UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

JUNIO 2021 - NOVIEMBRE 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ESTUDIO COMPARATIVO DE SOFTWARE BASADOS EN EL CIFRADO Y PROTECCIÓN DE DATOS

EGRESADO:

RONALD LEODAN COLOMA MACIAS

TUTOR:

ING. ENRIQUE ISMAEL DELGADO CUADRO

AÑO 2021

RESUMEN

La gran mayoría de empresas y organizaciones de todo el mundo deciden invertir como base sólida en el tema de la tecnología, específicamente en áreas de protección informática, esto con el propósito de mantener en buen recaudo sus activos críticos, su capital e información privada de los usuarios y de la misma entidad.

La seguridad de los datos, que a su vez es también conocida como la seguridad de la información, es un referente esencial en cualquier tipo de áreas, sin importar el tamaño y tipo. Esta encierra conceptos relevantes como la encriptación de datos y desarrollo de gestión de claves, la cuales colaboran para proteger dichos datos en cualquier aplicación y plataforma en ejecución.

La ingeniería de seguridad, busca acaparar el mayor terreno posible en cuanto a medidas de protección y revisiones de códigos, que anticipan al desarrollo de arquitecturas de seguridad y escenarios de amenazas para así establecer medios seguros.

El presente estudio comparativo realizó un análisis de herramientas o software basados en el cifrado y protección de datos e información, el cual especificó ciertos puntos infalibles al momento de mantener a salvo dichos datos personales en plena transportación de los mismos. Profundizar el funcionamiento en ese tipo de software le permite al usuario final poseer prevenciones frente a situaciones riesgosas de hurto de información considerable.

Palabras Clave: información, seguridad, encriptación

ABSTRACT

The vast majority of companies and organizations around the world decide to invest as a solid base in the subject of technology, specifically in areas of computer protection, this with the purpose of keeping their critical assets, their capital and private information of the users and the same entity.

Data security, which in turn is also known as information security, is an essential benchmark in any type of area, regardless of size and type. This contains relevant concepts such as data encryption and key management development, which collaborate to protect said data in any application and platform running.

Security engineering seeks to capture as much ground as possible in terms of protection measures and code reviews, which anticipate the development of security architectures and threat scenarios in order to establish secure means.

This comparative study carried out an analysis of tools or software based on the encryption and protection of data and information, which specified certain infallible points at the time of keeping such personal data safe while they were being transported. Deepening the operation of this type of software allows the end user to have precautions against risky situations of considerable theft of information.

Keywords: information, security, encryption

INTRODUCCIÓN

En algún momento de la vida de cada persona se ha sentido la necesidad de poder tener algún tipo de secreto y poder guardarlos a buen recaudo. Tan solo en algunas situaciones específicas se ha deseado poder compartirlos con amigos o aliados en concreto, asegurándose de que personas infiltradas no obtengan datos o información alguna.

Una de las maneras que se desarrolló para poder transformar el contenido de cualquier mensaje, siguiendo reglas que modifiquen de alguna manera la información, a tal forma que aplicando técnicas o procesos inversos sería posible recuperar el mensaje original.

Los avances científicos del siglo XX y sus efectos con respecto al diseño y desarrollo de nuevas tecnologías, han puesto en marcha el cambio por completo del panorama de la tecnología actual. Toda empresa invierte en cierto grado a la transformación digital, permitiendo así el reconocimiento de aplicaciones innovadoras de la tecnología, tales como la seguridad.

Sin embargo, en la actualidad, el 80% de los datos del mundo permanecen sin analizar, inaccesibles o no confiables; y gran parte de esos datos representan “Deep data”, es decir, datos que todavía no han sido desenterrados, examinados y extraídos para un análisis eficiente. La industria de la seguridad informática sigue desarrollándose con aumento, y en parte lo hace porque los delincuentes o atacantes informáticos han generado ataques con métodos más discretos y eficiente al momento de desarrollar dicho acto.

El desarrollo de una tabla comparativa permitirá tener conocimiento acerca de la eficiencia u otros puntos específicos que se debe tener en cuenta al momento de realizar una transportación de datos o información entre dos o más puntos.

El presente estudio de caso tiene como finalidad u objetivo, conocer diferentes tipos de software que permiten cifrar datos o información para así lograr la confidencialidad, integridad y autenticidad, mediante los métodos de cifrado de la criptografía.

Para poder conseguir el objetivo propuesto en el estudio comparativo se hace uso de la metodología cualitativa, la misma que ofrece una buena confiabilidad, aquella que mantiene una estabilidad en cuanto a seguridad y congruencia.

Técnica e instrumentos como la observación se generaron para la respectiva recolección de la información y así proceder a conocer el desarrollo y características que ofrecen los softwares de cifrado.

DESARROLLO

La criptografía es la ciencia que se encarga del cifrado y descifrado de información para ser transmitida de forma segura, garantizado que solo será entendida por el emisor y el destinatario final (Aguilera López, 2010).

Es una rama de las matemáticas que, al enfocarse en los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas vinculados con la autenticidad y la confiabilidad. El inconveniente de la confidencialidad es que se asimila normalmente con métodos de "encripción" y la autenticidad con técnicas denominadas de "firma digital", aunque el resultado de ambos se limita a la aplicación de procedimientos criptográficos de encripción y desencripción.

Dejando claro una diferencia notoria entre un modelo criptográfico y uno de seguridad informática es que, en la criptografía se generan dos puntos, "a" y "b", los cuales se consideran fiables a tal punto que se transmiten datos o información mediante un canal no fiable. En clara descripción esta se relaciona con la transmisión confidencial y segura por el medio no fiable, por otro extremo la seguridad informática se encarga de establecer la fiabilidad de los nodos existentes.

Cifrado de datos constituye uno de los métodos de protección más fiables. Consiste en la transformación de los datos, de forma que una persona que no deba tener acceso a ellos no sea capaz de entenderlos. El cifrado de datos se puede realizar a través de elementos lógicos o físicos, pero en cualquiera de los casos es un proceso que consume bastantes recursos (Sampalo de la Torre, Cortés, Garzón Villar, & Prieto Tinoco, 2003).

El cifrado activo es un punto clave para fortalecer las comunicaciones existentes en línea para todo tipo de persona, desde transacciones financieras, mensajería en línea, hasta atención médica. Es un método sustancial con el cual forma parte de la construcción de una internet confiable.

Para los datos que se comunican a través de una red, el cifrado moderno codifica los datos utilizando un valor secreto o una clave que solo conocen el destinatario y el remitente. En el caso de los datos almacenados, el valor secreto suele ser conocido solo por el propietario de los datos. Existen diferentes tipos de cifrado y los mejores sistemas informáticos en relación a esta área equilibran la seguridad y la eficiencia, tales como el cifrado simétrico y cifrado asimétrico los cuales son los principales.

Al debilitar un sistema de cifrado, se expone información como registros médicos, información bancaria personal, datos de tarjetas de crédito, identificación personal y otros datos importantes que facilitan que los ciberdelincuentes roben identidades de muchas personas.

Un cifrado deficiente amenaza la seguridad, estabilidad de las personas e incluso naciones en el mundo entero. Esto debido a que cualquier tipo de internauta que encuentre dichas falencias, trabajarán o desarrollaran métodos para encontrarlas y explotarlas, así surgiendo puertas traseras de cifrado, las cuales generan consecuencias notorias para la seguridad personal de miles o millones de personas.

Las puertas traseras de un tipo de cifrado pueden llegar a tal punto de crear nuevas oportunidades para que malos actores, incluidos los gobiernos hostiles, las organizaciones terroristas y las redes delictivas internacionales, accedan y exploten las comunicaciones confidenciales de los funcionarios gubernamentales, penetrar, atacar sistemas informáticos y bases de datos confidenciales. Esto podría causar interrupciones sistemáticas a gran escala en las economías, la infraestructura y la seguridad nacional.

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado (Cervigón Hurtado & Alegre Ramos , 2011).

Un método de cifrado se compone en primeras instancias de una estructura en la cual interfiere un algoritmo criptográfico y una o más claves.

Los algoritmos modernos de cifrado están estructurados para confrontar y resistir a ataques descubiertos por un criptoanalista. El algoritmo requiere de una combinación matemática sobre la información a proteger con una clave provista, teniendo como resultado los datos o información encriptada. Para poder desencriptar, el algoritmo realiza un cálculo combinando los datos encriptados con una llave provista, siendo el resultado los datos desencriptados.

En los tipos de cifrado, el simétrico o criptografía de una clave, emplea un proceso en el cual hace uso de la misma clave para cifrar y descifrar los datos o información. Tanto el emisor como el receptor deben conocer de antemano la clave o bien compartirla mediante un canal seguro, este sistema de cifrado debe integrar fuerza en la contraseña estipulada, ya que en esa comunicación previa se puede interceptar la clave.

Los algoritmos aplicados en la criptografía o cifrado simétrico se basan en cálculos tan simples como la sustitución y la permutación, estas operaciones se aplican de forma combinada y en ciclos de iteraciones consecutivas, así como las adiciones, multiplicaciones, aritmética modular y las operaciones XOR.

Las ventajas presentes en este tipo de cifrado son la facilidad de uso, lo que hace que se convierta sencillo al momento de ponerlo en ejecución, la velocidad, puesto que utiliza menos recurso informático que otro tipo de cifrado.

Una desventaja notoria en el cifrado simétrico es que, el compartir la clave secreta con el destinatario es inevitable, esto haciendo referencia a que el envío de la clave debe realizarse con un método seguro, de lo contrario, se es participe para el acceso indebido de la misma.

Los ataques por fuerza bruta son un rival constante de los algoritmos del cifrado simétrico, puesto que sus algoritmos son públicos y la fuerza de los mismo depende directamente de la dificultad que posea internamente el algoritmo, y a su vez la longitud de la clave generada para evitar dichos ataques.

El DES (Data Encryption Standar) es uno de los sistemas de cifrado, mediante clave privada, más sofisticados. El cifrado de datos se efectúa insertando bits clave y a continuación se ejecutan toda una serie de permutaciones no lineales (Heredero, López Hermoso Agius, Romo Romero, & Medina Salgado, 2019).

Este sistema ejecutado por bloques de 64 bits, de los cuales 8 bits se utilizan como control de paridad para verificar la integridad de la clave y después son descartados, ejecuta combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, de esta manera asegura que las operaciones puedan realizarse en ambas direcciones para el posterior descifrado.

El cifrado por bloques AES (Advance Encryption Standard), es el cifrado de elección para las aplicaciones futuras, tal como lo recomienda ENISA (The European Union Agency for Cybersecurity), AES posee un bloque de cifrado de un tamaño de 128 bits y soporta tres longitudes de clave: 128, 192 y 256. Las versiones con longitud de clave más grande utilizan más ciclos y por lo tanto son más lentas (Darahuge & Arellano Gonzáles, 2019). Estas secuencias en situaciones se denominan bloques y el número de los bits que contienen denominarán su longitud. No se permite otras longitudes de claves de entrada, salida y cifrado por este tipo de estándar.

AES es un estándar simétrico definido en el margen internacional y publicado por NIST (National Institute of Standard and Technology) como FIPS PUB 197, que a la distancia temporal se ha definido como unos de los más destacados y seguros (NIST, 2001).

Por lo contrario, el cifrado asimétrico genera dos claves distintas entre el emisor y el receptor. De esta manera, se ejecutaría una contraseña pública, la cual se comparte con todos aquellos que requieran enviar dicha información cifrada. Ambas claves están vinculadas lo suficientemente rígidas para que no se pueda extraer ninguna de ellas.

Para ejecutar la serie de pasos del cifrado asimétrico el receptor genera un par de claves y da a conocer la clave pública al emisor. El proceso de transferencia es simple y se lleva a través de métodos de certificación o servidores de claves, en los que se almacena la clave. El emisor codifica el contenido con la clave pública para enviarlo al destinatario como "texto privado". Desde el momento del cifrado, el destinatario únicamente podrá descifrar este mensaje con la clave privada generada con anterioridad. Por este motivo en el inicio el canal por el cual se trasmitirá es libre de elegir, si el mensaje cifrado es interceptado, su contenido permanece oculto para el atacante.

El cifrado asimétrico utiliza como base algoritmos tales como el DSA (Digital Signature Algorithm) y RSA (Rivest, Shamir y Adleman).

El algoritmo DSA es un cifrado asimétrico o de clave pública, mediante el cual se puede verificar la autenticidad de cualquier mensaje, cada una clave pública y la firma del mensaje. Es posible crear pares claves públicas, privada y generar firmas de datos usando la clave privada.

Este algoritmo hace uso de la firma digital, el cual utiliza más parámetros que el algoritmo RSA y así se puede obtener un grado más alto en cuestión de seguridad. Algunos de sus parámetros son los siguientes:

- KG claves públicas de grupo: Son comunes y públicas para un grupo de usuarios.
- KU clave pública: Se genera una por usuario a partir de las KG.
- KP clave privada: La obtiene cada usuario, y es privada, generando con las anteriores.
- K número aleatorio: Se genera uno por cada firma digital.
- S y R son palabras con 160 bits formando la firma de un texto en específico.
- El número K no permite que se genere una repetición de firmas

Algoritmo RSA es uno de los primeros esquemas de clave pública, concretamente del año 1977. Fue creado por Rivest, Shamir y Adleman, de ahí el nombre de RSA. Su seguridad se basa en la dificultad computacional de factorizar números muy grandes. Las claves se obtienen a partir de un dato que es el producto de dos números primos muy grandes (Maciá Pérez, y otros, 2008).

	Algoritmo simétrico **DES/AES**	**Algoritmo Asimétrico** **DSA/RSA**
Velocidad	Rápida	Lenta
Uso	Cifrado en grande cantidad de datos	Intercambio de claves Firma digital
Claves	Compartida entre emisor y receptor	Privada
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal. La privada nunca se comparte

Longitud de claves	56 bits 256 bits	1024 bits mínimo
Otros algoritmos	DES 3DES Blowsfish IDEA AES	Diffie-Hellman DSA RSA El Gamal
Seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación

Tabla 1. Cuadro comparativo de Algoritmos Simétrico y asimétrico

	Ventajas	Desventaja	Seguridad	Utilidades	Algoritmos	Longitud de la clave
SIMÉTRICO	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 en ambas partes.	• Confidencialidad • Integridad	• Cifrado de mensajes	**DES** tamaño de 56 bits **TRIPLE DES** tamaño 128 a 256 bits **AES** tamaño de 128, 192 o 256 bits.	56 bits/vulnerables 256 bits/seguros

Tabla 2. Características Cifrado Simétrico y Asimétrico.

ASIMÉTRICO	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 **DSA** con tamaño de 512 bits a 1024 bits **ELGAMAL** tamaño entre los 1024 bits y 2048 bits.	1024 bits mínimos

Esteganos Safe

Desde el año 1996, Steganos ofrece herramientas de software de alta seguridad y fáciles de usar las cuales protegen y aseguran los datos dentro y fuera de la web. Steganos brinda soluciones integrales para usuarios particulares, oficinas domésticas y pequeñas empresas (Steganos, Steganos, 2021).

Es un tipo de caja fuerte que permite mantener segura y confiable toda la información que se posea en el ordenador, se podrá almacenar de forma segura y protegida, esto mediante algoritmos de cifrado y contraseñas. La protección se aplica tanto en equipos portátiles como en un ordenador de sobremesa, la codificación se ejecuta al instante para todos esos archivos que se desea proteger, esto usando cifrados de hasta 128 bits, de la mano de un diccionario integrado que resguarda la integridad y seguridad de las contraseñas que se hagan uso.

Diversas características se prestan en este medio de seguridad, entre ellas se encuentra la encriptación de archivos en el PC y en la nube, Optimización y seguridad del PC, navegación segura y privada, protección y gestión de contraseñas, paquete completo de seguridad digital. Este software permite el anonimato verdadero, resultando ser una herramienta muy sofisticada.

El manejo de las contraseñas le brinda la posibilidad al usuario de gestionar todas sus contraseñas de una forma organizada, en una lista encriptada y segura: cuentas de usuario, números de tarjeta de crédito, códigos de acceso, PINS o contraseñas. El Steganos Password Manager le brinda la posibilidad de gestionar todas estas informaciones en una única lista (Steganos, Steganos, 2016).

Este software ofrece una excelente protección gracias a los modernos sistemas de encriptación AES-XEX de 384 bits con aceleración de hardware AES-NI, el programa ofrece una protección destacable. Para mayor seguridad puertas traseras, llaves maestras o contraseñas

duplicadas. Además, ofrece la función de ocultar safes para aumentar la protección (Steganos, Steganos, 2016).

Algoritmos	Contraseña	Seguridad	Compatibilidad
Cifrado AES-XEX con 384 bits (IEEE P1619)	o Crea cajas fuertes de hasta 2 TB (2.048 GB) de tamaño o Opción para configurar una contraseña de emergencia para sus dependientes sobrevivientes	Admite el cifrado de datos en; Dropbox, Microsoft OneDrive, Google Drive y MagentaCLOUD	Windows XP / Vista / 7 / 8 / 10

Tabla 3. Características técnicas Steganos

Axcrypt

La seguridad es fundamental por ende Axcrypt le otorga prioridad, así asegurándose de que nadie obtenga acceso a los archivos cifrados, siempre que se tenga el control de la propia contraseña. La simplificación para el manejo del cifrado es constante, desarrollando funciones que permiten el acceso o intercambio de claves de cifrado sea simples y seguros.

AxCrypt usa AES-128 o AES -256 en la versión Premium, pero si desea lograr ese nivel de seguridad, debe proporcionarle 128 o 256 bits de datos verdaderamente “aleatorios”. Para poder obtener realmente 128 o 256 bits, en la práctica se tendrá que guardar la contraseña en un archivo de texto y luego mantener ese archivo de texto en secreto.

Las primitivas criptológicas son AES-128 o AES-256 para el cifrado masivo, PBKDF2 con HMAC-512 para la derivación de la clave, RSA de 4096 bits para la clave de la cuenta y HMAC-512 para la verificación de la integridad. El ajuste de clave de la contraseña se realiza utilizando la especificación NIST para AES Key Wrap. La clave derivada de la contraseña con PBKDF2-SHA512 solo se utiliza como clave de cifrado de claves (AxCrypt, 2021).

Algoritmos	**Contraseña**	**Seguridad**	**Compatibilidad**
○ AES-128 ○ AES-256 ○ PBKDF2 con HMAC-512 RSA de 4096 bits ○ HMAC-12	Recuperación de datos como el nombre del archivo y su tamaño.	○ Salvapantallas protegidas con contraseña. ○ Detector de teclado, tanto en hardware y software.	○ Windows 7/8/10 (32 y 64 bits) ○ iOS ○ Mac ○ Android

Tabla 4. Características técnicas Axcrypt

Cryptoexpert

CryptoExpert 8 fue especialmente diseñado para proporcionar bóvedas de datos seguras a los propietarios de computadoras portátiles / de escritorio y garantizar la máxima seguridad de los datos. Al implementar innovaciones en conjunto con una operación rápida sobre la marcha, CryptoExpert proporciona mayor seguridad, mejor confiabilidad y facilidad de uso que el sistema de cifrado NTFS transparente e implementado en el sistema de archivos cifrado integrado de Windows. Las bóvedas seguras fluyen como discos duros normales para todas las aplicaciones de Windows y nadie puede desbloquear la bóveda sin una contraseña (cryptoexpert, 2021).

Este software cuenta con seguridad efectiva con los datos e información, el desbloqueo se ejecuta únicamente cuando se requiera para realizar una copia de seguridad de los archivos confidenciales, luego terminado el proceso bloquear.

Este software posee bóvedas seguras de tamaño ilimitado (10 GB y más), con tiene logaritmos altamente aclamado como lo son, BLOWFISH, CAST o 3DES, incluso el estándar de la industriaAES-256 para la máxima protección de los datos.

Algoritmos	**Contraseña**	**Seguridad**	**Compatibilidad**
○ Blowfish ○ Cast ○ 3des ○ 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

Tabla 5. Características técnicas CryptoExpert

Boxcryptor

Boxcryptor cifra sus archivos y carpetas sensibles en Dropbox, Google Drive, OneDrive y muchos otros almacenes en la nube. 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. Cifra sus datos directamente en su dispositivo antes de sincronizarlos con los proveedores de la nube de su elección (Boxcryptor, 2021).

Se trata de un medito resolutivo criptográfico de extremo a extremo en base a una colaboración segura en archivos en la nube, el cual mantiene regulaciones internar y externas.

Permite definir administraciones personalizadas, gestionando a los usuarios, brindando protección a las cuentas con autenticación de dos factores.

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.

Tabla 6. Características técnicas Boxcryptor

Cryptomator.

Cryptomator es un software de código abierto, con el software de código abierto, muchos ojos tienen una mirada escrutadora en el corazón del software de cifrado, es decir, el código fuente. Por lo tanto, pueden ver si el código fuente realmente hace lo que dice el algoritmo de cifrado. Y eso es exactamente lo que hace que el cifrado sea aún más seguro. El código es completamente accesible. No hay posibilidad de auditar solo una parte del código con fines de marketing o para ocultar vulnerabilidades de seguridad (Criptomator, 2021)

EL software cumple los últimos estándares y cantidad tanto archivos como nombres de los mismo con AES y una longitud de 265 bits. No cuenta con puertas traseras y posee código abierto el cual no estable una fecha de caducidad. Esta herramienta además de las auditorias de

seguridad independientes, el software se comprueba de manera continua y pública de forma automatizada lo cual tiene una calidad de código medible y una cobertura de prueba que sobrepasa el promedio de la industria.

Algoritmos	Contraseñas	Seguridad	Compatibilidad
AES-256	- Bóveda, dentro de su nube - Unidad virtual encriptada a la que puede transferir sus datos	Sin puertas traseras Auditoria continua Sincronización	- Windows - Android - MacOS - iOS - Linux

Tabla 7. Características técnicas Criptomator

Análisis

En base a las diferentes características que presentan los softwares criptográficos, se genera un cuadro comparativo de sus factores principales, entre los cuales están representado por la contraseña, seguridad, compatibilidad y algoritmos puestos en proceso, esto con el objetivo de focalizar a las herramientas que presentan una mayor ventaja funcional.

	Algoritmos	**Contraseña**	**Seguridad**	**Compatibilidad SO**	**Compatibilidad Nube**
Steganos Safe	Cifrado AES-XEX con 384 bits (IEEE P1619 AES 256	• Contraseña en imágenes PicPass • Sin contraseñas duplicadas	• Protocolo VPN moderno (IKEv2 u OpenVPN) • Cifrado en la nube • Sin puertas traseras, llaves maestras. • Encripta conexión y tráfico de datos	• Windows 7/8/10 (32 y 64 bits) • iOS • Mac • Android	• Dropbox • Google Drive • Microsoft OneDrive

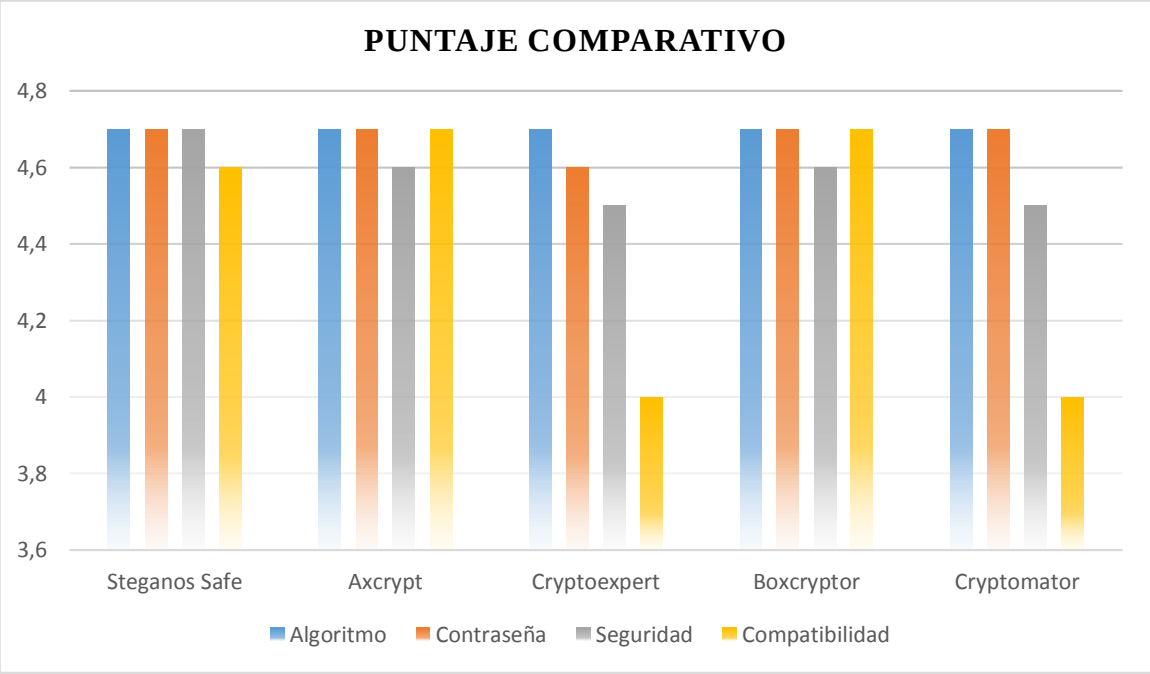
			• Controladores actualizados • Desfragmentación de registros		
Axcrypt	AES-128 AES-256 Integridad / Autenticación - Transmisión HMAC-SHA-512	• Intercambio de claves • Clave maestra • Exportación de claves	• Software libre • Controles de seguridad / integridad, cifrado AES-128 / AES-256 / HMAC-SHA-512	• Windows 7/8/10 (32 y 64 bits) • iOS • Mac • Android	• Dropbox • Google Drive
Cryptoexpert	• Blowfish • CAST • 3DES • AES-256	Acceso de datos denegado sin contraseña	• Bóvedas seguras de tamaño ilimitado • Acceso transparente a	Windows 10 / 8 /7 32 y 64 bits	

			archivos y carpetas		
Boxcryptor	• AES longitud de clave de 256 bits, CBC (Cipher Block Chaining) y relleno PKCS7. • RSA longitud de clave de 4096 bits y relleno OAEP.	• 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 revela contraseñas	• Windows • Mac OS • iOS • Android	• Google Drive • Dropbox • OneDrive • iCloud Drive

Cryptomator	AES-256	Asignación de contraseña para una carpeta o bóveda, dentro de la nube Se establece una unidad virtual cifrada	Cifrado de contenido de archivos Criptografía cuántica resistente Criptografía auditada	• Windows • Android • Mac OS • iOS • Linux	Dropbox

Tabla 8. Cuadro característico comparativo de softwares de cifrado

Ilustración 1. Puntaje comparativo de las herramientas de cifrado



Elaborado con los datos obtenidos de la tabla 8

Fuente: Elaboración Propia

CONCLUSIONES

Con la tabla 8 comparativa se pudo determinar con menos complejidad las herramientas más factibles para la seguridad de los datos e información del usuario, entre ellas están presente Esteganos Safe, Axcrypt, Boxcryptor y Cryptomator, recalcando que cada herramienta posee diferentes funcionalidades acordes al uso final.

Un claro ejemplo diferencial está en Cryptomator y Boxcryptor, en lo que el primer software corresponde a un código abierto y Boxcryptor es un software que ofrece un código cerrado. Mediante el código abierto es permitido evidenciar si realmente se cumple los establecido por el algoritmo de cifrado, lo que hasta cierto punto acarrea mayor seguridad. Como se pudo observar en pleno desarrollo, estas herramientas ofrecen el servicio de cifrado tanto de manera local como el cifrado en la nube.

Con la ejecución comparativa del presente estudio se pudo definir los tipos de algoritmos más robustos y eficaces al momento de ejecutar el proceso de cifrado tanto simétrico como asimétrico, entre estos tenemos el AES y RSA, puesto que la finalidad es mantener una excelencia en la confidencialidad, integridad y protección de los datos en los sistemas informáticos o cuando se transportan a través de internet.

Una vez concluida la ejecución del estudio comparativo propuesto se pudo recalcar cuán importante es la seguridad informática, en las cuales radica el uso malicioso de información privada y de los recursos internos, los mismo que pueden acarrear desastrosas consecuencias en las diferentes áreas de una organización. Por ende, la seguridad informática debe focalizarse en la prevención de ataques o amenazas que conllevan riesgos para los datos o información de alto valor.

Con las fuentes comparativas desarrolladas en proceso, es posible reducir los riesgos de la vulnerabilidad tanto de datos como cualquier conjunto de información. De esta manera se permite tener una red eficaz en base a la seguridad.

BIBLIOGRAFÍA

Aguilera López, P. (2010). *Seguridad informática.* Madrid: Editex, S.A.

AxCrypt. (16 de Agosto de 2021). *AxCrypt*. Obtenido de AxCrypt: https://www.axcrypt.net/information/security

Boxcryptor. (16 de Agosto de 2021). *Boxcryptor*. Obtenido de Boxcryptor: https://www.boxcryptor.com/es/

Cervigón Hurtado, C. H., & Alegre Ramos , M. d. (2011). *Seguridad Informática.* Madrid: Paraninfo, SA.

Criptomator. (16 de Agosto de 2021). *Criptomator*. Obtenido de Criptomator: https://cryptomator.org/boxcryptor-alternative/

cryptoexpert. (16 de Agosto de 2021). *cryptoexpert*. Obtenido de cryptoexpert: https://www.cryptoexpert.com/

Darahuge, M. E., & Arellano Gonzáles, L. E. (2019). *Manual de informática forense III.* Buenos Aires: ERREPAR S.A.

Heredero, C. d., López Hermoso Agius, J. J., Romo Romero, S. M., & Medina Salgado, S. (2019). *Organización y transformación de los sistemas de información en la empresa.* Pozuelo de Alarcón: ESIC EDITORIAL.

Maciá Pérez, F., Mora Gimeno, F. J., Martínez Abarca, J. A., Gilart Iglesias, V., Jorquera , D. M., Berná Martínez, J. V., . . . Hernández Sáez, A. (2008). *Administración de servicios de internet.* Alicante: Compobell S.L.

NIST. (26 de Noviembre de 2001). *National Institute of Standards and Technology.* Obtenido de National Institute of Standards and Technology: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901427

Sampalo de la Torre, M. d., Cortés, E. L., Garzón Villar, M. L., & Prieto Tinoco, J. I. (2003). *Informática Volumen III.* Sevilla: Mad, S.L.

Steganos. (29 de Agosto de 2016). *Steganos*. Obtenido de Steganos: https://www.segurisoft.es/tutorial/sobre-steganos-password-manager/

Steganos. (24 de Agosto de 2016). *Steganos*. Obtenido de Steganos: https://www.segurisoft.es/tutorial/encriptar-bandeja-de-correo-electronico/

Steganos. (16 de Agosto de 2021). *Steganos*. Obtenido de Steganos: https://www.segurisoft.es/sobre-nosotros/