CIFRADO DE LA INFORMACIÓN Y SU INCIDENCIA ACTUAL EN LA SEGURIDAD DE LA INFORMACIÓN PARA PEQUEÑAS EMPRESAS PYMES EN COLOMBIA

ING. LUIS ALEJANDRO QUEMBA MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

CIFRADO DE LA INFORMACIÓN Y SU INCIDENCIA ACTUAL EN LA SEGURIDAD DE LA INFORMACIÓN PARA PEQUEÑAS EMPRESAS PYMES EN COLOMBIA

ING. LUIS ALEJANDRO QUEMBA MARTINEZ

Trabajo de grado como requisito para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

ING. YOLIMA ESTHER MERCADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 25 mayo de 2020

AGRADECIMIENTOS

Agradezco al creador por la vida y todo aquello que la compone, por las bendiciones recibidas en cada momento y las constantes oportunidades que me ofrece en cada etapa de mí existir. Especialmente agradezco a mi esposa Pauline Gama quien ha sido mi apoyo en mi formación familiar, académica, laboral y sobre todo por ser mi guía en momentos arduos, por todo su amor, comprensión, enseñanzas y consejos para afrontar las situaciones cotidianas a las que me enfrento.

A mis padres y hermanos que me permitieron formarme en un entorno familiar pleno, lleno de amor, unión y bendición, por sus buenas acciones y respaldo durante toda mi vida de manera incondicional.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ARCHIVO: unidad de información formada por bytes almacenada en discos duros, USB, correo electrónico entre otros.

ACTIVOS INFORMÁTICOS: bienes materiales (físicos y lógicos) utilizados dentro de una organización.

ALGORITMO CRIPTOGRÁFICO: modifica los datos de un objeto con el fin de brindar seguridad como autenticación, integridad y confidencialidad.

AES: esquema de cifrado por bloques, algoritmo, para la conversión de datos electrónicos en una forma ininteligible, denominada texto cifrado

AMENAZA: es la actividad que se vale de una vulnerabilidad para violentar hacia la seguridad de un sistema de información.

ANTIVIRUS: es un software informático con la misión de encontrar y eliminar diferentes tipos de virus informático.

ATAQUE INFORMÁTICO: propósito para dañar, modificar y/o afectar recursos de informáticos

CERTIFICADO DIGITAL: técnica permitida para identificar correctamente a las personas en internet.

CIBERCRIMEN: actividades delictivas sobre recursos informáticos y personas en internet.

CIFRADO: práctica de codificar datos con el fin de modificar su formato original para que no sea posible leerlos.

CIFRADO ASIMETRICO: basado en utilizar dos claves la privada y la pública.

CIFRADO SIMETRICO: emplea una clave para el cifrado y descifrado del mensaje, previamente con conocimiento por parte del emisor y receptor.

CODIFICAR: proceso donde la información de un origen es convertido en caracteres y simbolismos para ser notificada.

CRIPTOANÁLISIS: metodologías y acciones para descifrar información.

CONFIDENCIALIDAD: prevención de la información a personal no autorizado.

DECODIFICAR: tomar la información y devolverla a su forma original.

DELITO INFORMATICO: actividad ilegal, dada por medios informáticos para destruir y dañar equipos, medios electrónicos y redes de Internet.

DES: sistema de cifrado simétrico por bloques de 64 bits

DISPONIBILIDAD: acceso a la información cuando es requerida por parte de los usuarios autorizados.

DISCRYPTOR: Herramienta informática para el cifrado de discos duros.

IDEA: Algoritmo usado para el cifrado de textos con un volumen de bloque de 64 bits.

FIRMA DIGITAL: acción de criptografía asociado a la identificación de las personas o una entidad sobre documentos informáticos.

FIREWALL: equipo de seguridad sobre la red informática que permite o deniega el tráfico de acuerdo a las políticas y controles de las organizaciones.

GPG4WIN: programa informático para el cifrado de la información localmente y por correo electrónico.

INFORMACION: procesamiento de datos organizados de utilidad constante para la sociedad.

INFRAESTRUCTURA: es el conjunto de hardware y software sobre el que se asientan los diferentes servicios informáticos.

INTEGRIDAD: gestión de mantener sin modificaciones y alteraciones la información ante acciones maliciosas o accidentales.

ISO 27001: estándar internacional que indica la gestión de la seguridad de la información en las organizaciones.

MAILVELOPE: programa que permite cifrar información en los correos electrónicos mediante los navegadores de internet.

MALWARE: acción maliciosa realizada por medio de software hacia dispositivos y equipos informáticos.

PGP: programa informático altamente utilizado para el cifrado y descifrado de datos sobre el correo electrónico.

PKI: infraestructura de clave pública para cifrado de la información.

POLITICAS DE SEGURIDAD: establece medidas técnicas y de organización, para garantizar la seguridad de la información.

PYMES: pequeña y mediana empresa.

RANSOMWARE: programa informático malicioso que busca secuestrar la información con el uso de cifrado.

RESGUARDAR: acción de proteger la información física o digitalmente en almacenamientos seguros.

RIESGO: posibilidad que se origine un suceso de seguridad, creando amenazas y vulnerabilidades informáticas.

SEGURIDAD DE LA INFORMACION: conjunto de tecnologías para control la información que se utilizan en un sistema informático.

TIC: Tecnologías de la Información y la Comunicación.

VULNERABILIDAD: falla en la seguridad de la información que expone la integridad, disponibilidad o confidencialidad de los mismos.

INTRODUCCIÓN

El cifrado de la información ha estado presente desde el comienzo de la humanidad, en cada civilización se utilizaron diferentes técnicas de cifrado con el fin de proteger la información que se transfería desde un lugar a otro, por ende en la actualidad se puede afirmar que el cifrado es la práctica de codificación y decodificación de los datos, mediante algoritmos sobre los datos a cifrar, transformándolos de un formato original, hacia un formato que no permite su lectura, para su descifrado se requiere una clave.

La tecnología ha concedido avances significativos en gran parte de las actividades cotidianas a nivel mundial tanto en las organizaciones públicas, privadas y en la sociedad en general, aunque en la actualidad es evidente que la información es un activo preciado en las organizaciones y un objetivo de alto valor para la ciberdelincuencia, cada vez se cuentan con mejores medidas tecnológicas para minimizar posibles ataques con fines de robo de información, pero el ingenio y otras actitudes de los delincuentes informáticos logran que algunos puedan obtener su cometido. Si las grandes organizaciones han sufrido ataques informáticos, las pequeñas empresas no son la excepción. El presente documento se desarrolló para evidenciar como el cifrado de la información incide en forma positiva en la gestión de datos sobre las pequeñas y medianas empresas en Colombia.

Las tecnologías de la información (TIC) ha permitido gestionar correctamente la información con el uso de recursos informáticos en las organizaciones, en busca de asegurar la integridad, disponibilidad y confidencialidad de los datos, mediante la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) según las normas ISO 27001 y ISO 27002. El cifrado de la información es

una medida de seguridad que cada vez toma más fuerza debido a las ventajas que ofrece.

En este documento se evidencia las técnicas más comunes de cifrado de la información, desde las primeras técnicas utilizadas por la humanidad como era el cifrado *cesar* y *afin,* hasta las técnicas de cifrado utilizadas actualmente mediante la modalidad de cifrado simétrico y asimétrico, como son el cifrado Data Encryption Standard (DES), Advanced Encryption Standard (AES), 3DES, cifrado RSA, criptografía de curva elíptica (ECC) y cifrado PGP (Pretty Good Privacy).

También es identificado los entornos informáticos que pueden emplear el cifrado de la información, a nivel de hardware y software, incluyendo el cifrado de las redes de comunicaciones, correo electrónico, archivos, bases de datos, servidores y aplicaciones.

Como experiencia de investigación en el desarrollo de la metodología se podrá observar el funcionamiento de algunas herramientas de código abierto como es el programa *DiskCryptor*, para el cifrado de discos duros y medios extraíbles, otra herramienta *Gpg4win* y *Mailvelope*, utilizados para cifrado de correo electrónico y archivos que se envían por este medio.

1. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

De acuerdo al Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) en la "Guía para la implementación de Seguridad de la información en una MYPIME", sobre el panorama de inseguridad y amenazas en Colombia afirma que "el 46 % de los crímenes informáticos se dan por la carencia de elementos de seguridad, mientras que la ausencia de políticas de seguridad de la información generaron perdida de utilidades en un 55% entre los años 2012 y 2014"[1], debido a que una de cada 15 empresas afectadas no tiene implementada ningún tipo de política en busca de la seguridad de la información, adicional 10 de cada 100 empresas no realizan gestión de alguna clase de activo para la valoración de los recursos críticos de la organización.

Las pymes regularmente pueden perder una gran cuantía de dinero por violación de los sistemas de seguridad y por ello deben pagar un elevado precio para recobrarse de las actividades de espionaje cibernético como también ataques de tipo phishing y DDoS. Kaspersky Lab en cooperación con B2B International, mostró que los tipos más caros de violaciones de seguridad son el fraude de empleados, el ciberespionaje, la intrusión en la red y el incumplimiento de proveedores. Los costos que se necesitan para la recuperación ante una falla de seguridad son de $551,000 dólares para las organizaciones y de $38,000 dólares para las Pymes.[2] De igual forma, aunque se cuente con la competencia y

---

1 MINTIC, guía para la Implementación de Seguridad de la Información en una MIPYME.Seguridad y Privacidad de la Información. [en línea] Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

2

experticia en el ámbito tecnológico, siempre habrá algún tipo de vulneración que podrá ser explotada con consecuencias inesperadas.

Las Pymes son un blanco muy interesante para los delincuentes informáticos, de acuerdo al fabricante McAfee, solo el 8% del gasto en TI de las pequeñas y medianas empresas está destinado a la seguridad informática. Para el caso de las Pymes en Colombia el 73% sufrió algún tipo ataque informático, estas empresas tienen movimientos superiores al 90% en la economía de la nación, es alarmante la deficiencia en seguridad informática.[3]

Las Pymes son vulnerables cuando suponen que tener implementados un antivirus y un firewall puede compensar posibles ataques informáticos, pero cada vez las técnicas de ataques son más avanzadas permitiendo atacar y quebrantar medidas de seguridad.

Según lo informado por el portal LatinPyme, Colombia es el cuarto país a nivel mundial con ataques de robo de identidad, y está expuesto a espionaje cibernético, obstrucción, supresión de datos o afectación a la reputación empresarial. Uno de los ataques más frecuentes es el de “troyanos”, un malware que ofrece acceso remoto de un equipo infectado al de un atacante para disponer de toda su información.[4]

CORPORACIÓN COLOMBIA DIGITAL. Violaciones de seguridad cuestan a las empresas hasta US$500,000 por ataque [2015]. [en línea] [citado el 1 de noviembre, 2018]. Disponible en internet:https://colombiadigital.net/actualidad/noticias/item/8559-violaciones-de-seguridad-cuestan-a-las-empresas-hasta-us-500-000-por-ataque.html

3 SingleClick Solutions. (2013). Los retos de seguridad para las pymes. [Internet]. Recuperado de: https://singleclick.com.co/contenido-los-retos-de-seguridad-para-las-pymes-167.html

4 LATINPYME. Las pyme con seguridad informática. [Internet]. Recuperado de:https://www.latinpymes.com/las-pyme-con-seguridad-informatica/

1.2 FORMULACIÓN DEL PROBLEMA

El diario “El Espectador” en su sección de tecnología, indica que en el año 2016 y 2017 se presentaron ataques globales mediante la técnica de “ransomware” secuestro de la información con fines extorsivos, donde solicitaban el rescate de la misma a cambio de dinero. “Colombia no ha sido la excepción, ya que de acuerdo a los datos informados por la compañía de tecnología Kaspersky, Colombia ocupo el tercer lugar en américa latina con un 5% del total de los ataques y una de cada cinco pymes ha sido objeto de algún tipo de ataque informático debido a que no utilizan medidas de seguridad adecuadas”[5]. Lo expuesto anteriormente nos indica que, si es necesario que las Pymes en Colombia adopten diferentes tipos de medidas de seguridad para la salvaguardar la información, el cifrado de la información es una medida de seguridad que permitirá a las Pymes fortalecer los sistemas informáticos las ante amenazas y ataques que se hacen diariamente por la delincuencia informática.

¿Cómo incide el cifrado de la información en la seguridad de la información de las pequeñas y medianas empresas Pymes en Colombia?

---

[5] REDACCIÓN TECNOLOGÍA. (2017). EL ESPECTADOR. COLOMBIA. [Internet]. Recuperado de https://www.elespectador.com/tecnologia/colombia-es-el-tercer-pais-mas-afectado-por-ataques-ciberneticos-en-la-region-articulo-714284

2. JUSTIFICACIÓN

La disponibilidad de la información y los sistemas de información es vital para las Pymes, si se considera que estas herramientas son fundamentales para la construcción de estrategias organizacionales que les permitan ser más competitivas.[6]

La delincuencia informática hace presencia en todo tipo de organizaciones a nivel mundial, Colombia no ha estado exenta, las empresas han sufrido algún tipo de ataque informático, debido a la baja implementación y medidas de seguridad informática o el desconocimiento en el uso de la seguridad de la información, lo informado en el estudio “Cyber Risk for Small and Medium- Sized Enterprises, el 93% de las Pymes a nivel mundial han sido víctimas de incidentes cibernéticos.

En el caso de Colombia es necesario y esencial la puesta en marcha de acciones cibernéticas en las Pymes, no obstante, el reintegro de la inversión no será observada desde un principio.”[7]

Otro estudio realizado sobre seguridad de los sistemas de información sobre un grupo de Pymes en Santiago de Cali (Colombia) del año 2014, indago el uso de mecanismos de seguridad (firma digital, encriptado, cifrado) en cuanto al envío y

---

6 RIASCO, Sandra. AGUILERA, Adriana. AVILA, Patricia. Seguridad de los sistemas de información en las Pymes de Santiago de Cali. Colombia. [2016]. [en linea]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/6586847.pdf

7 REDACCION PASSWORD. (2018). ACIS. Colombia. Aumenta en 30% la inversión de las Pymes en ciberseguridad [Internet]. Recuperado de http://acis.org.co/portal/content/NoticiaDelSector/aumenta-en-30-la-inversi%C3%B3n-de-las-pymes-en-ciberseguridad

recepción de información, el 60.75% confirmaron utilizar mecanismo de seguridad para envío y recepción de información, evidenciando mayor protección de los datos contra amenazas y factores de riesgo.[8]

Actualmente las Pymes se basan en gran medida a su creciente dependencia de Internet y a las Tecnologías de la Información y la Comunicación (TIC), para ser partícipes de los beneficios que ofrece la economía mundial, así como fortalecimiento de los procesos, la eficiencia y la innovación.

El nivel de conocimiento y preparación con respecto a la seguridad cibernética y la privacidad varía ampliamente según la PYME. Mientras que es posible que algunas hayan entendido y adoptado las medidas para proteger sus recursos y capacidades implementadas, otras tal vez no hayan implementado ninguna.[9]

Los cibercriminales están al acecho ante cualquier tipo de vulneración o falla en los recursos informáticos de las empresas para acceder o realizar ataques, permitiéndoles hacer secuestro de información privilegiada para posteriormente solicitar rescate, también el robo de cuentas bancarias en las compañías, obtención de las bases de datos e información confidencial como son, documentación, procedimientos, gestión comercial y producción empresarial, posibilitando imitar el modelo productivo y corporativo de la empresa atacada o incluso venderle la información valiosa a las compañías que son competencia directa.

---

8 RIASCO, Sandra. AGUILERA, Adriana. AVILA, Patrica. Seguridad de los sistemas de información en las Pymes de Santiago de Cali. Colombia. [2016]. [en linea]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/6586847.pdf

9 Equipo técnico de OEA. Oportunidades y desafios para las Pymes en el contexto de una mayor adopcion de las TIC. [2018]. [en linea]. Disponible en internet: http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

El riesgo que tiene la información confidencial en las organizaciones es tan alto, que se debe contar con protección interna ante los mismos empleados, un descuido mínimo podría filtrar datos sensibles de la empresa por parte de un empleado inescrupuloso.

Este documento permite conocer las diferentes técnicas y características del cifrado de la información, como elemento fundamental en un sistema de gestión de la seguridad de la información que puede implementarse en las Pymes de Colombia de acuerdo al tipo de cifrado que técnicamente mejor se ajuste a cada empresa según criterio, costos y valoración de la información.[10]

10 BKF. (2017). Las pymes son las más vulnerables a ataques cibernéticos. [Internet]. Recuperado de http://bkf.com.co/pymes-vulnerables-a-ataques-ciberneticos/

3. OBJETIVOS DE PROYECTO

3.1 OBJETIVO GENERAL

Realizar un análisis descriptivo con relación al cifrado de los datos en las pequeñas y medianas empresas (Pymes) en Colombia, como una acción preventiva para salvaguardar la seguridad en la información.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las técnicas de cifrado de la información más utilizadas en la actualidad y como estas permiten la protección de la información a nivel físico y lógico.

- Verificar las opciones de cifrado de la información que podrá emplearse en las Pymes de acuerdo a los riesgos y amenazas informáticas de la actualidad.

- Revisar el funcionamiento básico de las herramientas de software y hardware en el cifrado de datos, identificando el uso correcto sobre la información utilizada en las Pymes.

- Describir el cifrado de datos como medida de seguridad de la información, que puede ser implementada en las Pymes en Colombia, reconocida en la norma ISO 27001 en los controles criptográficos.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La criptografía es una técnica de escribir en forma secreta, generando dificultad de comprensión para aquellos que desean obtener la información, pero que no son los destinarios autorizados. La criptografía ha estado presente en la humanidad desde hace miles de años, por ejemplo, en siglo V a.c. civilización espartana utilizo la técnica de “escítala”, esta técnica utilizaba el cuero envuelto sobre un listón, allí se escribían los mensajes por parte del emisor para luego enviar la tirilla a un destinatario, al llegar a manos del receptor este tendría que tener un listón de similares características para enrollar el cuero y descifrar el mensaje.[11]

En la civilización mesopotámica, los escribas alteraban los signos de escritura para ocultar información, esto lo hacían con signos en forma cuneiforme, mientras que en la civilización china hicieron el uso de estenografía empleando el papiro envuelto en seda para el envío de mensajes de manera secreta.

En la edad contemporánea hacia 1844 se transmitieron mensajes mediante la telegrafía dando evolución a la criptografía debido a que se tenía que reducir el tamaño de los telegramas para reducir costos. En la primera guerra mundial el gobierno británico uso el cifrado Playfair creado por Charles Wheatstone, para el envío de mensajes a las tropas militares.

En el caso del gobierno Alemán utilizo el cifrado empleando gran cantidad de

---

[11] TABARA CARBAJO, José. Criptografía Clásica [2015]. [en línea] [citado el 20 de septiembre, 2018]. Disponible en internet: https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto03.html

números en sus mensajes dirigido al gobierno mexicano con fines políticos para una posible unión para atacar a Estados Unidos.

El espionaje a nivel político, militar o industrial conllevo a utilizar algoritmos de criptografía como método de defensa para el anti espionaje, en el desarrollo de la segunda guerra mundial Alemania utilizo la maquina “Enigma”, su funcionamiento estaba basado en rotores que substituían las letras unas a otras, con esta máquina el ejército Alemán intercambia mensajes que eran difíciles de descifrar por la inteligencia militar de otros países. Aunque matemáticos de Polonia y el matemático Alan Turing fueron los encargados de descifrar los mensajes, utilizando uno de los primeros computadores mecánicos de la época denominado “Bomba criptologica” junto a otro dispositivo llamado “Ciclometro” lograron identificar patrones derivados de la información que se podía interceptar.[12]

Hoy en día se han desarrollado diferentes técnicas de criptografía de acuerdo a las problemáticas y necesidad de las instituciones gubernamentales, sociales y empresariales a nivel global. El cifrado de la información asume un rol importante en las actividades cotidianas de la sociedad, algunas definiciones afirman “la criptografía establece técnicas para el cifrado de datos, obteniendo como finalidad la confidencialidad del mensaje. Si la criptografía establece los mecanismos para el cifrado de datos, el criptoanálisis son metodologías para “quebrar” los mecanismos y alcanzar la información. Cuando la información ha atravesado un procedimiento de criptografía, se puede decir que la información está cifrada.”

En las comunicaciones actuales los usuarios envían datos de un lugar a otro

---

[12] GALLARDO GOMEZ, Rocio. El ataque polaco al protocolo Enigma. Trabajo fin de grado. Sevilla, España 2016. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: https://idus.us.es/xmlui/bitstream/handle/11441/43789/Gallardo%20G%C3%B3mez%2C%20Roc%C3%ADo%20TFG.pdf?sequence=1&isAllowed=y

utilizando herramientas informáticas como internet, correo electrónico, chat, entre otros. La seguridad de las plataformas tecnológicas están expuestas ataques o vulnerabilidades que puedan ser explotadas por delincuentes informáticos, en el último año se presentaron ataques informáticos de tipo “ransomware” secuestro de la información mediante diferentes modalidades, ha sido el ataque que ha afectado a nivel mundial a todo tipo de organizaciones y particulares, las vulnerabilidades detectadas conllevaron a la ciberdelincuencia apropiarse de la información confidencial y luego exigir el rescate solicitando el pago económico mediante la moneda digital “Bitcoin”, paradójicamente estas acciones lo que realizaban era cifrar la información por parte de los atacantes.[13]

Conforme al portal web español Sophos News publicado el 30 de noviembre de 2016, informaba que un 53% de las pymes en España utilizaba el cifrado de la información, en el cual muchas empresas indicaban que el cifrado no es necesario, pero con la reglamentación de protección de datos de la unión europea a partir de mayo de 2018 las organizaciones que no administre adecuadamente la información estarán sujetas a multas del 4% de los ingresos anuales.

En el 2016 el ransomware (software malicioso) afecto a todo tipo de empresas en el mundo, evidenciando que la seguridad de la información cada vez es un tema altamente relevante, los ataques cibernéticos se hacen principalmente por medio del correo electrónico, esto genera además de perdida de información, pérdidas económicas, esta es una causa para que cada vez las empresas implementen medidas de seguridad con el cifrado de información.

Es evidente que el desconocimiento de esta medida de seguridad por parte de las empresas en general, ha concebido que la información no esté protegida sobre los

---

[13] ESET-LA. Guía de Ransomware [2017]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet:https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf

discos duros de los equipos tecnológicos, correos electrónicos, celulares inteligentes, aplicaciones, programas, etc.

El portal IT Digital Security, en el artículo publicado el 3 de enero de 2019, indico que científicos de IBM se encuentran trabajando sobre cifrados en ambientes de computación cuántica, esto debido que el computador cuántico estará en la capacidad de resolver aquellos problemas que hasta al momento no se podían solucionar, aunque esto conllevaría graves consecuencias de inseguridad en la comunicación sobre internet. Para dar solución a estas falencias, IBM trabaja en dos tipos de cifrado ellos son el cifrado homomórfico y cifrado en celosías. El cifrado homomórfico evita que los datos nunca estén desencriptados a la vez que permite su manipulación por las personas autorizadas y el cifrado en celosías oculta datos dentro de problemas matemáticos complejos sobre estructuras algebraicas llamadas celosías.[14]

Aunque las técnicas actuales de cifrado serán vulnerables con la computación cuántica, el cifrado homomórfico y celosías tendrán la responsabilidad de ofrecer la seguridad que se necesitara en la informática cuántica.

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad de la Información

La seguridad de la información tiene como pilares los siguientes tres elementos confidencialidad, integridad y disponibilidad como se refleja en la figura 1. La

[14] IT Digital Security. (2019) Científicos de IBM trabajan en soluciones de cifrado para entornos de computación cuántica. [Internet]. España. Recuperado de https://www.itdigitalsecurity.es/actualidad/2019/01/cientificos-de-ibm-trabajan-en-soluciones-de-cifrado-para-entornos-de-computacion-cuantica

confidencialidad tiene el objetivo de evitar la difusión de la información sin autorización, mientras que la integridad debe mantener la información protegida ante accidentes, acciones maliciosas y estados de alteración que no han sido autorizadas, y la disponibilidad refiere a que la información deberá estar accesible a los usuarios autorizados que la demanden. Los datos tienen cierta exposición pública y privada tanto en organizaciones y personas del común. Para afrontar los riesgos cotidianos con relación a la información, la seguridad informática ofrece medidas y controles que pueden resguardarla eficazmente.

Figura 1. Pilares seguridad de la información

Fuente: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=1

El cifrado es una de las principales medidas para asegurar la integridad y la confidencialidad de la información que se transmite a través de la red es la encriptación o codificación de los mensajes, evitando que, aun interceptando la comunicación, no sea posible su entendimiento.[15]

4.2.2 Cifrado de la Información

[15] Junta de Andalucia . [2019]. MADEJA Marco de Desarrollo de Software de la Junta de Andalucía.[en línea] [citado el 02 de setptiembre, 2019]. Disponible en internet: http://www.juntadeandalucia.es/servicios/madeja/contenido/subsistemas/desarrollo/cifrado

El cifrado de la información se puede hacer a nivel de software y hardware, sobre las comunicaciones de red, servidores, portátiles, celulares, discos duros, carpetas, documentos, correos electrónicos, unidades USB entre otros como se refleja en la figura 2. El cifrado puede realizarse con programas licenciados o software libre, permitiendo que las pequeñas y medianas empresas Pymes en Colombia accedan a soluciones que incidan en la seguridad de la información.

Figura 2. Cifrado de la información.

Fuente: https://www.tecnozero.com/cifrado/elegir-la-solucion-cifrado

Las pequeñas y medianas empresas Pymes en Colombia están en la capacidad de implementar medidas de seguridad, controles y políticas como elemento de gestión de seguridad de la información.

Básicamente el cifrado de la información utiliza algoritmos matemáticos para la codificación y decodificación de los mensajes que han sido transmitidos de un lugar a otro. Entre las características del cifrado de la información se puede señalar el control de acceso a los datos y en dado caso de robo o pérdida los datos no serán legibles para el que la posea, para ello es importante aplicar claves de acceso complejas y seleccionar la herramienta de cifrado que mejor se ajusta a los requerimientos de cada organización.

El cifrado de la información emplea técnicas que ofrecen alta seguridad, optimización y garantía en el manejo de los datos, estas técnicas son: RSA (Rivest, Shamir y Adleman) un sistema de criptografía de clave pública y la ECC (Elliptic curve Cryptography) criptografía de curva elíptica.

Con el avance informático y las telecomunicaciones, las actividades de criptología han tenido un desarrollo acelerado; el persistente duelo entre creadores de criptosistemas cada vez más seguros y complejos y los descifradores que a través de ataques cada vez más ininteligibles consiguen vulnerar y notar las debilidades de los "seguros" sistemas, llevando así una carrera que cada día cuenta con más recursos económicos, tecnológicos y humanos.[16]

[16] HERNÁNDEZ., Alexander y REYES, Alexander. Metaanálisis del estado actual de la criptografía cuántica identificando las áreas de desarrollo e implementación. [2017]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: https://repository.ucatolica.edu.co/bitstream/10983/1381/1/01%20-%20METAAN%C3%81LISIS%20DEL%20ESTADO%20ACTUAL%20DE%20LA%20%20CRIPTOGRAF%C3%8DA%20CU%C3%81NTICA%20IDENTIFICANDO%20LAS%20%C3%81REAS%20DE%20DESAR.pdf

5. TÉCNICAS DE CIFRADO DE LA INFORMACIÓN

Se conoce como cifrado o criptografía al proceso encargado de convertir la información en datos con caracteres que no permiten comprender su significado y por ende no es fácil de interpretar, por lo cual únicamente podrá ser descifrado por quienes tengan la clave o el procedimiento para interpretar la información cifrada.

Hay quienes consideran que la criptografía es un arte, otras aseguran que es una ciencia aplicada o sencillamente como un procedimiento. Pero la precisión de criptografía la brinda el Diccionario de la Real Academia Española (RAE) con la siguiente descripción: "Arte de escribir con clave secreta o de un modo enigmático". La criptografía se establecía matemáticamente, con la comprensión de abecedarios y procedimientos de comunicación para mayor seguridad.

Ahora la relación de la criptografía con varios ámbitos del conocimiento, como es la teoría de la información, hace que sea inevitable estudios sólidos para el desarrollo de los criptosistemas interdisciplinarios, se requiere del factor humano para su desarrollo, tanto para el criptoanálisis como para la criptografía.[17]

Uno de los primeros usos del cifrado de la información es el cifrado Cesar como se observa en la tabla 1, consistía en el remplazo de las letras del texto original escrito, con otra letra tres lugares siguientes del abecedario, por ejemplo, la letra B con un desplazamiento de tres posiciones, correspondería a la letra E.

---

[17] PABÓN CADAVID. Jhonny. La criptografía y la protección a la información digital.]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

Tabla 1. Cifrado Cesar

Alfabeto normal	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado cesar	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Ejemplo de la palabra *cifrado* utilizando el cifrado Cesar.

Texto original: cifrado

Texto cifrado: fliudgr

Afín es otro tipo de cifrado que consiste en realizar sustitución mono alfabética, cada carácter del alfabeto será remplazado por el carácter del alfabeto cifrado. Otro cifrado utilizado se llamaba *Polibio*, en este las letras del alfabeto se sustituían por la coordenada de la posición en un cuadrado, *Playfair* es un tipo de cifrado que utiliza un algoritmo utilizando poligramas, utilizando bloques de caracteres para cifrado.

Los cifrados afines son basados en aritmética modular, sin embargo, en un alfabeto de n caracteres tendremos solo n posibles cifrados afines, esto hace que un ataque por fuerza bruta sea factible. En general, asignando valores entre *0 y n−1* para un alfabeto de *n* caracteres, con una clave de cifrado dada, el cifrado afín será de la siguiente forma:

$$C \equiv M + Clave \text{ (mód n)}$$

Donde *M* es el carácter en el mensaje, *C* es el correspondiente carácter cifrado

Para poder obtener el mensaje original basta correr el alfabeto hacia la izquierda el número que indique la clave. A continuación, se observa ejemplo de cifrado afín:

Cifrar el mensaje: *“Una noche, una noche toda llena de perfumes, de murmullos y de músicas de alas”.*

Desplazando *UNA* letra el alfabeto. Con lo cual la relación entre los caracteres será:

a b c d e f g h i j k l m n o p q r s t u v w x y z

b c d e f g h i j k l m n o p q r s t u v w x y z a

Una noche,

una noche toda llena de perfumes, de murmullos y de músicas de alas

Vob opdif,

vob opdif upeb mmfob ef qfsgvnft, ef nvsnvmmpt z ef nvtjdbt ef bmbt[18]

También está el cifrado *Hill*, como se observa en la tabla 2, utiliza la sustitución poli alfabética, asociando las letras del alfabeto con números.

Tabla 2. Cifrado Hill

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

En realidad, el método de Hill no es excesivamente práctico, ya que las operaciones con matrices son lentas y además obligan en el caso de no utilizar dispositivos electrónicos a guardar la clave K en un medio físico. Sin embargo, es la primera aproximación seria de las matemáticas a la criptografía y quizás la

[18] TRIANA LAVERDE. Juan. Aplicaciones matriciales a criptografía [2011]. Universidad Nacional de Colombia. [en línea] [citado el 3 de diciembre, 2018]. Disponible en internet: http://bdigital.unal.edu.co/6255/1/Juangabrieltrianalaverde.2011.pdf

primera vez que se utilizaba un problema matemático, fuera de los clásicos de la permutación de elementos, como medio para cifrar información.[19]

PigPen o francmasón, es un tipo de cifrado bastante sencillo, realiza el remplazo de letras por símbolos, fue utilizado por los Masones para resguardar los secretos de sus archivos, *Vernam,* este un tipo de cifrado de flujo donde el texto claro es combinado y utiliza la operación XOR.

5.1 TIPOS DE CIFRADO

Se encuentran las siguientes opciones de cifrado que permiten entre el emisor y receptor intercambien información sin inconvenientes en el descifrado de los datos enviados, en la actualidad se utiliza la criptografía simétrica, criptografía asimétrica y criptografía hibrida.

5.2 CRIPTOGRAFÍA SIMÉTRICA

Este proceso consiste en que tanto como el emisor y receptor de la información usan la misma clave sobre el proceso de cifrado y descifrado, a esta técnica se le denomina también criptografía de clave secreta, como se observa en la figura 3.
El emisor desea enviar un documento al receptor, para ello le aplica al documento un algoritmo simétrico con una clave que también conoce el receptor. Cuando el receptor recibe el mensaje le aplica el mismo algoritmo (inverso) con la misma

[19] SOLER FUENSANTA, Jose. Una introducción a la Criptografía Clásica. [en línea] [citado el 3 de diciembre, 2018]. Disponible en internet: http://www.criptohistoria.es/files/cifras.pdf

clave. Si el documento no ha sido modificado en la transmisión, el resultado será el documento original.

Figura 3. Cifrado Simétrico

Fuente: https://sites.google.com/site/ticgorge2/actividades/cifrado-de-la-informacion

5.3 ALGORITMOS DE CIFRADO SIMÉTRICO

Se conocen dos algoritmos de cifrado, denominados algoritmos de cifrado por bloques y algoritmos de cifrado de flujo.

5.4 CIFRADO POR BLOQUES

Su funcionamiento radica en coger los bloques de tamaño fijo del texto visible, para convertirlo en un bloque de tamaño fijo encriptado, por lo cual se evidenciará el mismo tamaño del texto de entrada, el tamaño del bloque tendrá que ser bastante grande para impedir posibles ataques sobre el texto cifrado, el establecimiento de los bloques de entrada y salida deberá tener la capacidad de volver al estado anterior y ser aleatorio.

En el cifrado simétrico para determinar bloques de algoritmos, están las opciones por sustitución y permutación sobre el texto entendible hasta lograr el texto encriptado.

Sustitución, se fundamenta en remplazar el valor de la entrada, por un probable valor de salida, lo cual se puede expresar, si se utiliza un tamaño de bloque *d,* este podrá ser remplazado por algún de los d^2 de los bloques posibles.

Permutación, aplica sustitución en los bits de un bloque de entrada, reordenándolos y así de esta forma genera el bloque cifrado, manteniendo el registro del bloque de entrada como son los unos y ceros.

Ejemplos de cifrado por bloques:

- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Algorithm)
- AES (Advanced Encryption Standard)
- IDEA (International Data Encryption Algorithm)

5.4.1 Cifrado DES

DES (Data Encryption Standard) Utiliza un sistema mono alfabético mediante algoritmos de cifrados permanentes y el uso sucesivo de diversas permutaciones y sustituciones. DES emplea una clave simétrica de 64 bits, de estos 56 bits son utilizados para la encriptación, los otros 8 bits son de paridad y validación de errores en el procedimiento.

5.4.2 Cifrado 3DES

3DES (Triple Estándar de Cifrado de Datos) este algoritmo realiza triple cifrado del cifrado DES mencionado anteriormente, este presenta segmentación del texto en bloques de 64 bits (8 bytes), realiza permutación inicial de los bloques, adicional de fases de permutación y sustitución 16 veces llamadas rondas, este cifrado mejora la seguridad del cifrado DES.

5.4.3 Cifrado AES

AES (estándar de cifrado avanzado) el algoritmo está basado en diferentes sustituciones y permutaciones lineales, realizada en bloques de 16 bytes, este proceso se repite en varias rondas, este cifrado simétrico usa la misma clave para encriptar y desencriptar.

5.4.4 Cifrado IDEA

IDEA (International Data Encryption Algorithm) Algoritmo que cifra por bloques de 64 bits con clave de 128 bits, realiza ocho transformaciones similares, identificada como ronda, y una transformación de salida denominada media ronda, este cifrado es utilizado en cifrado de texto, en PGPy OpenPGP.

5.4.5 Cifrado de flujo

Consiste en la división de texto en bloques reducidos, de acuerdo a su extensión en bit o byte, para luego así codificar cada uno de los bloques de acuerdo a los bloques que lo anteceden, este tipo de cifrado emplea claves de codificación distintas, con valores que deben estar en el algoritmo según los byte o bit para

producir textos cifrados diferentes cuando se realiza codificación, el cifrado de flujo ha sido empleado para salvaguardar los datos en las comunicaciones inalámbricas.

5.4.6 Cifrado de Feistel

En este tipo de cifrado consta en dividir el bloque de datos de texto claro en dos partes, luego estas son procesadas por etapas, para combinarse y lograr crear el bloque de texto cifrado. En las etapas se mantiene la misma disposición, para luego hace la sustitución sobre la mitad de datos ubicados en la izquierda y aplicando una función sobre la mitad de la parte derecha de los datos, su funcionamiento correcto depende de los siguientes elementos.

Tamaño del bloque, con bloques mayores permite mejor seguridad, pero se disminuye las velocidades en el proceso de cifrado y descifrado, establece en el cifrado de bloques el tamaño de 64 bits.

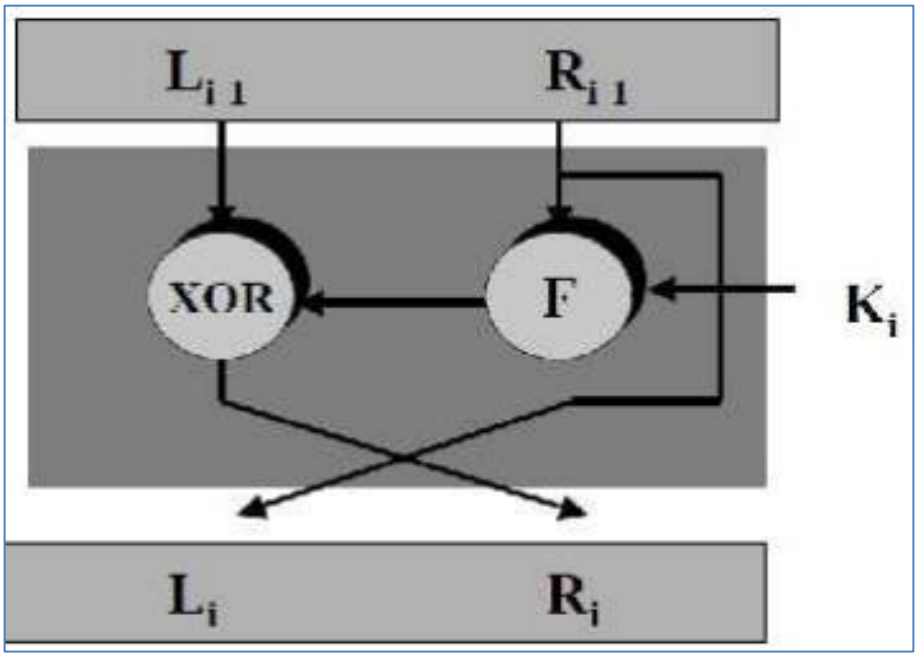
Tamaño de la clave, Con claves extensas la seguridad es mayor, también se aumenta el tiempo para el cifrado y descifrado, la longitud de clave es de 128 bits.

Numero de etapas, el uso de 16 etapas garantiza alta seguridad en el cifrado, utilizar pocas etapas genera baja seguridad.

Algoritmo de generación de subclaves, para dificultar su análisis se deberá crear un algoritmo complejo. En la figura 4, se detalla esquemáticamente como se encuentra formada una ronda de Feistel. En ella se ve que al lado derecho se le aplica junto con la subclave la función que luego con un XOR con el lado izquierdo

forma el lado derecho de la nueva ronda el lado izquierdo de la nueva ronda lo forma el derecho de la ronda anterior.[20]

Figura 4. Ronda Feistel



Fuente: http://opac.pucv.cl/pucv_txt/txt-0000/UCE0239_01.pdf

5.4.7 Técnicas confusión y difusión

Convierte los textos que no tienen formato en textos cifrados, la confusión busca que la clave del cifrado y el texto sin formato, presente alta complejidad, cada uno de los caracteres de la clave cifrada tendrá injerencia en el texto cifrado, por lo cual la difusión amplía la autoridad sobre los caracteres del texto sin formato para

[20] TUREO MUÑOZ, Daniel. Pontificia Universidad católica de Valparaíso Facultad de Ingeniería Escuela de Ingeniería informática uso de tecnologías Gpu para el desarrollo de algoritmos criptográficos. Pág. 30. [2013]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: http://opac.pucv.cl/pucv_txt/txt-0000/UCE0239_01.pdf

minimizar la disposición a técnicas de ataques de tipo estadístico. “En la criptografía simétrica se observa procedimientos como operaciones tan sencillas como la substitución y la permutación, que hoy se aplican al texto en claro de forma combinada y en rondas o iteraciones consecutivas, así como en las adiciones, las multiplicaciones, la aritmética modular y las operaciones XOR”[21].

Los métodos que se distinguen en la criptografía simétrica conocidos como el estándar de codificación de datos (Data Encryption Standard, DES), y el estándar de codificación avanzado (Advanced Encryption Standard, AES).

5.4.8 International Data Encryption Algorithm (IDEA)

Los diseñadores analizaron el cifrado IDEA, algoritmo de cifrado de 64 bits y con clave de 128 bits para medir su fortaleza frente al criptoanálisis diferencial y concluyeron que es inmune bajo ciertos supuestos. No se han reportado debilidades frente criptoanálisis lineal o algebraico.[22]

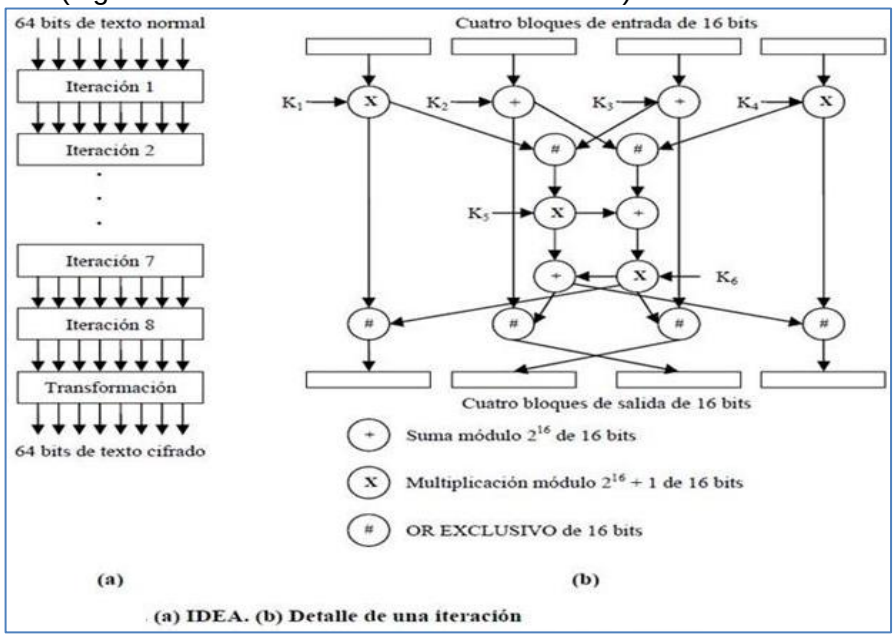
En la figura 5 se refleja el procedimiento de codificación, este realiza ocho sesiones de cifrado similares a excepción de las subclaves empleadas, fue muy utilizado en variedad de aplicaciones informáticas y en área de las redes de las comunicaciones, con relación a la seguridad de la información.

---

[21] SEGURIDAD, Digitalguide. (2017) El encriptado informático: así se protege la comunicación. [Internet]. España. Recuperado de https://www.1and1.es/digitalguide/servidores/seguridad/todo-sobre-los-metodos-de-encriptado/

[22] Alejandro. Algoritmos De Cifrado Para Claves PúBlicas Y Privadas. [2009]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet:https://es.slideshare.net/negro87/algoritmos-de-cifrado-para-claves-pblicas-y-privadas

Figura 5. IDEA (algoritmo internacional de cifrado de datos)



Fuente: http://www.authorstream.com/Presentation/drmakijero-1555992-slide-idea/

5.4.9 Data Encryption Standard (DES)

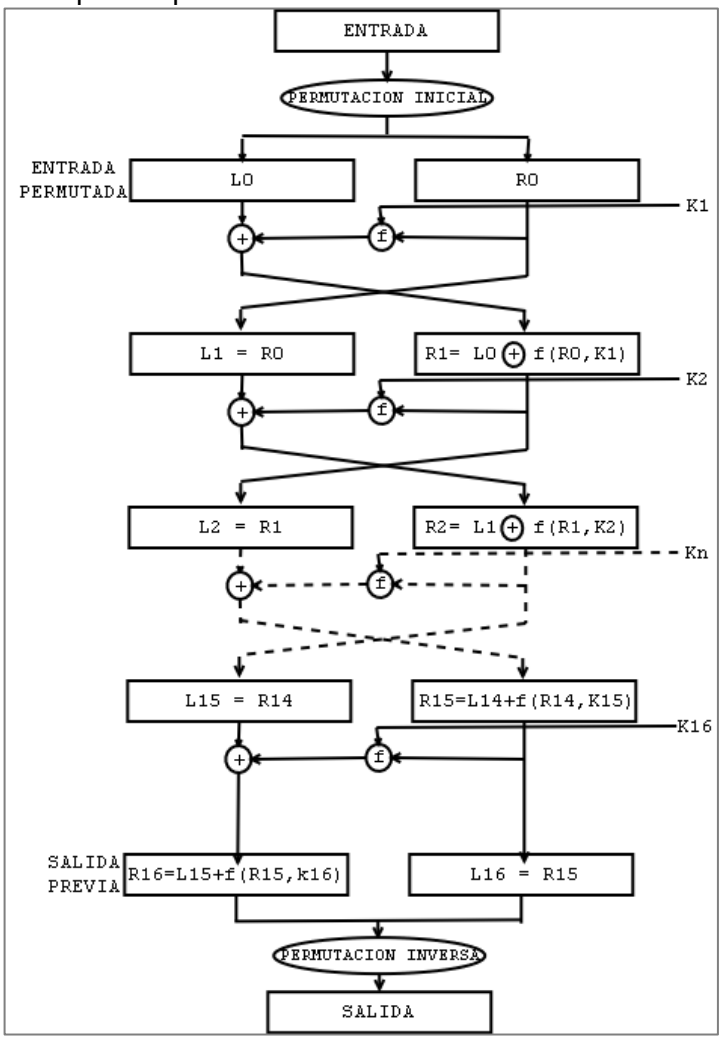
Este tipo de cifrado lo creo la multinacional de tecnología IBM en los años 70s y luego formalizado como estándar, como uno de los primeros procedimientos de encriptación, el cifrado DES utiliza algoritmo simétrico mediante el cifrado de bloques, emplea una clave de 56 bits con bloque de entrada y salida de 64 bits, hace algún tiempo bajo su uso debido a que se pudo establecer vulnerabilidades en este tipo de cifrado, aunque el DES está comprometido con dos elementos esenciales de la criptografía que son la autenticación y el secreto de los datos cifrados, en la autenticación el receptor descifrara el mensaje utilizando la clave compartida generada por el emisor del mensaje y el secreto será accedido con la clave privada. El DES utiliza el cifrado de productos el cual contiene confusión y difusión conceptos que se describieron anteriormente en el presente documento.

Para el descifrado su procedimiento es el mismo que se utiliza para cifrar, realizando un orden inverso.[23]

En la figura 6 se muestra los segmentos importantes del algoritmo, en el cual se encuentra el fraccionamiento del texto en bloques de 64 bits (8 bytes), seguido de la permutación inicial de los bloques, después esta la partición en dos partes L y R (derecha, izquierda) luego se observa las fases de permutación y sustitución reiterado en 16 ocasiones llamado rondas, para finalizar otra vez conectando la parte derecha e izquierda, seguido de la permutación inicial inversa.

[23] GUTIÉRREZ, Jaime. Las Redes Sustitución Permutación y el AES (Advanced Encryption Standard). [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet:https://grupos.unican.es/amac/articles/aes.pdf

Figura 6. Esquema del paso a paso de cifrado DES.



Fuente http://spi1.nisu.org/recop/al02/jgargallo/index.html#intro

5.4.10 Advanced Encryption Standard (AES)

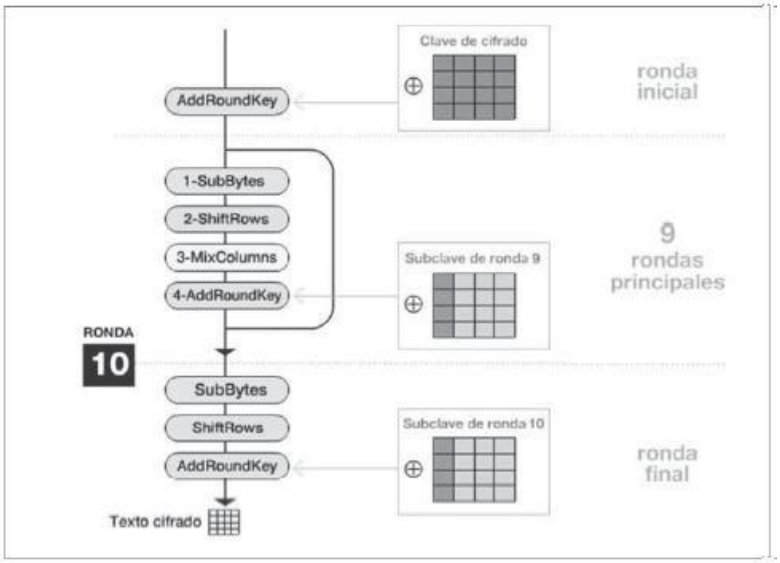
Esta técnica de cifrado logro remplazar el cifrado (DES) y aunque igualmente utiliza bloques, este tiene la capacidad de soportar claves de 128, 192 y 256 bits, el algoritmo se puede subdividir en cuatro etapas como son la expansión de claves, ronda previa, rondas de cifrado y etapa final.

Un equipo de investigadores de Microsoft y de la Dutch Katholieke Universiteit Leuven en 2011 informó de una falla en AES que permite “quebrar” el algoritmo. Pero la propia publicación se aseguró que inclusive con esta falla, un billón de computadores que realizaran cada uno examinar mil millones de claves por segundo, demorarían algo así como 2.000 millones de años para acertar con una clave del sistema AES-128, y adicional se debe tener entender que en la actualidad los equipos de cómputo únicamente consiguen comprobar 10 millones de claves por segundo. También AES evita ataques parecidos a los realizados en el cifrado DES. El uso de la inversa sobre cuerpos finitos en las s-cajas hace que los ataques lineales y diferenciales se vuelvan muy complicados.[24]

En la figura 7 se describe el funcionamiento del cifrado AES, en el cual se aplica de manera reiterada en la matriz de 128 bit cuatro operaciones invertibles en una ronda inicial, luego rondas principales para así terminar con en la ronda final en la generación del cifrado.

[24] MARTINEZ DE LA TORRES, Javier. Cifrado de clave privada: AES Grado en Matemática Computacional. Estancia en Prácticas y Proyecto Final de Grado. [2016]. en línea] [citado el 20 de septiembre, 2018]. Disponible en internet: http://repositori.uji.es/xmlui/bitstream/handle/10234/164666/TFG_Marti%CC%81nez%20De%20La%20Torre%2C%20Javier.pdf?sequence=1&isAllowed=y

Figura 7. Procedimiento cifrado AES



Fuente https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/7236/8892

5.4.11 (3DES)

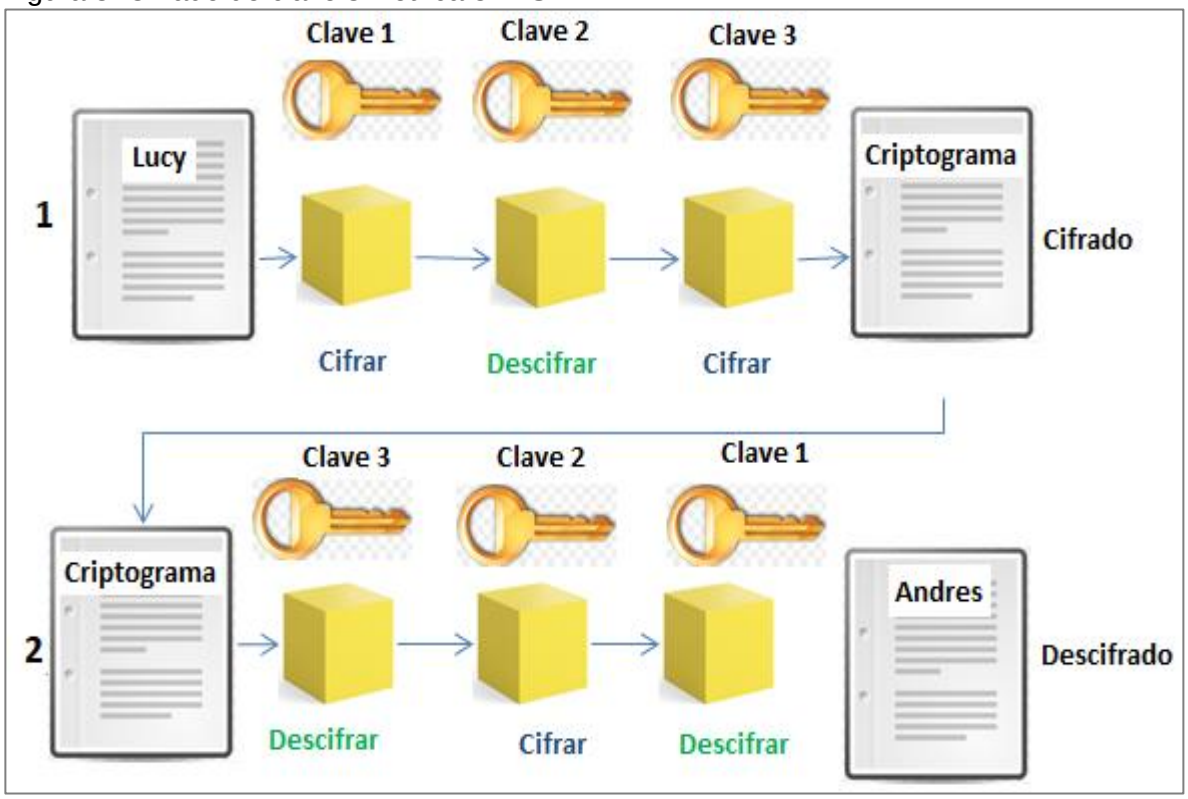
Este tipo de cifrado es la mejora del cifrado DES, tiene fraccionamiento del texto en bloques de 64 bits, tiene permutación inicial de bloques, los bloques están particionados en dos partes, designadas como I izquierda y D derecha, tiene 16 rondas en fases de permutación y sustitución, adicional de la reconexión de las fracciones izquierda y derecha, a continuación de la permutación inicial inversa.

Minimiza vulnerabilidades de ataques de fuerza bruta por el uso de clave la cual contiene longitud de 168 bits, básicamente emplea tres llaves en cada uno de los bloques de texto plano.

El nombre original del algoritmo, tal como lo denominó IBM, era Lucifer. Trabajaba sobre bloques de 128 bits, teniendo la clave igual longitud. Se basaba en operaciones lógicas booleanas y podía ser implementado fácilmente, tanto en software como en hardware.

Tras las modificaciones introducidas por el NBS, consistentes básicamente en la reducción de la longitud de clave y de los bloques, en la figura 8 se observa el funcionamiento de este cifrado, DES cifra bloques de 64 bits, mediante permutación y sustitución y usando una clave de 64 bits, de los que 8 son de paridad (esto es, en realidad usa 56 bits), produciendo así 64 bits cifrados.[25]

Figura 8. Cifrado de clave simétrica 3DES



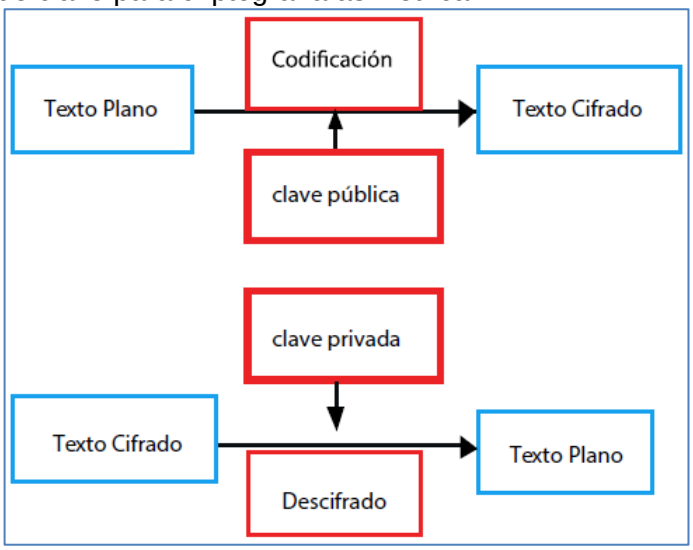
Fuente https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/article/view/7236/8892

[25] SÁNCHEZ ARRIAZU, Jorge. Descripcion del algoritmo DES (DATA Encryption Standard). [1999]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: http://www.satorre.eu/descripcion_algoritmo_des.pdf

5.5 CRIPTOGRAFÍA ASIMÉTRICA

En el cifrado asimétrico tanto el emisor como el receptor de la información crean claves desde su parte, por lo cual obtienen dos claves una en forma pública y la otra en forma privada, así de este modo la comunicación cifrada entre los dos participantes se conocen la clave pública con el uso de un servidor de claves, por ende las claves privadas no se intercambian entre el emisor y receptor, como se muestra en la figura 9 básicamente en esta técnica la clave publica esta en el proceso de cifrado y la clave privada está en el proceso de descifrado, el procedimiento también permite la creación de firmas digitales, comprobación de las firmas digitales, verificación de usuarios y autenticación de usuarios. En otras palabras, los datos cifrados por una clave pública pueden ser encriptados sólo por su clave privada correspondiente.[26]

Figura 9. Proceso de clave para criptografía asimétrica



Fuente https://dialnet.unirioja.es/descarga/articulo/5286657.pdf

5.5.1 Cifrado RSA

[26] MEDINA VARGAS. Yuri, MIRANDA, Andres. Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES REVISTA MUNDO FESC. [2015]. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/5286657.pdf

Creado por Ronald Rivest, Adi Shamir y Leonard Adleman, es un cifrado asimétrico de clave pública, la característica de esta técnica de cifrado, permite que sus dos claves indiferentemente puedan ser utilizadas para el cifrado o la autenticación, actualmente este algoritmo es de los más usados, evidenciándolos en la seguridad de los sitios web con la implementación de SSL/TLS. Este cifrado consta de dos claves, la clave pública y la clave privada, el emisor suministra a los interesados receptores la clave pública y la clave privada solo de conocimiento del dueño, de este modo cuando el mensaje ha sido enviado, el emisor utiliza la clave pública del cifrado del receptor para el cifrado del mensaje, cuando este llega al receptor, la clave oculta se encargará de descifrarlo.

De la siguiente forma funciona RSA:

Cifrado

$C=M^e \bmod n$

Descifrado

$M=C^d \bmod n=(M^e)^d \bmod n=M^{ed} \bmod n$

Generación de claves RSA

Se escogen 2 números primos grandes: p, q

Cálculo de modulo del grupo de trabajo n = p*q

nota ø (n) = (p-1) (q-1)

Selección clave de cifrado e

$1<e<ø(n)$, mcd (e,ø,(n))=1

Obtención clave de descifrado d

e*d=1 mod ø(n) y 0≤d≤n

Si d es inversa de e entonces e*d = 1+k*ø(n) para algún k

Clave publica

PU={e,n}

Clave privada

PR={d,n} Guarda en secreto o destruye p, q y ø(n)[27]

Cifrado ECC

Conocida como criptografía de curva elíptica (ECC) establece puntos sobre una curva para especificar los pares de claves públicas y claves privadas, presenta una seguridad alta con relación a claves cortas, es utilizado en dispositivos móviles, una comparación de su utilidad es que presenta la misma fortaleza en una clave de 256 bits ante una clave de 3072 bits.

Es utilizado también en sitios web, debido a la dificultad del logaritmo matemático, otra característica notable es su rendimiento debido al uso mínimo en la longitud de la clave.

Beneficios clave

[27] RSA. Creación de claves en el sistema RSA. [en línea] [citado el 25 de noviembre, 2018]. Disponible en internet: https://cs.uns.edu.ar/~ldm/mypage/data/ss/info/ejemplo-rsa.pdf

- *Seguridad superior:* ECC ofrece mayor protección contra los ataques que los métodos de cifrado actuales. El algoritmo ECC se basa en un problema matemático más difícil de atacar que el cifrado actual para los piratas informáticos, logrando sitios web e infraestructuras más seguras que con los métodos tradicionales.

- *Mejor rendimiento:* ECC requiere claves de menor longitud para brindar un nivel superior de seguridad. Por ejemplo, una clave ECC de 256 bits ofrece el mismo nivel de protección que una clave RSA de 3072 bits.

- *Protección de su inversión:* ECC permite proteger la inversión en infraestructura, ya que ofrece seguridad superior para administrar el exceso de conexiones de dispositivos móviles. La longitud de las claves ECC aumenta a una velocidad menor que las claves de otros métodos de cifrado y pueden ampliar el ciclo de vida del hardware existente.

- *Ventaja móvil:* cuanta más pequeña son las claves ECC, más pequeños son los certificados y menos ancho de banda consumen.[28]

5.5.2 Cifrado PGP

Esta técnica de cifrado PGP (Pretty Good Privacy), es la mezcla entre el cifrado simétrico y el cifrado asimétrico, los usuarios crean la clave pública y una privada, de esta forma el mensaje se cifra con la clave pública y se descifra con la clave privada o al revés cifran el mensaje con la clave privada y se descifra con la clave pública, no es posible cifrar con la misma clave, en el proceso de cifrado realiza

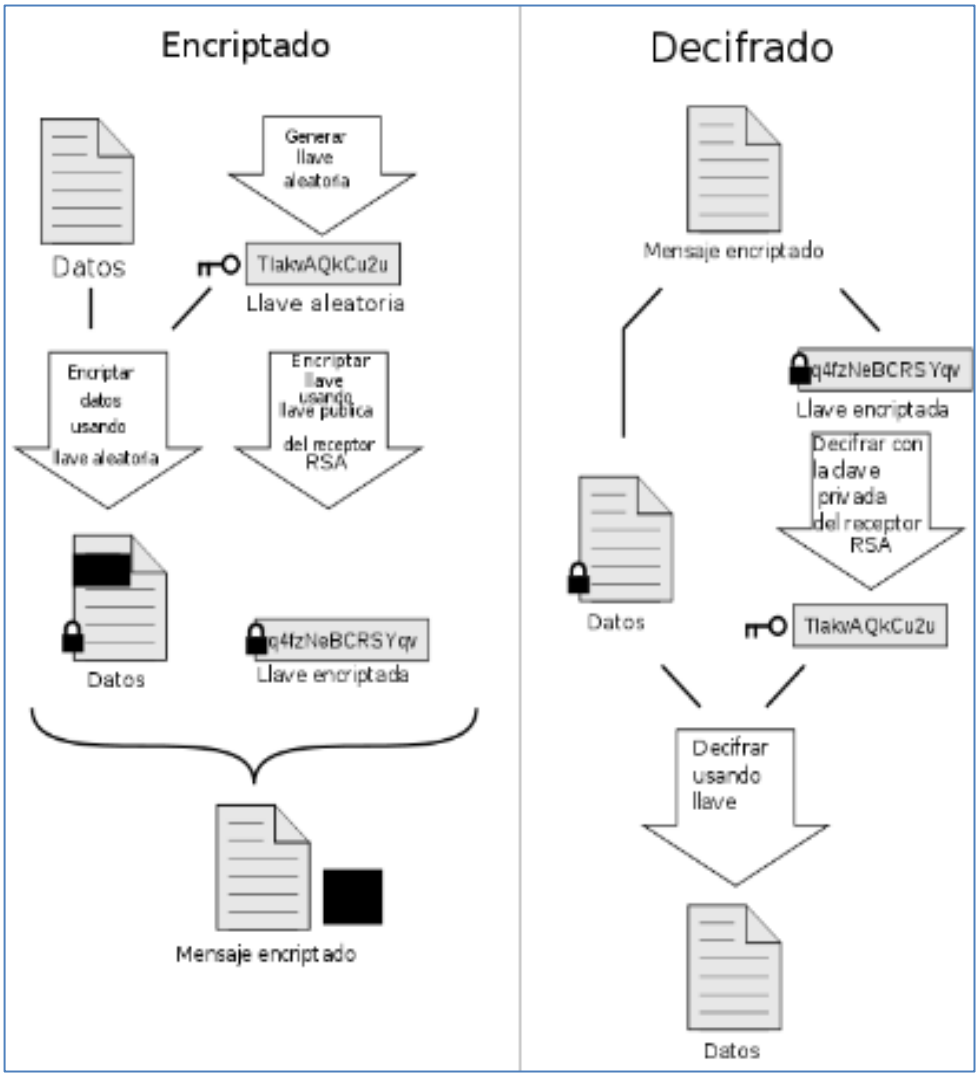
[28] Certificados SSL de Symantec con el algoritmo ECC. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: https://s3-eu-west-1.amazonaws.com/ssl247/1407851741_ECC_Algorithm_ES.pdf

compresión de datos, creando una clave aleatoria encargada de descifrar el mensaje, también es utilizado para firmas digitales garantizando autenticación e integridad del mensaje, evidenciando que este no ha sido modificado.

PGP proporciona lo que se denomina "anillo de claves" (llavero), que es un único fichero donde el usuario puede guardar todas sus claves, con facilidad para realizar inserción y extracción de claves de manera sencilla. Para autentificar claves, como se observa en la figura 10, PGP permite que los usuarios "firmen claves", por lo que podemos confiar en la autenticidad de una clave siempre que ésta venga firmada por una persona de confianza. Así la "autoridad de certificación" de otro tipo de sistemas (entidades que aseguran la autenticidad de las claves), en PGP son los propios usuarios.[29]

[29] Junta de Andalucía. Seguridad en Redes TCP/IP. Encriptación de la Información. . [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet:http://www.juntadeandalucia.es/empleo/recursos/material_didactico/especialidades/materialdidactico_administrador_servidores/Content/4-seguridad/6-Encriptacion.pdf

Figura 10. Funcionamiento PGP



Fuente http://www.wikiwand.com/es/Pretty_Good_Privacy

6. OPCIONES DE CIFRADO DE LA INFORMACIÓN PARA EMPLEAR EN LAS PYMES COLOMBIA

Las pequeñas empresas en Colombia cuentan con una infraestructura informática de menor alcance en tecnología a comparación de las grandes empresas y multinacionales que operan en el país, lo cual genera que sean un blanco fácil de ataques informáticos hechos por la ciberdelincuencia.[30]

Las actividades diarias en las empresas requieren realizar acciones donde se compromete información mediante el envío y recepción de la información utilizando el correo electrónico, aplicaciones, acceso a bases de datos, conexiones a las redes informáticas de la empresa, uso de FTP entre otros.

Como primera medida debe identificarse la información que requiere de cifrado, debido a que no es necesario realizar cifrado sobre todos los datos, se debe crear prioridades con la información sensible para aplicar técnicas de encriptación según corresponda el uso que se realiza con esta.

6.1 ENCRIPTACIÓN POR HARDWARE

Normalmente los cargos gerenciales en las empresas cuentan con información confidencial, esto sugiere que tanto equipos físicos como son discos duros, equipos portátiles, USB y medios de almacenamiento externo, utilicen tecnologías de cifrado de hardware evitando así el acceso no autorizado a las personas que

---

[30] FLOREZ, Wilmar. Arboleda, Carlos. Cadavid, Jhon. SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM. [2012]. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

no cuenten con los privilegios. Actualmente diferentes tipos de fabricantes de discos duros y memorias USB, tiene a disposición, el cifrado del disco duro transforma la información legible en información ilegible, complicando la lectura del mismo, el disco duro podrá ser encriptado en su totalidad, lo que significa que aplicara sobre todos los datos como son carpetas, subcarpetas, archivos de todo tipo que se incluyen dentro de las unidades del disco duro. El cifrado por archivo, son las que especifica el usuario de esta forma se selecciona la información que tiene relevancia y por ende el cifrado y descifrado es más rápido a comparación del funcionamiento del cifrado y descifrado de todo el disco.[31]

Para el cifrado de hardware en los discos duro de los computadores conlleva implementar dispositivos físicos adicionales y la instalación de partes, para no comprometer el funcionamiento del equipo, el sistema operativo e inicio del equipo para mantener la misma operatividad ante el usuario que lo utiliza.

El cifrado de USB por hardware, cuentan con un teclado alfanumérico para el bloque y desbloqueo, incluido en su diseño y ofrece encriptación de datos de 256 bits XTS, con la particularidad que en algunos fabricantes se puede realizar bloqueo remotamente y limitar su uso a ciertos lugares para evitar su uso.

Ventajas

- El cifrado de hardware tiene mayor seguridad al cifrado por software, debido a que mantiene distancia entre los equipos de cómputo, dificultando la interceptación de los datos cifrados.

[31] KINGSTON. Cifrados basados en hardware frente a los basados en software. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: https://www.kingston.com/es/usb/encrypted_security/hardware_vs_software

- El procedimiento de cifrado y descifrado no afecta el rendimiento de los equipos de cómputo porque este proceso actúa independientemente a los requerimientos físicos de cada uno.

- La autenticación se realiza en dispositivo que realiza la encriptación.

- No se requiere instalar controladores en el equipo de cómputo donde se aplica el cifrado de la información.

- Ofrece protección sobre los ataques informáticos que se presentan continuamente, códigos maliciosos y el uso de fuerza bruta.

- La encriptación siempre se encontrará activa sobre el equipo al cual realiza el cifrado.

Desventajas

Los costos de implementar la encriptación por hardware son altos a comparación de la encriptación por software.

Si los dispositivos de encriptación por hardware llegasen a fallar o presenta un deterioro físico dificultan el acceso a la información cifrada por parte del usuario autorizado.[32]

[32] Universidad Politécnica de Madrid. Curso de privacidad y protección de comunicaciones digitales. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion2/leccion2.html#apartado2

6.2 ENCRIPTACIÓN POR SOFTWARE

Con el cifrado utilizando software se busca proteger la información contenida en discos duros, carpetas, archivos, medios extraíbles y dispositivos USB, conservando el cifrado en el movimiento de la información de un lugar a otro, para que de esta forma pueda ser descifrado con el software y credenciales permitidas. El cifrado con software utiliza programas instalados dentro del mismo equipo donde se contiene la información a cifrar, no debería afectar el funcionamiento normal del equipo ofreciendo operación normal al usuario que lo manipula, para descifrar la información se debe ingresar la contraseña asignada, de lo contrario la información se mantendrá bloqueada, básicamente utilizando el algoritmo de cifrado y descifrado se podrá acceder a la información, en la actualidad se encuentra incluido en sistemas operativos de Microsoft, pero también hay otras herramientas licenciadas para realizar este proceso.

Este tipo de cifrado basado en software protege la confidencialidad de los datos incluso cuando el sistema operativo no está activo, por ejemplo, si los datos se leen directamente desde el hardware o desde otro sistema operativo. Además, la encriptación suprime la necesidad de borrar los datos al final del ciclo de vida del disco.

Ventajas

- La implementación de cifrado con el uso de software es más económico que el cifrado por hardware.

- El software de cifrado no requiere hardware ni tampoco software adicional para su correcto funcionamiento.

- Se puede implementar en varios equipos y dispositivos de cómputo para el cifrado y descifrado.

Desventajas

- El cifrado de software consume recursos del equipo o dispositivo en el cual está instalado, lo que conlleva que pueda afectar el rendimiento y velocidad del equipo informático.

- Si se aplica cifrado a un nivel superior, los archivos cifrados serán lentos al momento de utilizarlos.

- Puede ser susceptible ataque de fuerza bruta y requerir de actualizaciones para su correcto funcionamiento.[33]

6.3 ENCRIPTACIÓN CORREO ELECTRÓNICO

El texto plano, el contenido y archivos adjuntos que se envían y reciben por correo están en la posibilidad de ser interceptados por atacantes informáticos, el cifrado de correo electrónico permite minimizar riesgos de que los datos que se transmiten por este medio sean hurtado y modificados.

La implementación de software para cifrar el correo electrónico ha tomado gran fuerza en los últimos años, esto implica directamente al emisor de mensaje y al receptor del mensaje porque serán los únicos que contarán con la contraseña para el cifrado y descifrado del mensaje conocido también como cifrado de punto a

[33] Universidad Politécnica de Madrid. Curso de privacidad y protección de comunicaciones digitales. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion2/leccion2.html#apartado2

punto. Dentro de las opciones que se encuentran en la actualidad se encuentra el cifrado PGP (Prety good privacy) de código abierto, también se encuentra el cifrado basado en políticas para proteger el correo electrónico.

Ventajas

- Mantiene la privacidad de los correos, protege la información de ataques hechos sobre la red de comunicaciones.

- Utiliza seguridad empleando firmado digital, garantizando la autenticidad del remitente del correo e integridad en el mensaje.

- Opción de seleccionar los mensajes que se desean cifrar y aquellos que no requieren de cifrado.

- Uso de interfaz web para el descifrado de los mensajes del correo electrónico.

- Su implementación en costos económicos es baja.[34]

Desventajas

- Se pueden presentar inconvenientes con el emisor y receptor, en el desconocimiento del proceso de cifrado, se requiere de capacitación para su correcto funcionamiento.

[34] ESET. Cifrado de la Información. Guía Corporativa. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

- El software libre no contiene soporte de gestión y el caso de software licenciado el costo constituye en cada cuenta de correo, adicional de los costos de soporte.

6.4 CIFRADO DE REDES

Constituye la protección de datos que circulan por las redes informáticas, el uso de redes VPN (Virtual Private Network) utilizando la encapsulación y encriptación de paquetes de datos, manteniendo seguridad en el envío y recepción de información sobre redes públicas y privadas.

Las redes privadas virtuales utilizan protocolos de túnel entre los que se encuentran:

- *Protocolo de túnel punto a punto (PPTP)*, utiliza el puerto 1723, encapsula los paquetes del protocolo punto a punto, con en el protocolo Generic Routing Encapsulation (GRE) permite muy buenas velocidades de conexión, este protocolo está compuesto por un paquete de envió, un header IP, un header GREv2 y el paquete de carga, y utiliza el sistema RC4 de RSA para la encriptación con clave de 40 bits.

  Ventajas

  - Alta velocidad en la comunicación.
  - Funciona en equipos de tecnología anterior.
  - Soporta dispositivos móviles.

Desventajas

- Seguridad baja.
- Tiende a ser bloqueado por los proveedores de internet.[35]

- *Internet Protocol Security (IPSec) / L2TP,* protocolos que están en la capacidad de enviar datos cifrados en las redes IP, brinda encriptación Encapsulated Security Payload (ESP) y Authentication Protocol (AH) autenticación por cada paquete IP, utiliza el cifrado de AES-256 bit.

Ventajas

- Alta seguridad.
- Utiliza el protocolo de UDP para encapsular.
- Encapsula dos veces los datos.

Desventajas

- Configuración es tediosa.
- El firewall bloquea en algunas oportunidades
- La velocidad puede ser lenta.[36]

---

[35] MARIO, Galarza. SANTOS, Andres. FUNDAMENTOS DE COMPUTACION TECNOLOGIA VPN [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cestudiantes%5Ctrabajos_de_clases/1580_TRECALDE_0033.pdf

[36] LUJAN, Erick. Universidad de San Carlos de Guatemala Facultad de Ingeniería Escuela de Ingeniería en Ciencias y Sistemas SEGURIDAD EN IP CON EL PROTOCOLO IPSEC. [2005]. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://biblioteca.usac.edu.gt/tesis/08/08_0261_CS.pdf

- *SSL y TLS,* utiliza el cifrado simétrico, el tráfico es cifrado y descifrado desde los dos lados del canal con el uso de llaves, su funcionamiento se basa en ofrecer al usuario conexión a los recursos asignados como aplicaciones, pero no le permite acceder a la red completa, utiliza certificados digitales para que la comunicación se mantenga segura de las conexiones que viajan por internet.

  Ventajas

  - Seguridad en el acceso a los recursos de la red.
  - Instalación fácil en los navegadores web, no necesita instalación de software en los equipos de usuario final.
  - Añade aleatoriamente caracteres a los datos originales creando dificultad de ser interceptada e interpretada.

  Desventajas

  - Su implementación es costosa
  - El consumo de los recursos en los equipos y dispositivos informáticos es considerable.[37]

[37] GONZÁLEZ HERNÁNDEZ, Ana. Curso de Seguridad Informática Módulo 6. Redes Virtuales Privadas. [en línea] [citado el 4 de diciembre, 2018]. Disponible en internet: http://www.informatico-madrid.com/global/images/CursosSeguridadTema6.pdf

7. FUNCIONAMIENTO DE LAS HERRAMIENTAS Y SOFTWARE EN CIFRADO LA INFORMACIÓN

Los fabricantes de tecnología ofrecen variedad de herramientas para el cifrado de datos, en la actualidad las empresas disponen de software libre y licenciado para implementar sobre los recursos informáticos de las organizaciones, adicional otra opción es el cifrado de información basado en hardware como son discos duros y unidades flash USB. De acuerdo a los requerimientos técnicos, costos y funcionalidad, las Pymes en Colombia tiene la posibilidad de implementar una solución de cifrado para la protección de los datos confidenciales.

A continuación, se indican algunas herramientas de encriptación de datos, que pueden ser empleadas por las Pymes en Colombia.

7.1 DISKCRYPTOR

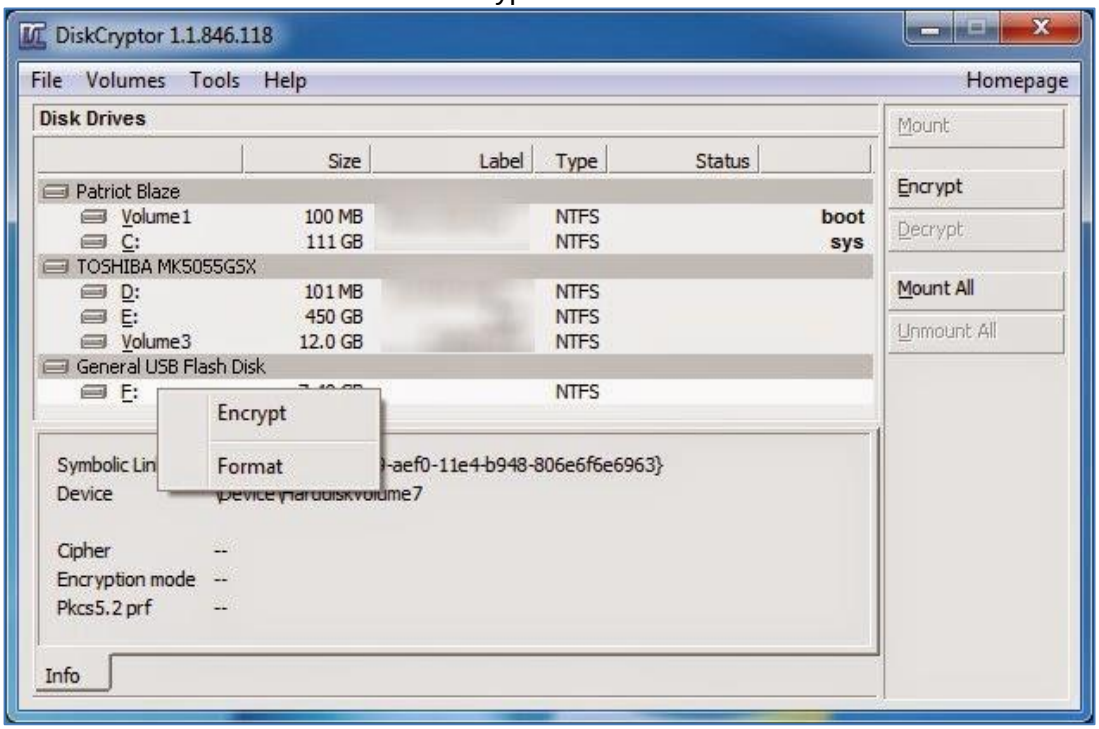
Es un programa de encriptación de código abierto, para discos duros, medios extraíbles, USB y CD/DVD, permite hacer cifrado de datos sobre particiones o sobre la unidad completa, emplea algoritmos AES-256, Twofish o Serpent, está disponible para Windows 2000, Windows XP, Windows server 2003, Windows 7 y Windows 2008 R2, se puede descargar de la página oficial https://diskcryptor.net/wiki/Downloads, es sencilla su instalación al ejecutar el programa este carga gráficamente para facilidad del usuario.

A continuación, se describe gráficamente el funcionamiento de la herramienta de cifrado “DiskCryptor”, esta opción puede ser implementada en las Pymes en Colombia, debido que no tiene costo por su licenciamiento, pero se deberá tener

en cuenta que no tiene soporte ante algún tipo de inconveniente con la herramienta.

En la figura 11, al ejecutar el programa carga la información de los discos y particiones que se desean cifrar, allí se procede a seleccionar la partición o el disco de unidad, hacer click con botón derecho, para optar por “Encrypt”.[38]

Figura 11. Herramienta de cifrado DiskCryptor



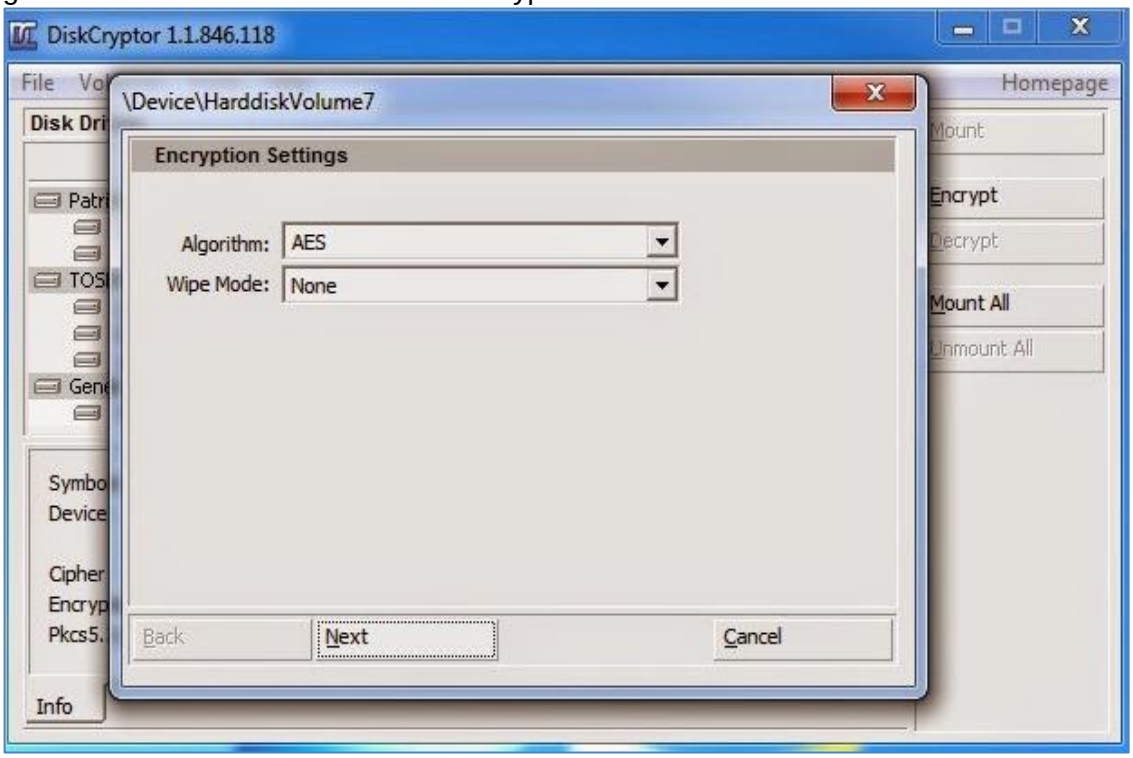
Fuente http://putoinformatico.blogspot.com/2015/02/como-cifrar-discos-con-diskcryptor.html

En el siguiente paso que se muestra en la figura 12 se deberá seleccionar el tipo de algoritmo de cifrado, según el criterio de cada usuario, para este caso la configuración de cifrado tiene seleccionado el algoritmo AES y wipe mode en None.

---

[38] DiskCryptor. Open source partition encryption solution. [en línea] [citado el 4 de diciembre, 2018]. https://diskcryptor.net/wiki/Screenshots

Figura 12. Herramienta de cifrado DiskCryptor Paso 2



Fuente http://putoinformatico.blogspot.com/2015/02/como-cifrar-discos-con-diskcryptor.html

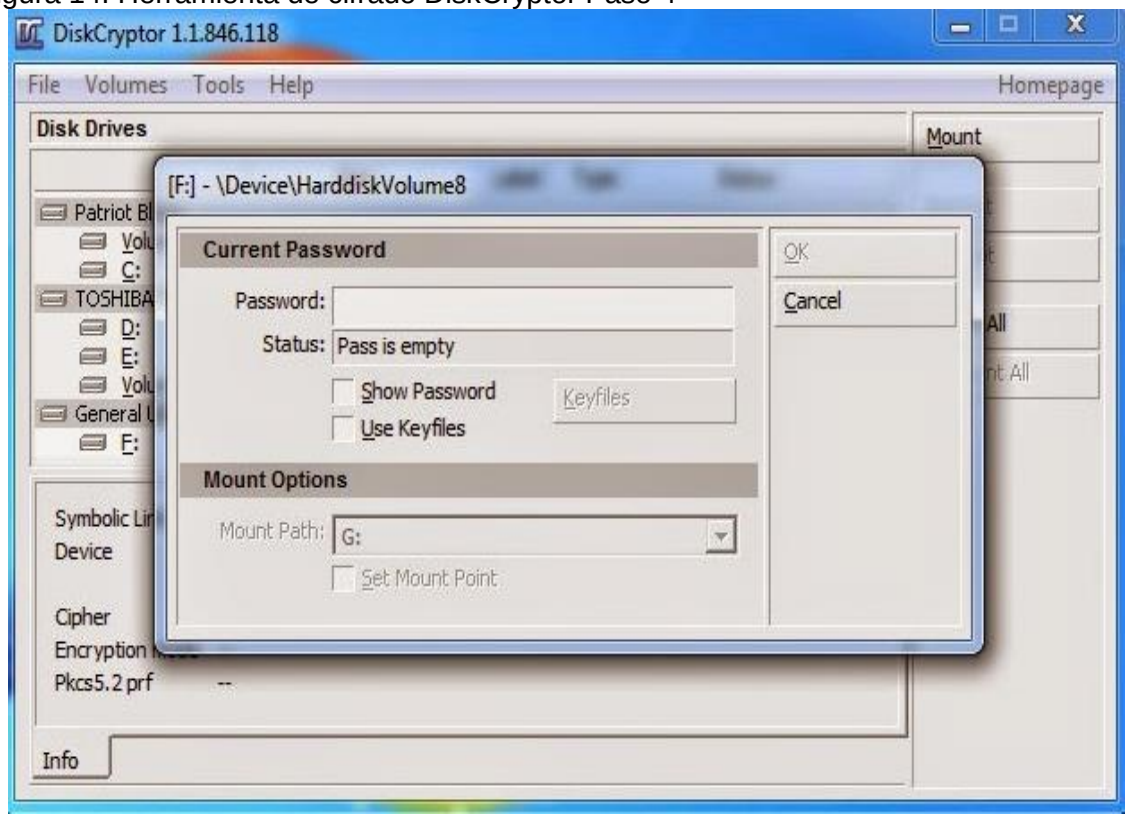
Luego en la siguiente fase de la figura 13, el usuario asigna la contraseña para el proceso de cifrado y descifrado de los datos y oprime en el botón “OK” para confirmar el cifrado.

Figura 13. Herramienta de cifrado DiskCryptor Paso 3

Fuente http://putoinformatico.blogspot.com/2015/02/como-cifrar-discos-con-diskcryptor.html

Para acceder a la información desde otro equipo, este debe tener instalado el mismo programa de encriptación y se tendrá que ejecutar de forma normal, en la figura 14 se muestra la ventana que aparecerá, al cargar las unidades de disco, debe dar clic con el botón derecho sobre la unidad cifrada, selecciona “Mount” en esta ventana para el ingreso de la contraseña generada.

Figura 14. Herramienta de cifrado DiskCryptor Paso 4



Fuente http://putoinformatico.blogspot.com/2015/02/como-cifrar-discos-con-diskcryptor.html

7.2 GPG4WIN

Es una herramienta de encriptación de código abierto, tiene como finalidad el transporte seguro de correos electrónicos y archivos, con el uso de cifrado y firmas digitales, el programa tiene los siguientes componentes:

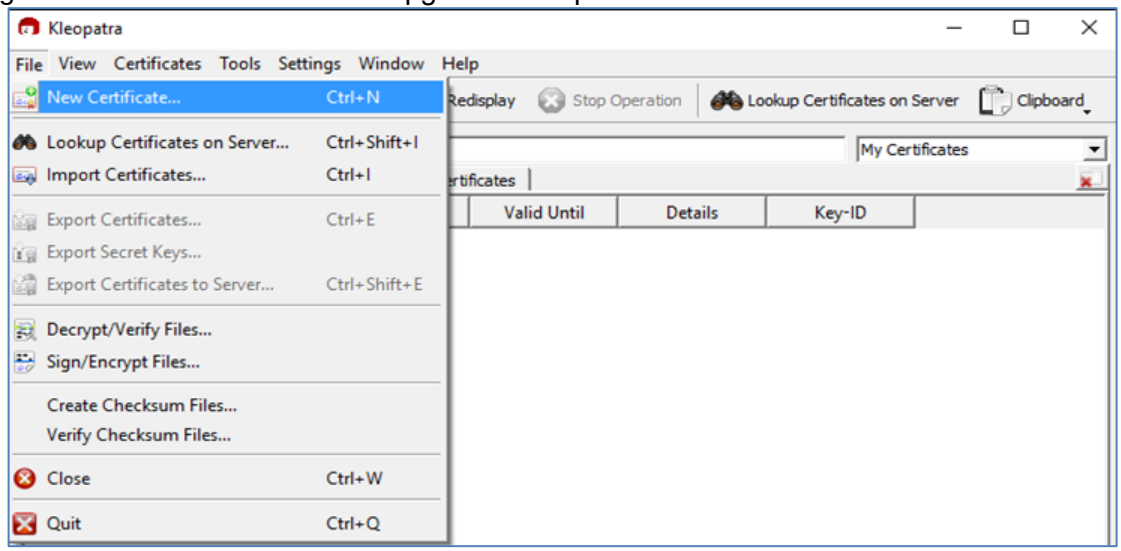
- *GnuPG,* herramienta para el cifrado, utiliza un sistema de cifrado asimétrico
- *Kleopatra,* administrador de certificados para OpenPGP y X.509 (S / MIME) y diálogos criptográficos comunes.
- *GpgOL,* complemento para Microsoft Outlook 2003/2007/2010/2013/2016 (cifrado de correo electrónico). Con Outlook 2010 y superior, GpgpOL es compatible con MS Exchange Server.

- *GpgEX,* Un plugin para Microsoft Explorer (cifrado de archivos).

- *GPA,* administrador de certificados alternativo para OpenPGP y X.509 (S / MIME).[39]

La herramienta se podrá descargar desde la página oficial https://www.gpg4win.org/ en el siguiente paso a paso se describe la creación de clave pública y privada para el cifrado de la información utilizando “Kleopatra”, al igual DiskCryptor, la instalación es bastante sencilla y amigable para el usuario como se observa en la figura 15, su entorno grafico facilita su uso, se hace doble clic sobre el icono de Kleopatra, carga la ventana, se dirige hacia "File" y se pulsa en "New certificate".

Figura 15. Cifrado herramienta Gpg4win “Kleopatra” Paso 1

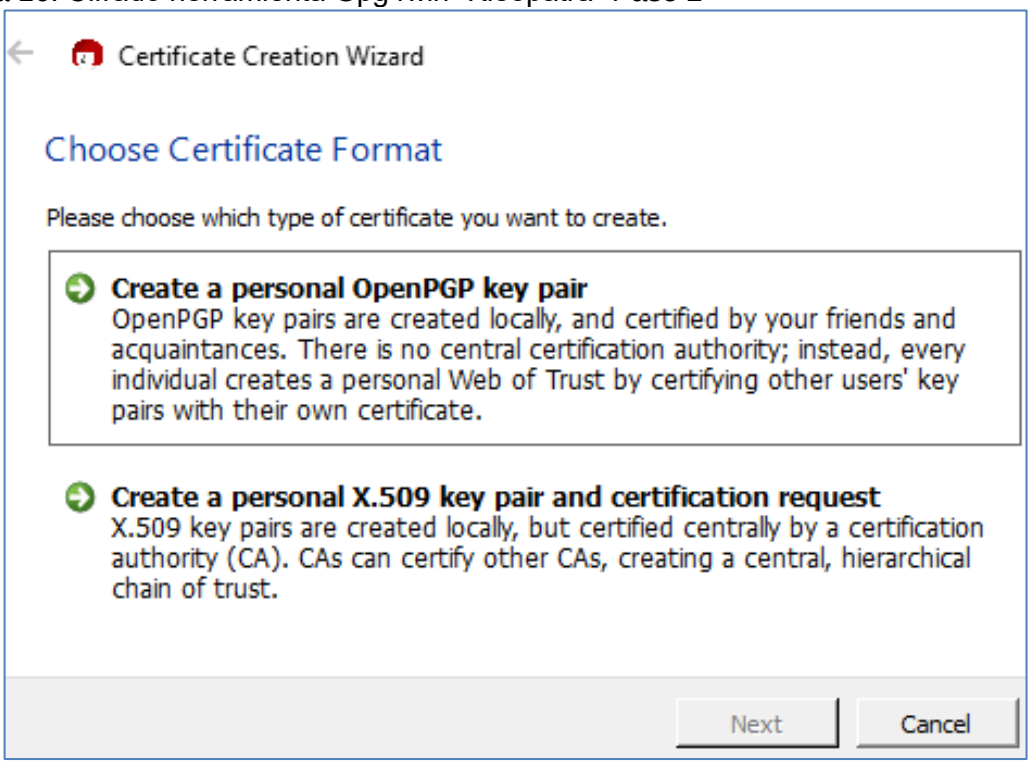


Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Luego en la figura 16 el usuario selecciona el tipo de certificado, para este ejemplo la opción seleccionada es la primera “Create a personal OpenPGP key pair.

[39] GPG4WIN. a secure solution. [2018]. [en línea]. Disponible en internet: https://www.gpg4win.org/

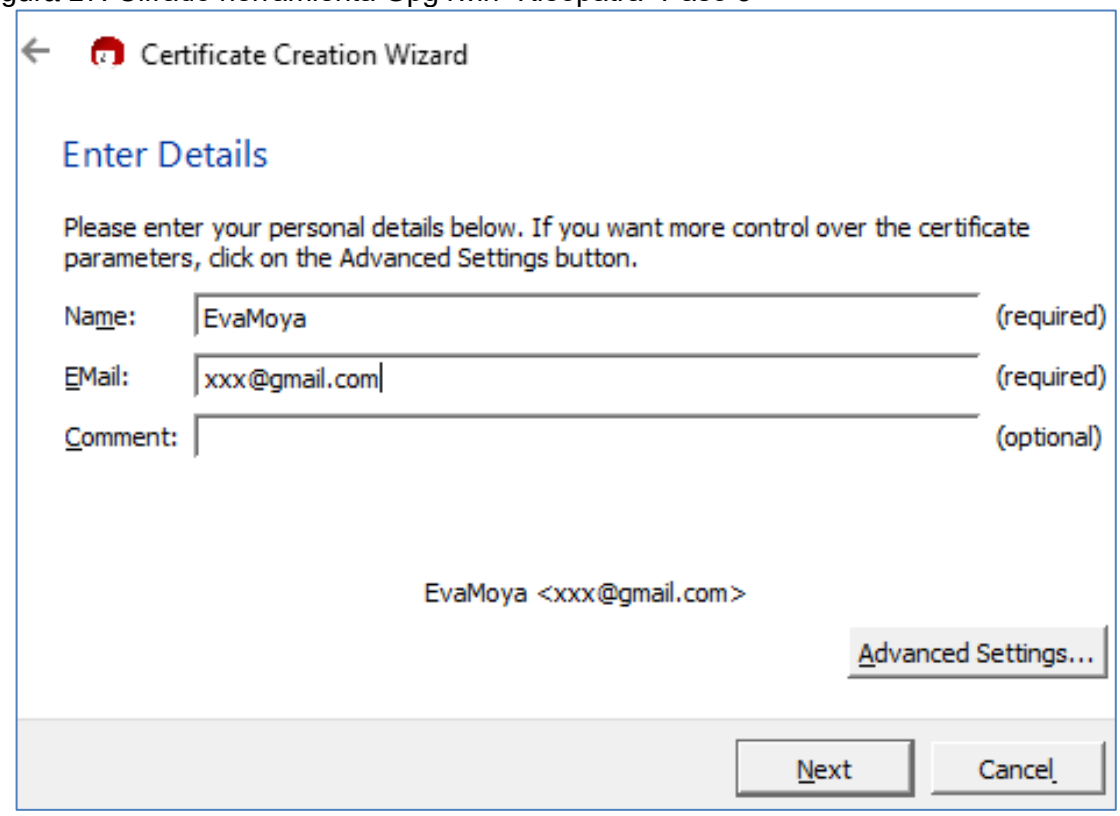
Figura 16. Cifrado herramienta Gpg4win “Kleopatra” Paso 2



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Ahora en la figura 17 en la siguiente ventana se ingresa el nombre y correo electrónico, opcionalmente se puede hacer un comentario en el campo que lo indica, también es opcional la configuración avanzada, de acuerdo al criterio y conocimiento de cada usuario.

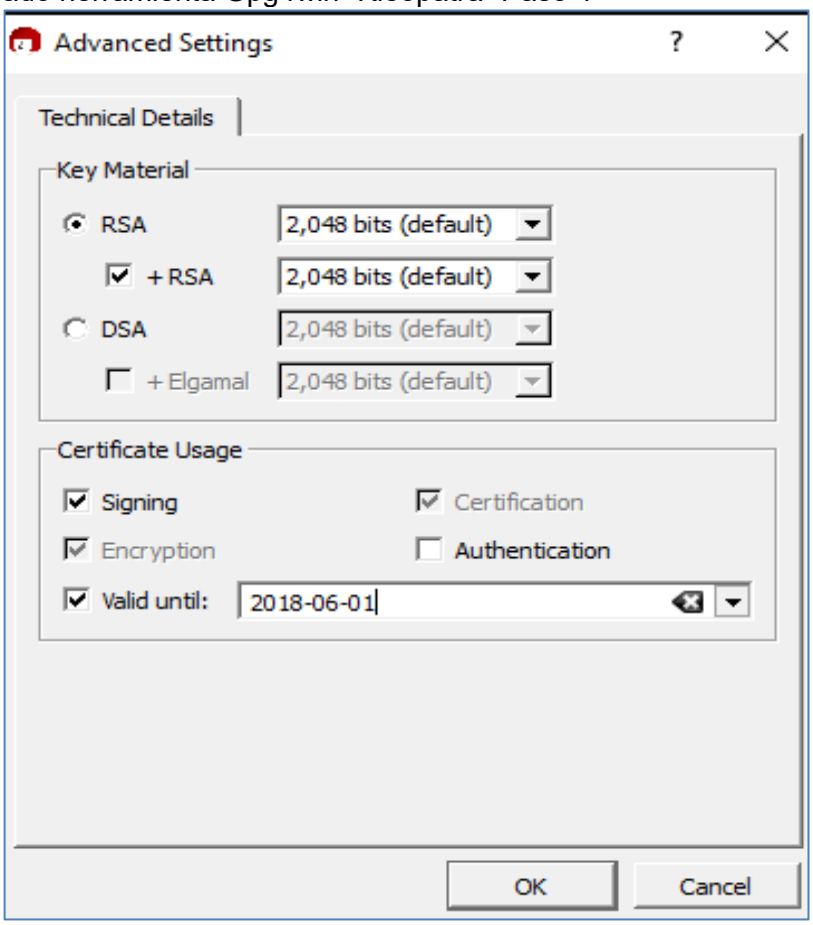
Figura 17. Cifrado herramienta Gpg4win “Kleopatra” Paso 3



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

El cifrado por defecto que aparece en la figura 18 corresponde “RSA” allí aparecen los detalles de las configuraciones avanzadas como es la opción “Certifícate Usage”

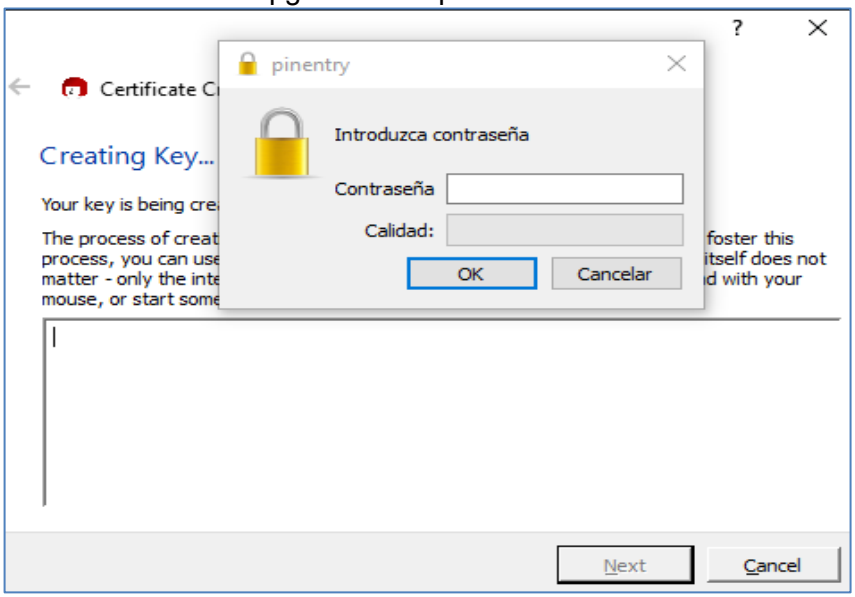
Figura 18. Cifrado herramienta Gpg4win “Kleopatra” Paso 4



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Ahora en la figura 19 en la siguiente ventana de la herramienta de cifrado Gpg4win se procede con la asignación de la contraseña de seguridad para el descifrado de los datos, es recomendable generar una contraseña compleja para asegurar un correcto cifrado.

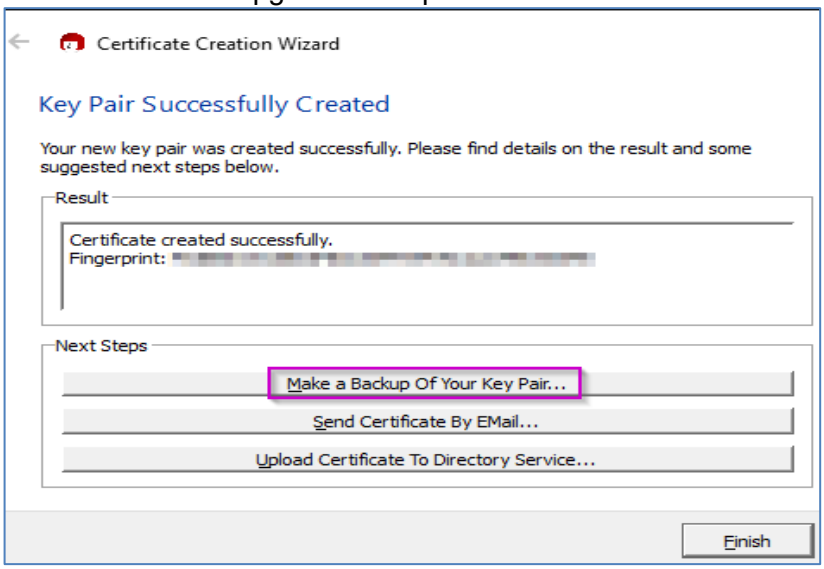
Figura 19. Cifrado herramienta Gpg4win “Kleopatra” Paso 5



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Confirmada la creación de la clave asimétrica como se demuestra en la figura 20, es recomendable hacer copia de seguridad, en caso de requerir restauración del programa, deberá seleccionar "Make a Backup".

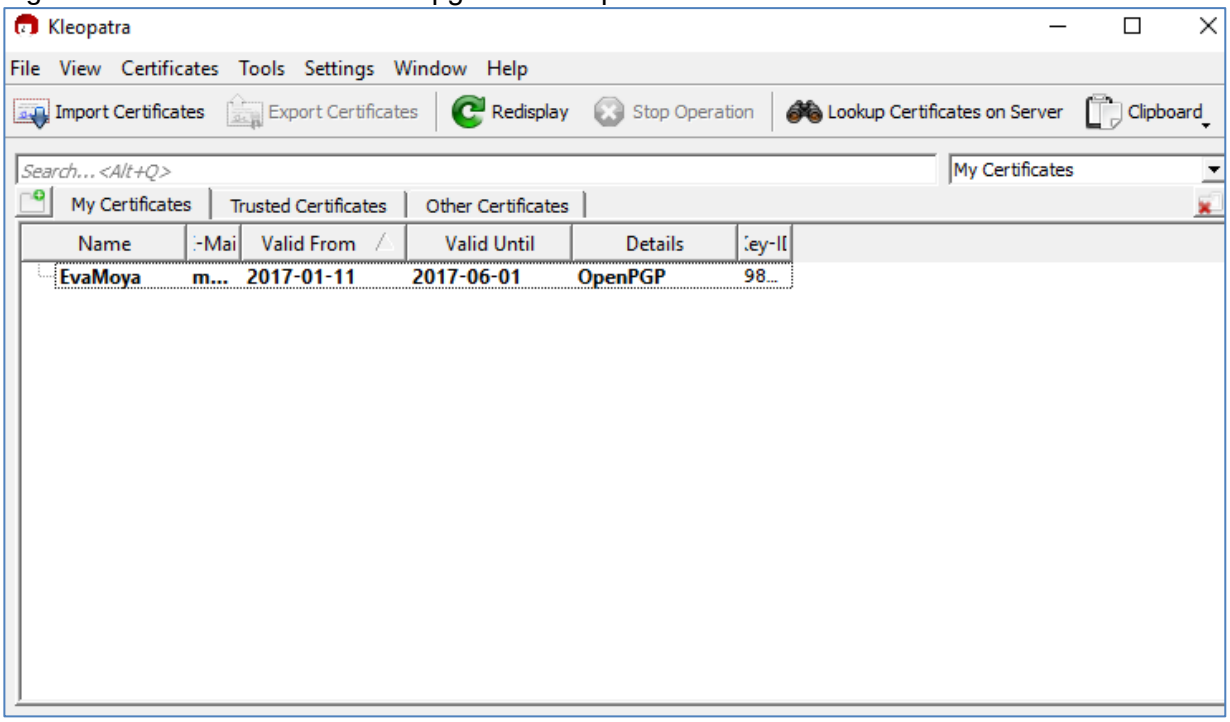
Figura 20. Cifrado herramienta Gpg4win “Kleopatra” Paso 6



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Luego de finalizado el proceso anterior, en la figura 21 se evidencia en la ventana principal las llaves creadas, también se observa en el menú opciones de importantes como importar y exportar certificados.

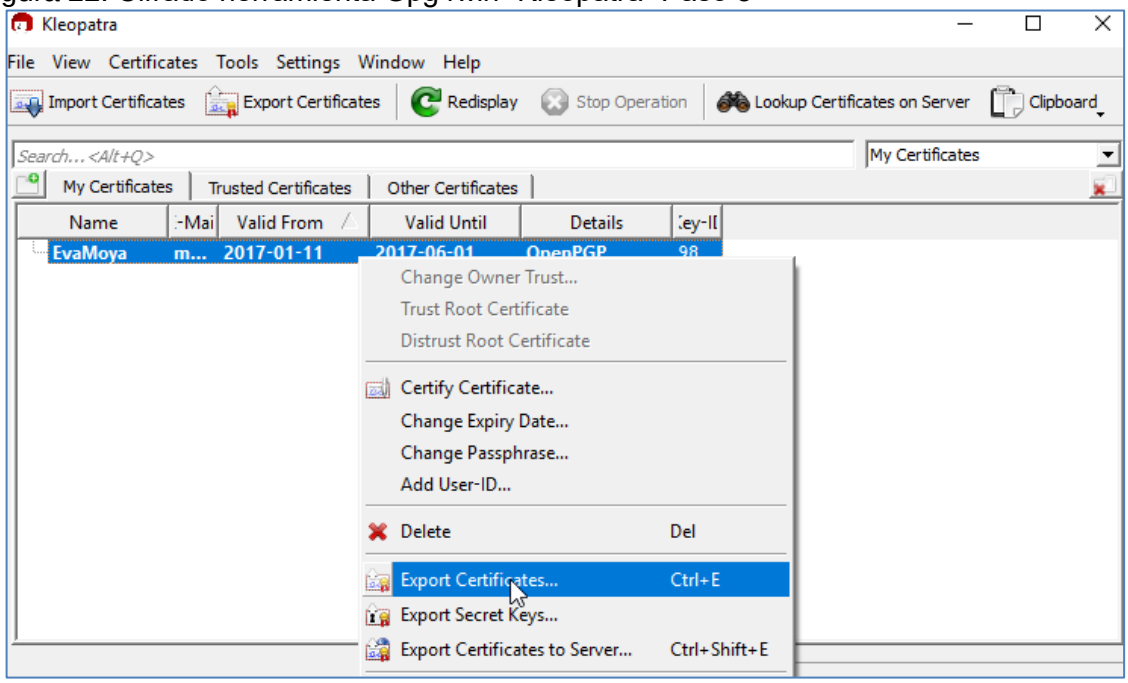
Figura 21. Cifrado herramienta Gpg4win “Kleopatra” Paso 7



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Para compartir la clave con el destinatario como se aprecia en la figura 22, se debe hacer clic derecho en la llave creada y seleccionar la opción "Export Certificates", el archivo creado estará en formato “.asc” este será enviado al destinatario, porque este corresponde a la clave pública.

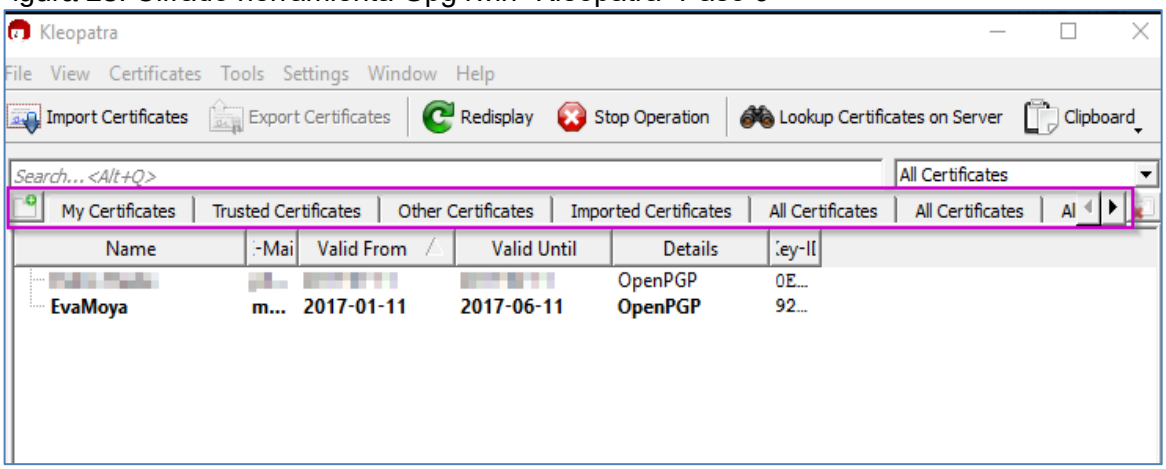
Figura 22. Cifrado herramienta Gpg4win “Kleopatra” Paso 8



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Para importar una clave pública como se detalla en la figura 23, en la ventana principal, se hace clic derecho y selecciona "Import Certificates" se busca el archivo “.asc” en la carpeta que previamente se guardó.

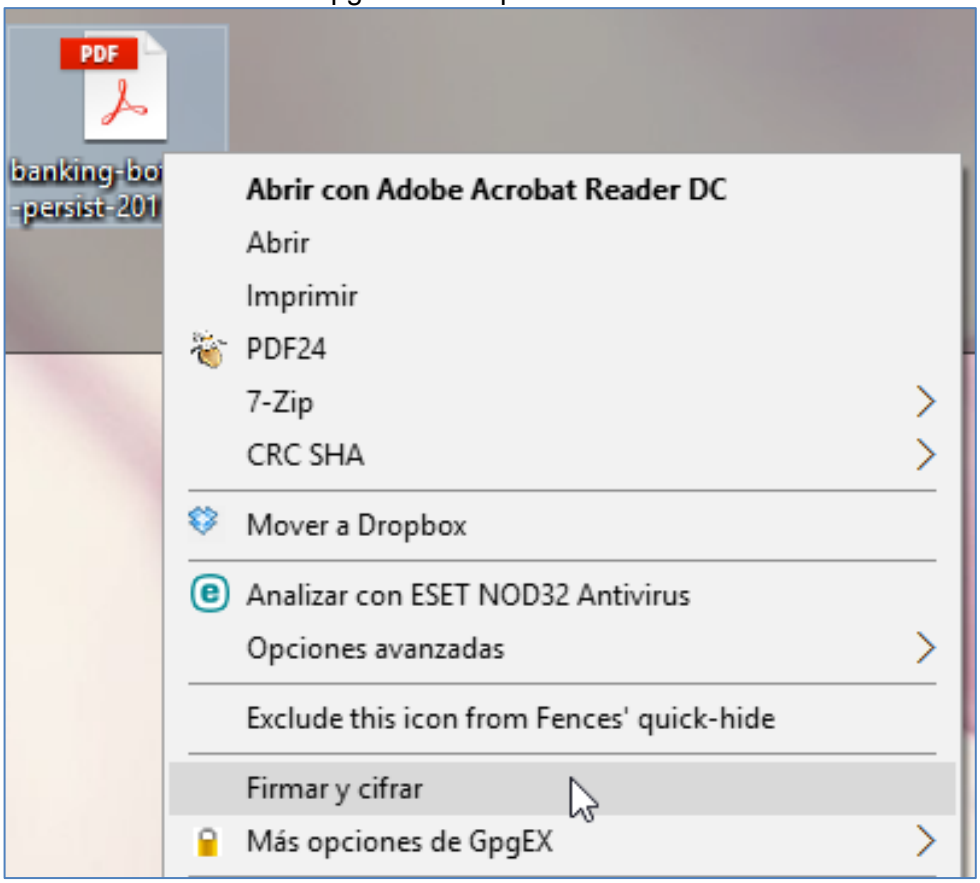
Figura 23. Cifrado herramienta Gpg4win “Kleopatra” Paso 9



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Ahora para enviar el archivo cifrado de un destino a otro en la figura 24, se procede a seleccionar el archivo desde el computador, sobre el archivo se realiza clic derecho y se escoge "Firmar y cifrar".

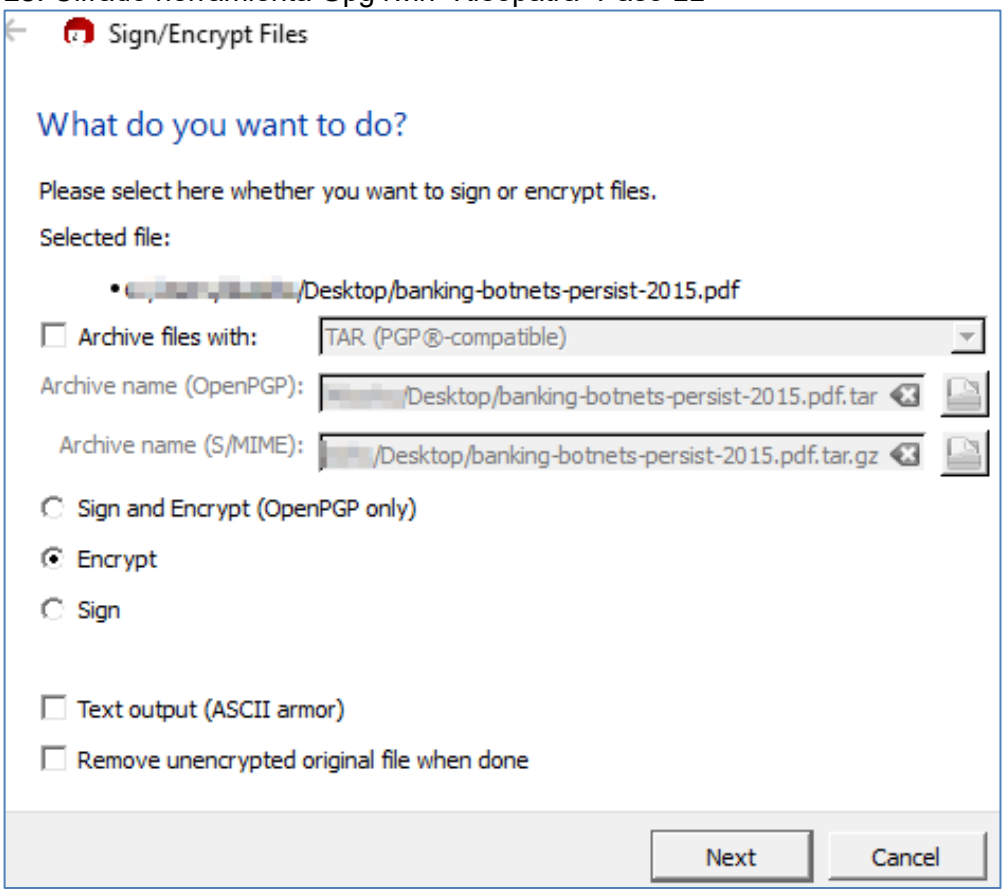
Figura 24. Cifrado herramienta Gpg4win “Kleopatra” Paso 10



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

En la siguiente ventana de la figura 25 selecciona “Next” manteniendo la configuración que esta por defecto como se puede apreciar cuenta con opciones modificables de acuerdo a las preferencias de cada usuario.

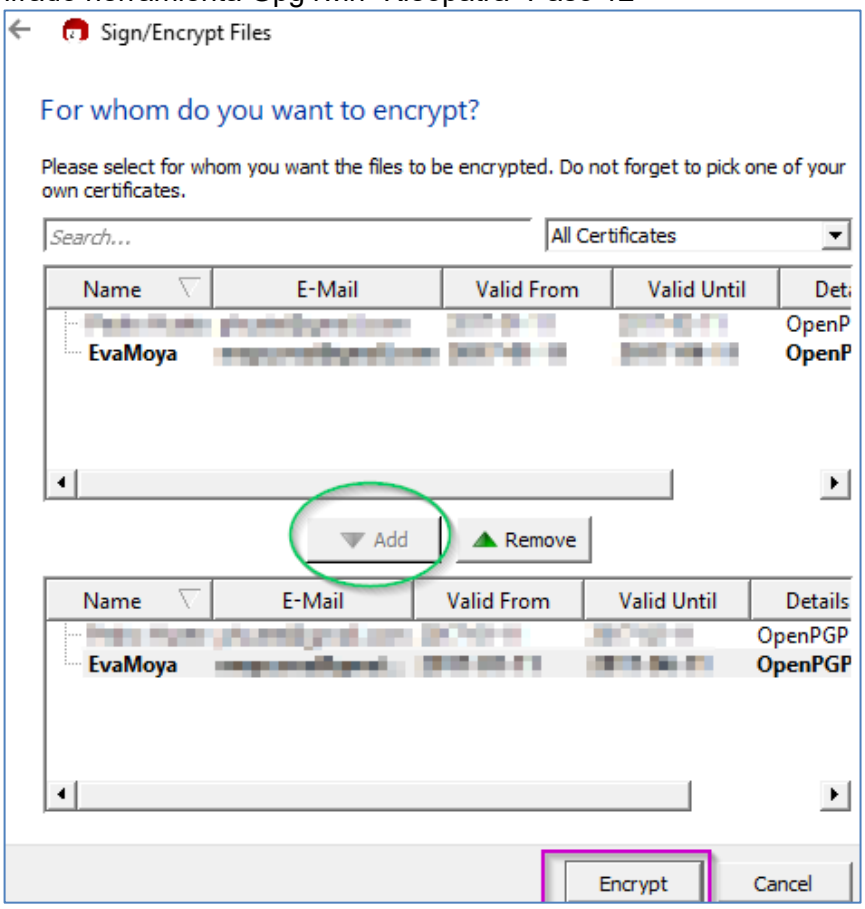
Figura 25. Cifrado herramienta Gpg4win “Kleopatra” Paso 11



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

En la siguiente ventana de la figura 26 se añade el destino o destinatarios que al cual va dirigido el archivo y luego se debe seleccionar en el botón “Encrypt”.

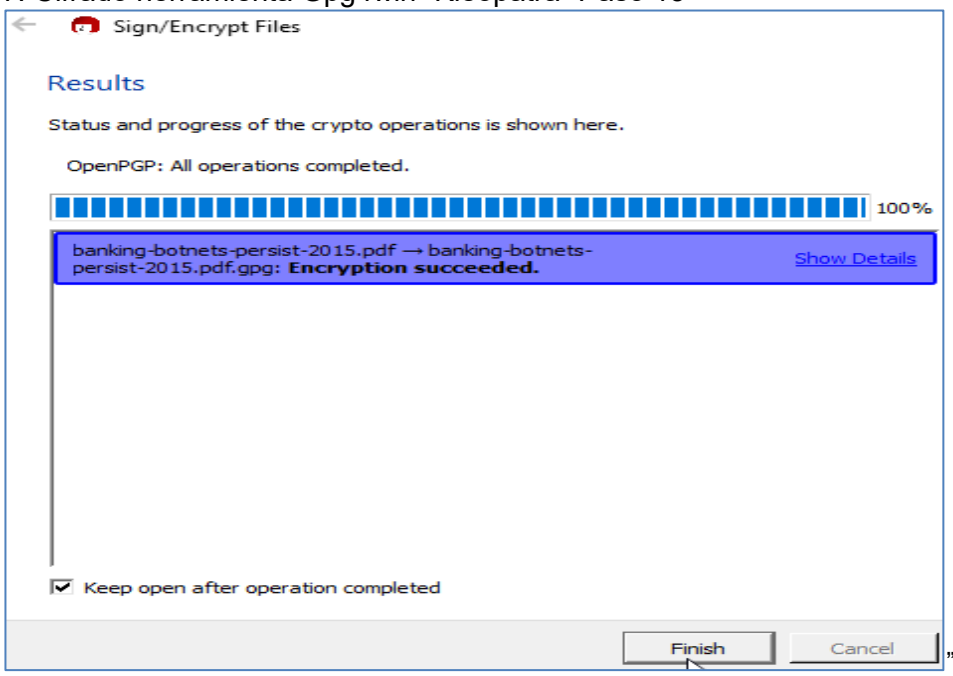
Figura 26. Cifrado herramienta Gpg4win “Kleopatra” Paso 12



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

En la figura 27 el siguiente paso se podrá observa el porcentaje del proceso y estado en el que se encuentra el cifrado.

Figura 27. Cifrado herramienta Gpg4win “Kleopatra” Paso 13



”.

Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

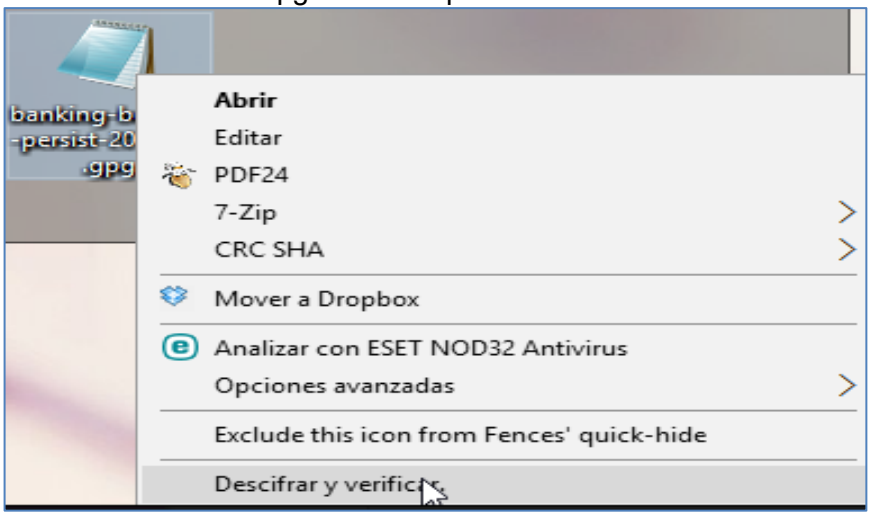
A continuación en la figura 28 se logra observa el archivo cifrado al abrirlo este aparece sin formato para quienes tienen acceso a él.

Figura 28. Cifrado herramienta Gpg4win “Kleopatra” Paso 14

Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Para realizar el descifrado como se muestra en la figura 29, se debe realizar el procedimiento contrario, clic derecho en el archivo y selecciona "Descifrar y Verificar".

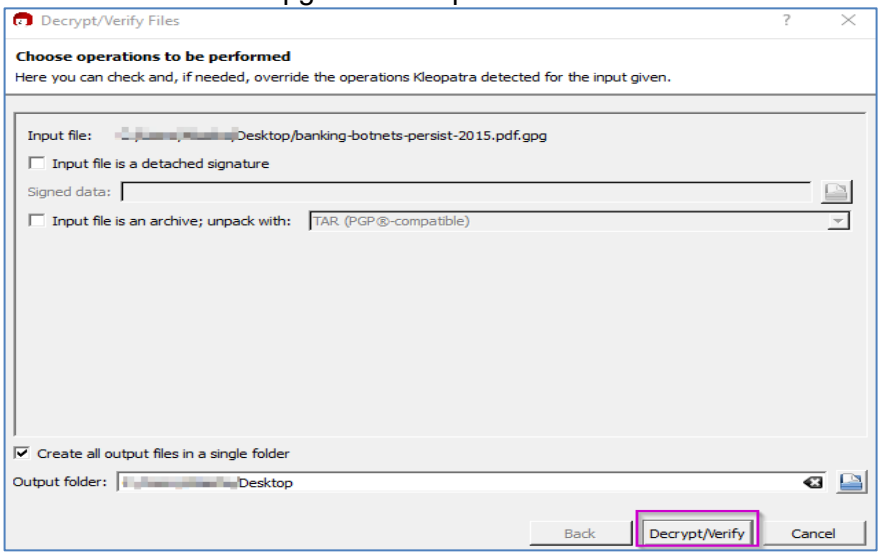
Figura 29. Cifrado herramienta Gpg4win “Kleopatra” Paso 15



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

En la siguiente ventana figura 30 únicamente click en el botón "Decrypt/Verify”.

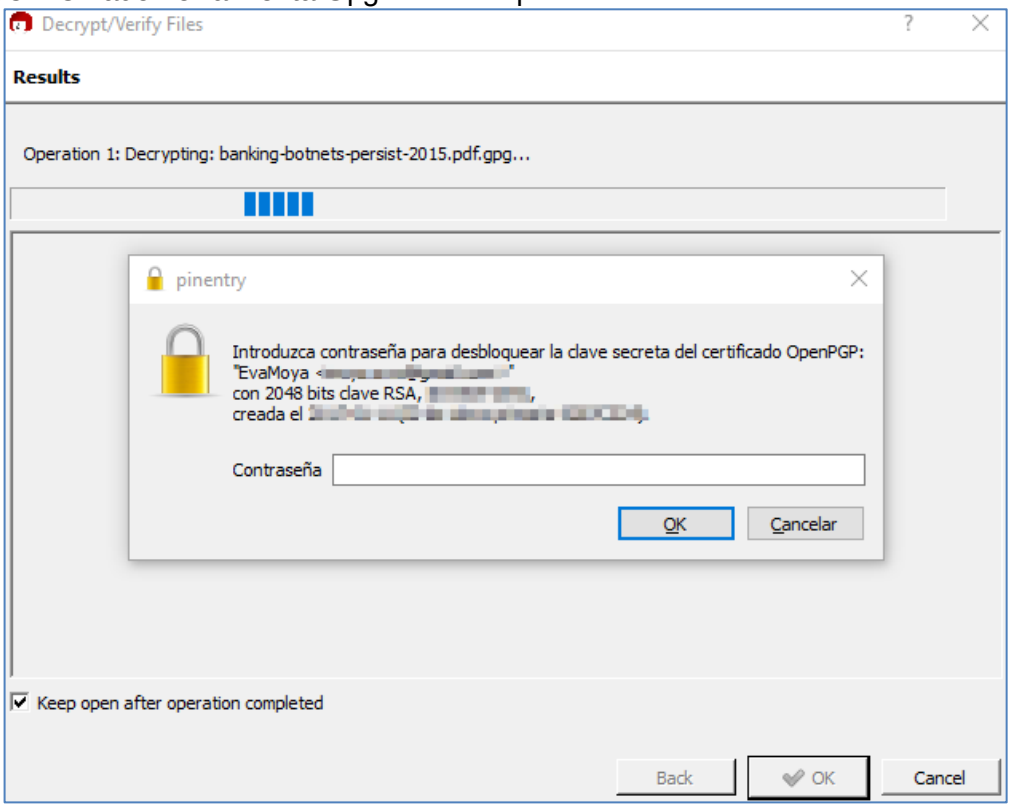
Figura 30. Cifrado herramienta Gpg4win “Kleopatra” Paso 16



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

Ahora en la siguiente ventana de la figura 31, solicitara la contraseña, esta es la que se creó al principio del procedimiento, por lo cual se ingresa en el respectivo campo y se presiona en “OK”.

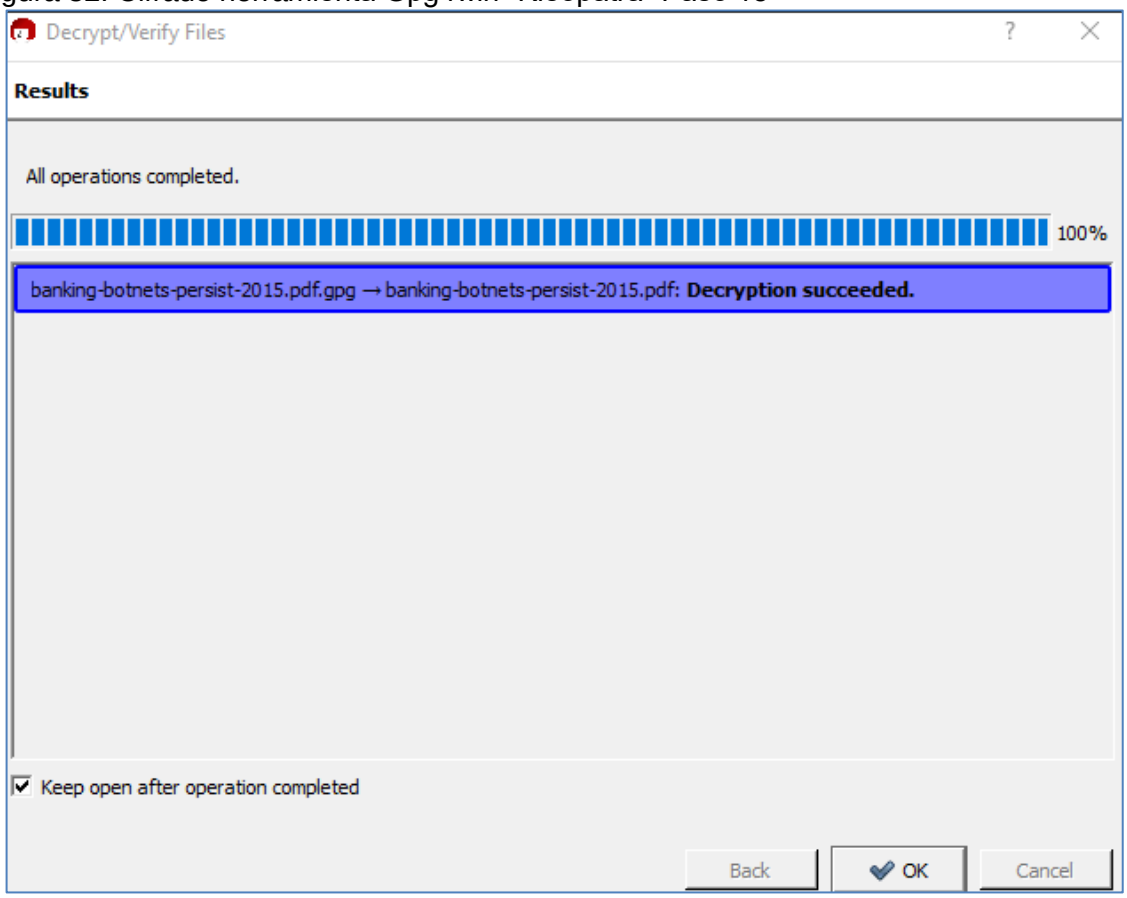
Figura 31. Cifrado herramienta Gpg4win “Kleopatra” Paso 17



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

De esta forma se ha descifrado exitosamente el archivo demostrado en los comentarios de la figura 32, se debe validar en la ruta que se guardó el archivo y hacer las validaciones correspondientes del mismo, de esta forma se cumple la confidencialidad, integridad y disponibilidad de la información transmitida de un lugar a otro.

Figura 32. Cifrado herramienta Gpg4win “Kleopatra” Paso 18



Fuente http://inteligenciacomunicaciononline.blogspot.com/2017/01/cifrar-y-descrifrar-archivos-con.html

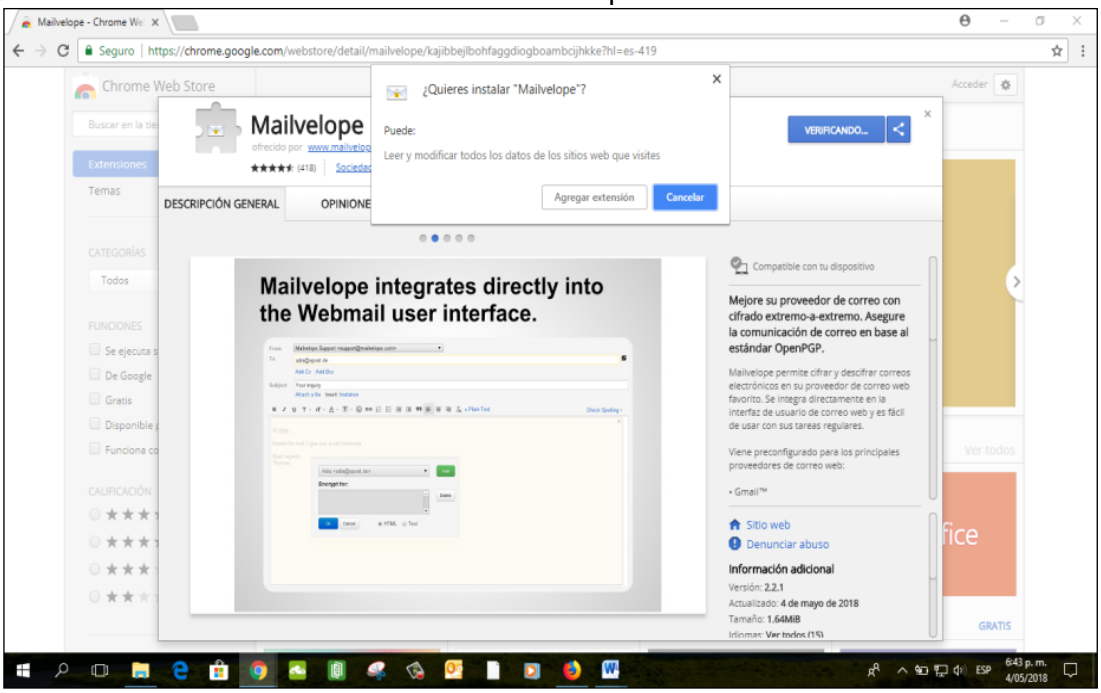
7.3 MAILVELOPE

Esta herramienta PKI funciona mediante la instalación de un complemento disponible en la mayoría de los navegadores web de internet, brinda cifrado para usarlo desde el correo electrónico mediante PGP, una de las ventajas de Mailvelope es que no necesita cambiar el entorno con el cual está familiarizado el usuario, ni requiere experiencia en el tema con las comunicaciones cifradas.[40]

[40] Mailvelope, comunicacion cifrada. [en línea] Disponible en internet: https://www.mailvelope.com/es/faq#about

Como se muestra en la figura 33 se utilizó el navegador web Google Chrome y Mozilla Firefox, inicialmente se realiza la instalación en Google Chrome, el complemento se encuentra disponible en “Extensiones” desde las opciones de configuración del navegador.

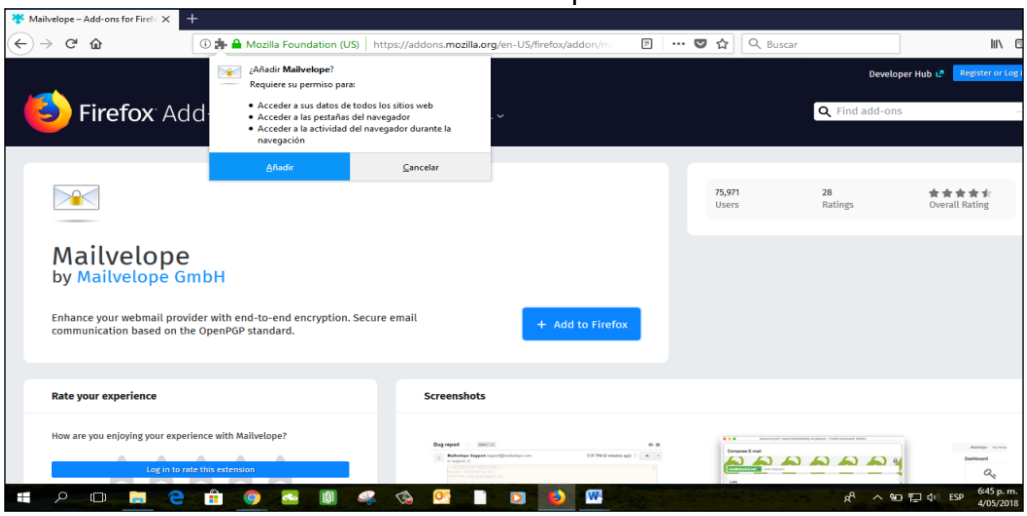
Figura 33. Cifrado de correo herramienta Mailvelope Paso 1



Fuente: El Autor

Ahora se realiza la instalación en Mozilla firefox figura 34 del complemento de encriptación Mailvelope.

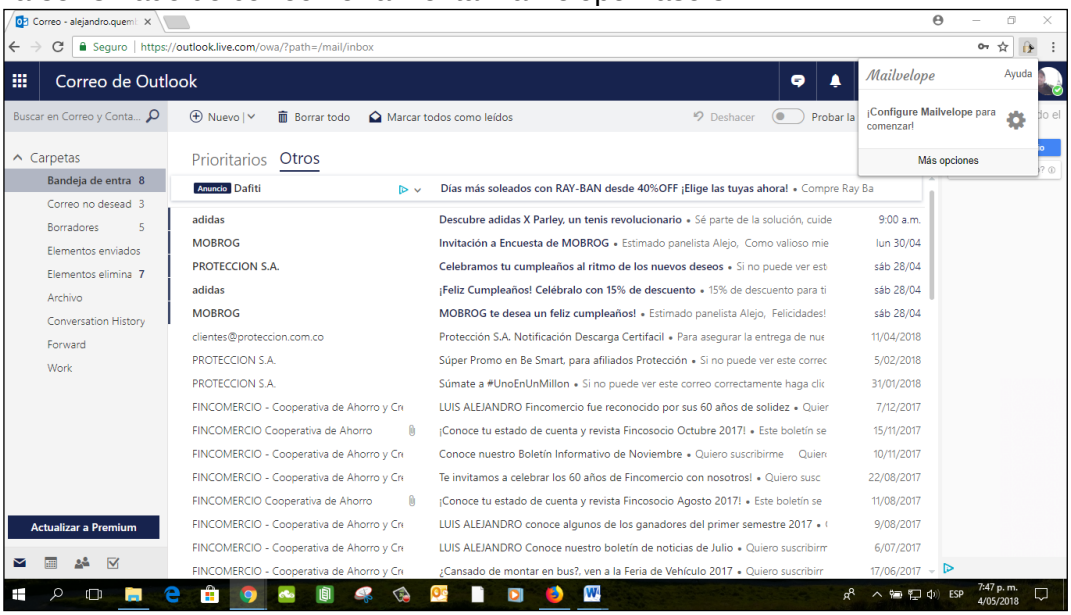
Figura 34. Cifrado de correo herramienta Mailvelope Paso 2



Fuente: El Autor

Para demostrar el funcionamiento de la aplicación de cifrado de correo Mailvelope, en la figura 35, se utilizaron las cuentas de correo electrónico personales creadas en Hotmail y Gmail, se inicia la configuración en la cuenta correo de Hotmail.

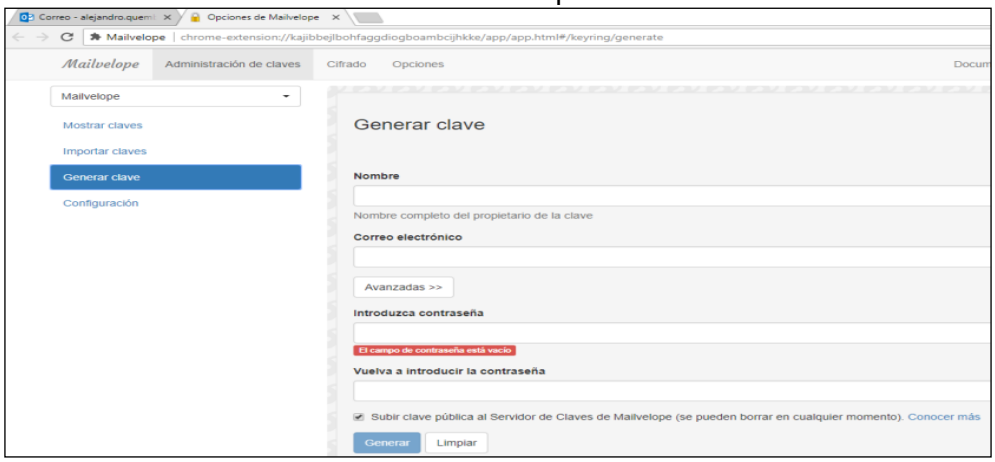
Figura 35. Cifrado de correo herramienta Mailvelope Paso 3



Fuente: El Autor

Desde las opciones de la herramienta PKI Mailvelope figura 36, se selecciona “Generar clave”.

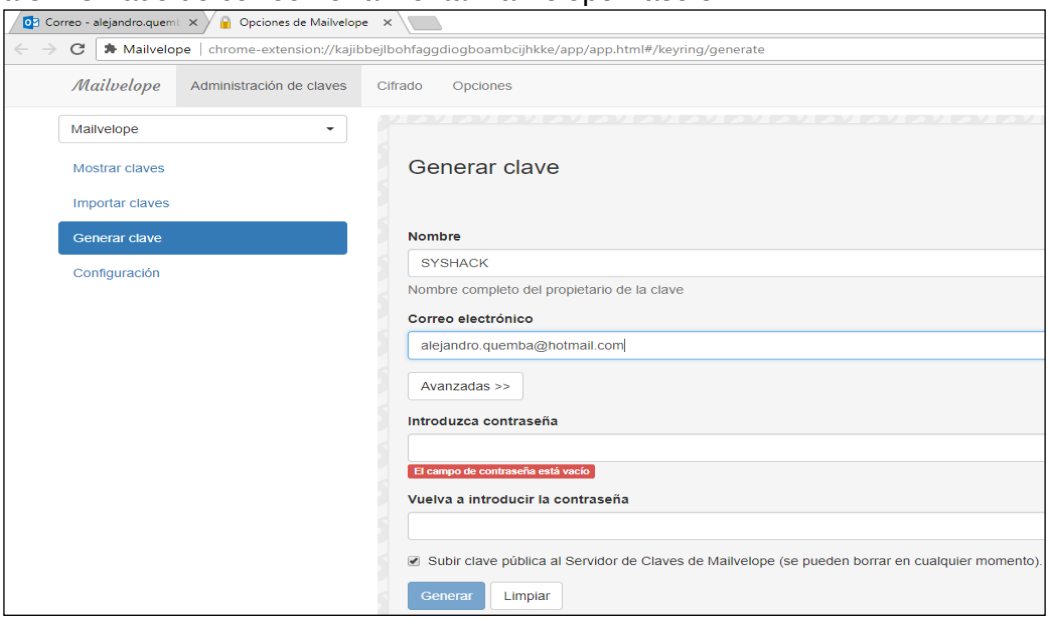
Figura 36. Cifrado de correo herramienta Mailvelope Paso 4



Fuente: El Autor

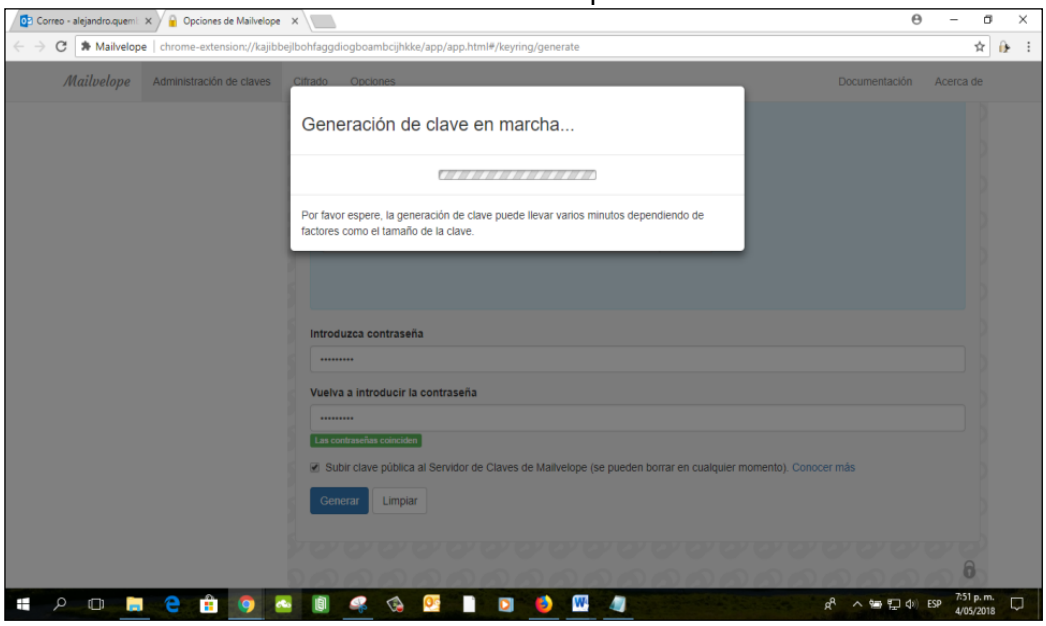
Ahora se ingresan los datos, como es el nombre, para este caso se coloca el correo electrónico como se observa en las figuras 37 y 38 con el cual se está trabajando Hotmail y se crea la contraseña.

Figura 37. Cifrado de correo herramienta Mailvelope Paso 5



Fuente: El Autor

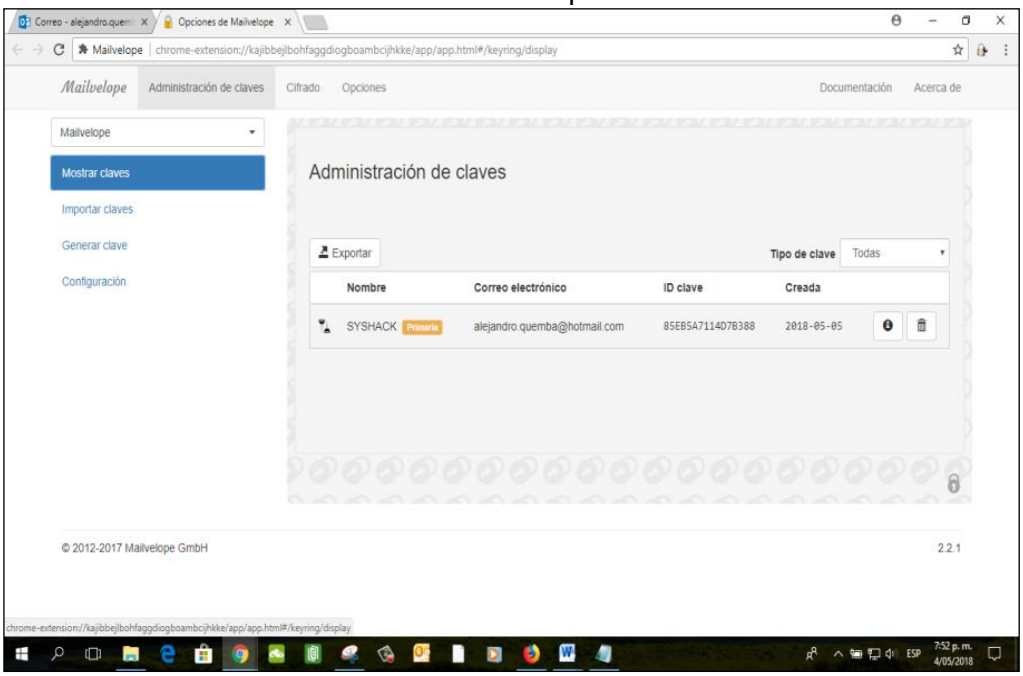
.Figura 38. Cifrado de correo herramienta Mailvelope Paso 6



Fuente: El Autor

Ahora desde “Mostrar claves” figura 39 se exportan los archivos generados.

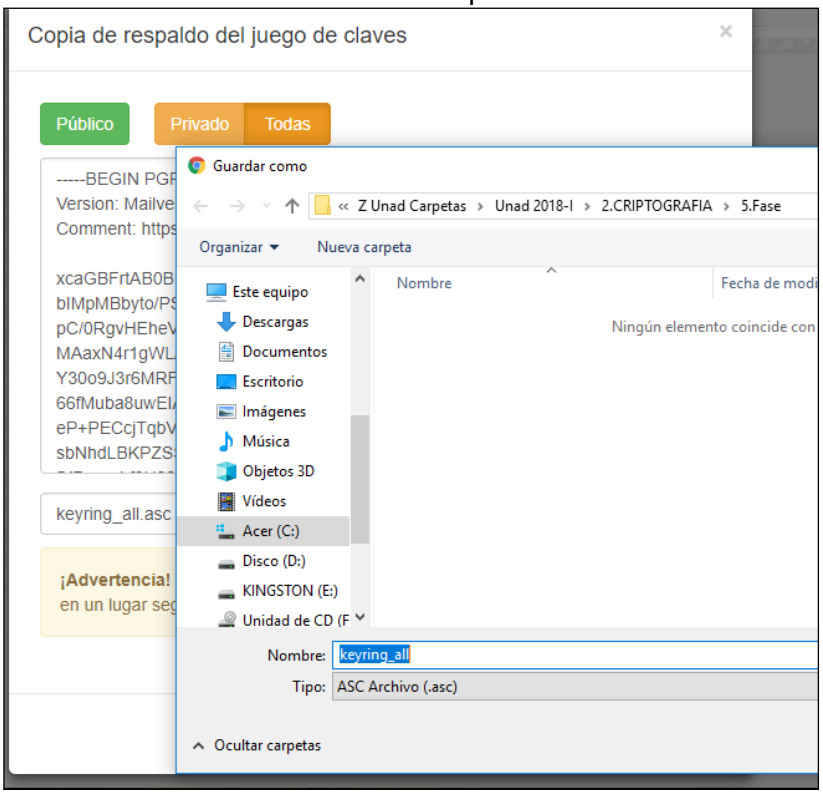
Figura 39. Cifrado de correo herramienta Mailvelope Paso 7



Fuente: El Autor

Se descargan localmente en el equipo de cómputo, la figura 40 muestra este proceso en el archivo de las claves públicas y privadas.

Figura 40. Cifrado de correo herramienta Mailvelope Paso 8



Fuente: El Autor

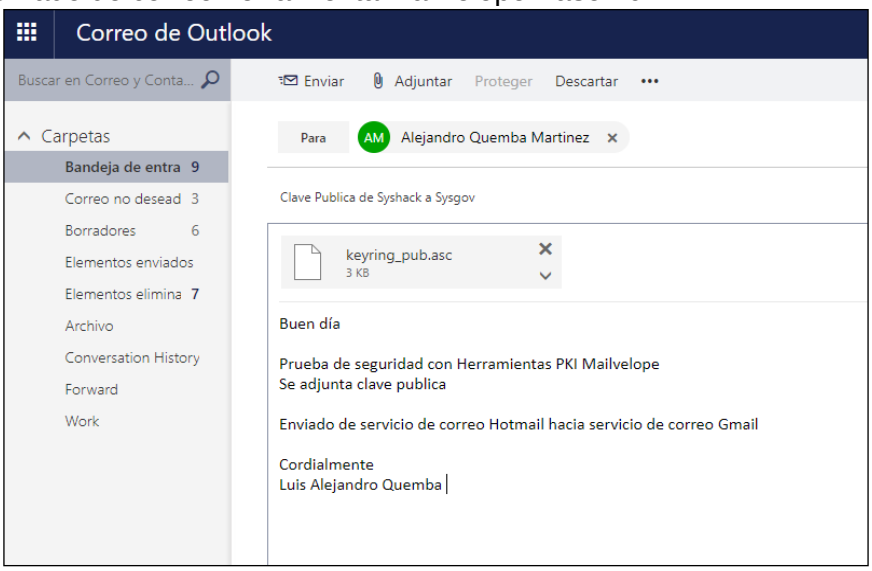
Ahora se descarga la clave publica, figura 41 se guarda localmente.

Figura 41. Cifrado de correo herramienta Mailvelope Paso 9

Fuente: El Autor

Ahora se procede a realizar el envió de la clave publica figura 42 desde el correo electrónico de Hotmail hacia al correo electrónico de Gmail adjuntando el archivo con la clave pública.

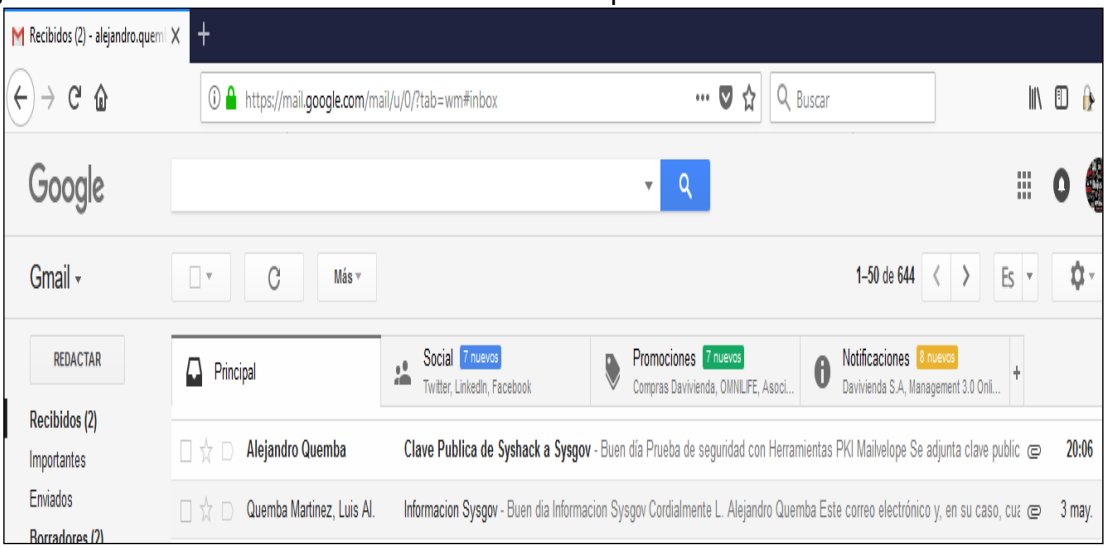
Figura 42. Cifrado de correo herramienta Mailvelope Paso 10



Fuente: El Autor

En la figura 43 se verifica en el correo de Gmail el correo enviado desde la cuenta de Hotmail.

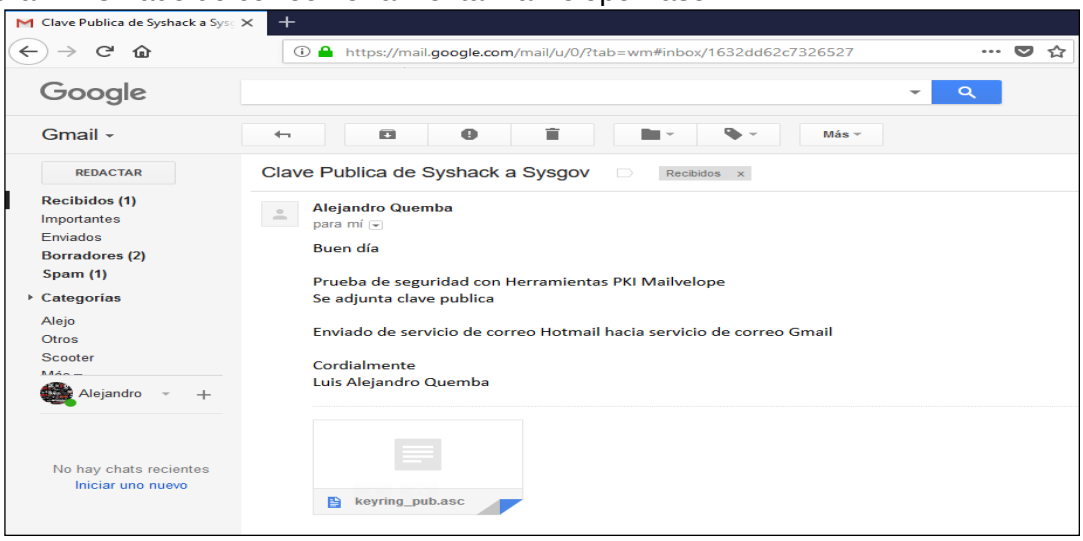
Figura 43. Cifrado de correo herramienta Mailvelope Paso 11



Fuente: El Autor

Efectivamente se recibe el correo y se descarga el adjunto figura 44, se guara localmente en la estación de trabajo.

Figura 44. Cifrado de correo herramienta Mailvelope Paso 12



Fuente: El Autor

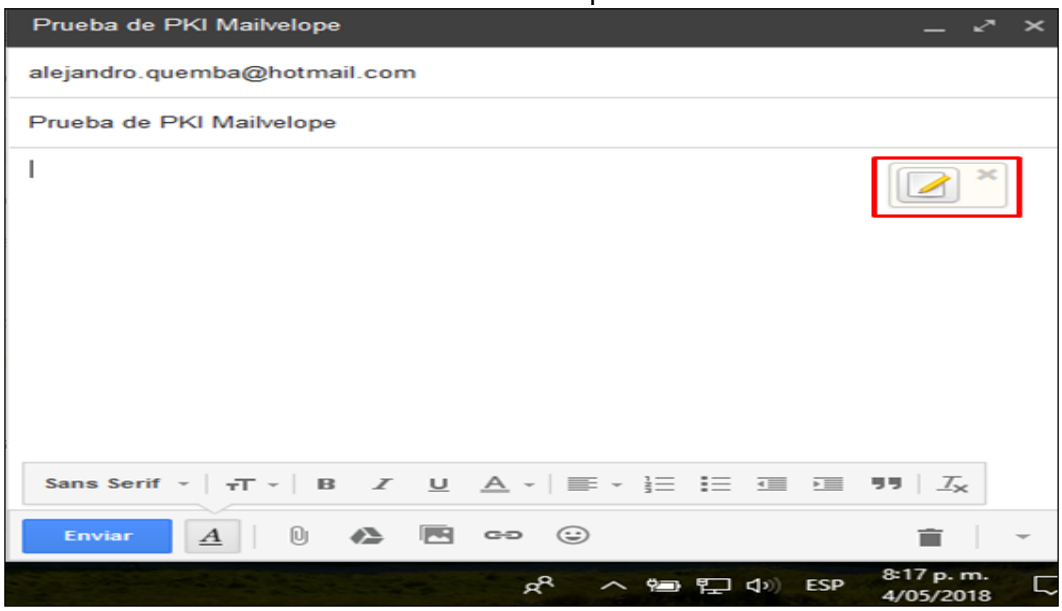
Ahora desde el complemento Mailvelope en el navegador de Mozilla Firefox figura 45 se despliegan las opciones y desde “Mostrar claves” se ha importado la clave publica generada desde la cuenta de correo de Gmail.

Figura 45. Cifrado de correo herramienta Mailvelope Paso 13

Fuente: El Autor

Luego desde la cuenta de correo de Gmail, se redacta un correo para la prueba de encriptado figura 46, como se observa en la siguiente imagen en el recuadro rojo, se hace clic allí para redactar el mensaje.

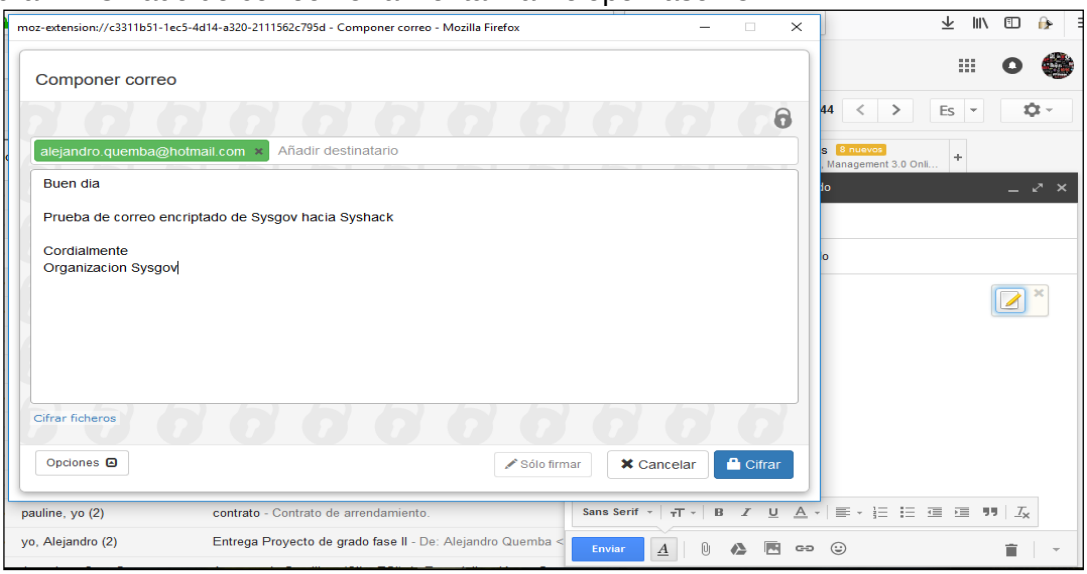
Figura 46. Cifrado de correo herramienta Mailvelope Paso 14



Fuente: El Autor

Como se muestra en la figura 47, se despliega el recuadro en color rojo de la imagen anterior y allí se procede a ingresar el texto, se selecciona “Cifrar” que se enviara desde la cuenta de correo de Gmail hacia la cuenta de correo de Hotmail.

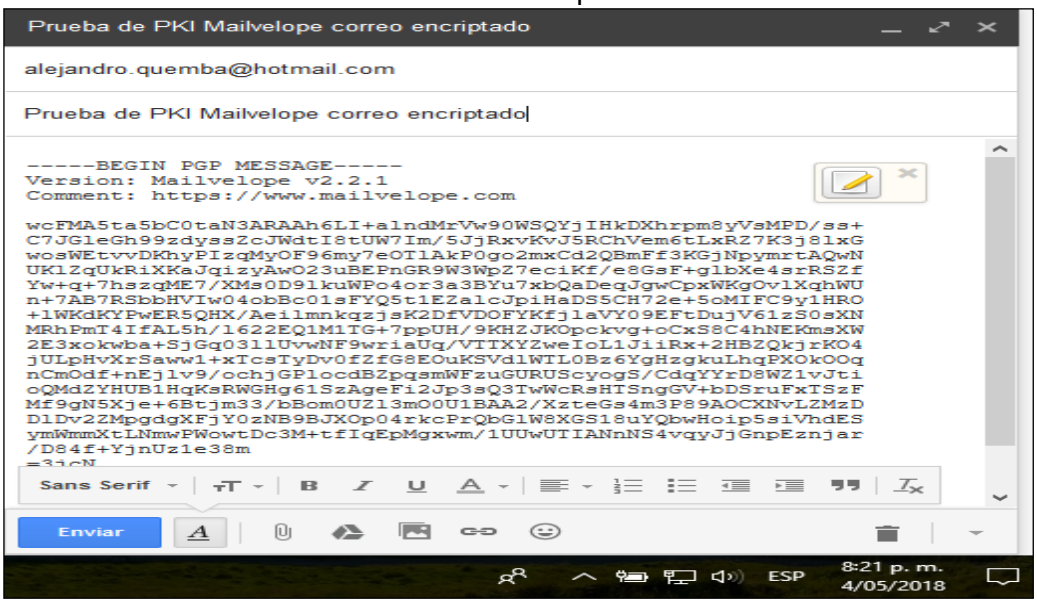
Figura 47. Cifrado de correo herramienta Mailvelope Paso 15



Fuente: El Autor

Se evidencia la información cifrada en el correo figura 48, el cual se procede a enviar al destinatario.

Figura 48. Cifrado de correo herramienta Mailvelope Paso 16



Fuente: El Autor

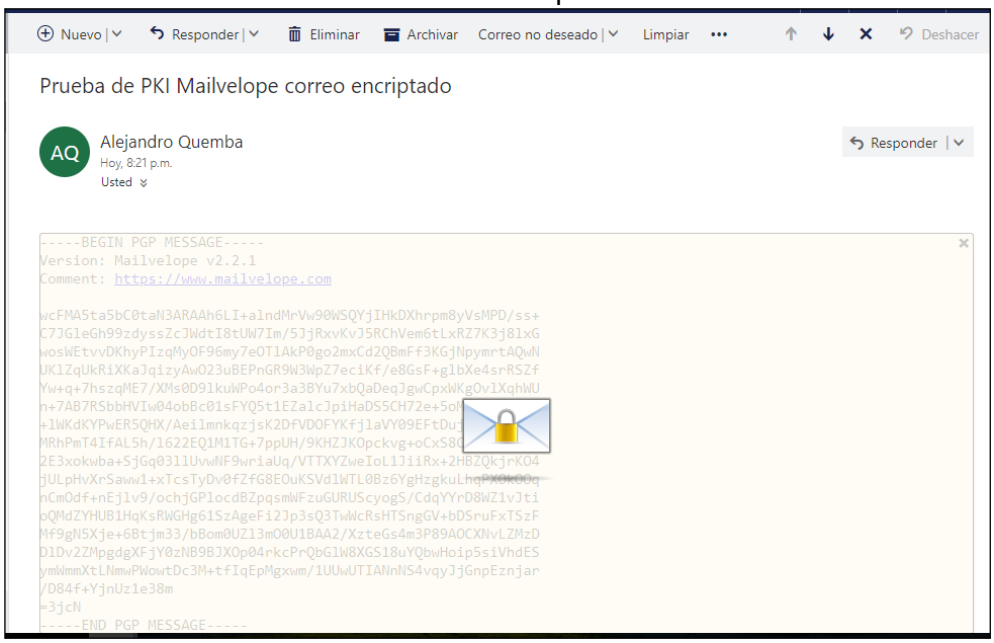
Se confirma la recepción del correo en la cuenta de correo como se evidencia en la figura 49, en la bandeja de entrada se encuentra el correo recibido.

Figura 49. Cifrado de correo herramienta Mailvelope Paso 17

Fuente: El Autor

Al abrir el correo electrónico como se observa en la figura 50, este aparece encriptado con un icono de candado en la parte central del correo, proveniente desde el correo electrónico de Gmail.

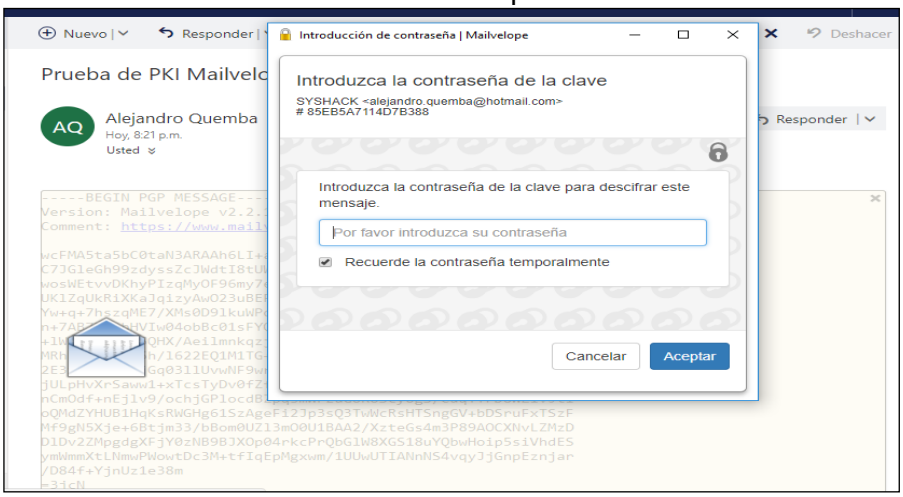
Figura 50. Cifrado de correo herramienta Mailvelope Paso 18



Fuente: El Autor

En el siguiente paso se hace clic en el candado como se refleja en la figura 51, este solicita el ingreso de la clave que se asignó inicialmente en la configuración de la creación de las claves, por lo cual se procede a ingresar la contraseña.

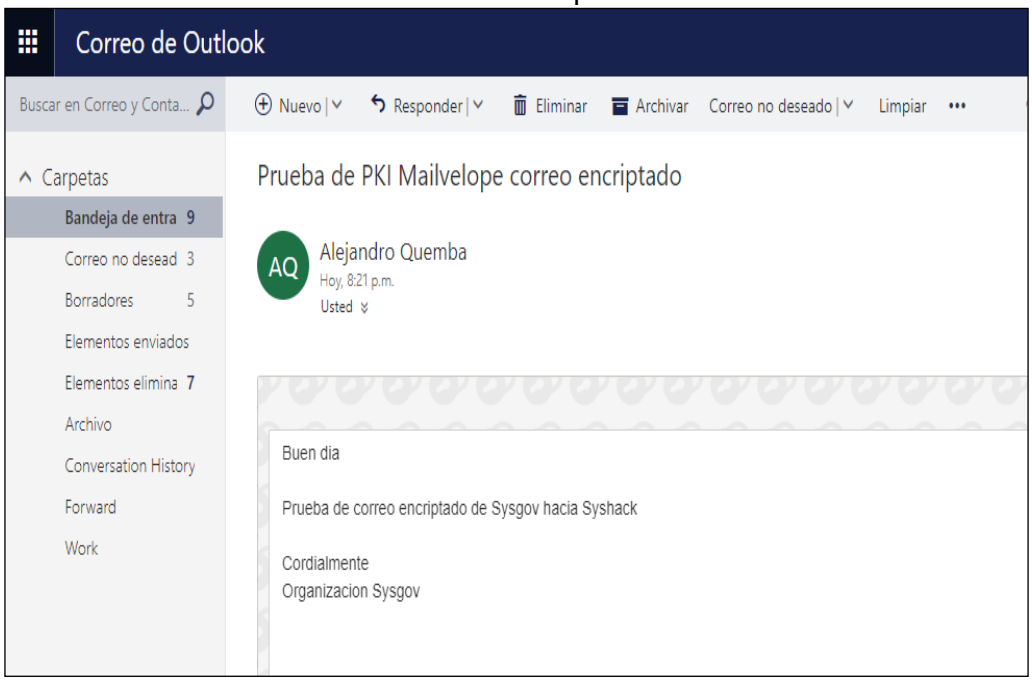
Figura 51. Cifrado de correo herramienta Mailvelope Paso 19



Fuente: El Autor

Satisfactoriamente el correo ha sido desencriptado observada en la figura 52, se demuestra el correcto cifrado y descifrado de la herramienta de cifrado de correo electrónico Mailvelope.

Figura 52. Cifrado de correo herramienta Mailvelope Paso 20



Fuente: El Autor

8. MEDIDA DE CONTROL CRIPTOGRAFICO ISO 27001 PARA PYMES EN COLOMBIA

La Norma Internacional ISO 27001 informa sobre los sistemas y componentes relacionados con la gestión de la seguridad de la información, el anexo A de la Norma ISO 27001 objetivos de controles contiene organizadamente un listado de controles de seguridad que pueden ser instaurados en las organizaciones, en el numeral 10 de este listado se encuentra los controles criptográficos de los cuales se desprende la política sobre el uso de controles criptográficos y la gestión de claves. Además, el control 18 aborda la reglamentación de controles criptográficos.

Los controles criptográficos buscan la protección de la información mediante la confidencialidad, autenticidad, integridad y el no repudio de los datos sensibles utilizados en las organizaciones, cuando estos presentan algún tipo de riesgo y otras medidas de control no suministren capacidad de resguardarlos, se deben utilizar sistemas y técnicas de criptografía que logren mantener protegida la información clasificada.

La política de uso de controles criptográficos debe estar desarrollada según la evaluación de riesgo de cada organización y de esta forma identificar el tipo de cifrado necesario para la información sensible que se encuentra almacenada en sus instalaciones o transportada fuera de ella, en él envió de correos electrónicos, credenciales de autenticación, firma electrónica, certificados web, accesos VPN, redes Wifi y protocolos de comunicación SSH para la administración de dispositivos y SFTPS en la transferencia de ficheros.

En cuanto a la gestión de claves se debe proteger de pérdidas y alteraciones de las mismas, tanto de claves secretas y privadas no tendrán que distribuirse a

personal no autorizado, mantener un correcto control en la creación, activación, modificación, almacenamiento, desactivación y eliminación de las claves asignadas a los usuarios de la organización, asegurando un tiempo y ciclo de vida para las claves criptográficas.

La reglamentación de los controles criptográficos indica el uso adecuado y eficaz de los controles criptográficos para dar cumplimiento a este factor en la seguridad de la información.

De acuerdo a portal web ISO 27002, afirma que las organizaciones deberían utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización. Sería necesario el desarrollo adicional de procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado. También establecer procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado y el uso de firmas digitales que proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso. [41]

Según lo anterior las Pymes en Colombia están en la capacidad de salvaguardar todos sus equipos con el uso fuerte de contraseñas e implementación de medidas

---

[41] ISO 27002.es. El portal de ISO 27002 en Español. Controles criptográficos. [en línea] [citado el 4 de diciembre, 2018].http://www.iso27000.es/iso27002_10.html

de encriptación sobre sus dispositivos habituales como son equipos de escritorio, portátiles, servidores, software, correo, etc. también es necesario hacerlo en equipos móviles, debido a que son objetivos de atacantes informáticos para vulnerar las organizaciones. El uso y almacenamiento de información confidencial, requiere ajustar medidas de seguridad, tanto en el plano físico como lógico, las Pymes en Colombia tienen actualmente opciones que se pueden adaptar a sus necesidades según a su infraestructura informática y presupuesto económico.

Conforme a lo informado por Pablo Teijeira, director general de sophos iberia, sobre la importancia del cifrado de datos para las empresas, “Ha de cifrar la información un gran número de empresas. Podríamos decir que deben hacerlo todos los sujetos que traten datos personales contenidos en ficheros a los que se deban aplicar medidas de seguridad de nivel alto. Sin embargo, el número es un poco más generoso, ya que debemos incluir también a otro tipo de sujetos que llevan a cabo actividades como el tratamiento de datos de carácter personal referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas; abogados en el ejercicio de su profesión; empresas que aceptan el BYOD; empresas que deseen adoptar medidas de seguridad que superen el mínimo exigido”.[42]

[42] TEIJEIRA,Pablo , Director general de SOPHOS iberia. Redseguridad
La importancia del cifrado de datos para las empresas. [2018]. [en linea]. Disponible en internet: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-del-cifrado-de-datos-para-las-empresas

9. RECOMENDACIONES

Con la exploración del cifrado de la información para las Pymes en Colombia, se puede evidenciar que son idóneas en la actualidad a posibles ataques informáticos, estas organizaciones deben reconocer la importancia de la información que crean, utilizan, almacenan y transfieren cotidianamente en sus operaciones, ello se hacen las siguientes recomendaciones:

- Clasificar la información que se debe cifrar como es información sensible, credenciales de autenticación, datos almacenados en equipos personales, medios extraíbles y USB.

- Uso de firma digital, utilizada para garantizar autenticidad y el no repudio de la información, facturación electrónica y gestiones públicas, en Colombia Certicámara provee este servicio y brinda soporte y actualización del mismo.

- El software libre es una opción que pueden probar e implementar las Pymes en Colombia, el cifrado de datos cuenta con variedad de software libre para su uso en caso de contar con presupuesto financiero, aunque carece de soporte técnico en caso de presentarse fallas.

- Cifrado en las comunicaciones externas con el uso de canales seguros, para transferencias financieras y comunicaciones en la nube.

- El teletrabajo cada vez toma más fuerza en las organizaciones, por lo cual la VPN es el medio utilizado para conectar externamente a los recursos internos de la empresa, mediante el cifrado seguro.

- Para la transferencia de archivos en forma segura se debe utilizar el protocolo FTPS y no el protocolo FTP que presenta vulnerabilidades y para el caso de administración segura de equipos el uso de SSH.

- El wifi en las empresas debe utilizar al menos el estándar WPA2 que utiliza el algoritmo de cifrado AES.

- La gestión de la seguridad de las Pymes en Colombia, requiere una inversión necesaria en el área de informática, actualmente los fabricantes ofrecen customización de software y hardware de acuerdo a las necesidades de cada organización, de esta forma los costos pueden disminuir considerablemente.

10 CONCLUSIONES

En el documento realizado y en las fuentes encontradas se evidenció que efectivamente a nivel de Latinoamérica las pymes son altamente susceptibles al robo de la información ya que carecen de conocimiento, personal especializado y/o infraestructura informática que le permita cifrar la información confidencial de la empresa o información que aparentemente no es importante para la compañía pero que puede ser usada por la competencia para afectar la estabilidad de la compañía.

En la actualidad se puede encontrar gran variedad de herramientas de seguridad para el cifrado de la información tanto licenciada como libre que pueden ser implementadas por las pequeñas empresas pymes de acuerdo a sus posibilidades económicas por lo que las empresas no pueden excusarse en la limitación de recursos para mantener salvaguardada la información.

Es importante que las empresas además de implementar herramientas de cifrado de la información, software de seguridad, equipos y demás para salvaguardar la información, se interese por crear una cultura en todos los miembros de la organización, no solo del uso del uso de herramientas de seguridad sino de buenas prácticas en el manejo de contraseñas, bloqueo del equipo, no divulgación de la información confidencial, uso de medios de transmisión de la información y medios de almacenamiento autorizados, entre otros.

El constante desarrollo tanto de nuevas formas de intrusión y robo de información hace que la industria de igual manera se encuentre en constaste búsqueda de nuevas técnicas de cifrado de la información por lo que las pymes deben contar con personal especializado que permanezca actualizándose e implementando

mejores o nuevas formas o herramientas para evitar el robo de la información no solo de la compañía, sino de clientes y proveedores.

11. BIBLIOGRAFÍA

BKF. (2017). Las pymes son las más vulnerables a ataques cibernéticos. [Internet]. Recuperado de http://bkf.com.co/pymes-vulnerables-a-ataques-ciberneticos/

CORPORACIÓN COLOMBIA DIGITAL. Violaciones de seguridad cuestan a las empresas hasta US$500,000 por ataque [2015]. [en línea] [citado el 1 de noviembre, 2018]. Disponible en internet:https://colombiadigital.net/actualidad/noticias/item/8559-violaciones-de-seguridad-cuestan-a-las-empresas-hasta-us-500-000-por-ataque.html

Equipo técnico de OEA. Oportunidades y desafios para las Pymes en el contexto de una mayor adopcion de las TIC. [2018]. [en linea]. Disponible en internet:

http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

ESET. (2014). Cifrado de la información [archivo PDF]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014v2.pdf

FERNANDEZ, Jacobo; CASANOVA, Maria. PGP. {En línea}. {2007} disponible en http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/02%20-%20PGP.pdf

MINTIC, guía para la Implementación de Seguridad de la Información en una MIPYME.Seguridad y Privacidad de la Información. [en línea] Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Mailvelope, comunicación cifrada. [en línea] Disponible en internet: https://www.mailvelope.com/es/faq#about

PABÓN CADAVID, Jhonny. La criptografía y la protección a la información digital. {En línea}. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636

REDACCION PASSWORD. (2018). ACIS. Colombia. Aumenta en 30% la inversión de las Pymes en ciberseguridad [Internet]. Recuperado de http://acis.org.co/portal/content/NoticiaDelSector/aumenta-en-30-la-inversi%C3%B3n-de-as-pymes-en-ciberseguridad

REDACCIÓN TECNOLOGÍA. (2017). EL ESPECTADOR. COLOMBIA. [Internet]. Disponible en: https://www.elespectador.com/tecnologia/colombia-es-el-tercer-pais-mas-afectado-por-ataques-ciberneticos-en-la-region-articulo-714284

RIASCO, Sandra. AGUILERA, Adriana. AVILA, Patricia. Seguridad de los sistemas de información en las Pymes de

Santiago de Cali. Colombia. [2016]. [en linea]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/6586847.pdf

SEGURIDAD, Digitalguide. (2017) El encriptado informático: así se protege la comunicación. [Internet]. España. Disponible en: https://www.1and1.es/digitalguide/servidores/seguridad/todo-sobre-los-metodos-de-encriptado/

STALLINGS, Williams. Fundamentos de seguridad en redes: aplicaciones y estándares. {En línea}. {Consultado septiembre 2018} Disponible en: https://www.academia.edu/22539038/Fundamentos_de_seguridad_en_redes_Aplicaciones_y_est%C3%A1ndares_2da_Edici%C3%B3n

TALENS-OLIAG, Sergio. Introducción a la Criptología. {En línea}. Disponible en: https://www.uv.es/sto/articulos/BEI-2003-04/criptologia.html#id2440584

TEIJEIRA,Pablo , DIRECTOR GENERAL DE SOPHOS IBERIA. Redseguridad

La importancia del cifrado de datos para las empresas. [2018]. [en linea]. Disponible en internet: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-del-cifrado-de-datos-para-las-empresas