación, les sugiero especificar su justificación en categorías de acuerdo con su contribución: social, académica-escolar, tecnológica y científica.

COMENTARIO 21.
Uso de **estándar de calidad de software** desactualizado.
En el segundo párrafo de la cuarta sección, mencionan el uso del ISO/IEC-9126 con el objetivo de buscar cierta calidad. No mencionan algún sustento de porqué usan un estándar que ya quedó reemplazado. Tampoco mencionan qué aspectos en particular del estándar pretenden atender o si buscar que se evalúe todo el estándar. Les sugiero consulten el ISO/IEC 25000 [5].

COMENTARIO 22.
Uso de **palabras clave** estandarizado.
Les sugiero que las palabras clave las tomen de un catálogo de artículos de proyectos de ingeniería. Pueden revisar editoriales como IEEE [6] o ACM [7]. Les invito a no limitarse a estas referencias que les menciono, pues es labor de los estudiantes hacer su propia investigación y con ayuda de la experiencia en publicaciones de sus directores mejorar la selección de estas palabras.

COMENTARIO 23.

Revisar exhaustivamente por detalles pendientes por mejorar.
Si bien traté de referir puntualmente a cada parte del texto en dónde hubiera algún comentario de mi parte, incluso tratando de poner ejemplo, eso no significa que sean los únicos fragmentos para corregir. Les sugiero hacer una revisión exhaustiva para encontrar fragmentos en donde se encuentren errores no señalados explícitamente, pero sí descritos en algunos de los comentarios.

[1]: "Mayúsculas | Diccionario panhispánico de dudas", URL: https://www.rae.es/dpd/mayúsculas
[2]: "Coma | Diccionario panhispánico de dudas", URL: https://www.rae.es/dpd/coma
[3]: "Números | Diccionario panhispánico de dudas", URL: https://www.rae.es/dpd/números
[4]: "Estilos de Aprendizaje", Elena Díaz Mosquera, Revista EÍDOS, DOI: https://doi.org/10.29019/eidos.v0i5.88, URL: https://revistas.ute.edu.ec/index.php/eidos/article/view/88
[5]: "ISO/IEC 25000:2014", URL: https://www.iso.org/standard/64764.html
[6]: https://ieeexplore.ieee.org/ielx7/9632874/9632875/09633101.pdf
[7]: https://www.acm.org/binaries/content/assets/publications/article-templates/ccs-howto-v6-12jan2015.pdf

=====

NOMBRE Y FIRMA DEL SINODAL:	Israel Buitrón Dámaso
ACADEMIA:	Ciencias Básicas
DEPARTAMENTO:	Formación Básica
CONTACTO:	ibuitron@ipn.mx, www.comunidad.escom.ipn.mx/ibuitron/contacto.html