EVALUACIÓN PARA PROPUESTAS DE TRABAJO TERMINAL

NO. DE REGISTRO DEL TT: 2020-A089

TÍTULO DEL TT: CRIPTOSISTEMA BIOMÉTRICO MEDIANTE LA RED CASCULAR DEL DORSO DE LA MANO

FECHA DE EVALUACIÓN: VIERNES 31 DE JULIO DE 2020

NO. DE VERSIÓN 1a. [X] 2a. [ ]

PREGUNTA	SI	NO	OBSERVACIONES
1. Título del TT. ¿El título corresponde al producto esperado?		X	El título podría ser más descriptivo y preciso.
2. Resumen. ¿El resumen expresa claramente la propuesta del TT, su importancia y aplicación?		X	El resumen no aporta una noción breve de las particularidades del proyecto.
3. Palabras clave. ¿Las palabras clave han sido clasificadas adecuadamente?	X		Podrían mejorar la selección de palabras clave, sin embargo, lo dejo a criterio de los autores.
4. Introducción. ¿La presentación del problema a resolver es comprensible?		X	La introducción debe mejorarse sustancialmente. Su contenido muy reducido y cuestionable.
5. Objetivo. ¿El objetivo es preciso y relevante?		X	
6. Planteamiento. ¿El planteamiento del problema y la tentativa solución descrita son claros?		X	No se incluyó el planteamiento del problema, ni la motivación del proyecto.
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	La justificación carece de una argumentación suficiente.
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	Debido a las deficiencias en las secciones anteriores del protocolo es intrascendente considerar los resultados hasta no contar con una versión que subsane los señalamientos.
9. Metodología. ¿La propuesta metodológica es pertinente?	X		
10. Cronograma. ¿El calendario de actividades por estudiante es adecuado?	X		

DICTAMEN

APROBADO [—] **NO APROBADO** [X]

RECOMENDACIONES DETALLADAS:

La primera recomendación general es revisar detalladamente la redacción para corregirla o mejorarla, según sea el caso. A lo largo del documento, se pueden encontrar numerosos errores de construcción de enunciados que forman un párrafo. También se encuentran errores en el uso de los signos de puntuación.

A continuación, menciono sólo algunos ejemplos explicitando que no se deben entender como los únicos en el texto.

El título del proyecto es *"Criptosistema biométrico mediante la red vascular del dorso de la mano"*. Este podría redactarse para expresar una idea más clara y precisa del proyecto. Decir *"…mediante la red vascular…"* puede expresar que el criptosistema funciona u opera en la red vascular. Evidentemente no es el caso, lo que se quiere dar a entender es que toma datos de entrada para algún proceso propio del criptosistema, pero esto no se entiende con claridad con esta redacción.

Sugiero pensar en una redacción más precisa que dé particularidades de este proyecto. Se propone tomar datos biométricos que serán usados como entrada en un proceso de generación de claves de cierto algoritmo para realizar un proceso de acreditación de la identidad en ciertas circunstancias. Así entonces, el título debería expresar estas particularidades con claridad, dentro de las limitaciones evidentes de un título, como una longitud adecuada.

El primer enunciado de la Introducción menciona "El reconocimiento biométrico como forma de autenticación e identificación se refiere al uso de…". Como se puede ver, la frase "como forma de autenticación e identificación" tiene una función de aposición explicativa y, por lo tanto, debe estar entre comas de acuerdo con las reglas del español [1].

El penúltimo enunciado del primer párrafo de la Introducción puede tener una redacción más sintética, por ejemplo "Esta base de datos es importante para comparar la información obtenida respecto de la almacenada". Incluso podrían denotar si la base de datos es requerida, optando por "indispensable" en lugar de "importante". Seguramente, el dominio de su propia propuesta que ustedes tienen les permitirá expresarlo de mejor forma.

La segunda recomendación general es formalizar y mejorar su base teórica. Sólo el segundo párrafo de la Introducción presenta la definición de un concepto. Excepto esto, no se presenta más información de un marco teórico que proponga un bosquejo del proyecto.

Sugiero cambiar su definición de "criptosistema". Actualmente menciona *"…es una 5-tupla (P,C,K,E,D) que satisface las siguientes condiciones…"* y una lista de "condiciones". Considero que estas no son condiciones sino la descripción de las entradas de la tupla; en ese sentido, podrían optar por una redacción como "es una 5-tupla… donde P es un conjunto de…, C es un conjunto de…". Si acaso alguna de las entradas debe satisfacer algún predicado lógico, entonces puede expresarse como una condición. Consideren detallar debidamente cada aspecto de la definición, ya que han omitido describir los símbolos E y D. Dado que se menciona *"existe una regla de cifrado eK∈E"*, entonces podemos pensar que E es un conjunto de reglas de cifrado. Sin embargo, es preferible mencionar lo que debe entenderse por cada concepto o símbolo y no dejar a la deducción o a la interpretación de lector.

Sugiero que utilicen el editor de ecuaciones de Word para escribir adecuadamente sus expresiones matemáticas. Podrían tener expresiones más claras como $K \in Q$, $e_K: P \to C$, o $d_K(e_K(x)) = x$, etc., en lugar de las expresiones actuales. A medida que las expresiones crezcan o incluyan más niveles de anidación se vuelven confusas y conviene utilizar los editores de ecuaciones.

La referencia que citan en esta definición es la 11 y conduce a una tesis. Salvo que esta definición de "criptosistema" sea imprescindible, sugiero que opten por citar algún otro libro que dé una definición más común en el área. En un libro del profesor Alfred Meneses se define *"cryptosystem"* como *"…is a general term referring to a set of cryptographic primitives used to provide information security services"*. Observen que es una definición muy general porque podría describir a un cifrador o funciones de resumen (*hash*), entre otras.

En varios lugares del texto mencionan algo relacionado con datos biométricos. Es sabido que el proceso de escaneo de una red vascular, la palma de la mano, la huella dactilar, etc., da como resultado una matriz. Sugiero también detallar estos datos obtenidos de los escaneos de su interés y que serán entrada para sus algoritmos .

La tercera recomendación es mejorar su planteamiento argumental. Considero que a lo largo del texto se pueden encontrar argumentos que no son claros o no están planteados de forma adecuada y, por lo tanto, no abona a su congruencia lógica. Este señalamiento se complementa con las dos recomendaciones anteriores. También mencionaré ejemplos.

En el tercer párrafo de la Introducción mencionan *"Los criptosistemas biométricos son similares a los sistemas de generación de claves basados en contraseñas…"*. Si consideramos esta definición de Meneses, entonces un *"criptosistema biométrico"* sería "un conjunto de primitivas criptográficas que toman como entradas datos de medidas biológicas". Dicho sea, sigue siendo algo muy general. Por otro lado, un "sistema de generación de claves basados en contraseñas" podemos entenderlo como "un conjunto de algoritmos que toman como entrada una cadena (de bits o caracteres, quizá), aquí llamada 'contraseña', y que dan como salida cadenas de bits dependientes de esa 'contraseña'". Si este razonamiento es correcto, no encuentro una relación de similitud en estos dos conceptos. Si acaso la hay, entonces sugiero expresarla con mayor claridad. En cambio, si no la hay, entonces se debe repensar esta idea.

En este mismo párrafo, mencionan *"…ya que se utilizan para asegurar o generar directamente la clave criptográfica a partir de características biométricas"*. Sugiero detallar lo que se debe entender por "asegurar" y contra qué se desea "asegurar". En otras palabras, detallar los ataques que se están previniendo, el objeto del posible ataque y la estrategia de protección o prevención.

Mencionan también *"Dado que las mediciones biométricas obtenidas durante la inscripción y las autenticaciones son diferentes, estas características no se pueden usar directamente para la generación de claves criptográficas."*. Es confuso que en este enunciado se dice que "las mediciones biométricas… no se pueden usar directamente" para generar claves, pero en el enunciado anterior afirma que los criptosistemas biométricos se utilizan para generar directamente la clave criptográfica. Podrían no referirse a la misma acción, o al mismo contexto, o a algo que haga que no sean una contradicción, pero no se especifica. El enunciado también habla de dos procesos: la inscripción y las autenticaciones. Sugiero explicar estos dos procesos, ya que se puede entender que ocurren en momentos distintos, pero no es clara la idea.

Siguiendo el párrafo mencionan *"Para facilitar la generación de claves, los datos auxiliares o el boceto seguro de las características biométricas se almacenan durante la inscripción"*. No logré entender el sentido de esta frase; no presenta el sujeto del enunciado y tampoco se puede deducir del enunciado anterior. Es necesario detallar cómo se "facilita" y con qué propósito, qué son los "datos auxiliares" y qué es un "boceto seguro". La construcción de esta frase se puede reducir a *"Para facilitar… se almacenan durante la inscripción."*; noten que parece una idea aislada en este párrafo, ya que no vincula los enunciados anteriores con el siguiente, ni complementa a alguno.

El cuarto párrafo de la Introducción expresa una noción de pasos: a partir de una imagen de la red vascular extraer patrones y formar una cadena que será cifrada usando RSA. Sugiero que detalles porqué deciden cifrar con un algoritmo de criptografía asimétrica, porqué particularmente utilizando RSA y no otro algoritmo, porqué la cifra resultante será la entrada para la *Ecuación Mapa Logística*, cómo generan once claves, qué tipo de claves son éstas, porqué once y no otro número, en cuál modo se utiliza el cifrador AES, cómo se genera y cómo interactúa la "llave única de cada persona".

El primer enunciado del primer párrafo de la Justificación menciona *"Actualmente el uso de sistemas biométricos es muy común en cualquier tipo de empresa, institución, etc."*. Acaso, ¿es realmente común?, ¿con cuáles datos estadísticos se sustenta esta afirmación de un "uso común"? Continúa el texto *"…debido a que tiene muchas aplicaciones y proporciona un alto nivel de seguridad para restringir accesos… permitiendo ingresar sólo a personas que se encuentran registradas previamente."*, ¿el supuesto uso común de sistemas biométricos ocurre debido a "tener muchas aplicaciones" en conjunto con "proporcionar un alto nivel de seguridad para restringir accesos" ?, ¿qué se entiende por un "alto nivel de seguridad"?, ¿a cuál registro se refiere dónde deben estar las personas registradas previamente?

El segundo enunciado en este mismo párrafo menciona *"El desarrollo de nuevos sistemas… sigue en desarrollo y, además…"*. Eviten estas redundancias. Menciona también *"…se busca que represente un ahorro significativo y que sean seguros"*, ¿a qué tipo de ahorro se refiere?, ¿en qué sentido se desea que sean seguros los sistemas?

El siguiente párrafo menciona *"Los criptosistemas biométricos son una nueva tecnología que representa una poderosa herramienta en la seguridad de los sistemas de información…"*. Los sistemas criptográficos biométricos llevan existiendo un largo tiempo, por lo tanto, no son nuevos. En la literatura básica de criptografía, se revisan los métodos de autenticación y se señala que se realizan principalmente por tres medios: con lo que se tiene, con lo que se sabe o con lo que se es. Aquí se incluye cualquier propiedad corporal para la identificación de personas. Difiero de que se califique como "nueva tecnología".

Considero que estos tres párrafos adolecen del sustento y coherencia suficiente, tal que compongan la justificación del proyecto. Adicionalmente, sugiero expresar la "motivación del proyecto" y "el planteamiento del problema". Ambos, componentes indispensables de la Justificación y, comúnmente confundidos entre sí.

La cuarta recomendación general es ser cuidadosos con las afirmaciones y aquellas que sean afirmaciones de terceros deberían estar sustentadas con su respectiva cita.

El último enunciado del tercer párrafo de la Introducción menciona *"Por lo tanto, los criptosistemas biométricos también se conocen como sistemas de datos auxiliares [2]."*. Esta referencia apunta a un artículo que no menciona en ningún lugar este enunciado, tampoco realiza ninguna declaración de la que pueda derivarse como una paráfrasis. Así entonces, con este enunciado están adjudicando una afirmación a terceros. Concediendo el beneficio de la duda, esto podría ser resultado de algún error al realizar la cita, pero podría ser también una adjudicación deliberada.

La quinta recomendación general es mencionar proyectos que efectivamente sean comparables con la propuesta que realizan.

La tabla que presentan al final de la Introducción tiene como columnas: “nombre” del proyecto con el cual comparar, algunas “características” arbitrarias, un “lugar” y un “año”. Si ustedes deciden usar una tabla para comparar otros proyectos y contrastar diferencias con su propuesta, entonces sugiero elegir criterios de comparación útiles para destacar las mejoras o las innovaciones que realiza su proyecto respecto a los otros. Esto en el entendido de que esos “otros proyectos” constituyen una idea de “Estado del arte”. Dado que su propuesta presenta un proyecto de ingeniería, resulta evidente que no es relevante destacar un “lugar” o un “año”, suponiendo que sea el lugar de creación, operación o desarrollo del proyecto y el año de desarrollo o puesta en funcionamiento, respectivamente.

De los proyectos descritos en la tabla, uno se enfoca a procesar imágenes vasculares, otro desarrolla un sistema criptográfico con base en las firmas autógrafas, otro implementa un sistema basado en biometría del iris y otro más desarrolla un sistema basado en variedades algebraicas. Sólo uno, excepcionalmente tiene un enfoque medianamente relacionado al de esta propuesta. El trabajo de Carrasco-Fuentes-García-López propone un sistema de verificación biométrico vascular y se limita a la verificación de datos biométricos; nunca propone un sistema criptográfico. Con base en lo anterior, considero que ninguno de los proyectos es, ni de lejos, similar a esta propuesta y, por lo tanto, no son comparables con este. Sugiero realizar una investigación seria a fin de proponer un estado del arte apropiado.

La sexta recomendación general es que las referencias sean más precisas y que permitan al lector localizar el trabajo citado.

De las trece referencias sólo la novena tiene un enlace a un recurso en internet. Es importante proporcionar la información suficiente que permita indagar en las referencias que citan. Una referencia que no se puede disponer, es una referencia inútil. Esto es más importante cuando se realizan afirmaciones, dentro de nuestros textos, que están basadas en trabajos de terceros.

Para mayor referencia de la información necesaria y suficiente en las citas, recomiendo consultar la documentación del paquete de LaTeX “biblatex”, misma que se encuentra actualmente en la versión 3.14. En la sección 2.1.1, podrán encontrar un listado de recursos que se pueden citar y sus campos indispensables y opcionales.

La octava recomendación general es incluir las contribuciones de este proyecto. Estas pueden ser científicas, tecnológicas o sociales, entre otras. Sugiero incluirlas ya que destaca las dimensiones en el que este trabajo tiene influencia y abona a destacar su importancia.

Particularmente en las contribuciones sociales, no debemos olvidar que están estrechamente vinculadas con los principios fundadores de nuestra institución. Ellos expresados en el artículo primero de nuestra Ley Orgánica y relacionados con el concepto de “independencia”.

La novena recomendación general es procurar elegir palabras del español y evitar barbarismos. Si bien algunos extranjerismos, principalmente del inglés, son ampliamente usados en las jergas técnicas o especializadas, no es una buena práctica de escritura. El idioma del texto es el español, no el inglés; por lo tanto, se debe observar sus reglas. Sólo cuando un término de otra lengua no tiene una traducción es cuándo surge la necesidad de incorporar términos, por ejemplo: *to tuit*, *facepalm*, *to bromance*, *unfriendable*, *break-even*, *to realise*, etc.

Por ejemplo: El término *“criptosistema”* tiene origen en el intento de traducción de *“cryptosystem”* pero no es una palabra incorporada al español por ninguna entidad normativa de la lengua. Una equivalencia puede ser simplemente “sistema criptográfico”. Si bien no es una sola palabra, es completamente válida su traducción en un grupo de palabras. Se debe entender que cada lengua tiene sus características prácticas y sus restricciones. La plasticidad del español no es la misma que del inglés.

Otro ejemplo ocurría con *“to encrypt”*, comúnmente traducido como *“encriptar”*, incluso por personas especializadas en criptografía. Hasta hace poco tiempo la traducción válida era “cifrar”, pero fue incorporado al Diccionario de la Lengua Española (DLE).

De los documentos académicos se espera un cierto rigor de sus planteamientos, debido a que suelen tomarse como *verdades*. Sugiero que todos los estudiantes se involucren en revisiones completas a fin de detectar posibles detalles, como primer filtro, y, posteriormente como segundo filtro, compartir a los directores el documento para ser revisado por ellos, ya que con su experiencia pueden detectar otros detalles omitidos por los estudiantes.

[1]: https://www.rae.es/dpd/coma

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

Nombre de archivo: 2020A089-protocolo-evaluacion-1.0.docx
Directorio: /Users/israel/Box Sync/Escom/Trabajos Terminales/2020-A089/protocolo/1.0
Plantilla: /Users/israel/Library/Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
Título:
Asunto:
Autor: UTEyCV-E
Palabras clave:
Comentarios:
Fecha de creación: 11/08/20 4:34:00
Cambio número: 2
Guardado el: 11/08/20 4:34:00
Guardado por: Israel Buitrón Dámaso
Tiempo de edición: 0 minutos
Impreso el: 11/08/20 4:34:00
Última impresión completa
Número de páginas: 3
Número de palabras: 2,767
Número de caracteres: 15,655 (aprox.)