UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 - MAYO 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS COMPARATIVO DE LOS MODELOS DE ENCRIPTACION SIMÉTRICA Y ASIMÉTRICA.

ESTUDIANTE:

XAVIER ALEXANDER CABRERA SERRANO

TUTOR:

ING. IVAN RUIZ PARRALES, MSc.

AÑO 2023

PLANTEAMIENTO DEL PROBLEMA.

Los modelos de encriptación a nivel mundial, son algoritmos que permiten transmitir de una forma segura de los mensajes con absoluta confidencialidad, es decir, que esté fuera del alcance de personas mal intencionadas cuyo objetivo es descifrar el mensaje, con el fin de saber y a su vez divulgar el contenido del mismo. La principal función es mantener la integridad, la confidencialidad de la información. (Montenegro, 2020)

La acción de encriptar proviene desde la antigüedad que datan del siglo V (A.C) y que a su vez fue empleada por los espartanos, cuya función hacen uso de fórmulas matemáticas cuyo propósito es tornar el formato simple de los textos, en un criptograma fuerte de varios caracteres que le da un nivel de seguridad al mensaje y que a su vez para el lector es algo difícil de interpretar o comprender.

En cuanto a este caso de estudio se realizará la un Análisis comparativo de dos métodos de encriptación simétricos o clave privada AES y asimétricos de clave pública RSA, donde estos métodos de encriptado son de vital importancia porque son capaces de proteger el contenido de nuestros archivos o mensajes.

El modelo de encriptación simétrico surgió en el año 1977 por el departamento de comercio y la oficina nacional de estándares EEUU, en colaboración con IBM donde su funcionalidad consiste en aplicar rondas alternas de sustitución de información.

De tal manera el modelo de encriptación asimétrico surge en el año 1978 donde sus creadores fueron Adi Shamir, Ronald Rivest y Leonard Adleman donde su funcionamiento es más complejo basándose en la división sucesiva de números primos grandes, en donde las claves se calculan en la obtención del producto de números primos.

Por medio de este caso de estudio se recopiló y se hizo un análisis de dicha información acerca de los modelos de encriptación para determinar cuál es el mejor en brindar seguridad entre los dos así para dar una buena encriptación y seguridad a los datos, en donde se analizaron cuáles fueron sus puntos débiles y fuertes, en tal sentido la criptografía es un pilar fundamental en la seguridad de la información permitiendo ocultar el contenido de un mensaje aplicando diferentes técnicas de cifrado, entre ellas está el cifrado asimétrico que utiliza distintas claves, por lo menos dos, para cifrar y descifrar el contenido de un archivo y el simétrico por lo consiguiente.

JUSTIFICACIÓN.

La sociedad actualmente está evolucionado debido a los grandes avances de la tecnología con respecto al manejo de la información en sus diversos aspectos son factores altamente relevantes. El presente caso de estudio es relevante en lo tecnológico porque aborda una temática de tendencia y de cómo nos conectamos hoy en día a un medio tan inseguro como es el internet, que resulta ser un tema de investigación constante debido a las nuevas tecnologías que aparecen constantemente. (Naranjo, 2022)

Mediante esta investigación surge la necesidad de realizar la comparación de los modelos de encriptación simétricos y asimétricos, cuyo propósito es dar a conocer cuales es el mejor, donde se conocerá sus ventajas, desventajas, funcionamiento, para así satisfacer el objetivo propuesto de nuestro estudio de caso planteado.

Por medio de esta investigación se busca brindar información que será de vital importancia para las personas que quieran saber acerca del tema de los modelos ya mencionados, para así tener en claro el funcionamiento entre otras características.

Por lo tanto, debido a que existe pocos estudios comparativos entre estos dos métodos, sus funcionalidades, sobre todo sus niveles de seguridad, en el presente caso de estudio es importante se plantea para reforzar un gran conocimiento sobre los modelos de encriptación que se van a investigar. (Piovani, 2017)

OBJETIVOS DEL ESTUDIO

OBJETIVO GENERAL

Analizar y comparar los modelos de encriptación simétrica y asimétrica y explicar el modelo más conveniente en redes privadas utilizadas en diferentes organizaciones que manejan información.

OBJETIVOS ESPECÍFICOS

- Identificar las ventajas y desventajas de los modelos de encriptación simétrico y asimétrico.
- Establecer las fortalezas y debilidades de los mecanismos de encriptación.
- Comparar los niveles de seguridad y analizar los diferentes componentes que tienen los modelos simétricos y asimétricos.

LÍNEA DE INVESTIGACIÓN

La metodología es la forma en la que el investigador ha seleccionado para realizar el proyecto investigativo propuesto, en el cual tiene serie de técnicas o procesos que se emplean para alcanzar los objetivos de la investigación. La metodología que se usó fue la descriptiva, ya que contiene un conjunto de procesos y procedimientos lógicos que permiten identificar las características de la población, el lugar y también hace un análisis detallado de la temática abordada. (Betty Pastora Alejo, 2020)

La investigación descriptivos analiza las características de una población o un fenómeno sin entrar en las relaciones entre ellos. Investigación descriptiva porque lo que hace es definir, clasificar, dividir o resumir donde se usa el enfoque mixto ya que contiene las características tanto de enfoque cualitativo y cuantitativo y tiene como finalidad la comprensión del problema a investigar. el instrumento utilizado para la recopilación de datos de este estudio de caso fue la encuesta. La cual se realiza a la población de estudiantes de la carrera de ingeniería en sistemas de información, en el cual la muestra fue de 100 estudiantes con el objetivo de obtener el nivel de conocimiento acerca de los métodos de encriptación. (Ramos, 2020)

El presente estudio de caso se destaca el análisis comparativo en los modelos de encriptación simétrica y asimétrica donde se hará una comparativa en donde se detallarán todo tipo de cualidades, fortalezas, defectos, etc. La línea de investigación para el desarrollo del presente estudio, se relaciona con la línea del desarrollar estrategias innovadoras y en el desarrollo de sistemas de información, comunicación, emprendimientos empresariales y tecnológicos conjuntamente relacionado con la sublínea de investigación Desarrollo de

Sistemas Informáticos proporcionada por la Facultad de Administración Finanzas e Informática de la Universidad técnica de Babahoyo.

MARCO CONCEPTUAL

¿Qué es encriptar?

La encriptación o también conocida como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea autorizada, consiste en copiar un mensaje utilizando una clave. (Urbina, 2022)

Encriptar, en definitiva, consiste en cifrar: es decir, en transcribir un texto en signos letras, números, entre otros de este modo es posible proteger su contenido”

¿Qué es la encriptación de información?

Encriptar una información significa ocultar el contenido de un mensaje a simple vista, de manera que haga falta una interacción concreta para poder desvelar ese contenido. El contenido de este mensaje pueden ser archivos, datos, mensajes o cualquier tipo de información que se te ocurra. En el contexto de Internet, cualquier contenido que envíes desde tu ordenador a la red puede ser cifrado donde la codificación es uno de los métodos de seguridad de datos más populares y eficaces que utilizan las empresas. (INESDI, 2021)

¿En qué consiste el cifrado actualmente?

El desarrollo de la tecnología y las matemáticas permitió la creación de nuevos métodos de cifrado basados en la aplicación de una función matemática a la información original donde estas operaciones matemáticas se basan en el uso de un algoritmo junto con variables que

cambian el resultado de la función. Son variables, conocidas como claves y son las que se mantienen en secreto para realizar el descifrado posteriormente a lo que cuyo objetivo es descifrar mensajes sin saber de antemano cómo fueron grabados. Cabe recalcar que cualquier intento de criptoanálisis se denomina ataque. Si un ataque tiene éxito, se dice que el sistema ha sido comprometido. (Sandoval, 2021)

Los métodos de cifrado se pueden clasificar de diferentes maneras. Sin embargo, la clasificación general más extendida la divide en dos grupos:

- Criptografía simétrica o de clave privada.
- Criptografía asimétrica o de clave pública.

Criptografía simétrica.

Es la técnica criptográfica más antigua que existe, pero sigue ofreciendo un alto nivel de seguridad y destaca en la utilización de una única clave secreta que se encargará de cifrar y descifrar la información, ya sea información en tránsito con protocolos como TLS, o información en un dispositivo de almacenamiento extraíble, se basa en la utilización de la misma contraseña para el cifrado y también el descifrado del mensaje, “esto significa que para poder ver el contenido del mensaje los usuarios deben de tener la clave secreta, de tal modo si no la tuviesen dicha clave no podrían desencriptar el mensaje y ver su contenido. (VIU, 2021)

Imagen 1 Cifrado Simétrico, 2021. Recuperado de: https://ginzo.tech/blog/tipos-criptografia-cifrados/

Esta criptografía se basa en la utilización de la misma contraseña para el cifrado y también el descifrado del mensaje, lo cual significa que para poder ver el contenido del mensaje los usuarios deben de tener la clave secreta, de tal modo si no la tuviesen dicha clave no podrían desencriptar el mensaje y ver su contenido.

Entre los principales algoritmos para este tipo de cifrados son:

- DES (Data Ecryption Standard). Fue introducido en año de 1973 y fue utilizado durante muchos años el cual tenía gran velocidad y fácil de implementar.
- 3DES. Se basa en el algoritmo DES utilizando claves de 128 bits y actualmente sigue siendo una buena solución en determinados sectores, por lo tanto, está en deterioro.
- AES (Advanced Encryption Standard). Fue creado con el fin de actualizar e creó para actualizar el algoritmo DES original donde algunas de las aplicaciones más habituales con el algoritmo AES son WinZip y las son las de mensajería, como el WhatsApp.
- IDEA (International Data Encryption Algorithm). Fue creado en el año de 1990 y sus creadores fueron Lai y Massey del Swiss Federal Institute of Technology. Una de sus cualidades es su libre distribución lo que ha hecho que se convierta muy popular, sobre todo fuera de EEUU.

- RC5. Inventado por el profesor Ronald L. Rivest del MIT (Massachusetts Institute of Technology) en el año de1994, y destaca siendo algoritmo rápido y simple que puede ser ajustado para conseguir distintos niveles de seguridad.
- Twofish. Se emplea tanto en software y hardware por lo que lo utilizan muchas aplicaciones al ser de uso público donde se puede encontrar en programas como PhotoEncrypt o LPG, así como software de código abierto TrueCrypt.

Criptografía Asimétrica

Se basa en el uso de dos claves, la pública que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado y la privada que no debe de ser revelada nunca. (VIU, 2021)

Imagen 2 Cifrado Asimétrico, 2021. Recuperado de: https://ginzo.tech/blog/tipos-criptografia-cifrados/

Este método de cifrado bastante nuevo, y según la historia cuenta que se basaba en utilizar claves distintas para cifrar y para descifrar un mensaje permitiendo cifrar una clave pública que cualquier persona puede conocer.

Entre los algoritmos de cifrado de clave pública más destacados son los siguientes:

- RSA. Acrónimo de Rivest, Shamor y Adleman, apellidos de los matemáticos que definieron por primera vez este algoritmo y fue el primer algoritmo de cifrado asimétrico ampliamente disponible. Este algoritmo es conocido por la longitud de su clave y su amplio uso para la transferencia segura de datos.
- DSA. Este algoritmo asimétrico es ampliamente utilizado como algoritmo de firma digital. Está disponible en todas las librerías criptográficas existentes como OpenSSL, GnuTLS o LibreSSL. Por lo general, no se usa para el cifrado de datos, sino solo para firmas digitales. DSA se usa más comúnmente en SSH (autenticación de servidor) que el popular RSA.
- Existen muchas otras como la criptografía elíptica, Diffie-Hellman, ElGamal, HASH Functions, MD5 o SHA-1. En cualquier caso, el uso de la criptografía de clave pública está evolucionando rápidamente en los sistemas de seguridad actuales y, por lo tanto, es de esperar que surjan nuevos algoritmos con nuevas funcionalidades.

Cada tipo de cifrado ofrece diferentes ventajas para la comunicación entre las partes. Sin embargo, todos ahora se utilizan en diversas situaciones debido a su singularidad. Por lo tanto, comprender sus diferencias nos permite definir cuál es la opción más factible para cada acción.

	Numero de claves	**Seguridad**	**Velocidad**
Simétrica	La comunicación se establece mediante una clave única.	La clave se envía sin protección, por lo que es baja.	Al solo existir una clave la comunicación es rápida.

Asimétrica	Se establecen dos claves para cada interlocutor.	El mensaje se cifra de manera única para cada usuario, de modo que es alta.	Cada mensaje requiere de 2 claves por lo que la velocidad es lenta

MARCO METODOLÓGICO

La metodología es la forma en la que el investigador ha seleccionado para realizar el proyecto investigativo propuesto, en el cual tiene serie de técnicas o procesos que se emplean para alcanzar los objetivos de la investigación. Por lo tanto, la que se utilizó fue descriptiva, ya que contiene un conjunto de procesos y procedimientos lógicos que permiten identificar las características de la población, la zona y además hace un análisis detallado del tema abordado, donde la Investigación descriptiva desempeña un cargo en definir, clasificar, dividir o resumir. (Alban, 2020)

En este presente estudio de caso se usó el enfoque mixto ya que contiene las características tanto de enfoque cualitativo y cuantitativo y tiene como finalidad la comprensión del problema a investigar. el instrumento utilizado para la recopilación de datos de este estudio de caso fue la encuesta. La cual se realiza a la población de estudiantes de la carrera de ingeniería en sistemas de información, en el cual la muestra fue de 100 estudiantes con el objetivo de obtener el nivel de conocimiento acerca de los métodos de encriptación. (Zeledón, 2020)

RESULTADOS

Mediante lo planteado en el marco metodológico del estudio de caso se implementó una encuesta que contenía 5 preguntas, a un total de 100 personas pertenecientes de la Universidad Técnica de Babahoyo mediante la plataforma Google Forms. Con la encuesta se determinó los resultados de las personas encuestadas con el fin de saber su de conocimiento del tema propuesto y, por otra parte, se llevó a cabo la comparativa de los modelos de encriptación partiendo desde las características de ambos para determinar diferencia entre ellos.

CUADRO COMPARATIVO DE LOS MODELOS DE ENCRIPTACION SIMÉTRICO Y ASIMÉTRICO		
Modelo de Encriptación	**Simétrico**	**Asimétrico**
Claves	Los datos se comparten desde el emisor y receptor	Los datos se comparten de forma Privada
Usos	Su uso es el cifrado de datos	Se utilizan en las Firmas digitales y el Intercambio de claves
Velocidad	Rápida	Lenta
Longitud	Su longitud está comprendida entre los 128 bits 192 bits, y 256 bits	Tiene una longitud constante de 1024 bits
Intercambio de Claves	Este modelo maneja un sistema complejo de intercambios de claves por el canal inseguro.	La clave pública se comparte en cualquier canal pero la privada no se comparte
Seguridad	Integridad, confidencialidad , autentificación	Integridad, confidencialidad , autentificación
Ventajas	Velocidad rápida Eficiencia en grupos reducidos, puesto que sólo es necesaria una clave.	Velocidad lenta No se requiere compartir la clave privada entre emisor y receptor

Desventajas	Requiere compartir la clave entre el emisor y receptor por medios pueden ser inseguros. No permite autenticar al emisor puesto que se usa la misma clave en ambas partes.	Se requiere de un proceso computacional para la generación de las claves

Con el respectivo análisis comparativo en los modelos de encriptación se pudo determinar que los métodos de encriptación escogidos en este estudio de caso son muy eficaces y robustos, ya que tiene como objetivo mantener la integridad, confidencialidad y protección de la información. Por si estos métodos de encriptación no tuviesen algunas de estas funciones existiría el riesgo de perder información importante y estos pueden desencadenar consecuencias no favorables en las áreas de las organizaciones.

Por lo tanto, es complicado determinar cuál es el método de encriptación que sobresale o cuál es el método de encriptación más seguro de entre los dos. El ámbito de la seguridad, se debe centrar en la prevención de ataques o acciones que tengan malas intenciones, con el fin de traer riesgos a la información que está protegida y que es considerada como clasificada. Se ha revisado los dos enfoques destacando tanto sus virtudes como sus debilidades pues como hemos podido comprobar no existe un único sistema de cifrado perfecto que englobe todas las características deseables. Por esta razón se puede deducir que no hay un ganador a la pregunta de cuál es mejor, si la criptografía simétrica o la asimétrica, puesto que dependerá del entorno en el que se vaya a necesitar el cifrado de la información.

En la siguiente tabla se muestra una comparación entre las ventajas y desventajas más destacadas de estos dos modelos de encriptación.

Tipo de Cifrado		
	Ventajas	**Desventajas**
Modelo Simétrico	• Alta tasa de cifrado de datos • Es muy eficaz en entornos reducidos y cerrados • Infraestructura sencilla • Claves de menor tamaño	• Problema en la distribución de claves • La seguridad recae únicamente sobre la clave secreta • No permite la autenticación, de todas formas, la clave no es asociada a un usuario • Gestión de clases compleja a medida que aumenta el número de usuarios
Modelo Asimétrico	• Gestión de claves sencilla • Complejidad computacional de la clave sencilla • No es necesario transmitir la clave privada • Permite intercambio de clave computacionalmente segura • Permite autenticación	• Baja tasa de cifrado • La generación de claves requiere procesos diferentes para cada modelo de cifrado • Tamaños de clave muy grandes • Infraestructura compleja que requiere la participación de una autoridad certificador externa

Como se puede comprobar, muchas de las ventajas que tiene la cifra simétrica son desventajas de la cifra asimétrica. Las fortalezas y debilidades de ambos tipos de criptografía ocasionan que cada uno de estos tipos posea una serie de cualidades y se utilicen para cometidos diferentes.

DISCUSIÓN DE RESULTADOS

De acuerdo a los temas abordados en este estudio de caso y los resultados que se obtuvieron en la realización de la recolección de datos, se puede decir que la acción de encriptar o cifrar, nos es nada más ni menos que transformar texto simples a textos que contiene signos, letra y números, con finalidad darle seguridad a una información, con el fin de tener o mantener intacto e íntegro el contenido del mismo y a su vez mantener alejada de las personas que quieran irrumpir la seguridad del mensaje.

Hoy en día la encriptación es uno de los métodos más usado por instituciones importantes a nivel mundial, con el objeto de proteger información muy importante y delicada, en el mundo de la criptografía existen dos categorías que son: criptografía asimétrica que es conocida como clave pública y criptografía simétrica como clave privada. La criptografía asimétrica, es un método más antiguo que existe, pero a pesar de su tiempo de aparición sigue dando mayor seguridad de los datos, ya que utiliza una clave de forma secreta para encriptar y otra para descifrar el contenido del mensaje.

Para poder descifrar el mensaje el usuario debe de tener la clave secreta, porque si no la tuviese no podría ver el contenido del mensaje. La criptografía asimétrica se basa en el uso de dos claves que es la pública y la privada, la pública se puede difundir sin ningún problema, la privada no se debe revelar para así proteger la información. Por otro lado, se tiene los métodos de encriptación escogidos en el caso de estudio en el cual son modelos de encriptación Simétrico y Asimétrico.

CONCLUSIONES

Una vez dado por desarrollado el presente caso de estudio, tomando en cuenta el respectivo análisis de los resultados se llegó a las siguientes conclusiones: tanto las ventajas y desventajas de los cifrados son ideales para determinar su rendimiento.

El nivel de seguridad de los modelos de encriptación es favorable porque es importante para la seguridad, confiabilidad y confidencialidad de la información de una determinada empresa, organización, etc.

Un Modelo de encriptación ideal para la seguridad de la información es algo complejo de decidir ya que ambos métodos tienen su nivel de protección a la hora de encriptar la información encomendada aplicando sus acciones de seguridad.

RECOMENDACIONES

Determinadas las conclusiones de este estudio de caso se procede a realizar las siguientes recomendaciones:

- Insistir en continuar el proceso de estudio de las ventajas y desventajas con el fin de detallar cual es el método que tiene más ventaja sobre el otro.
- Sugerir trabajando con los tres pilares de la información para tener una buena seguridad de la información.
- Debido al avance de la tecnología, se recomienda seguir el respectivo estudio de los métodos de encriptación que se escogieron para su pertinente comparación, para así decidir cuál es el más robusto a la hora de brindar seguridad de la información.

BIBLIOGRAFÍA

Alban, G. P. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Recimundo*.

Betty Pastora Alejo, A. F. (2020). Importancia de la asignatura metodología de la investigación para la formación investigativa del estudiante universitario. *Conrado, 16(73)*, 295-302.

INESDI. (24 de Agosto de 2021). *Breve introducción a la Criptografía.* Obtenido de INESDI: https://www.inesdi.com/blog/breve-introduccion-a-la-criptografia/

Montenegro, I. (Febrero de 2020). *Encriptación Simétrica y Asimétrica: Conoce sus diferencias*. Obtenido de Tech-Blog: https://www.gb-advisors.com/es/encriptacion-simetrica-y-asimetrica-conoce-sus-diferencias/

Naranjo, G. (2022). écnicas, mecanismos de seguridad y encriptación de la información y desarrollo de aplicaciones: estudio de mecanismos de detección de mensajes ocultos utilizando modelos estadísticos. *http://bibdigital.epn.edu.ec/handle/15000/22405*.

Piovani, J. I. (2017). Los Estudios Comparativos:algunas notas históricas,epistemológicas y metodológicas. *Scielo*.

Ramos, C. (2020). Los Alcances de una investigación. *CienciAmérica, ,* 1-6.

Sandoval, J. R. (2021). Sistema de cifrado para computadores portatiles para instituciones publicas ecuatorianas. *Pontifica Universidad Católica del Ecuador - Sede Ambato*.

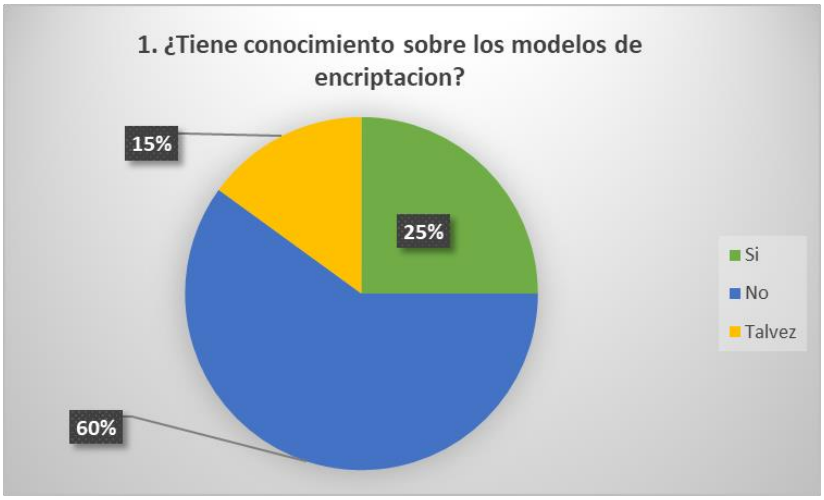
Urbina, H. C. (2022). Análisis de algoritmos de encriptación de datos de texto, una revisión de la literatura científica. *Universidad Privada del Norte*.

VIU. (9 de Agosto de 2021). *Qué es la criptografía y cuáles son sus usos.* Obtenido de Universidad VIU: https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos

Zeledón, L. N. (2020). Investigación en Informática: el enfoque alternativo. . *Technology Inside by CPIC*, 1-15.

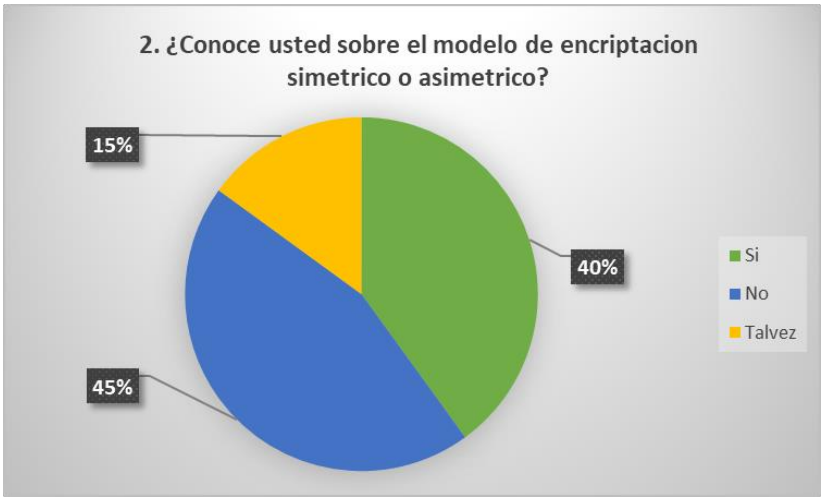
ANEXOS

Resultado de las encuestas tomadas en Google Drive



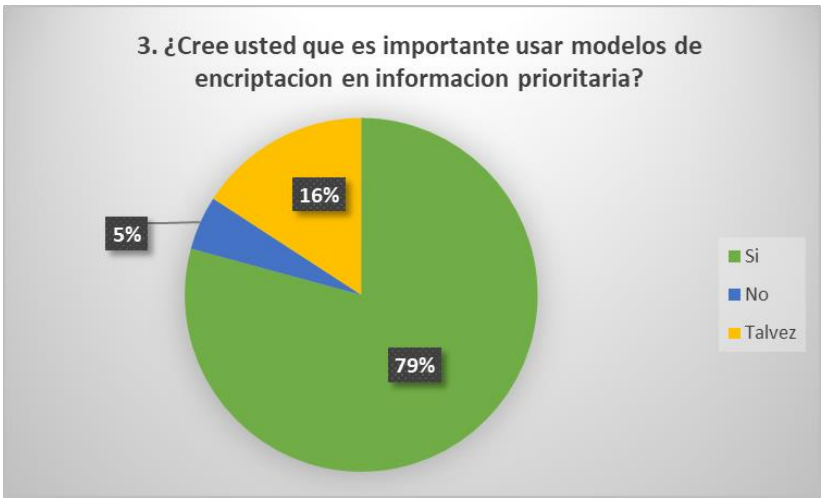
1 Grafico estadístico de resultados de la pregunta No. 1

Análisis: El 60% de las personas que respondieron las encuestas respondieron que no tienen conocimiento acerca de los modelos de encriptación, tanto el 25% si lo tiene y el 15% talvez; dando en cuenta que pocos tienen conocimiento sobre el tema.



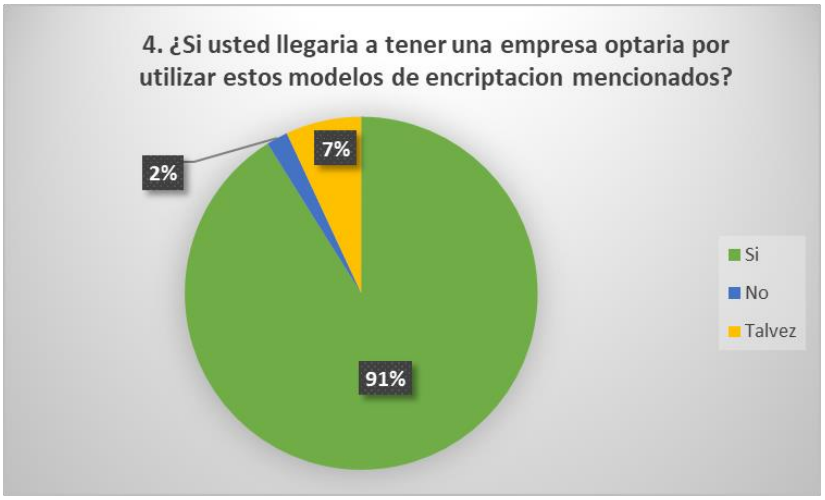
2 Grafico estadístico de resultados de la pregunta No. 2

Análisis: Sobre si tienen conocimiento acerca de los modelos planteados los resultados obtenidos de esta pregunta son valores neutros. Estando entre un 40%, 45% y un 15%.



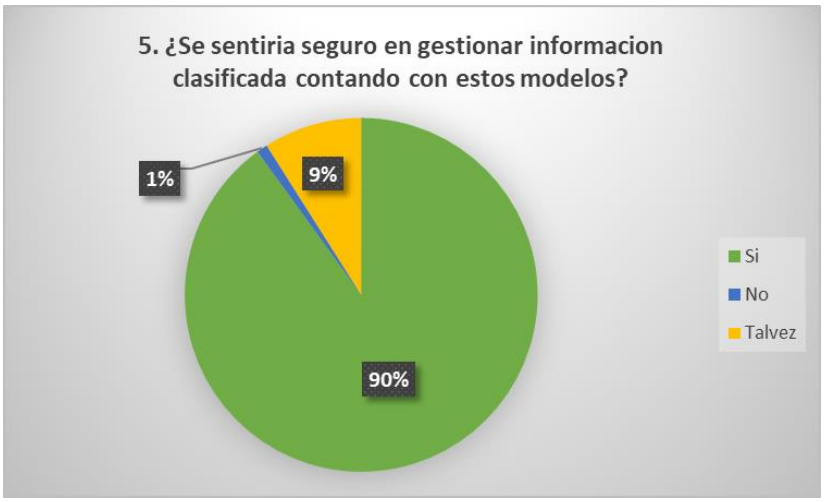
3 Grafico estadístico de resultados de la pregunta No. 3

Análisis: Acorde a la pregunta si es importante usar modelos de encriptación prioritaria con un 79% las personas encuestadas respondieron, mientras que con un 16% y un 5% estarían en dudas, sabiendo que no pueden tener conocimiento previo acerca de los modelos.



4 Grafico estadístico de resultados de la pregunta No. 4

Análisis: Con el 91% de personas encuestadas si optarían por utilizar los modelos de encriptación teniendo en cuenta que en una empresa se debe de proteger la información, mientras que un 2% responden negativamente y un 7% talvez le gustaría implementar.

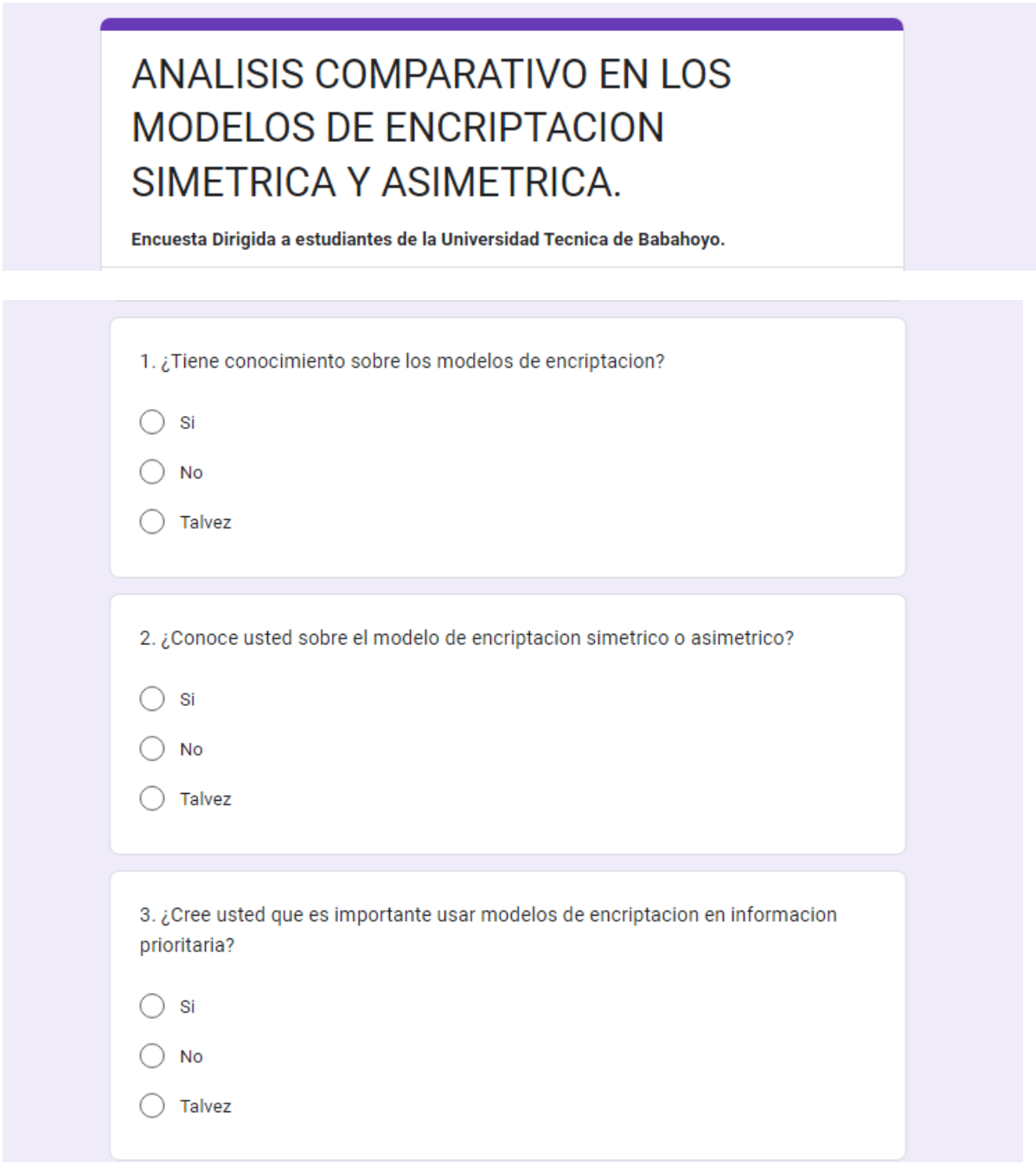


5 Grafico estadístico de resultados de la pregunta No. 5

Análisis: Un 90% de aciertos afirma que las personas encuestadas si se sentirían seguros en gestionar su información en base a modelos de encriptación ya que actualmente en la actualidad existen varios modos de sustraer información y es de vital importancia optar por esta alternativa que puede ser favorable en varias entidades.

Encuesta en Google Drive

Enlace: https://forms.gle/zMgY8m4RzYntMVWq7



ANALISIS COMPARATIVO EN LOS MODELOS DE ENCRIPTACION SIMETRICA Y ASIMETRICA.

Encuesta Dirigida a estudiantes de la Universidad Tecnica de Babahoyo.

1. ¿Tiene conocimiento sobre los modelos de encriptacion?

- ◯ Si
- ◯ No
- ◯ Talvez

2. ¿Conoce usted sobre el modelo de encriptacion simetrico o asimetrico?

- ◯ Si
- ◯ No
- ◯ Talvez

3. ¿Cree usted que es importante usar modelos de encriptacion en informacion prioritaria?

- ◯ Si
- ◯ No
- ◯ Talvez

4. ¿Si usted llegaria a tener una empresa optaria por utilizar estos modelos de encriptacion mencionados?

- ◯ Si
- ◯ No
- ◯ Talvez

5. ¿Se sentiria seguro en gestionar informacion clasificada contando con estos modelos?

- ◯ Si
- ◯ No
- ◯ Talvez

Enviar

Borrar formulario

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMACION

Babahoyo 29 de Marzo del 2023

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: el/la, Sr./Sra./ Srta.: **CABRERA ZAMBRANO XAVIER ALEXANDER**, cuyo tema es: **ANáLISIS COMPARATIVO DE LOS MODELOS DE ENCRIPTACION SIMéTRICA Y ASIMéTRICA.,** certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de **[7 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.


CERTIFICADO DE ANÁLISIS

CASO DE ESTUDIO XAVIER CABRERA

7%

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1		2%		
2		1%		
3		< 1%		

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

Ing. Sist. Iván Rubén Ruiz Parrales, Msg
DOCENTE DE LA FAFI.