UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2021 – ABRIL 2022

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 MÉTODOS DE ENCRIPTACIÓN AES Y RSA, PARA LAS SEGURIDADES DE LOS SISTEMAS DE INFORMACIÓN

ESTUDIANTE:

CARLOS ELIAS YANCE SÁNCHEZ

TUTOR:

ING. NARCISA MARIA CRESPO TORRES, MSc.

AÑO 2022

Resumen

Las organizaciones a nivel mundial tienen en mente la inversión de la seguridad de los datos, con el fin de dar una mayor seguridad de la información que guardan en ciertas áreas de dichas empresa u organizaciones.

La seguridad de los datos, tiene como finalidad ganar más terreno, en cuanto avanza la tecnología y el ingreso de volumen de datos e informaciones importantes, de modo que esta seguridad de los datos tiene tres pilares clave que son la integridad, confidencialidad, disponibilidad de la información.

La metodología que se usó fue la descriptiva ya que analiza las características que ayudan a identificar los puntos del tema a investigar. Es por eso, que en este estudio de caso comparativo se realizó el análisis de los métodos de encriptación AES y RSA para la seguridad de los sistemas de información, en donde se mencionó puntos clave de cada uno de estos métodos aplicados a los sistemas de información, como su funcionalidad, nivel de seguridad, longitudes de claves, compatibilidad.

Por lo tanto, se hizo recolección datos, para obtener información para así determinar el nivel de conocimientos se tiene acerca de los métodos que se escogieron a analizar en este estudio de caso, por lo cual se obtuvo datos favorables.

Palabras claves: métodos de encriptación, seguridad de información, criptografía asimétrica y simétrica.

PLANTEAMIENTO DEL PROBLEMA

Los métodos 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 de los algoritmos de encriptación es mantener la integridad, la confidencialidad, la refutabilidad de la información.

Con respecto al primer punto se dice que los algoritmos o métodos de encriptación tienen la finalidad de cifrar los mensajes, hay que mencionar que esta acción de encriptar proviene desde la antigüedad que datan del siglo V(a.c) y que a su vez fue empleada por los espartanos, además que los algoritmos de encriptación 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.

La criptografía simétrica surgió desde la antigüedad como ya se mencionó antes, pero su desarrollo fue durante la segunda guerra mundial, en donde la parte bélica la uso con la finalidad de encriptar las comunicaciones, es decir fue la pionera en aparecer, mientras tanto la criptografía asimétrica se creó en el año 1976 por Ralph Merkel, Whitfield Diffie y Martin Hellman, la criptografía asimétrica surgió para no generar problemas con la criptografía simétrica a la hora de realizar el intercambio de sus claves.

En cuanto a este caso de estudio se realizará la comparación de dos métodos de encriptación de clave privada AES (simétricos) y de clave pública RSA (asimétricos), el ámbito

de encriptación, estos métodos de encriptado son de vital importancia porque son capaces de proteger el contenido de nuestros archivos o mensajes.

El método de encriptación AES surgió en el año 1977 por el departamento de comercio y la oficina nacional de estándares de los Estados Unidos en colaboración conjunta con la empresa IBM y su funcionalidad consiste en tomar textos planos y aplicar rondas alternas de sustitución y permutación.

El método de encriptación RSA surgió en el año 1978 y fue creado por los inventores Ronald Rivest, Adi Shamir y Leonard Adleman y su funcionamiento es más complejo y se basa 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 métodos o algoritmos de encriptación para determinar cuál es el mejor en brindar seguridad entre los dos métodos para dar una buena encriptación y seguridad a nuestros datos, en donde se analizaron cuáles fueron sus puntos débiles y fuertes de estos métodos de encriptación.

JUSTIFICACIÓN

El presente estudio de caso de centra en la investigación de los métodos de encriptación ideales para la seguridad de los datos de los sistemas de información, con la finalidad de determinar cuál es el método más factible que brinda mayor seguridad de los datos, en el cual es muy importante conocer cómo es su funcionamiento en base a la información que se va a encriptar o codificar, con el fin de darles seguridad a los mismo, ya que hoy en día existen muchas maneras de conseguir información de otras personas sin su consentimiento.

Mediante esta investigación surge la necesidad de realizar la comparación de los métodos de encriptación simétricos y asimétricos, con el propósito de dar a conocer cuales es el mejor entre los dos métodos que se va comprar, en donde se conocerá sus ventajas, desventajas, funcionamiento, para así satisfacer el objetivo propuesto de nuestro estudio de caso.

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 métodos de encriptación, para así tener en claro el funcionamiento sobre estos métodos de encriptación escogidos en esta investigación.

Debido a que existe pocos estudios comparativos entre estos dos métodos, como son el método de encriptación AES y RSA, sobre sus funcionalidades, sobre sus niveles de seguridad, el presente caso de estudio es importante para reforzar un gran conocimiento sobre los métodos de encriptación que se van a investigar.

OBJETIVOS

Objetivo general

- Analizar los métodos de encriptación AES y RSA ideal para la seguridad de los datos.

Objetivos específicos

- Identificar las ventajas y desventajas de los métodos de encriptación AES y RSA.
- Comparar el nivel de seguridad de los métodos de encriptación dirigidos a los sistemas de información.
- Determinar el método de encriptación ideal para la seguridad en los sistemas de información.

LÍNEAS DE INVESTIGACIÒN

En el siguiente caso de estudio está enmarcado bajo la línea de investigación que es Sistemas de información y comunicación, emprendimiento e innovación con su referente sublínea en redes y tecnologías inteligentes de software y hardware.

La línea y sublínea de investigación que se utilizó en este estudio de caso tienen correlación porque tiene que ver con el uso de desarrollo tecnológico, combinación de tecnológica, también en la utilización de dispositivos tecnológicos con la finalidad de obtener datos o información mediante la conexión en la red y también a la seguridad de la información.

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 (Romero et al., 2018, p 21)”.

La acción de encriptar consiste en copiar un mensaje utilizando una clave. “Encriptar, en definitiva, consiste en cifrar: es decir, en transcribir un texto en signos letras, números, entre otros. De acuerdo con una determinada clave. De este modo es posible proteger su contenido” (Pérez Porto & Merino, 2019).

¿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” (FERNÁNDEZ, 2020). 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.

“Actualmente, la codificación es uno de los métodos de seguridad de datos más populares y eficaces que utilizan las empresas” (Access Quality, 2021). Existen dos tipos principales de cifrado de datos: el cifrado asimétrico, también conocido como cifrado de clave pública, y el cifrado simétrico.

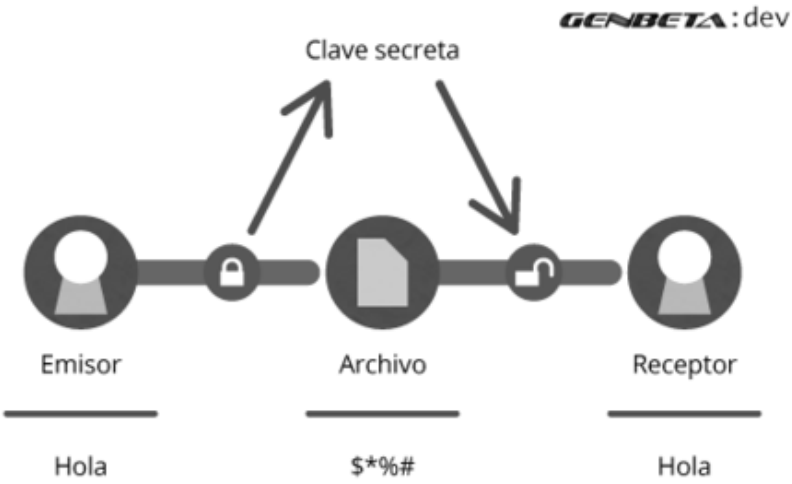
Tipos de encriptación: Criptografía simétrica, Criptografía asimétrica.

Criptografía simétrica

Es la técnica criptográfica más antigua que existe, pero sigue ofreciendo un alto nivel de seguridad. “Se basa 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" (López A. , 2021).

Figura 1 *Método de la Criptografía Simétrica*



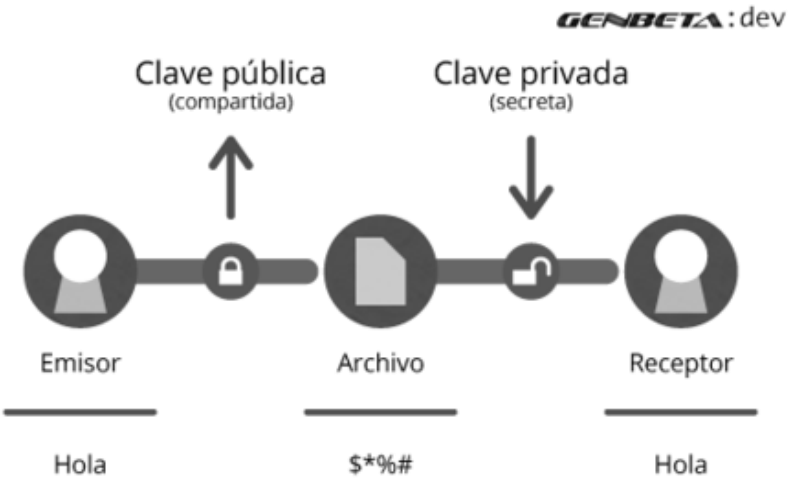
Fuente*:* Funcionalidad de la criptografía simétrica. Tomada de Pedro Gutierrez, 2017 (www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida).

Esta criptografía 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" (López A. , 2021).

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" (GUTIÉRREZ, 2017).

Figura 2 *Método de la Criptografía Asimétrica*



Fuente: Funcionalidad de la criptografía simétrica. Tomado de Pedro Gutierrez, 2017 (www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida).

El origen del AES o Rijndael

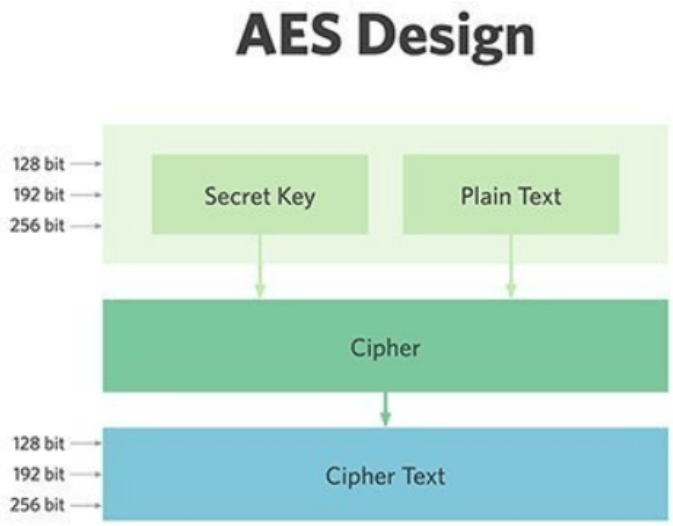
Al estándar Advanced Encryption Standard también se le llama Rijndael, en honor a los dos criptógrafos belgas que lo desarrollaron: Vicent Rijmen y Joan Daemen. Este nació en 1997, cuando el Instituto Nacional de Normas y Tecnología estadounidense (NIST) decidió empezar a desarrollar este nuevo estándar, después de que el Data Encryption Standard (DES) existente en aquel momento empezase a ser susceptible a ataques de fuerza bruta. (Gómez, 2021)

¿Qué es el método de encriptación AES?

“Es el algoritmo más popular empleado en criptografía simétrica, es decir, misma clave para el cifrado y descifrado. El algoritmo es fácil de implementar, requiere poca memoria y opera sobre una matriz de cuatro bytes” (Palacios, 2020, p. 131-132).

“Es un sistema de clave simétrica, lo cual le otorga una mayor seguridad, ya que la clave usada debe ser conocida para el cifrado como para el descifrado, tanto emisor como receptor necesitan una copia de la llave maestra correspondiente” (López J. , 2021).

Figura 3 Método de encriptación AES (Advanced Encryption Standard)



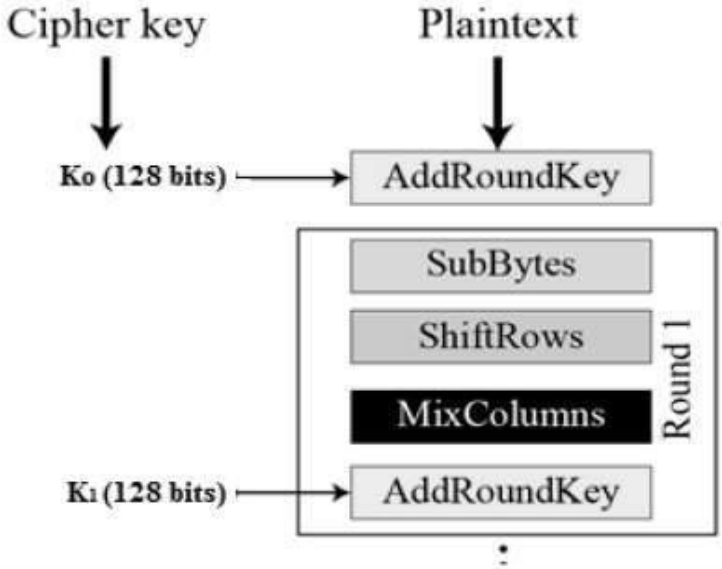
Fuente: Estructura de la funcionalidad del método de encriptación AES. Tomado de Damaris, 2021

(https://www.guiahardware.es/que-es-como-funciona-y-cuan-segura-es-la-encriptacion-aes-256-bits/#Que_es_el_AES)

¿Cómo funciona este sofisticado cifrado?

Según (Miltrucos, 2021) dice que “El algoritmo de cifrado AES pasa por múltiples rondas de cifrado. Incluso puede pasar por 10, 12 o 14 rondas de esto”. Este método de encriptación usa diferentes rondas como se mencionó antes, 10 rondas para claves de 128 bits, 12 rondas para claves de 192 bits y 14 rondas para las claves de 256 bits.

Figura 4 *Intercambio de filas y columnas del método de encriptación AES*



Fuente: Subprocesos del método de encriptación AES. Tomado de tutorials points, 2021 (https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm)

Expansión de claves

"Crea nuevas claves, conocidas como claves redondas, para cada ronda de cifrado posterior, utilizando el programa de claves de Rijndael" (Daniel, 2021).

Adición de clave de ronda

"Durante la cual la clave de ronda inicial se agrega a la combinación de datos que se ha dividido" (Daniel, 2021).

Sustitución de bytes (SubBytes)

"Sustituye cada byte con un byte diferente según el cuadro de sustitución de Rijndael S-box" (Daniel, 2021).

Cambio de fila

"Mueve cada fila de los datos divididos un espacio a la izquierda para la segunda fila, dos espacios a la izquierda para la tercera fila y tres espacios a la izquierda para la cuarta fila" (Daniel, 2021).

Mezcla de columnas

"Utiliza una matriz preestablecida para multiplicar las columnas de datos divididos y crear un nuevo bloque de código" (Daniel, 2021).

Adición de clave redonda

"Durante la cual se añade otra clave redonda a la mezcla de columnas" (Daniel, 2021).

"Este método de encriptación realiza la sustitución de bytes muchas veces, en donde cambia filas y mezcla columnas para agregar nuevas claves. Esto se hace dependiendo de la longitud de la clave" (Daniel, 2021).

"El proceso de descifrado es el proceso de cifrado realizado a la inversa. Cada una de las rondas consta con 4 procesos de forma inversa, como son: agregar clave redonda, mezclar columnas, cambiar filas, sustitución de bytes" (Daniel, 2021).

¿Qué es el método de encriptación RSA?

"El criptosistema RSA es el algoritmo criptográfico de clave pública más utilizado en el mundo. Puede usarlo para cifrar un mensaje sin necesidad de intercambiar una clave secreta por separado (Telsy, 2021)".

El cifrado RSA es una tecnología de criptosistema de clave pública que emplea el algoritmo RSA. Este algoritmo se centra en la dificultad de factorizar números muy

grandes. La persona que encripta un mensaje con encriptación RSA necesita encontrar el producto de dos números primos grandes. Estos números se utilizarán como claves privadas. Los números primos grandes se descartan para aumentar la dificultad del descifrado no deseado. (History Computer Staff, 2021)

Función del método de encriptación RSA

Este método genera claves de forma pública y privada con anterioridad al ejecutar las funciones con el fin de generar texto cifrado y sin el formato, por lo cual este método usa variables y parámetros.

- Elige dos números primos grandes (p y q)
- Calcular n = p*q y z = (p-1)(q-1)
- Elija un número e donde 1 < e < z
- Calcular d = e-1mod(p-1)(q-1)
- Puede agrupar un par de claves privadas como (n, d)
- Puede agrupar un par de claves públicas como (n,e)

Función de cifrado/descifrado

“Al realizar la generación de claves, esta entrega los parámetros a las funciones que realizan en cálculo del texto cifrado y texto sin el formato empleando la clave referente” (Simplilearn , 2022).

- Texto sin formato es m, texto cifrado = me mod n.
- Texto cifrado es c, texto sin formato = cd mod n

“Para comprender mejor los pasos anteriores, puede tomar un ejemplo donde p = 17 y q = 13. El valor de e puede ser 5 ya que satisface la condición 1 < e < (p-1) (q-1)” (Simplilearn , 2022).

- norte = p * q = 91
- D = e-1mod(p-1)(q-1) = 29
- Par de claves públicas = (91,5)
- Par de claves privadas = (91,29)

El valor del texto sin formato (m) es 10, en donde se usa la fórmula me mod n = 82 para cifrarlo.

Para realizar el descifrado del texto cifrado (c) de los datos originales, usa la fórmula cd mod n = 29.

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. “Este método se basa en la formulación de hipótesis las cuales pueden ser confirmadas o descartadas por medios de investigaciones relacionadas al problema” (Palestina, 2021). Al mismo tiempo, en el actual trabajo se ha seleccionado el caso de estudio como modelo de investigación debido a las cualidades que posee el mismo.

En este trabajo investigativo, que es el estudio de caso, se usó el método no experimental ya que según (Wilson, 2021) “la investigación no experimental es aquella que carece de la manipulación de una variable independiente”. En lugar de manipular una variable independiente, los investigadores que realizan investigaciones no experimentales simplemente miden las variables tal como ocurren naturalmente (en el laboratorio o en el mundo real). 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.

“La investigación descriptiva analiza las características de una población o fenómeno sin entrar a conocer las relaciones entre ellas. La investigación descriptiva, por tanto, lo que hace es definir, clasificar, dividir o resumir” (Arias, 2021).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.

RESULTADOS

Mediante lo planteado en el marco metodológico del estudio de caso se implementó una encuesta que contenía 5 preguntas (ver anexo 2) a un total de 100 personas pertenecientes de la Universidad Técnica de Babahoyo mediante la plataforma Google Forms. Mediante esta encuesta se conoció los valores numéricos concretos de cada una de las preguntas antes planteadas y dirigidas a personas con el fin de saber su nivel de conocimiento del tema a investigar, por otra parte, se llevó a cabo la comparativa de los métodos de encriptación partiendo desde las características de ambos para determinar diferencia entre ellos.

Tabla 1 *Cuadro comparativo de Algoritmos Simétrico y Asimétrico*

Algoritmos	**AES**	**RSA**
Claves	Se comparte desde el emisor y receptor	Privada
Usos	Cifrado de datos	Firmas digitales Intercambio de claves
Velocidad	Rápida	Lenta
Longitud	128 bits 192 bits 256 bits	1024 bits
Intercambio de claves	Complejo el intercambio por el canal inseguro	La clave pública se comparte en cualquier canal, pero la privada nunca se comparte.

Seguridad	Integridad , confidencialidad, autenticación.	Integridad , confidencialidad, autenticación.

Fuente: Ronald Leodan Coloma Macias. Tomado de estudio comparativo de software basados en el cifrado y protección de datos, 2021 (http://dspace.utb.edu.ec/bitstream/handle/49000/10508/E-UTB-FAFI-SIST-000228.pdf?sequence=1&isAllowed=y)

Tabla 2 Característica de método de encriptación AES Y RSA

	Ventajas	**Desventajas**	**Seguridad**	**Utilidades**	**Algoritmos**	**Longitud de claves**
Simétricos	Velocidad rápida Eficiencia en grupos reducidos, puesto que sólo es necesaria una clave.	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	• Confidencialidad • Integridad	• Cifrado de mensajes	AES tamaño de 128, 192 o 256 bits.	56 bits/vulnerables 256 bits/seguros

		en ambas partes.				
Asimétricos	Velocidad lenta No se requiere compartir la clave privada entre emisor y receptor	Se requiere de un proceso computacional para la generación de las claves	• Confidencialidad • Integridad • Autenticidad de origen	• Cifrado de mensajes • Firma digital • Intercambio de claves	RSA tamaño mayor o igual a 1024 bits	1024 bits mínimos

Fuente: Ronald Leodan Coloma Macias. Tomado de estudio comparativo de software basados en el cifrado y protección de datos, 2021 (http://dspace.utb.edu.ec/bitstream/handle/49000/10508/E-UTB-FAFI-SIST-000228.pdf?sequence=1&isAllowed=y)

CryptoExpert

Es un software diseñado específicamente para proporcionar almacenamiento de datos seguro para ordenadores portátiles y ordenadores de sobremesa y garantizar una seguridad de datos óptima. CryptoExpert ofrece mayor seguridad, mejor fiabilidad y facilidad de uso que el sistema de cifrado NTFS transparente implementado en el sistema de archivos integrado de Windows. La caja fuerte de seguridad aparece como un disco duro regular para todas las aplicaciones de Windows y nadie puede desbloquear sin una contraseña. (CryptoExpert, 2021)

Tabla 3 características técnicas CryptoExpert

Algoritmo	Contraseña	Seguridad	Compatibilidad
AES- 256	Acceso a datos denegado sin contraseña	• Bóvedas seguras de tamaño ilimitado. • Acceso transparente a archivos y carpetas	Windows 10,8 Windows 7 32 y 64 bits

Fuente: Ronald Leodan Coloma Macias. Tomado de estudio comparativo de software basados en el cifrado y protección de datos, 2021 (http://dspace.utb.edu.ec/bitstream/handle/49000/10508/E-UTB-FAFI-SIST-000228.pdf?sequence=1&isAllowed=y)

Boxcryptor

"Ciframos tus archivos y carpetas sensibles tanto de tu ordenador como de servicios como Dropbox, Google Drive, OneDrive y muchos otros almacenes en la nube" (Boxcryptor, 2022).

"Combina los beneficios de la mayoría de los servicios de almacenamiento en nube fácil de usar con los mejores estándares de seguridad en todo el mundo" (Boxcryptor, 2022).

Esta parte trata de un software que cifra los datos de un dispositivo antes de realizar la sincronización y de forma extrema y los mantiene en la nube de una forma segura. Permite realizar administración personalizada, gestión de usuarios y protección de cuentas.

Tabla 4 *Características técnicas Boxcryptor*

Algoritmos	Contraseñas	Seguridad	Compatibilidad
AES-256 RSA	➢ Se puede exportar las claves a un archivo de clave local Hash codificado en el servidor. ➢ Autenticación de usuario y descifrado de la clave privada del usuario	➢ Datos confidenciales y la información personal se cifran adicionalmente. ➢ Clave disponible durante el tiempo de ejecución.	➢ Windows ➢ Android ➢ MacOS ➢ iOS ➢ Portable ➢ Microsoft Teams ➢ Dropbox ➢ Google drive ➢ One Drive, Box, iCloud Drive.

Fuente: Ronald Leodan Coloma Macias. Tomado de estudio comparativo de software basados en el cifrado y protección de datos, 2021 (http://dspace.utb.edu.ec/bitstream/handle/49000/10508/E-UTB-FAFI-SIST-000228.pdf?sequence=1&isAllowed=y)

Análisis

De acuerdo con las diversas características que presentan los softwares criptográficos, se elaboró un cuadro comparativo de sus elementos clave, expresados en criptografía, seguridad, compatibilidad y algoritmos de procesamiento, con el objetivo de enfocarse en las herramientas de mayor impacto.

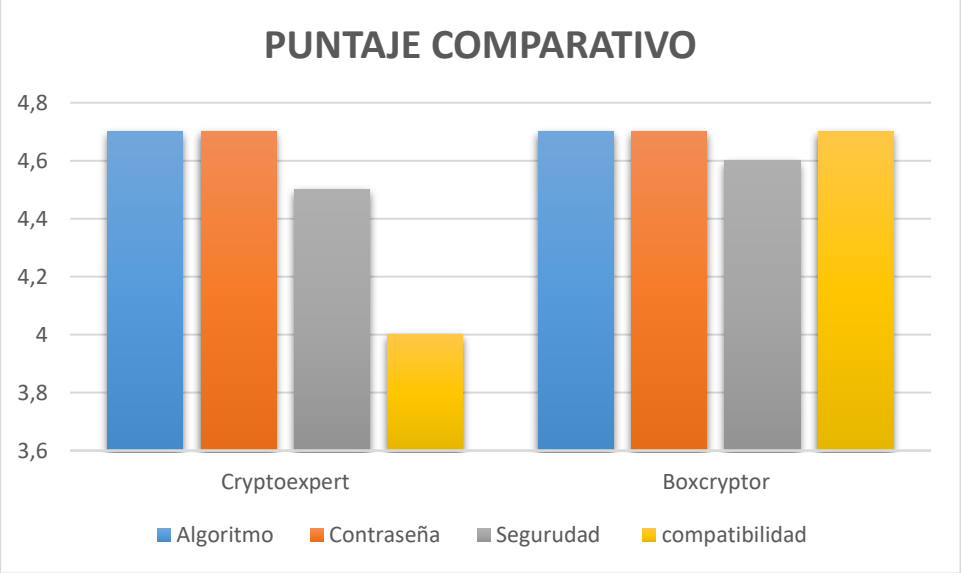
Tabla 5 *Cuadro característico comparativo de softwares de cifrado*

	Algoritmos	Contraseña	Seguridad	Compatibilidad SO	Compatibilidad en la Nube
	AES-256	Acceso de datos denegado sin contraseña	• Bóvedas seguras de tamaño ilimitado	Windows 10 / 8 /7 32 y 64 bits	

Cryptoexpert			• Acceso transparente a archivos y carpetas		
Boxcryptor	• AES longitud de clave de 256 bits • RSA longitud de clave de 4096 bits	• Administración de claves cifradas • Has cifrado • Claves almacenadas en el servidor • Restablecimiento de contraseña	• Auditoria de actividades • Estándar PBKDF2 con HMACSHA512 de estiramiento y fortalecimiento • Compartir sin revelar contraseñas	• Windows • Mac OS • iOS • Android	• Google Drive • Dropbox • OneDrive • iCloud Drive

Fuente: Ronald Leodan Coloma Macias. Tomado de estudio comparativo de software basados en el cifrado y protección de datos, 2021 (http://dspace.utb.edu.ec/bitstream/handle/49000/10508/E-UTB-FAFI-SIST-000228.pdf?sequence=1&isAllowed=y)

Ilustración 1 Puntaje de comparación sobre las herramientas de cifrado



Elaboración con los datos de la tabla 5

Fuente: Yance Sánchez Carlos Elías

En definitiva, se realizado la comparación entre los métodos de encriptación relacionados a los sistemas de información mediante una tabla comparativa con el fin de determinar la seguridad de los mismos como son CryptoExpert, boxcryptor, cabe mencionar que estos softwares tienen funcionalidades diferentes cryptoexport es un software de código abierto y el boxcryptor es de código cerrado, en el cual hacen énfasis en la seguridad en la nube, forma que ofrece cifrado de forma local en la nube.

Mediante la comparativa se pudo determinar que los métodos de encriptación escogidos (AES y RSA) en este estudio de caso son muy robustos y eficaces, 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. Es por eso, que es complicado determinar cuál es el método de encriptación que sobresale del otro 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.

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 método de encriptación AES y método de encriptación RSA. Hablemos primero del AES (Advanced Encryption Standard), este es un método de encriptación simétrico, que fue creado por los criptógrafos belgas Vicent Rijmen y Joan Daemen, junto al Instituto Nacional de Normas y Tecnología estadounidense (NIST).

Este método de encriptación otorga seguridad a los datos, su clave la usa tanto el emisor como el receptor para poder descifrar el mensaje y su funcionamiento consiste en hacer rondas múltiples de cifrado. Estas rondas de se realizan dependiendo el tamaño de los bits entre estas tenemos de 128 bits (10 rondas), 192 bits (12 rondas) y 256 bits (14 rondas). Este método de encriptación realiza las siguientes acciones que son: expansión de claves, adición de claves, sustitución de bytes, cambio de filas, mezcla de columnas.

Mientras tanto, el método de encriptación RSA, es un método de encriptación de clave pública en el cual lo utiliza todo el mundo. Este método de encriptación es un método de intercambiar la clave secreta por separado.

Este algoritmo se centra en el nivel de dificultad de factorizar números muy complejos, ya que usa dos números primos, en donde estos números se usan como clave de forma privada.

La función de este método de encriptación consiste en elegir dos números primos grandes, los calcula (multiplica y resta), elige un número mayor.

Por otro lado, se realizó la comparación de software como son: CryptoExpert, Boxcryptor que usan estos métodos de encriptación en donde se tuvo en cuenta ciertos parámetros como contraseña, seguridad, compatibilidad, con la finalidad de determinar cuál es el más sobresaliente de entre los dos.

CONCLUSIONES

Una vez desarrollado el estudio de caso tomando en cuenta el respectivo análisis de los resultados se llegó a las siguientes conclusiones: las ventajas y desventajas de los métodos de encriptación son ideales para determinar su funcionamiento al momento de encriptar.

El nivel de seguridad de los métodos de encriptación es favorable ya que es importante para la seguridad, fiabilidad, confidencialidad de la información.

El método 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.

REFERENCIAS

Access Quality. (12 de enero de 2021). *El Cifrado de Datos (Tipos y Soluciones)*. Obtenido de https://www.accessq.com.mx/cifrado-de-datos/

Arias, E. R. (05 de Febrero de 2021). *Investigación descriptiva*. Obtenido de Economipedia: https://economipedia.com/definiciones/investigacion-descriptiva.html

Boxcryptor. (31 de Enero de 2022). *Boxcryptor*. Obtenido de FileHorse: https://www.filehorse.com/es/descargar-boxcryptor/

CryptoExpert. (12 de 03 de 2021). *CryptoExpert*. Obtenido de taiwebs.com: https://es.taiwebs.com/windows/download-cryptoexpert-6361.html

Daniel, B. (31 de Marzo de 2021). *¿Qué es el cifrado AES? [La guía definitiva de preguntas y respuestas]*. Obtenido de Trenton Systems: https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered

FERNÁNDEZ, Y. (6 de Marzo de 2020). *Qué significa cifrar o encriptar algo*. Obtenido de Xataka Basics: https://www.xataka.com/basics/encriptar-que-sirve-como-cifrar-tus-archivos

Gómez, B. (18 de Abril de 2021). *AES-256 ¿Qué es? ¿Cómo funciona? (Mejor explicación)*. Obtenido de Seguridad informática: https://www.profesionalreview.com/2021/04/18/aes-256/#El_origen_de_Rijndael

GUTIÉRREZ, P. (25 de Agosto de 2017). *Tipos de criptografía: simétrica, asimétrica e hibrida*. Obtenido de GENBETA: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

History Computer Staff. (25 de Octubre de 2021). *Explicación del cifrado RSA: todo lo que necesita saber*. Obtenido de History Computer: https://history-computer.com/rsa-encryption/

López, A. (04 de abril de 2021). *Todo sobre criptografía: Algoritmos de clave simétrica y asimétrica*. Obtenido de RZ redeszone: https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

López, J. (29 de Septiembre de 2021). *Así funciona el sistema de cifrado AES-256 bits, ¿es realmente seguro?* Obtenido de HZ hardzone: https://hardzone.es/tutoriales/rendimiento/cifrado-aes-256-bits-como-funciona/

Miltrucos. (31 de Mayo de 2021). *Qué es el cifrado AES, ejemplos de cómo funciona el estándar de cifrado avanzado*. Obtenido de Miltrucos: https://miltrucos.com/que-es-el-cifrado-aes-ejemplos-de-como-funciona-el-estandar-de-cifrado-avanzado/#Que_es_AES

Palacios, A. P. (2020). *Seguridad informatica .* Madrid: Ediciones Paraninfos, SA.

Palestina, A. C. (2 de Abril de 2021). *¿Qué es el marco metodológico en una investigación?* Obtenido de ALEPH: https://aleph.org.mx/que-es-el-marco-metodologico-en-una-investigacion

Pérez Porto, J., & Merino, M. (2019). *Definición de encriptar*. Obtenido de Definicion.de: https://definicion.de/encriptar/

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Manabi: 3Ciencias.

Simplilearn . (15 de Febrero de 2022). *¿Qué es el algoritmo RSA y cómo funciona en criptografía?* Obtenido de Simplilearn : https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm#steps_in_rsa_algorithm

Telsy. (26 de Mayo de 2021). *CRIPTOGRAFÍA RSA: HISTORIA Y USOS*. Obtenido de CRIPTOGRAFÍA: https://www.telsy.com/rsa-encryption-cryptography-history-and-uses/#:~:text=The%20RSA%20encryption%20is%20a,project%20remained%20secret%20until%201997.

Wilson, M. (16 de 02 de 2021). *¿Qué son los métodos de investigación no experimental?* Obtenido de restaurantenorman: https://www-restaurantnorman-com.translate.goog/what-are-non-experimental-research-methods/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc

ANEXOS

Universidad Técnica de Babahoyo

Facultad de Administración Finanzas e Informática

Tema: Análisis comparativo de los métodos de encriptación AES y RSA, para las seguridades de los sistemas de información.

Encuesta

1) **¿Conoce usted la función principal de los métodos de encriptación?**

   Si ☐

   No ☐

   Talvez ☐

2) **¿Tiene usted conocimiento sobre los métodos de encriptación AES y RSA?**

   Si ☐

   No ☐

   Talvez ☐

3) **¿Se sentiría usted seguro usando los métodos de encriptación?**

   Si ☐

   No ☐

   Talvez ☐

4) **¿Cree usted que al momento de enviar una información el método de encriptación cumple con su función?**

   Si ☐

   No ☐

   Talvez ☐

ANEXOS

5) ¿Cree usted que los métodos de encriptación son seguros?

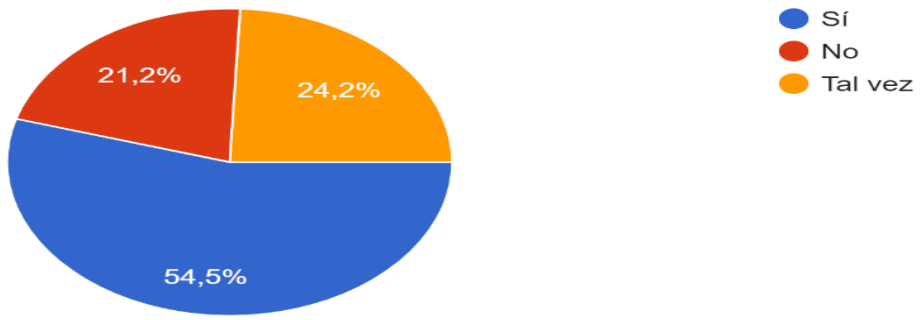
Si ☐

No ☐

Talvez ☐

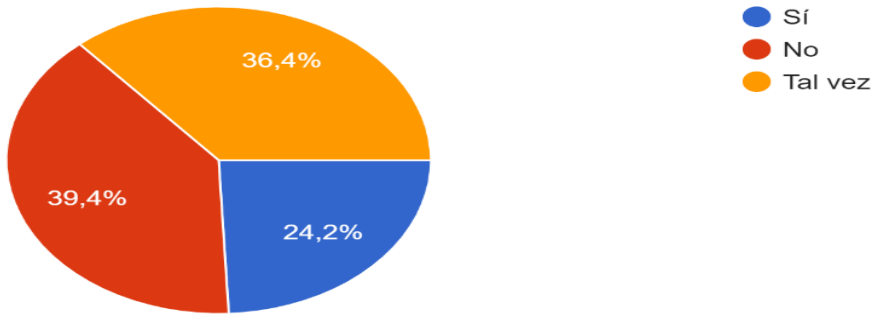
Anexo Nº2

1.-¿Conoce usted la función principal de los métodos de encriptación?



Pregunta #1: se realizó una pregunta sobre la función principal de los métodos de encriptación donde el 54,5% dijo que, si conocen dicha función, el 21,2% dijo que no, el 24,2% dijo que tal vez.

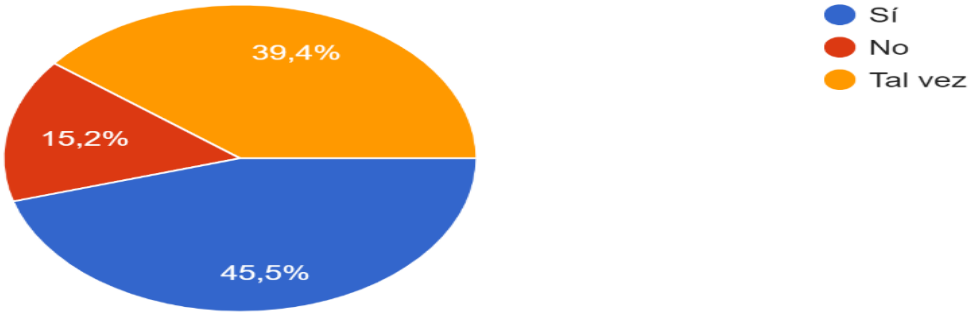
2.-¿Tiene usted conocimiento sobre los métodos de encriptación AES y RSA?



Pregunta #2: se realizó una pregunta a los encuestados sobre conocimiento que tienen de los métodos AES y RSA donde el 24,2% dijo que, si tienen conocimiento, el 39,4% dijo que no, el 36,4% dijo que tal vez.

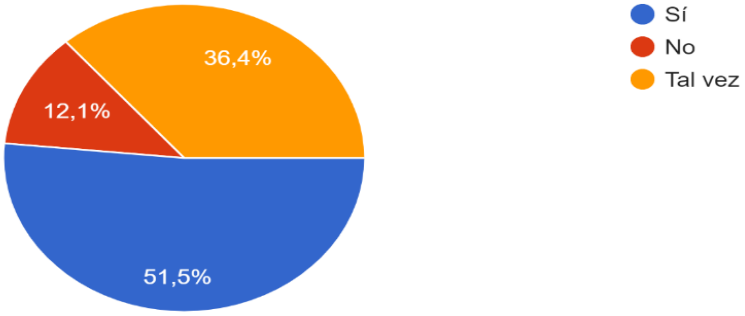
Anexo Nº2

3.-¿Se sentiría usted seguro usando los métodos de encriptación?



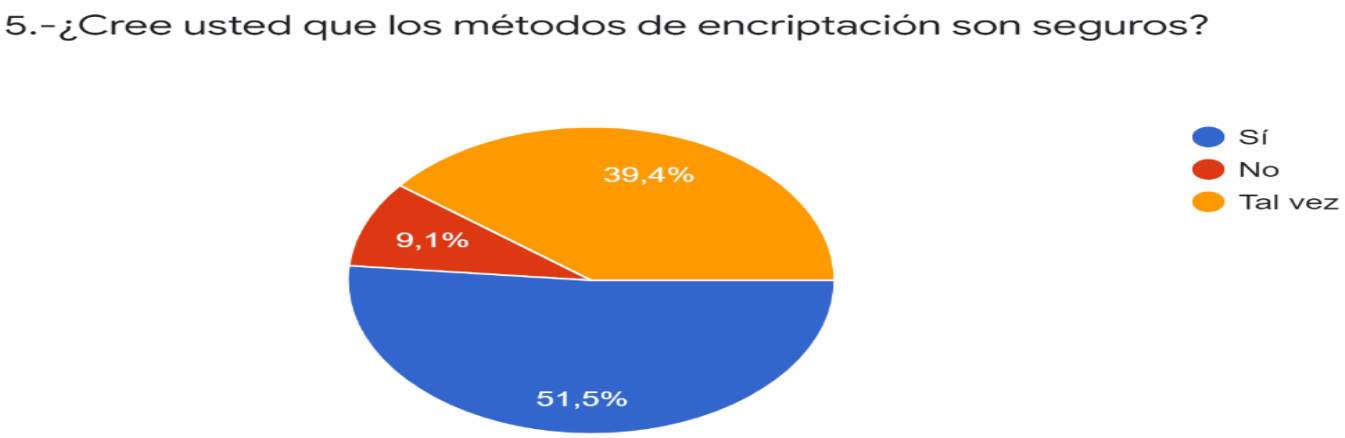
Pregunta #3: se realizó una pregunta a los encuestados sobre si se sienten seguro usando los métodos de encriptación donde el 45,5% dijo que, si se sienten seguros, el 15,2% dijo que no, el 39,4% dijo que tal vez.

4.-¿Cree usted que al momento de enviar una información el método de encriptación cumple con su función?



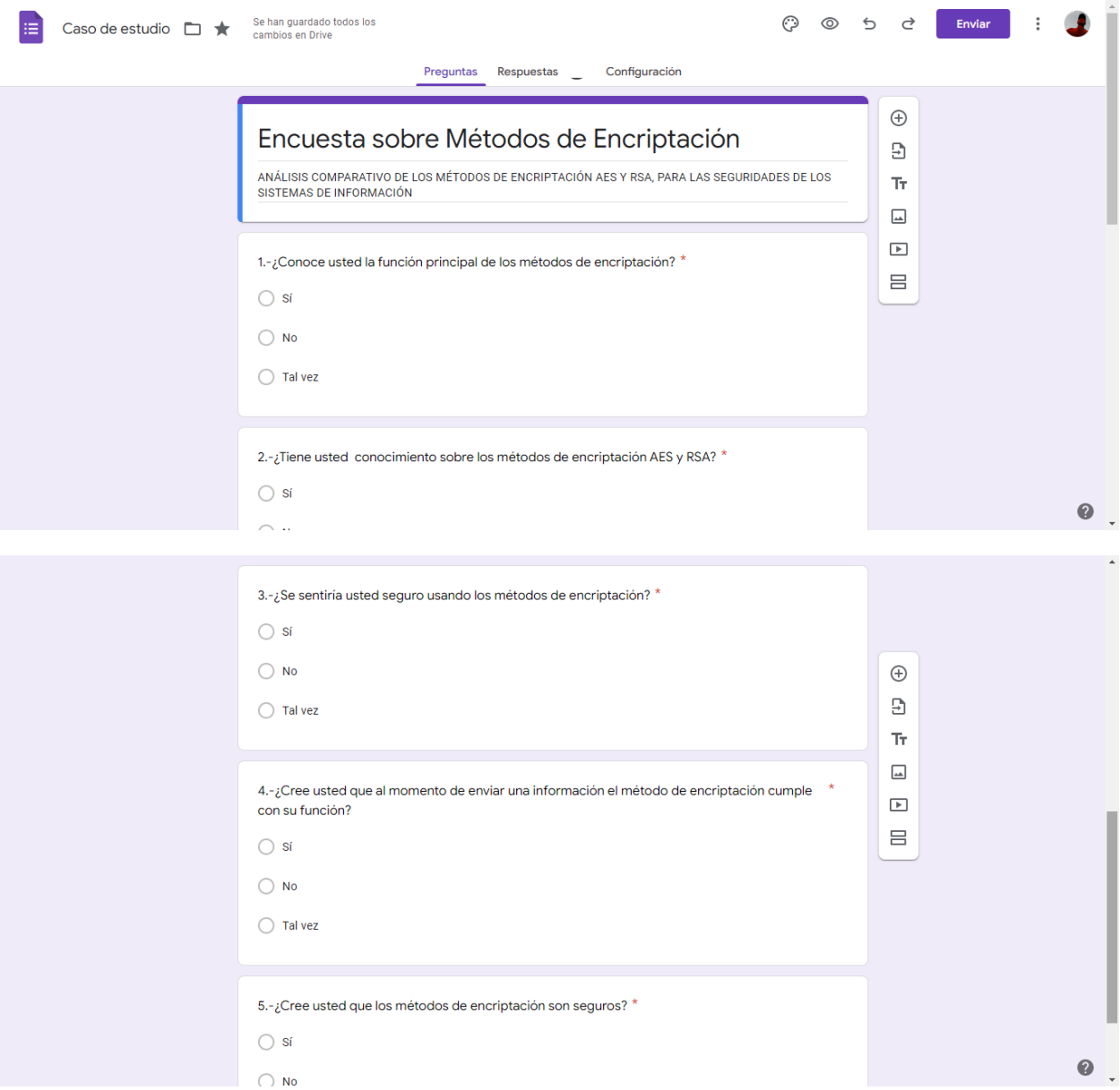
Pregunta #4: se realizó una pregunta a los encuestados sobre el cumplimiento de los métodos de encriptación donde el 51,5% dijo que, si se sienten seguros, el 12,1% dijo que no, el 36,4% dijo que tal vez.

Anexo Nº3



Pregunta #5: se realizó una pregunta a los encuestados sobre la seguridad de los métodos de encriptación donde el 51,5% dijo que, si se son seguros, el 9,1% dijo que no, el 39,4% dijo que tal vez.

Anexo Nº4



Nota: elaboración de la encuesta con sus respectivas preguntas.