UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CARRERA: MAESTRÍA EN COMPUTACIÓN

MENCIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO DE INTEGRACIÓN CURRICULAR,
MODALIDAD PROYECTO DE
INVESTIGACIÓN

TEMA:

"IMPLEMENTACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA PGP PARA LA PROTECCIÓN DE DATOS EN COMUNICACIONES SMTP Y SFTP DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIOTAVALO LTDA."

Trabajo de titulación previo a la obtención del título de Magister en Computación con mención en Seguridad Informática

Línea de investigación: Criptografía

AUTOR:

Solano Santacruz Jaime Alexander

DIRECTOR:

Ortiz Garcés Iván Patricio

Ibarra – Ecuador

2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	100280776-4		
APELLIDOS Y NOMBRES	Solano Santacruz Jaime Alexander		
DIRECCIÓN	Calles Leopoldo Chávez - Cdla. 31 de Octubre - Otavalo		
EMAIL	jasolanos@utn.edu.ec		
TELÉFONO FIJO		**TELÉFONO MÓVIL:**	0982258116

DATOS DE LA OBRA	
TÍTULO:	Implementación de criptografía asimétrica PGP para la protección de datos en comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.
AUTOR (ES):	Solano Santacruz Jaime Alexander
FECHA: DD/MM/AAAA	20-11-2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	PREGRADO [ ] POSGRADO [X]

TITULO POR EL QUE OPTA	Magister en computación con mención en Seguridad Informática
TUTOR	MSc. Iván Patricio Ortiz Garcés

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 20 días de noviembre de 2025

EL AUTOR:

Ing. Jaime Alexander Solano Santacruz
C.C: 1002807764

Ibarra, 22 de septiembre de 2025

Dr. Jorge Gordón
Decano (e)
Facultad de Posgrado

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado **Implementación de criptografía asimétrica PGP para la protección de datos en comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda**. del maestrante **Jaime Alexander Solano Santacruz**, de la **Maestría en Computación Mención Seguridad Informática en Línea (CSI-L), cohorte V**, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	Ing. Iván Patricio Ortiz Garcés, Msc.	Firmado electrónicamente por: IVAN PATRICIO ORTIZ GARCES Validar únicamente con FirmaEC
Asesor/a	Ing. Henry Patricio Farinango Endara, Msc.	Firmado electrónicamente por: HENRY PATRICIO FARINANGO ENDARA Validar únicamente con FirmaEC

DEDICATORIA

Quiero dedicar este trabajo de tesis a mi esposa y a mis hijas, quienes han sido los pilares fundamentales de mi vida. Su amor, apoyo e inspiración me han impulsado a buscar siempre nuevos conocimientos y a enfrentar con determinación los retos profesionales y personales. Ellas son el motor que me anima a superarme y a ser un ejemplo de perseverancia.

A mi amada esposa, Lorena, quiero expresarle mi más sincero agradecimiento por su constante apoyo, paciencia y comprensión durante todo el proceso de elaboración de esta tesis. Su acompañamiento incondicional fue la fuerza que me mantuvo motivado y enfocado para alcanzar esta meta.

A mi hija Danae, le doy las gracias por su comprensión y por ser una fuente constante de motivación. Su presencia y palabras de aliento contribuyeron a que este proyecto se convirtiera en una realidad.

A mi hija Victoria, le agradezco profundamente su cariño y su aliento, que me dieron ánimo en los momentos más desafiantes. Su apoyo y confianza fueron un impulso invaluable para seguir adelante.

Jaime Alexander Solano Santacruz

AGRADECIMIENTO

Agradezco profundamente a Dios, por iluminar mi camino y guiarme siempre por el sendero del bien, brindándome fortaleza y sabiduría para superar cada desafío.

Mi más sincero agradecimiento a mi familia, cuyo apoyo incondicional ha sido la base fundamental para alcanzar cada uno de mis objetivos. Su amor y confianza me han motivado a seguir adelante en todo momento.

De manera especial, agradezco a mis profesores de la Universidad Técnica del Norte, y en particular a mi director y asesor de tesis, por su orientación, paciencia y dedicación. Su guía ha sido esencial para la realización de este trabajo y para mi crecimiento profesional.

A todos ustedes, mi más profundo reconocimiento y agradecimiento por formar parte de este logro.

Jaime Alexander Solano Santacruz

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

FACULTAD DE POSTGRADO

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

IMPLEMENTACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA PGP PARA LA PROTECCIÓN DE DATOS EN COMUNICACIONES SMTP Y SFTP DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIOTAVALO LTDA.

Autor: Ing. Jaime Alexander Solano Santacruz

Director: MSc. Iván Patricio Ortiz Garcés

Año: 2025

RESUMEN

Actualmente la información es el activo más valioso de cualquier organización y resulta fundamental mantener al personal actualizado en seguridad de datos para proteger la confidencialidad integridad y disponibilidad de la información facilitando así el cumplimiento de la misión institucional sin embargo los ciberataques especialmente vía correo electrónico mediante phishing suplantación de identidad y malware representan una amenaza creciente y sofisticada para las organizaciones esta investigación aborda la necesidad de proteger las comunicaciones SMTP y SFTP en la Cooperativa de Ahorro y Crédito Uniotavalo Ltda proponiendo la implementación de un mecanismo de cifrado asimétrico basado en PGP y el algoritmo RSA mediante la extensión GnuPG para fortalecer la seguridad en el intercambio de información confidencial el cifrado del correo electrónico es crucial pues muchas agresiones explotan la falta de protección en este medio la implementación siguió la metodología estructurada MAGERIT iniciando con un análisis para identificar información sensible y flujos de datos críticos PGP fue seleccionado por su cifrado robusto y eficiente gestión de claves garantizando confidencialidad integridad y autenticidad la planificación incluyó capacitación definición de políticas generación y distribución segura de claves y diseño de procesos para cifrado y descifrado posteriormente se realizó la implementación técnica integrando PGP con sistemas corporativos validando interoperabilidad y tiempos en la fase de pruebas ajustando según retroalimentación brindando soporte y formación continua los resultados cuantificables reflejan el cifrado del 90% de correos con datos confidenciales y del 95% de documentos críticos reduciendo en 75% incidentes por accesos no autorizados y cumpliendo al 100% los requisitos normativos con esta medida Uniotavalo fortalece significativamente la protección de sus canales de comunicación y la seguridad de su información crítica.

PALABRAS CLAVES: Cifrado Asimétrico, PGP, comunicaciones SMTP y SFTP, metodología MAGERIT.

ABSTRACT

Currently information is the most valuable asset of any organization making it essential to keep personnel updated on data security to protect confidentiality integrity and availability of information thus facilitating the fulfillment of the institutional mission however cyberattacks especially via email through phishing identity theft and malware pose an increasingly sophisticated threat to organizations this research addresses the need to protect SMTP and SFTP communications at Uniotavalo Savings and Credit Cooperative Ltd proposing the implementation of an asymmetric encryption mechanism based on PGP and the RSA algorithm through the GnuPG extension to strengthen security in the exchange of confidential information email encryption is crucial because many attacks exploit the lack of protection in this medium the implementation followed the structured MAGERIT methodology starting with an analysis to identify sensitive information and critical data flows PGP was chosen for its robust encryption and efficient key management ensuring confidentiality integrity and authenticity planning included training policy definition secure key generation and distribution and design of encryption and decryption processes then technical implementation was carried out integrating PGP with corporate systems validating interoperability and timing during testing phase adjusting based on feedback providing ongoing support and training measurable results were encryption of 90% of emails with confidential data and 95% of critical documents reducing security incidents due to unauthorized access by 75% and achieving 100% compliance with regulatory requirements with this measure Uniotavalo significantly strengthens the protection of its communication channels and the security of its critical information.

KEYWORDS: Asymmetric Encryption, PGP, SMTP and SFTP communications, MAGERIT methodology.

CAPITULO I

1. EL PROBLEMA

1.1 PROBLEMA DE INVESTIGACIÓN

Actualmente ya no es sorprendente decir que vivimos rodeados de información o que es uno de los activos más importantes en el panorama empresarial. Ese volumen de datos se traduce en valor económico para las empresas, y, por tanto, en el camino que marca su éxito o su fracaso en el futuro.

En un mundo sumido en una transición hacia lo completamente digital, necesitamos implementar los mecanismos necesarios para proteger y gestionar la información, no solo desde el punto de vista tecnológico sino también legal (INCIBE, s.f.); “No decir más de lo que haga falta, a quien haga falta y cuando haga falta” (A. Maurois), una afirmación tan sencilla como fundamental, y es que en eso se basa el mecanismo principal de protección de la información contra la revelación de secretos.

El desarrollo tecnológico y la creciente adopción de plataformas digitales han revolucionado la ciberseguridad, pero también han incrementado y sofisticado las amenazas cibernéticas. La expansión de la transformación digital en las instituciones financieras eleva el riesgo de ataques y fraudes, demandando estrategias de defensa más avanzadas para enfrentar a los ciberdelincuentes.

En el dinámico sector financiero, la protección de los datos es una prioridad indiscutible. Las organizaciones invierten significativamente en infraestructura tecnológica para protegerse contra ataques cibernéticos. De hecho, según un informe del laboratorio de análisis e inteligencia de amenazas de Fortinet, los países de América Latina y El Caribe experimentaron aproximadamente 200 mil millones de intentos de ataques en 2023. Este número alarmante destaca a México, Brasil y Colombia como las naciones con mayor actividad maliciosa en la región, un estudio de ITahora indica que el Ecuador experimento un crecimiento del 4,9% en amenazas convirtiéndose en el tercer país más atacado de la región de América Latina, después de Perú y Colombia, según el estudio realizado por (Check Point, 2024).

En el ámbito nacional existen entidades que regulan al sector financiero, una de ellas es la Superintendencia de Economía Popular y Solidaria (SEPS), que a través de una resolución normativa emitida en mayo de 2022, referente a la NORMA DE CONTROL

RESPECTO A LA SEGURIDAD DE LA INFORMACION EN LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO BAJO CONTROL DE LA SUPERINTENDECIA DE ECONOMIA POPULAR Y SOLIDARIA, menciona que *"La presente norma tiene como objeto regular los niveles mínimos para la administración de seguridad de la información que las entidades, la CONAFIPS y las empresas, deben definir e implementar con el fin de resguardar y proteger sus activos de información, preservando su confidencialidad, disponibilidad e integridad"*.

La Cooperativa de Ahorro y Crédito Uniotavalo Ltda., es una entidad financiera del Sector Popular y Solidaria cuyo giro de negocio es la intermediación financiera y se encuentra regulada por la Superintendencia de Economía Popular y Solidaria (SEPS) y se encuentra dentro del segmento 3 dentro de la clasificación de las Cooperativa de Ahorro y Crédito del Sector Popular y Solidario, para una mejor comprensión de la problemática se indica que la información confidencial o critica de cualquier entidad financiera, como datos personales, información de las cuentas bancarias entre otros, que es compartida entre funcionarios, socios y proveedores, debe ser asegurada tanto al tenerla almacenada como al enviarla a través de correo electrónico SMTP para evitar ataques dirigidos de robo de información; estos archivos viajan en texto plano solo asegurando el canal de comunicación vía SFTP.

Por ello el principal problema y la exigencia a nivel normativo es que los datos viajen cifrados de extremo a extremo, para evitar que un atacante interno o externo pueda interceptarlo, leerlo y modificarlo en cualquier punto de la ruta de entrega, en este sentido se propone implementar un mecanismo de protección de la información (cifrado asimétrico) aplicando el estándar PGP para asegurar la confidencialidad e integridad de la información en las comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

1.2 Interrogantes de la investigación

De acuerdo al problema identificado en la sección anterior, se plantean las siguientes preguntas de investigación, mismas que guiarán el desarrollo del presente trabajo:

¿Cuáles son los activos de información críticos de la Cooperativa Uniotavalo Ltda., de acuerdo a la metodología de riesgos aplicada?

¿Qué metodología asimétrica de cifrado puede proteger el correo electrónico y

transferencia de archivos con la integración del estándar PGP?

¿Cómo el mecanismo de cifrado PGP, permite cumplir con la normativa emitida por la Superintendencia de Economía Popular y Solidaria?

1.3 Objetivos de la investigación

1.3.1. Objetivo general

Establecer un mecanismo de protección de datos en reposo y en tránsito, mediante la implementación del estándar PGP, para asegurar la información en las comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

1.3.2 Objetivos específicos

1. Evaluar los activos de información críticos de la Cooperativa Uniotavalo Ltda. aplicando una metodología de gestión de riesgos.
2. Seleccionar una metodología asimétrica de cifrado para proteger el correo electrónico y transferencia de archivos, que permitan la integración de PGP.
3. Implementar un mecanismo de cifrado PGP, cumpliendo con la normativa emitida por la Superintendencia de Economía Popular y Solidaria.

1.4 Hipótesis de Trabajo.

El presente estudio será en esencia de tipo cualitativo, y no pretende demostrar una hipótesis utilizando técnicas de análisis cuantitativos, sin embargo, es pertinente formular una hipótesis de trabajo en función del objetivo general planteado. Esto es:

Al establecer un mecanismo de protección de datos en reposo y en tránsito, mediante la implementación del estándar PGP, se asegurará la información en las comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

1.5 Hipótesis Alterativa

Para la hipótesis de trabajo antes definida, la hipótesis alternativa (llamada hipótesis nula en investigación cuantitativa) que se plantea es la siguiente:

Al establecer un mecanismo de protección de datos en reposo y en tránsito, mediante la implementación del estándar PGP, no se asegurará la información en las comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

1.6 Categorización de variables

Las variables que se derivan de la hipótesis planteada son:

Variable independiente: Mecanismo de protección de datos en reposo y en tránsito,

mediante la implementación del estándar PGP.

Variable dependiente: Aseguramiento de la información en las comunicaciones SMTP y SFTP de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

1.7 Justificación

Hoy en día el principal activo de una empresa es la información, por tanto se debe mantener actualizado al personal de la organización respecto a las tendencias de seguridad de datos, pues el objetivo de esta transferencia de conocimiento es velar por que el personal en su actividad cotidiana preserve la confidencialidad, integridad y disponibilidad de los mismos, facilitando en un alto porcentaje el cumplimiento de la misión y visión de la organización, lo cual es satisfactorio para el personal y los clientes.

La mayoría de los ciberataques comienzan por correo electrónico: se engaña al usuario para que abra un archivo adjunto malicioso, haga clic en un enlace malicioso y divulgue sus credenciales, o responda con información confidencial. Los atacantes engañan a las víctimas mediante correos electrónicos cuidadosamente redactados para generar una falsa sensación de confianza o urgencia. Para ello, emplean diversas técnicas: suplantar dominios o marcas de confianza, hacerse pasar por usuarios conocidos, usar contactos previamente comprometidos para lanzar campañas o incluir contenido atractivo pero malicioso en el correo electrónico. En el contexto de una organización o empresa, cada usuario es un objetivo y, si se ve comprometido, una vía para una posible vulneración que podría resultar muy costosa. (Chander Girish, 2019)

Ya sean sofisticados ataques de estados-nación, esquemas de phishing dirigidos, vulnerabilidades de correo electrónico empresarial o ataques de ransomware, estos ataques están aumentando a un ritmo alarmante y su sofisticación también es cada vez mayor. Por lo tanto, es imperativo que la estrategia de seguridad de toda organización incluya una solución robusta de seguridad de correo electrónico. (Chander Girish, 2019)

Dentro de la experiencia del autor es valedero mencionar que múltiples instituciones financieras no incluyen dentro de sus políticas de seguridad de la información técnicas de cifrado de datos en su medio de transmisión de correos electrónicos, teniendo en cuenta que la ventaja de aplicar estos métodos radica en que los datos lleguen a su destino de una forma segura, preservando la confidencialidad de la misma al no permitir que se acceda a ella por personal ajeno a la entidad (principalmente intrusos informáticos o ciberdelincuentes).

El mundo empresarial funciona con el correo electrónico. Es nuestro principal medio de comunicación, tanto interna como externa, lo que lo convierte en una necesidad y un riesgo a la vez. Dado que compartimos información por correo electrónico —parte de ella confidencial—, es importante garantizar que la información permanezca protegida, segura y cumpla con las normativas, por eso, el cifrado de correo electrónico es fundamental para la seguridad de datos de cualquier organización. (Leader Megan, 2024).

¿Cuál es la diferencia entre un correo electrónico cifrado y uno no cifrado?

La diferencia clave entre un correo electrónico cifrado y uno no cifrado radica en el nivel de seguridad y privacidad que proporciona cada uno, un correo electrónico cifrado está diseñado para proteger su contenido del acceso no autorizado. Esto implica codificar el contenido para que solo pueda descifrarse con una clave adecuada, por el contrario, un correo electrónico sin cifrar permanece en formato de texto plano, lo que lo hace fácilmente legible para cualquier persona. Esta falta de protección significa que los datos confidenciales contenidos en correos electrónicos sin cifrar son vulnerables a escuchas, ataques de hackers y ciberdelincuentes, así como a filtraciones de datos, lo que supone riesgos significativos para la privacidad y la ciberseguridad empresarial. (Lepilkina Diana et al., 2024).

Los proveedores de correo electrónico cifrado ofrecen servicios especializados que protegen sus comunicaciones mediante técnicas de cifrado robustas. Esto suele implicar el uso de la infraestructura de clave pública (PKI), donde la remitente cifra el correo electrónico con la clave pública del destinatario y este lo descifra con su clave privada, de forma predeterminada, la mayoría de los clientes de correo electrónico garantizan el cifrado TLS. Sin embargo, si necesita cifrado de extremo a extremo, deberá realizar configuraciones adicionales, por ejemplo, Outlook, Gmail y Apple Mail admiten S/MIME (con restricciones), mientras que Yahoo! no tiene ningún cifrado de extremo a extremo, lo que obliga a sus usuarios a buscar un complemento profesional para habilitarlo. (Lepilkina Diana et al., 2024).

La presente investigación de tesis surge de la necesidad de proteger la confidencialidad e integridad de la información en las comunicaciones SMTP y SFTP en la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., con el propósito de mantener la información segura en todo momento ya sea en reposo o en tránsito, así como las estrategias de prevención incorporadas para los datos que se envían vía SFTP.

La investigación busca proporcionar un mecanismo de criptografía asimétrica que será útil para toda la Cooperativa, para mejorar uno de los eslabones más débiles dentro de la seguridad que es utilizado en la actualidad por los ciberdelincuentes como lo es el usuario final de la organización. Debido a que no se cuenta con una estrategia de concientización a usuarios sobre este tipo de ataques y sus estrategias de prevención, dentro de la presente tesis de investigación es conveniente indicar que se aplicará la extensión GnuPG basada en el estándar PGP y el algoritmo de criptografía asimétrica basada en RSA.(INCIBE, 2019) Además, la investigación contribuye a ampliar las capas de seguridad que tiene implementado la entidad financiera, que dará confianza a todos los usuarios de la Cooperativa para intercambiar datos confidenciales a través de las comunicaciones SMTP y SFTP.

CAPITULO II

2. MARCO REFERENCIAL.

2.1 Antecedentes

Con el fin de contextualizar y fundamentar la presente propuesta de investigación, se ha llevado a cabo una revisión narrativa de la literatura, que permite una exploración amplia y reflexiva del estado del arte. Este proceso se ha desarrollado siguiendo un protocolo de búsqueda flexible, propio de las revisiones narrativas, que privilegia la interpretación crítica y la integración de diversas perspectivas relevantes para el tema en cuestión.

En un primer momento, se definió una cadena de búsqueda cuidadosamente diseñada, cuyo propósito es dar respuesta a la interrogante central que guía esta investigación. Este proceso inicial sentó las bases para una exploración orientada y coherente del material bibliográfico pertinente, facilitando así una aproximación reflexiva y fundamentada al problema planteado: **¿Cómo se ha implementado seguridad en los protocolos SMTP y SFTP utilizando criptografía con el estándar PGP?**

Con el objetivo de localizar los artículos que permitan responder a esta interrogante, se diseñó una cadena de búsqueda específica y estratégica. Esta herramienta metodológica facilitó la identificación precisa de fuentes relevantes, orientando la selección documental hacia la construcción de un marco teórico sólido y pertinente, para esto se definió la siguiente cadena de búsqueda: **("All Metadata":PGP) OR ("Document Title":ENCRYPTION) AND ("Document Title":MECHANISM) OR ("Publication Title":Securing) AND ("Document Title":SMTP) OR ("All Metadata":SFTP)**

La cadena de búsqueda fue corrida en la base de datos de IEEE Xplore (IEEEX), misma que mostró un total de 359 publicaciones entre (conferencias, normas, artículos, libros y revistas). Se estableció como criterio de inclusión para priorizar aquellos trabajos que aborden el manejo de sistemas criptográficos con el estándar PGP, específicamente aquellos publicados en los últimos 15 años. Esta delimitación temporal y temática permitió focalizar la revisión en 293 fuentes actuales y pertinentes en relación a conferencias, garantizando la relevancia y vigencia de los hallazgos en el marco de la investigación, que estén en idioma inglés y que hagan referencia al estándar PGP, como se muestra en la Figura1.

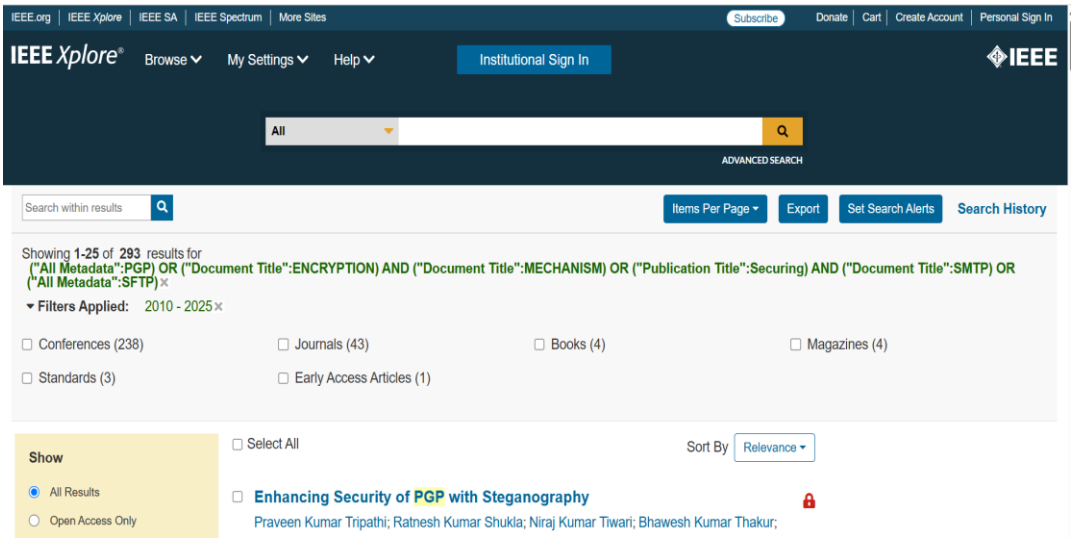


Figura 1. Verificación IEEE Xplore (Fuente Propia)

Posteriormente, se llevó a cabo un análisis minucioso de los resúmenes de los 293 artículos identificados, con el fin de discernir cuáles resultaban pertinentes para el desarrollo del estudio. De esta selección inicial, se eligieron cinco trabajos que, por su relevancia y aporte conceptual, fueron sometidos a un análisis detallado que se expone a continuación.

En el estudio de (Yusuf Kurniawan; Aan Albone; Hari Rahyuwibowo,2011), menciona que PGP ha sido una herramienta fundamental para la seguridad digital durante casi dos décadas, valorada por su código abierto que supuestamente permite una revisión amplia y constante por parte de expertos. Sin embargo, esta confianza es cuestionable, ya que no todos poseen el conocimiento necesario para evaluar su seguridad, y advertencias importantes sobre posibles debilidades han sido eliminadas de la documentación oficial. La falta de documentación clara y la complejidad derivada de múltiples parches dificultan una revisión exhaustiva del código. Además, la dificultad para compilar versiones antiguas lleva a que la mayoría use ejecutables precompilados, generando incertidumbre sobre la correspondencia entre el código fuente y el software utilizado. Esto pone en evidencia que la apertura del código no garantiza seguridad automática, y que es necesario un análisis crítico y riguroso para confiar verdaderamente en la protección que ofrece PGP.

Dentro del estudio de (Man Young Rhee, 2013), menciona que Pretty Good Privacy (PGP) fue inventada por Philip Zimmermann, quien lanzó la versión 1.0 en 1991. Las versiones posteriores 2.6.x y 5.x (o 3.0) de PGP han sido implementadas por una colaboración totalmente voluntaria bajo la guía de diseño de Zimmermann. PGP es

ampliamente utilizado en las versiones individuales y comerciales que funcionan en una variedad de plataformas en toda la comunidad informática. PGP utiliza una combinación de cifrado simétrico de clave secreta y cifrado asimétrico de clave pública para proporcionar servicios de seguridad para el correo electrónico y archivos de datos. También proporciona servicios de integridad de datos para mensajes y archivos de datos mediante el uso de firma digital, cifrado, compresión (zip) y conversión radix-64 (ASCII Armor).

Con la creciente dependencia explosiva del correo electrónico y el almacenamiento de archivos, los servicios de autenticación y confidencialidad se han convertido en demandas cada vez mayores. MIME es una extensión del marco RFC 2822 que define un formato para mensajes de texto que se envían utilizando correo electrónico. MIME está destinado a abordar algunos de los problemas y limitaciones del uso de SMTP. La Extensión de Correo de Internet Seguro/Múltiples Propósitos (S/MIME) es una mejora de seguridad al estándar de formato de correo electrónico MIME, basada en tecnología de RSA Data Security. Aunque tanto PGP como S/MIME están en una pista de estándares de IETF[1], parece probable que PGP siga siendo la opción para la seguridad del correo electrónico personal para muchos usuarios, mientras que S/MIME surgirá como el estándar de la industria para uso comercial y organizacional.

Según (Anuradha Anugurala; Anshu Chopra,2016), aborda la seguridad en sistemas distribuidos, destacando la gestión de credenciales como un elemento clave para mejorar la protección cuando los usuarios acceden a servicios a través de Internet. Propone un marco de seguridad basado en certificados Open PGP (RFC 4880), un estándar de cifrado originalmente diseñado para correo electrónico, para fortalecer la red contra ataques como el man in the middle (hombre en el medio). A diferencia de los certificados X.509, que dependen de autoridades certificadoras y pueden ser vulnerables en infraestructuras distribuidas, el uso de Open PGP permite prevenir estos ataques mediante la autenticación y cifrado robustos en las comunicaciones de red. Así, se busca proporcionar un sistema distribuido más seguro y resistente frente a amenazas comunes en entornos de computación en red. Esta propuesta enfatiza la necesidad de un enfoque criptográfico adaptado a las particularidades de sistemas distribuidos para garantizar la integridad y confidencialidad de las credenciales y las comunicaciones.

[1] IETF: Internet Engineering Task Force

En el trabajo de investigación de (Rakesh Shukla; Hari Om Prakash; R. Phanibhusan, 2016), se considera la seguridad del correo electrónico como una preocupación crucial en la comunicación digital, dado que los mensajes viajan por redes abiertas y están expuestos a ataques de interceptación y manipulación. PGP (Pretty Good Privacy) surge como una solución eficaz para proteger la privacidad y la integridad de los correos electrónicos mediante un sistema de cifrado híbrido que combina criptografía de clave pública y simétrica. Este método utiliza una clave pública para cifrar la información y una clave privada para descifrarla, asegurando que solo el destinatario previsto pueda acceder al contenido. Además, PGP permite la firma digital, que autentica la identidad del remitente y garantiza que el mensaje no ha sido alterado durante la transmisión. A diferencia de otros sistemas comerciales que suelen estar estrechamente ligados a servidores o navegadores específicos, PGP ofrece un marco flexible, transparente y seguro, ideal para entornos web y clientes de correo electrónico diversos. Su diseño también incluye la compresión de datos para optimizar el tamaño y la velocidad de transmisión. En conjunto, PGP proporciona una herramienta robusta para mantener la confidencialidad, autenticidad y seguridad en las comunicaciones por correo electrónico frente a las amenazas presentes en el ciberespacio.

Dentro del estudio de comunicaciones inalámbricas según (Milan Kumar Dholey; G. P. Biswas, 2018) menciona que el cifrado PGP (Pretty Good Privacy) es un método criptográfico que combina técnicas de cifrado simétrico y asimétrico para garantizar la privacidad, autenticación e integridad de los datos en comunicaciones digitales. En el contexto del protocolo DSR para redes MANET, el uso de PGP permite que la fuente pueda autenticar al receptor original antes de iniciar la transmisión de datos, impidiendo así que nodos maliciosos desvíen el enrutamiento enviando paquetes a destinos incorrectos.

Esto se logra mediante la identificación segura del destinatario a través de claves públicas y privadas, donde la clave pública cifra la clave de sesión que a su vez cifra el mensaje, asegurando que solo el receptor legítimo pueda descifrar y recibir la información. De esta manera, el algoritmo propuesto fortalece la seguridad del protocolo DSR al prevenir la desviación de datos, aunque no aborda ataques grupales de nodos maliciosos. En resumen, PGP[2] aporta un mecanismo eficaz para autenticar y proteger la transmisión de datos en

[2] **Pretty Good Privacy (PGP):** Estándar de seguridad utilizado para descifrar y cifrar correos electrónicos, así como para autenticar mensajes mediante firmas digitales y cifrado de archivos

entornos dinámicos y vulnerables como las MANETs, mejorando la confiabilidad del enrutamiento frente a nodos adversarios.

Conclusión de la revisión de literatura:

A partir del análisis detallado de los estudios revisados, se evidencia una amplia variedad de enfoques y experiencias en la implementación y evaluación de la seguridad en correos electrónicos mediante cifrado PGP. Estas investigaciones reflejan tanto los desafíos como las mejores prácticas adoptadas por distintas organizaciones para mitigar ataques en los protocolos SMTP y SFTP. Para facilitar una comprensión integral de estos hallazgos, se presenta a continuación la Tabla 1. que sintetiza las principales características, resultados y enfoques de cada estudio, ofreciendo así una visión clara y estructurada del estado actual y las tendencias en la adopción del cifrado asimétrico PGP en el ámbito de la seguridad de la información.

ART NO.	AUTOR	AÑO PUB.	TIPO DE ORGANIZACIÓN ESTUDIADA (GUBERNAMENTAL, EMPRESARIAL, SERVICIOS, ETC)	FACTORES DE ÉXITO	FACTORES DE ÉXITO
1	Yusuf Kurniawan; Aan Albone; Hari Rahyuwibowo	2011	Empresarial	Mini PGP tiene mejor seguridad que algunos tipos de PGP y GPG en términos de seguridad hacia adelante y seguridad hacia atrás, además el algoritmo 3DES con 3 claves diferentes (168 bits) tiene una longitud de clave efectiva tan grande como 112 bits, en lugar de 168 bits al enfrentarse a un ataque de fuerza bruta.	Mini PGP es más resistente contra ataques de diccionario y spyware que PGP convencional.
2	Man Young Rhee	2013	Empresarial	PGP utiliza una combinación de cifrado simétrico de clave secreta y cifrado asimétrico de clave pública para proporcionar servicios de	Aunque tanto PGP como S/MIME son estándares de IETF , parece probable que PGP siga siendo la opción para la seguridad del correo electrónico personal

				seguridad para el correo electrónico y archivos de datos	para muchos usuarios, mientras que S/MIME surgirá como el estándar de la industria para uso comercial y organizacional.
3	Anuradha Anugurala; Anshu Chopra	2016	Empresarial	Ataques de correo electrónico pueden ser posibles como ataque de hombre en el medio, suplantación, phishing, etc. se puede resolver cuando usamos Open PGP que está certificado por solo una empresa que es IETF (fuerza de tarea de ingeniería de internet)	El rendimiento del algoritmo PGP utilizado es mejor que X.509 PKI. La posibilidad de ataque de hombre en el medio disminuye.
4	Rakesh Shukla; Hari Om Prakash; R. Phanibhusan	2016	Empresarial	PGP permite la firma digital, que autentica la identidad del remitente y garantiza que el mensaje no ha sido alterado durante la transmisión	PGP proporciona una herramienta robusta para mantener la confidencialidad, autenticidad y seguridad en las comunicaciones por correo electrónico frente a las amenazas presentes en el ciberespacio.
5	Milan Kumar Dholey; G. P. Biswas	2018	Empresarial	El algoritmo propuesto fortalece la seguridad del protocolo DSR al prevenir la desviación de datos, aunque no aborda ataques grupales de nodos maliciosos	PGP aporta un mecanismo eficaz para autenticar y proteger la transmisión de datos en entornos dinámicos y vulnerables

Tabla 1. Cifrado Asimétrico PGP (Fuente Propia)

La implementación de PGP (Pretty Good Privacy) como estándar de criptografía asimétrica ofrece ventajas significativas en seguridad, pero también plantea retos operativos y económicos que deben evaluarse. Estudios como los de Rodríguez et al. (2023) advierten que el 40% de las implementaciones de PGP en instituciones financieras presentan fallos críticos debido a, configuraciones incorrectas en algoritmos (ej. uso de RSA-1024 en lugar de RSA-4096) y falta de auditorías periódicas para detectar claves expiradas o

vulnerabilidades en clientes de correo.

Aunque PGP es una herramienta robusta, su efectividad depende de una implementación rigurosa y actualizaciones constantes. Organizaciones como la Electronic Frontier Foundation (EFF) recomiendan complementarlo con protocolos como TLS 1.3 y autenticación DMARC para mitigar riesgos residuales.

En conclusión y luego del análisis de literatura realizado, se considera que PGP sigue siendo un estándar vital para la seguridad asimétrica, pero su adopción exitosa exige equilibrar recursos técnicos, económicos y humanos, priorizando siempre la gestión proactiva de riesgos, este estudio de cierta manera contribuirá al aseguramiento de la información enviada a través del servicio de correo y la transmisión de la información a través de canales SFTP, a su vez toda información que se encuentre en reposo será asegurada con la utilización del cifrado PGP implementado dentro del ecosistema de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

2.2 Marco Teórico.

2.2.1. Gestión de riesgos de seguridad de la información.

La gestión de riesgos se define como el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y de aumentar la probabilidad y ocurrencia de oportunidades con efectos negativos. Se trata de una metodología o conjunto de metodologías encaminadas a gestionar correctamente las incertidumbres de una amenaza. En el ámbito de la gestión de riesgos, entra en juego el concepto de seguridad de la información: la seguridad se define como el conjunto de medidas y capacidades de los sistemas de información para resistir a las amenazas manteniendo la disponibilidad, autenticidad, integridad y confidencialidad de los datos (Chicano Tejada, E., 2023). De este modo, una correcta gestión de riesgos utilizará unas medidas de seguridad que protejan sus datos e información en cuanto a:

Disponibilidad: la información debe estar disponible a los usuarios siempre que sea necesario. Una carencia de disponibilidad provoca interrupciones de servicio y mermas de calidad.

Integridad: la información debe ser correcta y completa. La seguridad debe impedir que se manipule, corrompa o elimine información sin autorización.

Confidencialidad: la información debe estar disponible solo para los usuarios que

estén correctamente autorizados. La seguridad debe encargarse en todo momento de proteger la información ante accesos no autorizados.

Autenticidad: garantía de la fuente de la que proceden los datos. La seguridad de la organización debe asegurar que los datos proceden de sitios seguros sin haber sufrido manipulación alguna.

Trazabilidad: se debe conocer en todo momento quién y cuándo ha realizado cada acción con la información de la información. Esta característica es muy útil para analizar los incidentes y para detectar a los atacantes.

2.2.2. Metodologías de Gestión de Riesgos.

Las normas de la Organización Internacional de Normalización (ISO) permiten evaluar el nivel de calidad organizacional, aunque carecen de un protocolo detallado para alcanzar los objetivos establecidos, por lo contrario, no está descartado optar por adaptar marcos ya consolidados, como OCTAVE (evaluación de amenazas y activos críticos), CRAMM (gestión de riesgos basada en análisis de activos) y MAGERIT (metodología pública para riesgos TIC), aplicadas mediante desarrollos internos o en colaboración con entidades externas. Estas herramientas buscan sistematizar la identificación, análisis y mitigación de riesgos operativos, tecnológicos y estratégicos, tal como se muestra en la Figura 2.

METODOLOGIA	PROPOSITO	ENFOQUE	ETAPAS	ORIGEN
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Identificación y priorización de amenazas organizacionales y tecnológicas	Enfoque organizacional y basado en activos criticos, autogestionado	Perfiles de amenazas basados en activos, Identificación de vulnerabilidades de infraestructura, Desarrollo de estrategia de seguridad	Carnegie Mellon University, EE.UU.
CRAMM (CCTA Risk Analysis and Management Method)	Análisis y gestión de riesgos en sistemas de información	Evaluación estructurada y cualitativa del riesgo con énfasis en activos, amenazas, vulnerabilidades y contramedidas	Establecimiento de objetivos y valoración de activos, Evaluación de amenazas y vulnerabilidades, Identificación y selección de contramedidas	Reino Unido, gobierno (CCTA), versión 5.0
MAGERIT	Gestión y análisis formal de riesgos en sistemas de información	Análisis sistemático de riesgos en sistemas de información con evaluación cuantitativa y cualitativa	Identificación de activos, análisis de amenazas, valoración de riesgos, tratamiento de riesgos	Gobierno español
PRIMA	Clasificación supervisada basada en reconocimiento de patrones	Análisis estadistico basado en medidas de distancia Euclidiana para clasificación de riesgos	Entrenamiento y reconocimiento/clasificación de patrones	Académico / estadistico

Figura 2. Principales métodos de análisis y gestión de riesgos. (Fuente Propia)

2.2.2.1. OCTAVE. (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

La metodología Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) para la Gestión de Riesgos se enfoca en la Evaluación de amenazas, activos y vulnerabilidades operativamente críticas. Fue desarrollada por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, con la finalidad de brindar un nivel de análisis estructurado, enfocado en los activos y la mitigación de amenazas (Gartner Research, 2010).

2.2.2.2. CRAMM. (CCTA Risk Analysis and Management Method)

CRAMM es una metodología de análisis y gestión de riesgos desarrollada en 1985 por la Agencia Central de Informática y Telecomunicaciones (CCTA), perteneciente al gobierno de Reino Unido, sus siglas corresponden a CCTA Risk Analysis and Management Method (Crespo & Cordero, 2018).

CRAMM fue diseñada principalmente como metodología de apoyo para los analistas de sistemas con el fin de cumplir los intereses de protección referentes a confidencialidad, integridad y disponibilidad de la información y activos relacionados (Crespo & Cordero, 2018).

2.2.2.3. MAGERIT. (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

El ministerio de Hacienda y Administraciones Públicas de España define a la metodología a MAGERIT como:

Una metodología que ha sido elaborada como respuesta a la percepción de la administración pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. Así, menciona que el uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012).

2.2.2.4. PRIMA. (Prevención de riesgos informáticos con metodología abierta)

Es un compendio de metodologías españolas desarrolladas entre los años 1990 y la actualidad con un enfoque subjetivo. Sus características esenciales son:

• Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad.

• Fácilmente adaptable a cualquier tipo de herramienta.

• Posee cuestionarios de preguntas para la identificación de debilidades o faltas de controles. Posee listas de ayuda para los usuarios menos experimentados de debilidades, riesgos y contramedidas (sistema de ayuda).

• Permite fácilmente la generación de informes finales.

• Las "Listas de ayuda" y los cuestionarios son abiertos y por tanto es posible introducir información nueva o cambiar la existente. De ahí la expresión Abierta de su nombre.

• Tiene un "¿qué pasa si...?" cualitativo, pero al tener capacidad de aprendizaje con su uso posee en su base de conocimiento una base o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo. (Piattini Velthuis, M., 2015).

2.2.3. Introducción a la Criptografía.

A lo largo de la historia, el ser humano ha desarrollado métodos ingeniosos para proteger información sensible, motivado por la necesidad de compartir secretos con aliados y ocultarlos de enemigos. Este impulso dio origen a dos estrategias fundamentales:

Ocultar la existencia del mensaje (Esteganografía), que consiste en esconder el hecho mismo de que existe un mensaje secreto, evitando que un adversario sospeche de su presencia, ejemplos históricos: mensajes escritos con tinta invisible, textos camuflados en objetos cotidianos (ej. tablillas de madera en la Antigua Grecia) o micro-puntos en cartas durante la Segunda Guerra Mundial. (Hernández Encinas, L., 2016).

Transformar el mensaje (Criptografía), que consiste en modificar el contenido para que sea incomprensible para quienes no posean la clave o método para descifrarlo. Técnicas antiguas: sustitución de caracteres (ej. cifrado César), transposición de letras o uso de símbolos crípticos, como los jeroglíficos egipcios o los quipus incas. (Hernández Encinas, L., 2016).

Ambos enfoques perseguían un equilibrio entre acceso selectivo (solo aliados autorizados) y protección contra intrusiones. Mientras la esteganografía explotaba el factor sorpresa ("si no sabes que existe, no lo buscas"), la criptografía priorizaba la resistencia ("aunque lo encuentres, no podrás entenderlo"). (Hernández Encinas, L., 2016).

Esta dualidad sentó las bases de la seguridad de la información moderna. Hoy, conceptos como el cifrado asimétrico (PGP) o la comunicación cuántica heredan estos principios, evolucionando desde métodos físicos y manuales hasta sistemas matemáticos y digitales. Sin embargo, el objetivo central sigue siendo el mismo: garantizar confidencialidad, autenticidad y control en un mundo donde la información es poder. Al respecto (Van Tilborg et al., 2005) señala que:

Este procedimiento de transformar un mensaje en claro en otro ininteligible, llamado criptograma o mensaje cifrado (texto cifrado), se conoce como criptografía, término que procede de la palabra griega kryptos, cuyo significado es “secreto”, “oculto” o “disimulado”. Así pues, el objetivo de la criptografía es permitir el intercambio de información haciendo el mensaje ilegible sin ocultar la existencia de dicho mensaje. (Hernández Encinas, L., 2016).

De forma más general, el objetivo de la criptografía es garantizar que la información transmitida (o almacenada) posea las siguientes tres cualidades: confidencialidad, integridad y autenticidad. La confidencialidad consiste en lograr que la información permanezca secreta y solo sea conocida por quienes tienen autorización para ello. Por su parte, la integridad hace referencia a la necesidad de que la información no haya sido manipulada ni alterada desde su origen a su destino. Finalmente, la autenticidad obliga a que tanto el origen como la información transmitida sean auténticos, es decir, no se produzcan suplantaciones. Otras cualidades relacionadas con la información que considera la criptografía son su disponibilidad y no repudio (Hernández Encinas, L., 2016).

2.2.4. Criptografía Simétrica.

Un sistema de cifrado es simétrico o de clave privada cuando se utiliza la misma clave para cifrar como para descifrar, o bien la clave de descifrar se obtiene fácil- mente de la clave de cifrado. a nivel matemático es un método poco complejo y se ha utilizado durante años. La seguridad de estos sistemas se reduce únicamente a la seguridad de la clave. para realizar un cifrado simétrico se tienen que realizar dos operaciones distintas: sustitución y transposición. La primera operación consiste en sustituir cada uno de los elementos que

forman el texto por otro a través de unas reglas conocidas por el emisor y el receptor. La segunda operación consiste en la reordenación de los elementos obtenidos en la primera operación utilizando unas normas establecidas por emisor y receptor. Estas dos operaciones por separado no constituyen un buen sistema criptográfico, pero juntas puede llegar a serlo. (Hernández Encinas, L., 2016). La operación de sustitución puede ser de dos tipos: monoalfabética y polialfabética, tal como se muestra en la Figura 3.

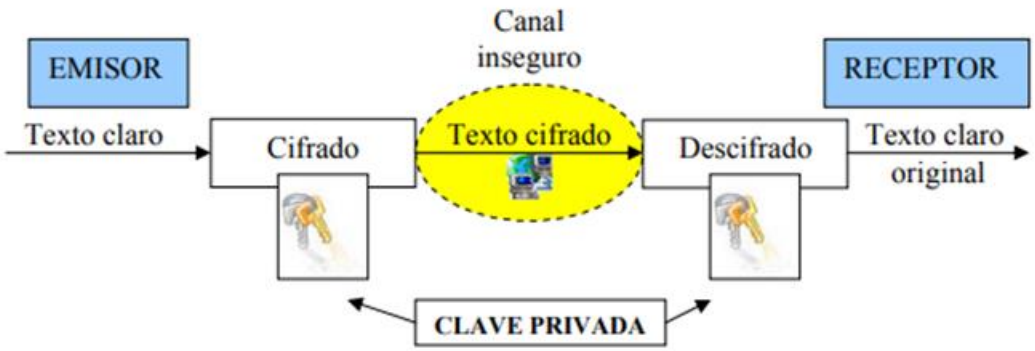


Figura 3. Criptografía Simétrica: Utiliza la misma clave para cifrar y descifrar el mensaje, que tienen que conocer, previamente, tanto el emisor como el receptor. (INCIBE, 2019)

2.2.4.1. Algoritmos de la Criptografía Simétrica.

2.2.4.1.1. Algoritmo DES (DATA ENCRYPTION ESTANDAR).

En la década de 1970 IBM desarrolló un sistema criptográfico llamado LUCIFER basado en las ideas propuestas por Shannon. a partir de este algoritmo y gracias al apoyo del gobierno estadounidense, la propia compañía IBM desarrolló un nuevo sistema criptográfico que se bautizó con el nombre DES. El sistema es un producto de sustituciones y transposiciones, lo que le convierte en un sistema simétrico. El algoritmo DES distribuye el texto que se desea cifrar en bloques de 64 bits y los modifica mediante una clave del mismo tamaño (64 bits). Tras esta codificación el texto sigue teniendo el mismo tamaño.

En el año 1977 los autores Diffie(71) y Hellman(72) hicieron público que utilizando una técnica de prueba y ensayo a través de las claves posibles, el algoritmo DES era vulnerable. Con este estudio se demostró que una clave de 64 bits era insuficiente para garantizar la seguridad del algoritmo. En un principio se había pensado en la utilización de una clave de 128 bits, al igual que la utilizada por LUCIFER pero el cambio a 64 bits no está todavía aún claro porque se hizo. Otro de los asuntos que no está todavía claro es el motivo por el cual IBM eligió y diseñó las S-Cajas. La respuesta a esta pregunta que más se escucha

es que la NSA (Nacional Security Agency) de Estados Unidos fue la que impidió a IBM publicar las respuestas a las preguntas que ahora se han planteado. El motivo de esta prohibición no sería otro que permitir que el gobierno estadounidense pudiera descifrar los mensajes, esto por un lado, y por otro, conociendo el diseño de las S-Cajas, podría destruir el sistema. (García, R. D. M., 2009)

2.2.4.1.2. Algoritmo TRIPLE DES.

Para corregir los problemas detectados en el algoritmo DES se diseñó el Triple DES TDES o 3DES. La gran diferencia que existe sobre el DES es que se utiliza una clave de 192 bits, en realidad 156 bits si se eliminan los bits de paridad. (García, R. D. M., 2009). El Triple DES consiste en aplicar el algoritmo DES tres veces como se muestra en la Figura 4.

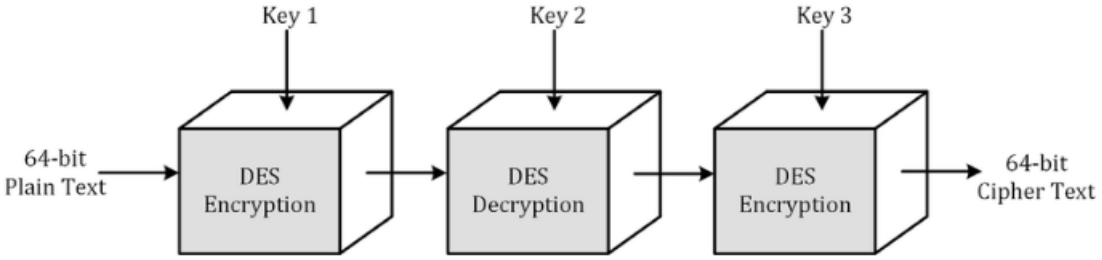


Figura 4. Esquema del cifrado Triple DES. (Procedia Ciencias de la Computación, 2020)

2.2.4.1.3. Algoritmo IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM).

Algoritmo desarrollado en Suiza (en el Instituto Federal Suizo de Tecnología, Swiss Federal Institute of Technology) a principios de los noventa, fruto del trabajo de los investigadores Xuejia Lai y James Massey. Este algoritmo, que destaca por ser muy rápido, realiza sus operaciones en 8 rondas, emplea claves de 128 bits y trabaja con bloques de 64 bits, siendo bastante resistente a las técnicas de criptoanálisis lineal y diferencial. (Gómez Vieites, Á., 2015).

2.2.4.1.4. Algoritmo Blowfish.

Algoritmo desarrollado por el experto en seguridad Bruce Schneier en 1993. Se trata de un algoritmo de cifrado que trabaja con bloques de 64 bits y que realiza 16 rondas, consistente cada una de ellas en una permutación dependiente de la clave y una sustitución dependiente de la clave y de los datos, empleando claves variables de hasta 448 bits. Ha sido optimizado para poder ser ejecutado en procesadores de 32 bits y resulta bastante más rápido

que el DES, por lo que ha sido elegido por bastantes empresas en los últimos años. (Gómez Vieites, Á., 2015).

2.2.4.1.5. Algoritmo Skipjack.

Algoritmo desarrollado por la NSA para el gobierno de Estados Unidos, dentro del proyecto del polémico chip cifrador Clipper. Se trata de un algoritmo clasificado como secreto, que trabaja con bloques de 64 bits, claves de 80 bits y que realiza sus operaciones en 32 rondas. (Gómez Vieites, Á., 2015).

2.2.4.1.6. Algoritmo CAST.

Algoritmo que realiza sus operaciones en 8 rondas sobre bloques de 64 bits y emplea claves de 40 a 64 bits. Debe su nombre a sus inventores: Carlisle, Adams, Stafford y Tavares. (Gómez Vieites, Á., 2015).

2.2.4.1.7. Algoritmo RC2.

Desarrollado por la empresa RSA Labs como un algoritmo de cifrado simétrico que trabaja con bloques de 64 bits y claves de tamaño variable, diseñado para operar con los mismos modos de trabajo que el DES, pero siendo el doble de rápido.(Gómez Vieites, Á., 2015).

2.2.4.1.8. Algoritmo RC4.

Algoritmo desarrollado por la empresa RSA Labs y presentado en diciembre de 1994, fue diseñado para el cifrado en flujo y permite trabajar con claves de tamaño variable. (Gómez Vieites, Á., 2015).

2.2.4.1.9. Algoritmo RC5.

Se trata de un algoritmo propuesto por RSA Labs como una mejora del RC4, para incrementar su robustez y ofrecer una mayor eficiencia computacional. Se trata, por lo tanto, de un rápido sistema de cifrado en bloque, que se basa en la realización de varias rotaciones dependientes de los datos (entre 0 y 255 rondas), trabajando sobre bloques de tamaño de 32, 64 ó 128 bits, y claves de tamaño variable (entre 0 y 2.048 bits).(Gómez Vieites, Á., 2015).

2.2.4.1.10. Algoritmo RC6.

A partir del algoritmo RC5, que utilizaba Netscape en su navegador web, RSA Laboratorios presentó como alternativa a DES el RC6. Este algoritmo se desechó por motivos de seguridad ya que el algoritmo predecesor al RC5, el RC4, fue ata- cado con éxito y su seguridad estaba en entredicho. (García, R. D. M., 2009).

2.2.4.1.11. Algoritmo GOST.

Este algoritmo es un estándar desarrollado por el gobierno de la antigua URSS como respuesta al algoritmo norteamericano DES. GOST realiza sus operaciones en 32 rondas y emplea claves de 256 bits. (Gómez Vieites, Á., 2015).

2.2.4.1.12. Algoritmo AES (ADVANCED ENCRYPTION STANDARD).

Algoritmo conocido como "Rijndael" y diseñado por los belgas Vicent Rijmen y Joan Daemen. Resultó el ganador de un concurso convocado por el NIST (National Institute of Standards Technology) para la elección de un algoritmo sustituto del DES, concurso al que se presentaron 15 algoritmos candidatos. AES fue adoptado como estándar FIPS 197 (Federal Information Processing Standard) en noviembre de 2002. Se trata de un algoritmo de cifrado en bloque, que utiliza bloques de 128 bits y claves variables de longitudes de entre 128 y 256 bits, con varios modos de operación. (Gómez Vieites, Á., 2015).

2.2.5. Criptografía Asimétrica.

En la criptografía asimétrica, se crean dos llaves de cifrado al mismo tiempo, la llave pública se comparte públicamente y llave privada se usa para descifrar el mensaje cifrado con la llave pública.

Los algoritmos asimétricos en vez de usar una sola llave para proceder con la encriptación y la desencriptación, se recurren a dos llaves diferentes: una para encriptar y otra para desencriptar. Estas dos llaves se encuentran coligado matemáticamente, cuya característica principal es que la llave pública no puede desencriptar lo que se encripta.

Cuando se finaliza la creación de una llave asimétrica, se define una llave de encriptado (llave pública) y una llave de desencriptado (llave privada); la primera puede ser compartida por todo el mundo, pero, de otro lado se debe tener mucho cuidado en resguardar la llave privada. (Mendoza (2015). Las llaves asimétricas tienen la formidable propiedad de que lo que se está encriptando con una llave sólo se puede desencriptar con la llave privada, tal como se muestra en la Figura 5.

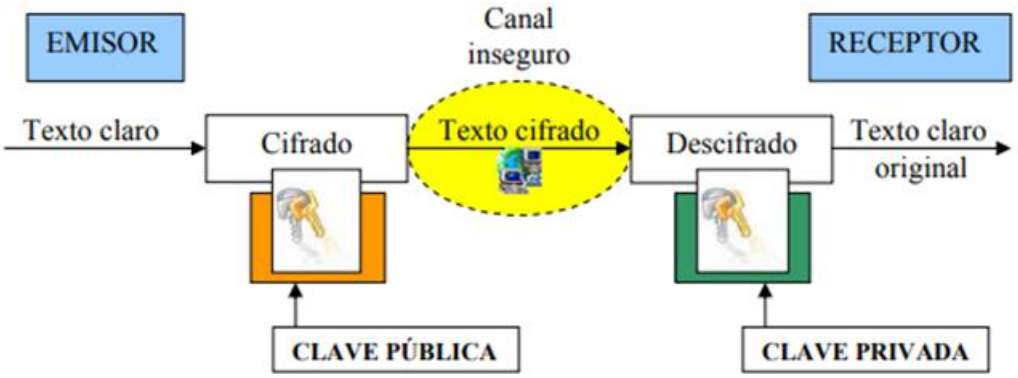


Figura 5. Criptografía asimétrica: se basa en el uso de dos claves. (INCIBE, 2019)

2.2.5.1. Algoritmos de la Criptografía Asimétrica.

2.2.5.1.1. Algoritmo Diffie-Hellman.

Este protocolo recibe el nombre de sus autores, esto es, Protocolo de acuerdo (o intercambio) de clave de Diffie-Hellman o DHKA (Diffie-Hellman Key Agreement). Debe tenerse en cuenta que este protocolo no es un criptosistema en sí mismo, puesto que no se lleva a cabo ningún tipo de cifrado de información; lo que permite es que, al final del mismo, ambas partes puedan utilizar la información que acaban compartiendo como si fuera una semilla que luego les permite acordar una clave. Lo más importante es que la información resultante solo la conocerán ambas partes, aunque haya adversarios que puedan llegar a conocer la información intercambiada a lo largo del protocolo. (Hernández Encinas, L., 2016).

2.2.5.1.2. Algoritmo RSA.

El criptosistema RSA, llamado así en honor a los tres investigadores que lo propusieron (Rivest et al., 1978), Ronald Rivest (1947-), Adi Shamir (1952-) y Leonard Adleman (1945-), es uno de los sistemas de cifrado asimétrico más utilizado en la actualidad y consta, como es habitual en la clave asimétrica, de tres procedimientos: generación de las claves, cifrado y descifrado (Durán et al., 2005; Fúster et al., 2012).

La implementación de los protocolos de cifrado y descifrado es, básicamente, la misma, dado que en ambos casos se llevan a cabo las mismas operaciones matemáticas, esto es, elevar un número a un exponente y hacer módulo otro número. (Hernández Encinas, L., 2016).

2.2.5.1.3. Algoritmo ElGamal.

El criptosistema de ElGamal fue publicado por Taher ElGamal (1955-) (ElGamal, 1985) y, además de ser otro de los criptosistemas de clave asimétrica más extendidos, es el que ha dado lugar a los criptosistemas con mayor futuro, los basados en curvas elípticas, que veremos posteriormente. Al igual que el sistema RSA, este criptosistema necesita generar unas claves y luego definir los procesos de cifrado y descifrado. (Hernández Encinas, L., 2016).

2.2.5.1.4. Algoritmo Curvas Elípticas.

El conjunto más empleado como alternativa a los mencionados anteriormente es el grupo que forman los puntos de un tipo especial de curvas, llamadas curvas elípticas (Fúster et al., 2012, cap. 8), y que ha dado lugar a lo que se conoce como Criptografía basada en curvas elípticas o ECC (Elliptic Curve Cryptography). Estas curvas suelen representarse mediante la ecuación conocida como de Weierstrass, cuya expresión es de la siguiente forma: y2 + a1 x y + a3 y = x3 + a2 x2 + a4 x + a6.

Con relación a la seguridad, se puede decir que, si esta depende de la dificultad de resolver el logaritmo discreto, como sucede con ElGamal, en el caso de las curvas elípticas esta dificultad se basa en la dificultad de resolver el problema del logaritmo elíptico. En todo caso, la ventaja del utilizar curvas elípticas como grupo base para definir un criptosistema radica, fundamentalmente, en que es posible llevar a cabo implementaciones eficientes en dispositivos de poca capacidad física, como es el caso de las tarjetas inteligentes. (Hernández Encinas, L., 2016).

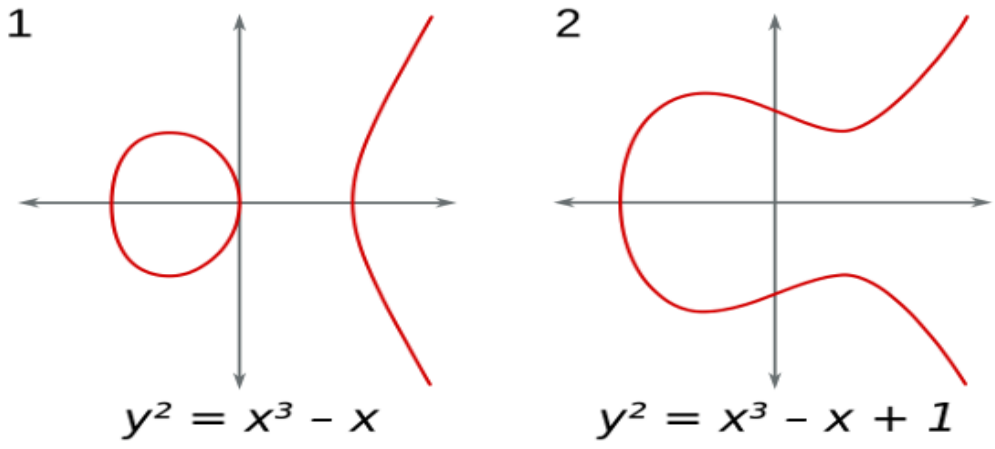


Figura 6. Concepto de criptografía con curvas elípticas, (Ecured, 2018)

2.2.6. Criptografía Cuántica.

La criptografía cuántica hace uso de la mecánica cuántica en vez de algoritmos numéricos para originar una llave secreta. Esto se conoce como difusión cuántica de Llaves o QKD. Para ejecutar QKD, se recurre a dos canales de comunicación. Entre Alice y Bob. Esto abarca un canal público, que es solo un enlace de comunicaciones clásico; podría ser el Internet, un teléfono móvil o el teléfono de su hogar. Los mensajes encriptados se envían a través de esta línea. Además, se utiliza una segunda pieza del rompecabezas QKD: un canal de comunicaciones cuánticas sobre el cual se distribuye la llave cuántica. En la consecuencia, esto se hace usando fotones individuales en diferentes estados de polarización. La mecánica cuántica se fundamenta en un principio de la teoría cuántica: que la medición perturba un estado cuántico. Para aprender algo sobre una llave codificada como un estado cuántico, se debe realizar una medición. Entonces, si Eve toca la línea, tiene que hacer mediciones, perturbando el sistema de tal manera que Alice y Bob puedan detectar su presencia. (McMahon, 2018).

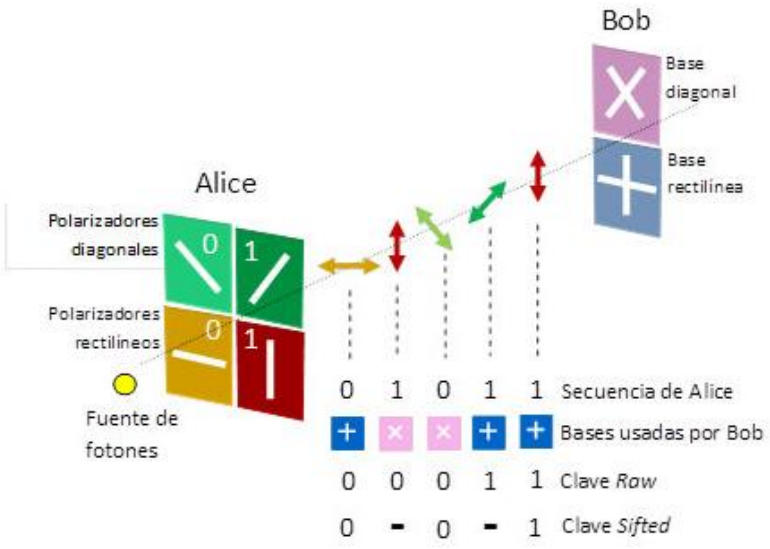


Figura 7. Protocolo de distribución cuántica de clave BB84. (GICSI)

2.2.7. Amenazas.

2.2.7.1. Ataques informáticos a servicios SMTP y SFTP.

Un ataque cibernético como se muestra en la Figura 8. implica aprovechar deficiencias o vulnerabilidades en sistemas informáticos (software/hardware) o en los usuarios asociados a estos, con la finalidad de lograr una ventaja mayormente económica,

provocando un daño en la seguridad del sistema que posteriormente se traduce en pérdidas para los recursos de la entidad (Mendoza, 2015).

Figura 8. El Hombre de en Medio y el Cifrado Electrónico. (Miriam J. Padilla Espinosa,2018)

Para poder llevar a cabo un ataque informático los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido). (Gómez Vieites, Á. 2010). Estos tres factores constituyen lo que podríamos denominar como el "Triángulo de la Intrusión", concepto que se presenta de forma gráfica en la Figura 9.

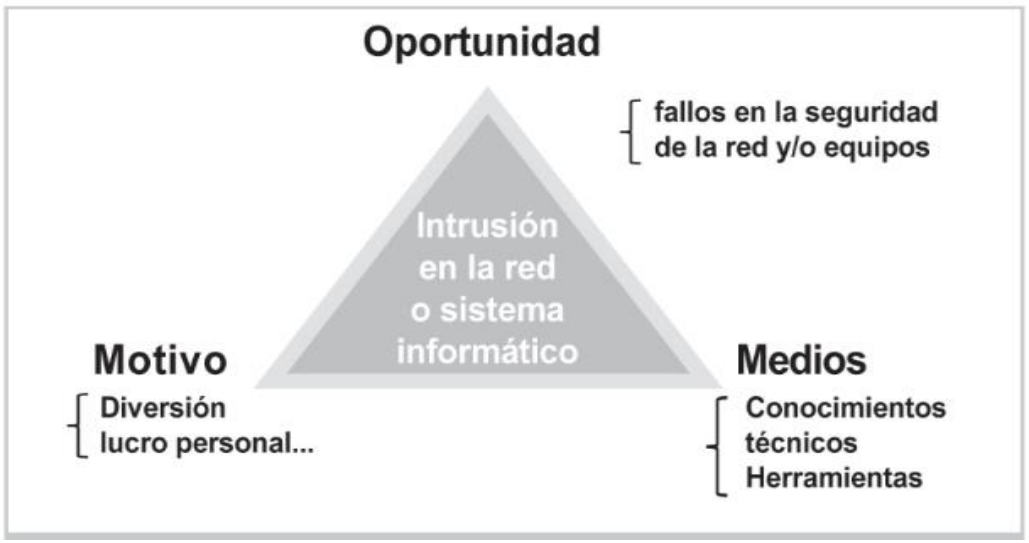


Figura 9. triangulo de la intrusión, (Gómez Vieites, Á. (2010).)

El ataque Smuggling SMTP se basa en las inconsistencias en el manejo de las secuencias de datos por parte de los servidores SMTP entrantes y salientes. En este caso los

atacantes pueden enviar correos electrónicos falsos con direcciones de remitentes manipuladas y eludir las medidas de seguridad. Esta vulnerabilidad es global y puede afectar a servidores SMTP vulnerables en todo el mundo.

Esta técnica fue denominada "Smuggling del Protocolo simple de transferencia de correo (SMTP)" y resalta la importancia de fortalecer las medidas de ciberseguridad para mitigar posibles amenazas.

Los actores de amenazas pueden abusar de servidores SMTP vulnerables en todo el mundo para enviar correos electrónicos maliciosos desde direcciones de correo electrónico falsas. Esto facilita la realización de ataques de phishing dirigidos, donde los mensajes falsificados pueden parecer provenir de remitentes legítimos, evitando las medidas de autenticación como DKIM, DMARC y SPF. (Edigital, 2024).

El Protocolo de Transferencia de Archivos Seguros (SFTP) es un componente crítico para la transferencia segura de datos. Sin embargo, como cualquier otro sistema tecnológico, no está completamente libre de vulnerabilidades. Estas vulnerabilidades ponen a las organizaciones y los archivos confidenciales que transfieren a través de SFTP en riesgo de una violación de datos, incumplimiento normativo o ambos. Esta guía identifica estas vulnerabilidades, presenta las principales amenazas asociadas con transferencias seguras de archivos en general, pero SFTP en particular, y sugiere estrategias de protección efectivas.

Existen tres tipos principales de protocolos de cifrado de correo electrónico que pueden ayudar a satisfacer los requisitos de seguridad anteriores: Protocolo simple de transferencia de correo (SMTP), extensión segura/multipropósito de correo de Internet (S/MIME) y Pretty Good Privacy (PGP). El inconveniente de SMTP es que una persona con privilegios administrativos para los servidores SMTP puede modificar o incluso eliminar el correo electrónico enviado por otras personas a través de los servidores SMTP. (Abdelkader, 2019).

En su núcleo, SFTP ofrece más que solo transferencia segura de datos. También proporciona integridad de comandos y datos, asegurando que los archivos transferidos permanezcan intactos y sin alterar. Esto es crucial para mantener la integridad de los datos, especialmente cuando se trata de información crítica o documentos sensibles. Un IDS es una herramienta de defensa que monitorea la red en busca de posibles accesos no autorizados o ataques. Funciona detectando anomalías y actividades sospechosas que podrían indicar una

violación de seguridad. Al implementar un IDS, las organizaciones pueden detectar y mitigar amenazas en tiempo real, mejorando así la seguridad de sus sistemas SFTP. (Freestone Tim, 2024).

2.2.8. Gestión de la Información.

Para asegurar que se aplican medidas de seguridad proporcionales a la sensibilidad de la información. Se incluyen tres controles:

Clasificación de la información. - Debe clasificarse la información de acuerdo a su sensibilidad y criticidad y su valor para la organización, considerando los criterios de los responsables identificados. Una vez clasificada, deberán establecerse medidas de seguridad apropiadas a cada nivel de seguridad.

Etiquetado de la información. - Los usuarios deberán poder identificar el nivel de seguridad de la información que se está gestionando en cada momento. Una posibilidad, aunque no la única, sería establecer sistemas de marcado de la información, considerando los distintos soportes en que esta pueda encontrarse.

Manipulado de la información. - Deberían establecerse e implantarse procedimientos para el tratamiento de la información, en función de la clasificación que se le haya asignado, generalmente aplicando mecanismos de protección más restrictivos a la información más sensible.

La información secreta de autenticación (por ejemplo, contraseñas) debe custodiarse rigurosamente. Para ello los usuarios deben estar concienciados, firmar compromisos de mantener secreto sobre los mismos y, cuando sea necesario almacenarlos, deberá considerarse la necesidad del uso de mecanismos de cifrado. También se debe tener en cuenta la importancia de modificar la información secreta de autenticación que pudieran incorporar por defecto los nuevos sistemas.

Asegurar los servicios de aplicaciones en redes públicas. Cuando las aplicaciones de la organización están accesibles mediante redes públicas por ejemplo Internet, están sujetas a mayores riesgos que cuando solo están accesibles a través de las redes controladas por la organización. Por ello es necesario considerar medidas de protección adicionales, como el cifrado de las comunicaciones, los mecanismos de autenticación a utilizar, la identificación válida del origen y del destino mediante el uso de certificados, etc. (Gómez Fernández, L. y Fernández Rivero, P. P., 2018).

2.2.9. PGP. (PRETTY GOOD PRIVACE)

Durante mucho tiempo el cifrado, solo ha sido importante en ámbitos concretos tales como gobierno y ejércitos, pero hoy, en la era de la información, la protección de la información que se transmite en todos los ámbitos, es cosa de la criptografía. Cifrados como el RSA proporciona mecanismos que solucionan problemas tales como la distribución de la clave y asegura las comunicaciones. Cuando en 1977 apareció el RSA el proceso de cifrado requería gran potencia informática en comparación con otros procesos tales como el DES. Ese es el motivo por el cual, organismos poderosos como el gobierno de una nación, tenían los suficientes mecanismos para la utilización del RSA en sus comunicaciones. (García, R. D. M., 2009)

El caso más conocido es el del sistema de correo PGP, que emplea "Anillos de Confianza". En estos sistemas, para aceptar la identificación de un nuevo usuario a través de su clave pública se considerará suficiente con que ésta venga firmada por un determinado número de claves válidas (claves privadas) de otros usuarios que forman parte de la red y que se consideran de confianza. (Gómez Vieites, Á., 2015)

Según Atkins et al. (1996), afirma que los principales servicios ofrecidos por PGP incluyen los siguientes:

En PGP, la firma digital se genera al encriptar un hash del mensaje con la clave privada del remitente. El destinatario desencripta este hash usando la clave pública del remitente y lo contrasta con el hash del mensaje recibido para validar su origen e integridad. Las firmas pueden adjuntarse al mensaje o enviarse posteriormente.

Para la confidencialidad se usa una clave de sesión aleatoria para cifrar el mensaje, la clave de sesión se protege con la clave pública del receptor y se envía junto al mensaje cifrado, el receptor desencripta la clave de sesión con su clave privada y posteriormente descifra el mensaje, si existe una firma adjunta, esta y el mensaje se cifran juntos con la clave de sesión antes de la transmisión, este enfoque combina eficiencia y seguridad, asegurando tanto autenticación como protección de datos.

PGP no se basa en certificados emitidos por autoridades de confianza, en su remplazo utiliza un modelo de red de confianza, donde los usuarios pueden crear sus propias claves e intercambiarlas con otros. Los usuarios también pueden firmar y responder por las claves de los demás, creando una red de relaciones de confianza como se muestra en la Figura 10. El

remitente también firma el mensaje con su propia clave privada y el destinatario verifica la firma con la clave pública del remitente. De esta manera, PGP también garantiza tanto la confidencialidad como la autenticidad de la comunicación por correo electrónico (Aidan Dickenson, 2023).

Figura 10. Usos de cifrado PGP. (Panda Security, 2023)

2.2.10. GPG. (GNU PRIVACY GUARD, GnuPG)

(GNU Privacy Guard, GnuPG), desarrollado por Werner Koch, nace a partir del estándar OpenPGP ya mencionado en el punto anterior, con la finalidad de ofrecer un sistema de cifrado y de firma digital gratuito frente a PGP.

Su funcionamiento, al estar basado en OpenPGP, es muy similar al que hemos visto en el apartado anterior, pero al estar pensado como una alternativa de software libre, los algoritmos que se usan en él no están restringidos por patentes. Por ejemplo, mientras que PGP empleaba como algoritmo de cifrado simétrico IDEA, el cual sí requiere licencia de pago en algunos países, GPG opta por otros algoritmos como CAST5, Triple DES, AES o Blowfish para realizar este proceso. (Maillo Fernández, J. A., 2017)

GPG, a.k.a. GnuPG, es una alternativa gratuita y de código abierto para Symantec's patentado PGP. Desarrollado por el Software Libre Fundación, GPG cumple con RFC 4880. Lo que significa que se adhiere al Estándar openPGP y por lo tanto posee la funcionalidad central de PGP. Es compatible con el cifrado de mensajes, autenticación, y verificación de integridad. (Villanueva, John Carl., 2025).

2.2.11. S/MIME.

S/MIME es una tecnología que permite a los usuarios aplicar un algoritmo de cifra asimétrica a sus correos electrónicos para mantener la privacidad de estos, así como poder firmarlo electrónicamente para garantizar la veracidad del autor de los mismos. Su nombre proviene de Secure/Multipurpose Internet Mail Extensions, por sus siglas en inglés, o Extensiones de Correo de Internet de Propósitos Múltiples Seguro en Español. En sus orígenes, S/MIME fue desarrollado por RSA a partir de las especificaciones marcadas por MIME, que fueron desarrolladas entre 1.991 y 1.994 por la IETF (Internet Engineering Task Force) dirigidas al intercambio de archivos de cualquier formato a través de la red. (Maillo Fernández, J. A., 2017).

2.2.11.1. Cifrado.

S/MIME emplea, al igual que se hacía en PGP, un sistema híbrido de cifrado para el contenido de los mensajes. Se genera una clave de sesión aleatoria, que se utilizará con un algoritmo simétrico de cifrado para el texto. Después de cifrará con la clave pública del destinatario mediante un algoritmo asimétrico y se enviarán ambos resultados para que pueda ser descifrado a su llegada.

S/MIME implementa Triple DES como algoritmo de cifra simétrico para la codificación de los mensajes. Además, debe ser compatible con RC2 de 40 bits (aunque se considere inseguro en la actualidad) para mantener la compatibilidad con las versiones anteriores de S/MIME. Con respecto a los algoritmos asimétricos para el cifrado de las claves de sesión, este protocolo implementa Diffie- Hellmann, incorporando además compatibilidad para RSA. (Maillo Fernández, J. A., 2017).

2.2.11.2. Firma Digital.

Para realizar la función resumen del texto o función Hash, S/MIME puede emplear tanto SHA-1 como MD-5. Una vez obtenido el resumen, este se cifra empleando DSS (del inglés, Digital Signature Services), aunque el protocolo también incorpora compatibilidad con RSA para esta tarea. En cuanto a la gestión de las claves, se emplean certificados X.509 v3 para comprobar la confianza de las claves empleadas. S/MIME incluye una serie de certificados raíz, normalmente pertenecientes a entidades de certificación, que se consideran de confianza; cada certificado que se use posteriormente, y haya sido firmado por uno de estos, será considerado como válido de manera automática. (Maillo Fernández, J. A., 2017).

2.2.12. Estándares de cifrado de datos en tránsito.

2.2.12.1. STARTTLS Everywhere.

Los protocolos que intervienen en intercambio de correo electrónico son tres, SMTP, POP y IMAP. Gillula (2018), define que:

El principal objetivo es proporcionarle seguridad a las conexiones de los protocolos antes mencionados, específicamente en el protocolo SMTP utilizando el puerto 465.

La Electronic Frontier Foundation (EFF) lanzó una iniciativa de un proyecto llamado STARTTLS Everywhere, es un complemento a SMTP (Protocolo de Transferencia de Correo Simple). Donde el servidor de correo electrónico remitente le indica al servidor destinario que va enviar un mensaje a través de un canal de comunicación cifrado, el servidor destinatario debe aceptar y negociar para establecer el canal de comunicaciones encriptado para intercambiar correo de forma segura utilizando certificados SSL. Cualquier tipo de interceptación como hombre en el medio (Man in The Middle) solo verá mensajes cifrados, porque el cifrado es de salto a salto o por su nombre en inglés (hop-to-hop).

"Hoy anunciamos el lanzamiento de STARTTLS Everywhere, la iniciativa de EFF para mejorar la seguridad del ecosistema de correo electrónico. Gracias a los esfuerzos anteriores como FEP Vamos Cifrar y Certbot, así como la ayuda de los navegadores web más importantes, hemos visto importantes victorias en el cifrado de la web. Ahora queremos hacer por correo electrónico lo que hemos hecho para la navegación web: hacer que sea simple y fácil para todos ayudar a garantizar que sus comunicaciones no sean vulnerables a la vigilancia masiva".

2.2.12.2. NIST.SP.800-175B

Instituto Nacional de Estándar y Tecnología (NIST), responsable de desarrollar estándares y pautas solicitó sobre SP 800-175B, Guía para el uso de estándares criptográficos en el gobierno federal: Mecanismos criptográficos. Las publicaciones del SP 800-175 están destinadas a ser un reemplazo del SP 800-21, Guía para implementar la criptografía en el gobierno federal, pero con un enfoque en el uso de las ofertas criptográficas actualmente disponibles, en lugar de construir la propia implementación, el SP 800-175B está destinado a proporcionar orientación al Gobierno Federal para el uso de la criptografía y los estándares criptográficos del NIST para proteger la información digitalizada sensible pero no clasificada durante la transmisión y durante el almacenamiento. (Barker, 2016).

2.2.12.3. FIPS - 186

FIPS 186-4 especifica un conjunto de algoritmos que se pueden utilizar para generar una firma digital: DSA, ECDSA y RSA. Esta Norma incluye métodos para la generación de firmas digitales, métodos para la generación de parámetros de dominio (para DSA y ECDSA) y métodos para la generación de pares de claves, y requiere ciertas garantías para el uso de firmas digitales: garantía de validez de parámetros de dominio (DSA y ECDSA), y garantía de validez de clave pública y garantía de posesión de clave privada para los tres algoritmos. (Barker, 2016)

2.2.12.4. FIPS - 140-2

FIPS 140-2 especifica los requisitos que deben cumplir Módulos criptográficos que protegen la información del gobierno de EE. UU. El estándar proporciona cuatro niveles de seguridad crecientes y cualitativos. Los requisitos de seguridad cubren áreas relacionadas con el diseño seguro e implementación de un módulo criptográfico. (Barker, 2016).

2.2.12.5. FIPS - 197

Federal Information Processing Standard 197, Advanced Encryption Standard (AES), noviembre de 2001. FIPS 197 especifica un algoritmo de cifrado de bloque de clave simétrica. El estándar admite tamaños de clave de 128, 192 y 256 bits y un tamaño de bloque de 128 bits. (Barker, 2016).

2.2.13. Cifrado de datos en reposo.

En la aplicación de la criptografía para la protección de datos y ficheros almacenados en un soporte informático, la clave utilizada para el cifrado adquiere el mismo valor que el documento o fichero cifrado. En este caso, la criptografía convierte un secreto de mayor tamaño, el documento o fichero a proteger, en un secreto de menor tamaño, la clave de cifrado que se ha utilizado. Por este motivo, resulta de vital importancia una adecuada conservación de las claves, a fin de evitar su pérdida o que éstas pudieran ser consultadas por personal no autorizado. En la transmisión de datos a través de una red de ordenadores, la pérdida de la clave de cifrado representa un problema menor, ya que siempre se podrán retransmitir los datos cifrados con una nueva clave. Sin embargo, cuando los datos y documentos se almacenan cifrados en un determinado soporte informático, la pérdida de la clave puede provocar que no sea posible recuperar los documentos que hayan sido protegidos mediante dicha clave. Además, convendría evitar que el mismo fichero o documento

protegido se haya guardado sin cifrar en otro soporte informático, ya que en ese caso un atacante podría obtener suficiente información como para tratar de descubrir la clave de cifrado recurriendo a distintas técnicas de criptoanálisis, para posteriormente poder utilizar esa clave para leer otros ficheros y documentos protegidos. (Gómez Vieites, Á., 2015).

2.2.14. Plataformas de protección del correo electrónico.

La colaboración con servicios de terceros y la entrega de soluciones de gestión de detección y respuesta (MDR) están jugando un papel importante en esta transformación. De este modo, las empresas pueden delegar en especialistas la monitorización de amenazas y la respuesta ante incidentes, lo que les permite centrar sus esfuerzos en otras áreas críticas de la seguridad. (Gartner, 2024).

Productos del cuadro comparativo de cuadrante mágico de Gartner 2024, las empresas principales de cifrado de correo electrónico son: CrowdStrike, Microsoft, SentinelOne, Palo Alto Networks, Trend Micro ,Sophos, entre otros, tal como lo muestra la Figura 11.

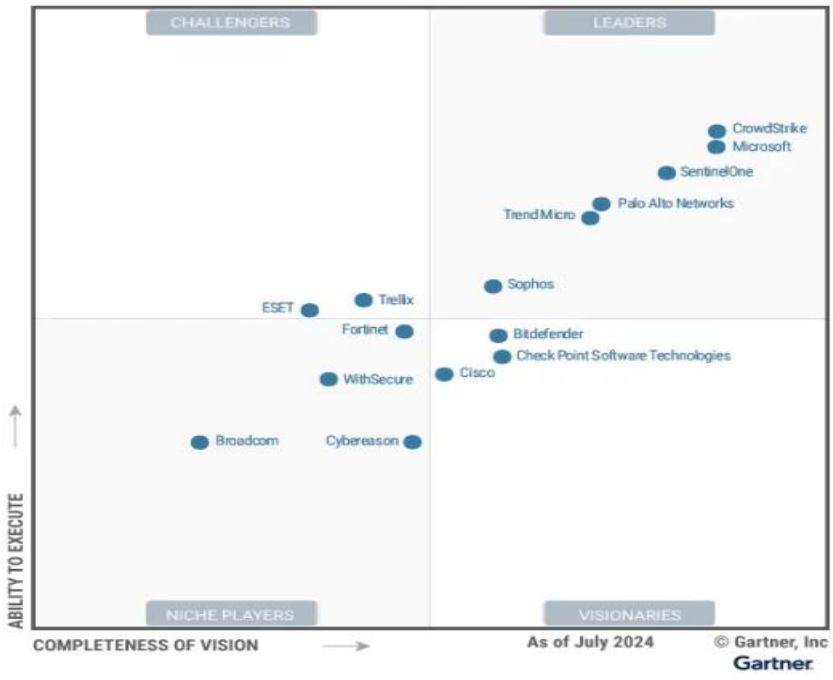


Figura 11. Plataformas de protección del correo electrónico. (Gartner, 2024)

2.2.14.1. CrowdStrike.

Clasificado como Líder, CrowdStrike Falcon se distingue por su capacidad de respuesta a incidentes y su integración con tecnologías de seguridad emergentes. Pese a un incidente reciente que afectó a sus clientes, CrowdStrike mostró una fuerte recuperación y

compromiso con la mejora continua, lo que refuerza su posición en el mercado.

2.2.14.2. Microsoft.

Considerado un Líder, Microsoft Defender for Endpoint se beneficia de su amplia integración con el ecosistema de Microsoft. Su enfoque en la consolidación de herramientas de seguridad y la facilidad de administración le ha permitido ganar una gran cuota de mercado, aunque algunos clientes mencionan desafíos en la gestión de licencias y soporte técnico.

2.2.14.3. SentinelOne.

Otro de los Líderes, SentinelOne se caracteriza por la facilidad de uso de su plataforma Singularity y su enfoque en la integración de EPP con capacidades XDR. Aunque su cuota de mercado sigue creciendo, su presencia geográfica y soporte de idiomas podría mejorar para competir a la par con otros líderes.

2.2.14.4. Palo Alto Networks.

Líder en el cuadrante, su producto Cortex XDR ofrece una sólida protección y capacidades avanzadas de respuesta. Palo Alto Networks ha mejorado su oferta con nuevas funcionalidades y adquisiciones estratégicas. Sin embargo, su precio elevado y la complejidad de configuración pueden ser un reto para algunas organizaciones.

2.2.14.5. Trend Micro.

Líder en el cuadrante, Trend Micro se destaca por su enfoque en la gestión de la superficie de ataque y la integración de XDR. Aunque su enfoque en la protección del endpoint es sólido, su crecimiento en algunos mercados es más lento, y su penetración geográfica fuera de Europa y Japón podría ser mejor.

2.2.14.6. Sophos.

Líder en el cuadrante, Sophos Intercept X destaca por su facilidad de uso y su enfoque en la protección para pequeñas y medianas empresas. Sus mejoras recientes se han centrado en la respuesta a ataques y la protección adaptativa. Sin embargo, su capacidad de personalización es más limitada que la de otros líderes, y su penetración en ciertos mercados verticales es menor.

2.2.15. Perspectiva.

PGP inicialmente fue creado por Phil Zimmerman, y es uno de los métodos de encriptado más robustas que existe hasta la actualidad, en 1992 un grupo de trabajo llamado

PGP con el apoyo de ingeniería de Internet (IEFT) creó la versión de PGP de código abierto para superar barreras de intercambio de llaves que existía hasta entonces. Por otro lado, PGP es la herramienta de encriptado de correo electrónico más difundido. En 2011 la licencia de PGP fue adquirida por la compañía Symantec, por esta razón, nace GnuPG (GPG) es una implantación del estándar PGP y se considera una alternativa sólida al PGP de Symantec. (Fernandez, Asensios et al.,2021)

En cuanto a uso de algoritmos de cifrado son intercambiables entre ambas opciones, tanto como en licenciado y de código libre. En la actualidad mayoría de los programas hacen uso de PGP, que admite el envío seguro de archivos e información en general por correo electrónico, ofreciendo también la firma del mensaje con la llave del emisor, además, PGP proporciona una gran cantidad de compatibilidad entre distintas plataformas porque es un estándar. (Fernandez, Asensios et al.,2021)

En la actualidad, un equipo tradicional de escritorio estándar tardaría muchos billones de años en desencriptar un certificado SSL RSA de 2048 bits. Esto implica que, si se comenzó a desencriptar ese certificado en el momento del Big Bang, aún no se terminaría antes del fin del universo. El algoritmo RSA de 2048 bits se usa comúnmente como un estándar para PGP.

Gnu Privacy Guard utiliza el algoritmo AES de forma predeterminada. AES es uno de los algoritmos de encriptado más potentes disponibles para el público. Como indicador, el gobierno de los Estados Unidos especifica algo como de alto secreto, lleva encriptación AES-256. Y es lo suficientemente robusto para las agencias de seguridad nacional y el gobierno, es lo suficientemente robusto y confiable para nosotros. (DIGICERT, 2020).

2.2.16. Aporte académico.

Esta tesis examina la facilidad de uso del software de cifrado PGP, el cual brinda a los usuarios dos funciones criptográficas esenciales: el cifrado y descifrado de archivos para preservar la privacidad, y la protección de archivos mediante encriptación para un almacenamiento seguro. PGP utiliza criptografía asimétrica, también conocida como criptografía de clave pública, donde cada usuario dispone de un par de claves: una clave pública, que puede compartirse libremente con cualquier persona con la que se desee intercambiar información de manera segura, y una clave privada, que debe mantenerse confidencial y solo ser conocida por su propietario. Cuando un archivo se cifra con la clave

pública de un destinatario, únicamente esa persona podrá descifrarlo empleando su clave privada.

De este modo, para enviar un mensaje seguro, el remitente obtiene la clave pública del destinatario y la utiliza para cifrar el mensaje, garantizando que solo el destinatario designado pueda acceder al contenido protegido, adicional se implementará nuevos esquemas de administración de claves públicas para sistemas de archivos criptográficos que serán almacenados en la nube de acceso público. Este trabajo académico explora dominios interrelacionados: técnicas criptográficas, almacenamiento de información y modelos de distribución segura, proponiendo un marco de bajo coste y alta efectividad para la protección de datos críticos en entornos corporativos.

CAPITULO III

3. MARCO METODOLÓGICO

La protección de comunicaciones electrónicas mediante PGP (Pretty Good Privacy) se fundamenta en estándares criptográficos como OpenPGP, que establecen protocolos para garantizar la confidencialidad, integridad y autenticidad de los mensajes. Este marco metodológico se alinea con la normativa de la Superintendencia de Economía Popular y Solidaria SEPS, bajo su Resolución SEPS-IGS- IGT-IGJ-INGINT-INTICINSESF-INR-DNSI 2022-002 y se integra en sistemas de gestión de seguridad de la información (SGSI), como ISO/IEC 27001, para mitigar riesgos asociados a la exposición de datos sensibles, basados en los componentes claves que son:

- **Estándar OpenPGP:** Que define algoritmos asimétricos (RSA, ECC) y simétricos (AES-256), combinados en un enfoque híbrido para optimizar seguridad y rendimiento.
- **Gestión de Ciclo de Vida de Claves:** La generación segura de claves se la realiza mediante el uso de HSM (Hardware Security Modules) para crear claves con entropía certificada, la renovación de claves se las debe aplicar cada 90-180 días en roles críticos (ej. Gerencia, Contabilidad, Tecnología) y su revocación se las debe realizar mediante listas de revocación (CRL).
- **Procesos de Cifrado y Firma:** Se debe aplicar un cifrado hibrido basado en la generación de una clave de sesión aleatoria (AES) para cifrar el mensaje, una clave pública del destinatario para cifrar la clave de sesión y una firma digital aplicando el hash del mensaje (SHA-512) cifrado con la clave privada del remitente, validando autenticidad e integridad.
- **Integración con Infraestructura Existente:** Debe existir compatibilidad con clientes de correo existentes (Thunderbird, Outlook) mediante plugins como Gpg4win o Enigmail.
- **Cumplimiento normativo:** Alineación con la normativa SEPS-IGS- IGT-IGJ-INGINT-INTICINSESF-INR-DNSI 2022-002 y Leyes de Protección de Datos Personales.
- **Reducción de riesgos:** Mitiga amenazas como phishing, Man-in-the-Middle y fugas de datos, disminuyendo costos asociados a brechas (promedio: $3.9 millones por

incidente, IBM 2023).

- **Confianza institucional:** Aseguramiento de comunicaciones con clientes, socios y reguladores, reforzando reputación corporativa.

3.1 Descripción del área de estudio.

La propuesta contempla la implementación de un mecanismo de cifrado asimétrico se lo aplico dentro de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda. en su oficina matriz, con operaciones en Imbabura, parte de Carchi y Pichincha, se enfrentó el reto de proteger la información sensible que maneja en sus procesos de intermediación financiera y no financiera. Con una estructura organizacional compuesta por 8 directivos, una gerente y 30 empleados, la cooperativa administra datos críticos de más de 5,000 socios, lo que la convierte en un objetivo relevante frente a amenazas cibernéticas como el phishing, la interceptación de correos electrónicos y la fuga de información.

El área de estudio se orienta a fortalecer la seguridad de la información institucional, alineándose con los requerimientos normativos de la Superintendencia de Economía Popular y Solidaria (SEPS) y la Ley Orgánica de Protección de Datos Personales. El objetivo principal es implementar un mecanismo de cifrado basado en PGP (Pretty Good Privacy) para los correos electrónicos, asegurando la confidencialidad, integridad y autenticidad de las comunicaciones internas y externas de la cooperativa.

La implementación del cifrado PGP no solo responde a la necesidad de cumplimiento normativo, sino que también contribuye a la reducción significativa de riesgos operativos y reputacionales. Al asegurar que los datos transmitidos por correo electrónico estén protegidos contra accesos no autorizados y ataques de intermediarios, la cooperativa fortalece su posición institucional y la confianza de sus socios en un entorno cada vez más digitalizado.

3.2 Enfoque y tipo de investigación.

Tipo de investigación según su enfoque:

La investigación propuesta, basada en un enfoque cualitativo y respaldada por Santander Open Academy (2024), aborda la seguridad en correos electrónicos mediante cifrado. A continuación, se analiza su alineación con estándares criptográficos y metodologías de gestión de riesgos.

De manera específica, la identificación de activos se realizó utilizando un enfoque

cualitativo mediante la aplicación de una encuesta, adicionalmente la definición de riesgos, actividades de mitigación y la integración del mecanismo de cifrado en los protocolos SMTP y SFTP, aplicando la técnica del juicio de expertos.

Investigación Aplicada

La investigación aplicada es una forma no sistemática de encontrar soluciones a problemas o cuestiones específicas. Estos problemas o cuestiones pueden ser a nivel individual, grupal o social. Se llama «no sistemática» porque va directamente a buscar soluciones, suele llamarse «proceso científico» porque utiliza las herramientas científicas disponibles y las pone en práctica para encontrar respuestas. (Ortega Cristina, 2025).

Además, Este proyecto se lo considera como una investigación aplicada en razón de que, con la identificación de las vulnerabilidades en los activos de la Cooperativa, se buscó soluciones de mejora para que los riesgos puedan minimizarse y recomendar técnicamente soluciones para mejorar la ciberseguridad de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

Grupo de Estudio

En el contexto de la normativa emitida por la Superintendencia de Economía Popular y Solidaria (SEPS) en Ecuador, las entidades financieras del sector popular y solidario deben implementar rigurosas medidas de seguridad de la información en sus canales electrónicos, en este sentido el mecanismo de cifrado asimétrico fue adaptado a la infraestructura tecnológica actual, la gestión segura de claves públicas y privadas, y la capacitación del personal en el uso de herramientas PGP y buenas prácticas de ciberseguridad, concretamente esto se enfocó en las áreas administrativas, Gerencia, Contabilidad, Tesorería, Talento Humano, Tecnología de la Información, Seguridad de la Información, Riesgos, Captaciones, Control Interno , Crédito y Auditoría Interna. Este enfoque permitirá proteger la información crítica que circula por correo electrónico, especialmente en procesos como la gestión de créditos, reportes contables y comunicaciones estratégicas, protegiendo la integridad, confidencialidad y disponibilidad de los datos de los usuarios mediante protocolos criptográficos robustos que cifren la información en tránsito y en reposo, siguiendo estándares internacionales y buenas prácticas reconocidas.

Además, se requiere que las entidades utilicen algoritmos y certificados digitales seguros para garantizar la autenticidad y no repudio en las operaciones financieras realizadas

a través de canales electrónicos, incluyendo el uso de técnicas de cifrado como las que provee PGP para proteger correos electrónicos y documentos sensibles. (ITahora, 2022).

3.3 Procedimiento de investigación.

El servicio de correo electrónico, del cual dependen las comunicaciones tanto internas con los usuarios de la Cooperativa como externas con los socios de negocio, proveedores y clientes, posee características de seguridad de la información básicas. Ello se debe a que, a diferencia de un servicio de correo electrónico interno, en el cual la mayor cantidad de tráfico de la información pasa a través de la red privada, un servicio de correo electrónico basado en Cloud como cPanel, donde envía todo el tráfico de su servicio a través de internet. Debido a la naturaleza de esta tecnología, de la cual no se duda que traiga muchos más beneficios, existe un riesgo intrínseco toda vez que la comunicación y el flujo de datos de los mensajes de correo electrónico se realizan a través de internet.

En respuesta a esta problemática identificada, se plantea tres fases de desarrollo, mismas que enmarcan el alcance para este trabajo de grado:

1. **Identificación de activos de información críticos**

En primera instancia se realizará la investigación de todo el contexto del cifrado asimétrico y su vínculo con el estándar PGP, con la finalidad de poder ir interpretando el diseño del mecanismo a seleccionar para el cifrado posterior. Luego a través de la metodología MAGERIT se realizará un levantamiento de activos de información que serán clasificados de acuerdo a su criticidad para poder tener un listado de que documentos requieren cifrado para su envío ya sea por medio SFTP o SMTP, contemplando lo mencionado en la Resolución emitida por la Superintendencia de Economía Popular y Solidaria (2022-002), dentro del apartado cifrado del anexo 1-Controles obligatorios de seguridad de la información.

2. **Selección de una metodología asimétrica de cifrado**

Luego se analizó la herramienta con la que se cifrará la información utilizando el estándar PGP, y una vez establecido la herramienta se procedió a la generación de las claves tanto públicas como privadas para ser gestionadas por parte de los usuarios.

La selección de una metodología de cifrado para proteger la información, en este caso utilizando el estándar PGP, requirió de un análisis cuidadoso tanto de la herramienta como de los procesos asociados. PGP, basado en criptografía asimétrica, permite la

generación y gestión de pares de claves públicas y privadas que garantizan la confidencialidad, autenticidad e integridad de los datos. La elección de esta metodología respondió a la necesidad de implementar un sistema robusto que asegure la protección de la información en entornos donde la seguridad es crítica, como en entidades financieras.

Una vez seleccionada la herramienta PGP, el siguiente paso fue la generación de las claves criptográficas, que fueron gestionadas por los usuarios responsables de cifrar y descifrar la información. Este proceso consideró aspectos como la correcta administración de las claves, políticas de rotación, almacenamiento seguro y revocación en caso de compromisos. Además, la metodología se integró dentro de un marco de gestión de riesgos y supervisión continua, alineado con estándares internacionales y mejores prácticas, para garantizar la efectividad del cifrado y la mitigación de posibles vulnerabilidades.

3. Implementación de un mecanismo de cifrado PGP

La selección de una metodología de cifrado adecuada para la Cooperativa consideró la automatización del proceso de cifrado de la información crítica, utilizando el estándar PGP para garantizar la seguridad en la transmisión de datos sensibles. Una vez generado el par de claves públicas y privadas, se implementó un mecanismo que permitió enviar la información cifrada de forma segura, minimizando riesgos de interceptación o fuga de datos, especialmente ante ataques Man-in-the-Middle, comunes en protocolos como SMTP y SFTP.

Este enfoque es fundamental dado que, según datos de la Superintendencia de Economía Popular y Solidaria (SEPS), muchas cooperativas cuentan con infraestructura tecnológica básica y acceso a internet, pero enfrentan limitaciones en la adopción de tecnologías avanzadas por factores como costos y cobertura. Por ello, la automatización del cifrado con PGP no solo fortalece la confidencialidad y autenticidad de las comunicaciones, sino que también se adapta a las capacidades tecnológicas existentes en el sector.

La metodología seleccionada se integró en todas las áreas de la Cooperativa, garantizando la protección continua de la información financiera y operativa reportada a la SEPS. Además, se contempló la gestión segura de claves, políticas de rotación y revocación, y la capacitación de usuarios para asegurar una correcta implementación y uso. Así, la Cooperativa pudo cumplir con los requerimientos regulatorios y mejoró la confianza de sus socios mediante la protección efectiva de sus datos críticos.

3.4 Consideraciones Bioéticas.

En el marco de esta investigación, se llevaron a cabo entrevistas con el personal de la Cooperativa, siguiendo un protocolo riguroso. En primera instancia, se informó a los jefes de área sobre la naturaleza y objetivos del estudio, a fin de obtener su consentimiento y colaboración. Posteriormente, se comunicó a los participantes que la información suministrada sería tratada con la máxima confidencialidad y bajo estricta observancia de la normativa vigente en materia de protección de datos personales, garantizando que no se divulgaría ni se emplearía de manera indebida o contraria a los fines establecidos. Durante todo el desarrollo del estudio se observaron rigurosamente los principios éticos y las disposiciones legales aplicables, asegurando un manejo responsable y respetuoso de la información y del personal involucrado, tal como se puede evidenciar en el apartado de ANEXOS en donde se visualiza la solicitud de autorización para ejecución del proyecto de investigación (Anexo 1) y el respectivo documento de autorización por parte de la Gerente General de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda. para poder acceder a la información interna y poder ejecutar la investigación (Anexo 2), así como los resultados de las encuestas realizadas a los empleados como se evidencia en las preguntas ejecutadas (Anexo 3 al Anexo 12).

CAPITULO IV

4. RESULTADOS.

4.1 Identificación de activos de información de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda.

En esta etapa se centralizo en la identificación y valoración de los activos de información, constituyendo la base fundamental para el posterior análisis de amenazas, vulnerabilidades y riesgos, en el contexto de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., la Fase 1 inicia con la delimitación del alcance del análisis, identificando los sistemas, procesos y áreas críticas relacionadas con la intermediación financiera y no financiera. Este proceso involucra la elaboración de un inventario exhaustivo de activos de información, que incluye no solo los datos digitales (bases de datos, correos electrónicos, archivos electrónicos), sino también los soportes físicos (documentos impresos, contratos, registros contables), los recursos tecnológicos (servidores, estaciones de trabajo, dispositivos de red), y los recursos humanos (usuarios, administradores y directivos).

La identificación de activos se realiza a través de entrevistas y revisión documental, involucrando a los responsables de cada área funcional. Cada activo es catalogado según su naturaleza, localización, propietario y función dentro de los procesos críticos de la cooperativa. Posteriormente, se procede a la valoración de los activos, evaluando su importancia de acuerdo con los criterios definidos por MAGERIT.

Esta valoración permite priorizar los activos según el impacto que tendría su pérdida, alteración o divulgación no autorizada en la operatividad y reputación de la cooperativa. Por ejemplo, la base de datos de socios, los sistemas de gestión financiera y los correos electrónicos institucionales suelen ser catalogados como activos de máxima criticidad, dado que su compromiso podría derivar en sanciones regulatorias, pérdidas económicas y daños a la confianza de los socios.

Durante esta fase, es fundamental documentar las relaciones de dependencia entre activos, identificando cuáles son esenciales para la continuidad de los servicios y cuáles pueden representar puntos únicos de fallo. La correcta identificación y valoración de los activos de información sienta las bases para el análisis de amenazas y vulnerabilidades en fases posteriores, permitiendo a la organización enfocar sus recursos en la protección de los elementos más sensibles y estratégicos.

En esta etapa, se aplica lo mencionado en el método de análisis de riesgo de la metodología MAGERIT, según se muestra a continuación:

4.1.1 MAR – Método de Análisis de Riesgos

MAR.1 – Caracterización de los activos

- MAR.11 – Identificación de los activos
- MAR.12 – Dependencias entre activos
- MAR.13 – Valoración de los activos

MAR.2 – Caracterización de las amenazas

- MAR.21 – Identificación de las amenazas
- MAR.22 – Valoración de las amenazas

MAR.3 – Caracterización de las salvaguardas

- MAR.31 – Identificación de las salvaguardas pertinentes
- MAR.32 – Valoración de las salvaguardas

MAR.4 – Estimación del estado de riesgo

- MAR.41 – Estimación del impacto
- MAR.42 – Estimación del riesgo

MAR 11. Identificación de los activos

La identificación y clasificación de activos permitiendo entender el valor del activo dentro de la Cooperativa y el nivel de protección necesario. Los activos más sensibles se clasificaron como restringidos o confidenciales, indicando un mayor nivel de protección requerido.

Código	**Activo**	**Área**	**Descripción**	**Propietario**	**Clasificación Uso**
A1	Documentos estratégicos	Gerencia	Planes, actas, reportes	Gerente General	Restringido
A2	Libros contables	Contabilidad	Registros contables	Contador	Confidencial

Código	Activo	Área	Descripción	Propietario	Clasificación Uso
A3	Comprobantes y registros	Tesorería	Recibos, transferencias	Jefe de Tesorería	Confidencial
A4	Expedientes de personal	Talento Humano	Contratos, evaluaciones	Jefe de RRHH	Restringido
A5	Servidores y respaldos	Tecnología de la Información	Hardware, software, respaldos	Administrador de TI	Uso interno
A6	Políticas y procedimientos	Seguridad de la Información	Manuales, protocolos	Responsable Seguridad	Uso interno
A7	Matriz de riesgos	Riesgos	Identificación y evaluación	Analista de Riesgos	Confidencial
A8	Base de datos captaciones	Captaciones	Información financiera	Jefe de Captaciones	Confidencial
A9	Informes de control	Control Interno	Reportes de auditoría y cumplimiento	Responsable Control Int	Uso interno
A10	Expedientes de crédito	Crédito	Solicitudes y análisis crediticio	Jefe de Crédito	Confidencial

Código	Activo	Área	Descripción	Propietario	Clasificación Uso
A11	Informes de auditoría	Auditoría Interna	Resultados de auditorías	Auditor Interno	Confidencial

Tabla 2. Identificación de activos (Fuente Propia)

MAR 12. Dependencias entre activos

- Los activos tecnológicos (A5) son soporte crítico de la mayoría de los activos informativos y de control.
- Documentos estratégicos (A1) dependen del correcto funcionamiento de los servidores y backups (A5).
- Informes de control y auditoría (A9, A11) dependen de la integridad de los libros contables, expedientes y bases de datos (A2, A4, A8).

MAR 13. Valoración de los activos

Según la metodología MAGERIT versión 3.0, la valoración de activos debe considerar varias dimensiones de análisis para evaluar su importancia y el impacto que una amenaza podría causar al materializarse. Las dimensiones clave incluyen:

- Confidencialidad (C)
- Integridad (I)
- Disponibilidad (D)
- Autenticidad (A)
- Trazabilidad del uso (TU)
- Trazabilidad de acceso (TA)

Código	C	I	D	A	TU	TA
A1	A	A	M	A	M	M
A2	A	A	A	M	B	B

Código	C	I	D	A	TU	TA
A3	A	M	A	B	B	B
A4	A	A	M	A	M	M
A5	A	A	A	M	M	M
A6	A	A	M	M	M	M
A7	A	A	M	B	M	M
A8	A	A	A	M	B	B
A9	A	A	M	B	B	B
A10	A	A	M	M	B	B
A11	A	A	M	B	B	B

Tabla 3. Valoración de los activos (Fuente Propia)

Para cada activo se establece una valoración en cada dimensión mediante una escala común (por ejemplo: 0 a 10 o categorías como Muy Bajo a Muy Alto), que mide el daño potencial a la organización si el activo se ve afectado en esa dimensión.

MAR.21 – Identificación de las amenazas

Se identificó de manera sistemática las amenazas relevantes que pueden afectar a los activos de información de la organización. Esta etapa implica caracterizar las amenazas

considerando su naturaleza, origen y posible efecto sobre los activos.

A partir de la información analizada para Uniotavalo Ltda., se presenta la identificación de amenazas para cada activo, siguiendo la estructura recomendada en MAGERIT 3.0:

Código	**Amenaza**	**Activos Relacionados**	**Descripción**	**Probabilidad**
T1	Acceso no autorizado	A1, A4, A8	Usuarios no autorizados acceden a información sensible	Media
T2	Filtración de datos	A1, A11	Divulgación inapropiada de datos o documentos	Media
T3	Manipulación o fraude	A2, A3, A10	Cambios intencionados en registros contables o pagos	Baja
T4	Robo de identidad	A4	Uso ilícito de datos personales para suplantación	Alta
T5	Malware y fallas técnicas	A5	Infección, ataques o fallos en sistemas y servidores	Media
T6	Modificaciones no autorizadas	A6	Cambios ilegítimos en políticas, protocolos o documentos	Media
T7	Errores en la matriz de riesgos	A7	Evaluaciones incorrectas que afectan la gestión del riesgo	Baja
T8	Robo y acceso indebido a base datos	A8	Acceso y exfiltración de datos sensibles	Media

Código	Amenaza	Activos Relacionados	Descripción	Probabilidad
T9	Manipulación de informes	A9, A11	Alteración de reportes y resultados de auditorías	Baja

Tabla 4. Identificación de las amenazas (Fuente Propia)

MAR.22 – Valoración de las amenazas

La valoración de las amenazas dentro de la metodología MAGERIT versión 3.0 (MAR.22) consiste en asignar una calificación basada en la probabilidad de que la amenaza se materialice y el impacto que tendría sobre los activos afectados. Este análisis es fundamental para priorizar adecuadamente los riesgos y determinar las salvaguardas necesarias.

A continuación, se muestra la aplicación de MAR.22 con valoración cualitativa de amenazas para la organización Uniotavalo Ltda., considerando las amenazas previamente identificadas (MAR.21):

Código	Amenaza	Activos Relacionados	Probabilidad (P)	Impacto (I)	Valoración Riesgo (P x I)	Comentarios
T1	Acceso no autorizado	A1, A4, A8	Media (M)	Alto (A)	Alto	Amenaza frecuente con impacto alto en confidencialidad
T2	Filtración de datos	A1, A11	Media (M)	Alto (A)	Alto	Riesgo relevante para información sensible

Código	Amenaza	Activos Relacionados	Probabilidad (P)	Impacto (I)	Valoración Riesgo (P x I)	Comentarios
T3	Manipulación o fraude	A2, A3, A10	Baja (B)	Medio (M)	Medio	Control presente reduce probabilidad
T4	Robo de identidad	A4	Alta (A)	Muy Alto (MA)	Muy Alto	Alta prioridad para datos personales
T5	Malware y fallas técnicas	A5	Media (M)	Alto (A)	Alto	Riesgo operativo elevado
T6	Modificaciones no autorizadas	A6	Media (M)	Medio (M)	Medio	Impacto más controlable con buenas salvaguardas
T7	Errores en matriz de riesgos	A7	Baja (B)	Medio (M)	Medio	Impacto bajo moderado, revisiones periódicas son clave
T8	Robo y acceso indebido	A8	Media (M)	Alto (A)	Alto	Riesgo significativo para información financiera

Código	Amenaza	Activos Relacionados	Probabilidad (P)	Impacto (I)	Valoración Riesgo (P x I)	Comentarios
T9	Manipulación de informes	A9, A11	Baja (B)	Medio (M)	Medio	Controles estrictos mitigando amenaza

Tabla 5. Valoración de las amenazas (Fuente Propia)

MAR.31 – Identificación de las salvaguardas pertinentes

El objetivo fue elegir salvaguardas que contrarresten eficazmente las amenazas, considerando tipo (preventivas [PR], disuasorias [DR], eliminatorias [EL], minimizadoras [IM], correctivas [CR], recuperativas [RC], de monitorización [MN], de detección [DC], de concienciación [AW], administrativas [AD]), con aplicabilidad al activo y amenaza, y balance costo-beneficio.

Para Uniotavalo Ltda., con base en las amenazas y activos identificados, se asignan las siguientes salvaguardas pertinentes:

Código amenaza	Amenaza	Salvaguardas Pertinentes	Tipo de protección
T1	Acceso no autorizado	Control de accesos, autenticación fuerte, gestión de identidades	Preventivas, Disuasorias
T2	Filtración de datos	Cifrado de datos y comunicaciones, clasificación de información	Preventivas, Minimizadoras
T3	Manipulación o fraude	Sistemas de autorización, auditorías, segregación de funciones	Preventivas, Correctivas

Código amenaza	Amenaza	Salvaguardas Pertinentes	Tipo de protección
T4	Robo de identidad	Políticas estrictas de protección de datos personales, capacitación, cifrado	Preventivas, Administrativas
T5	Malware y fallas técnicas	Antimalware, parches de seguridad, backups periódicos	Preventivas, Recuperativas
T6	Modificaciones no autorizadas	Gestión de cambios, control de versiones, seguimiento de auditoría	Preventivas, Detectivas
T7	Errores en matriz de riesgos	Revisiones periódicas, doble verificación	Correctivas, Administrativas
T8	Robo y acceso indebido	Autenticación multifactor, monitoreo continuo	Preventivas, Detectivas
T9	Manipulación de informes	Control documental, firmas digitales	Preventivas, Correctivas

Tabla 6. Identificación de las salvaguardas pertinentes (Fuente Propia)

MAR.32 – Valoración de las salvaguardas

Consistió en evaluar la eficacia de las salvaguardas identificadas para mitigar las amenazas que afectan a los activos. Esta valoración considera:

La capacidad de la salvaguarda para reducir el impacto (eficacia frente al impacto, e_i).

La capacidad para reducir la probabilidad (eficacia frente a la probabilidad, e_f)

El grado de implantación, calidad y formación sobre la salvaguarda.

La existencia de procedimientos de revisión y control de efectividad.

La eficacia total *e* de una salvaguarda o paquete de salvaguardas se calcula como:

$e = 1 – (1 - e_i) \times (1 - e_f)$

Donde e_i y e_f *varían entre 0 (sin eficacia) y 1 (total eficacia).*

Aplicando esta valoración a las salvaguardas del caso Uniotavalo Ltda., se asignan valores cualitativos estimados para cada salvaguarda contra su amenaza correspondiente:

Amenaza	**Salvaguarda**	**Eficacia Impacto** e_i	**Eficacia Probabilidad** e_f	**Eficacia Total** e	**Comentarios**
T1	Control de accesos, autenticación	0.8	0.7	0.94	Salvaguardas bien implantadas
T2	Cifrado y clasificación de datos	0.85	0.6	0.94	Adecuada protección en comunicaciones
T3	Sistemas de autorización, auditoría	0.7	0.5	0.85	Eficaz, pero faltan controles puntuales
T4	Políticas, capacitación, cifrado	0.75	0.65	0.91	Requiere mejora en concienciación
T5	Antimalware y backups	0.9	0.6	0.96	Alta eficacia técnica
T6	Gestión de cambios, auditorías	0.65	0.55	0.82	Salvaguardas parcialmente implantadas

T7	Revisiones periódicas y doble check	0.6	0.4	0.76	Mejorable con automatización
T8	Autenticación multifactor, monitoreo	0.85	0.7	0.96	Salvaguardas adecuadas
T9	Control documental y firma digital	0.7	0.5	0.85	Sólidas pero deben perfeccionarse

Tabla 7. Valoración de las salvaguardas (Fuente Propia)

MAR.41 – Estimación del impacto

Consistió en determinar la magnitud del daño o perjuicio que implicaría para un activo la materialización de una amenaza. Se puede usar una tabla que relacione la degradación sufrida por el activo y el valor del mismo en una escala cualitativa como Muy Bajo (MB), Bajo (B), Medio (M), Alto (A) y Muy Alto (MA).

Considerando la degradación y valoración de cada activo, se asigna la siguiente estimación de impacto para Uniotavalo Ltda.:

Código	**Activo**	**Valoración Uso**	**Degradación (%)**	**Estimación Impacto (MB/B/M/A/MA)**	**Comentarios**
A1	Documentos estratégicos	Restringido	70	Alto (A)	Información crítica para la gestión
A2	Libros contables	Confidencial	55	Medio (M)	Alta disponibilidad y precisión requerida

Código	Activo	Valoración Uso	Degradación (%)	Estimación Impacto (MB/B/M/A/MA)	Comentarios
A3	Comprobantes y registros	Confidencial	65	Alto (A)	Impacto financiero y operativo
A4	Expedientes de personal	Restringido	85	Muy Alto (MA)	Datos altamente sensibles y legales
A5	Servidores y respaldos	Uso interno	75	Alto (A)	Soporte crítico TI
A6	Políticas y procedimientos	Uso interno	50	Medio (M)	Afecta gestión y cumplimiento
A7	Matriz de riesgos	Confidencial	30	Bajo (B)	Evaluación de riesgos con impacto bajo
A8	Base datos captaciones	Confidencial	70	Alto (A)	Información financiera sensible
A9	Informes de control	Uso interno	30	Bajo (B)	Acceso controlado por perfiles

Código	Activo	Valoración Uso	Degradación (%)	Estimación Impacto (MB/B/M/A/MA)	Comentarios
A10	Expedientes de crédito	Confidencial	65	Alto (A)	Impacto financiero y riesgo crédito
A11	Informes auditoría	Confidencial	30	Bajo (B)	Información de auditoría

Tabla 8. Estimación del impacto (Fuente Propia)

Esta estimación de impacto refleja la gravedad potencial del daño para la organización, útil para priorizar riesgos y definir medidas de protección según criterios claros y estandarizados

MAR.42 – Estimación del riesgo

Se basa en combinar la estimación del impacto del activo afectado y la probabilidad de que la amenaza suceda, ajustando por la eficacia de las salvaguardas existentes. Se busca calcular el riesgo residual real al que está expuesta la organización.

Para la organización Uniotavalo Ltda., se calcula la estimación del riesgo residual para cada activo y su amenaza asociada según:

Riesgo = (1 – *e*) x Impacto x Probabilidad

Donde *e* es la eficacia total de las salvaguardas (de 0 a 1).

Se utiliza la siguiente tabla para asignar valores numéricos a probabilidad e impacto cualitativos:

Nivel Cualitativo	Valor Numérico
Muy Bajo (MB)	0.1

Nivel Cualitativo	Valor Numérico
Bajo (B)	0.3
Medio (M)	0.6
Alto (A)	0.9
Muy Alto (MA)	1.0

Tabla 9. Estimación del riesgo (Fuente Propia)

Se aplican los valores para cada activo y amenaza, con la eficacia de salvaguardas ya asignada.

Ejemplo resumido para activo A4 (Expedientes de personal) y amenaza T4 (Robo de identidad):

Impacto: Muy Alto (1.0)

Probabilidad: Alta (0.9)

Eficacia total salvaguardas: 0.91

Cálculo:

R = (1 – 0.91) x 1.0 x 0.9 = 0.081

La tabla completa simplificada:

Activo	Amenaza	Impacto (num)	Probabilidad (num)	Eficacia total (e)	Riesgo Residual = (1-e)*I*P
A1	T1	0.9	0.6	0.94	0.0324

Activo	Amenaza	Impacto (num)	Probabilidad (num)	Eficacia total (e)	Riesgo Residual = (1-e)*I*P
A1	T2	0.9	0.6	0.94	0.0324
A2	T3	0.6	0.3	0.85	0.027
A4	T4	1.0	0.9	0.91	0.081
A5	T5	0.9	0.6	0.96	0.0216
A6	T6	0.6	0.6	0.82	0.0648
A7	T7	0.3	0.3	0.76	0.0216
A8	T8	0.9	0.6	0.96	0.0216
A9	T9	0.6	0.3	0.85	0.027

Tabla 10. Valores para cada activo y amenaza. (Fuente Propia)

Estos valores muestran que el riesgo residual más alto es para el activo A4 frente a la amenaza T4, indicando que, aunque las salvaguardas son bastante efectivas, el riesgo sigue siendo notable y requiere atención continua. Otros riesgos son significativamente menores, reflejando el efecto protector de las salvaguardas implantadas.

Este cálculo permite a la Cooperativa entender la exposición real y orientar adecuadamente recursos y esfuerzos para reducir el riesgo a niveles aceptables usando la metodología MAGERIT.

4. Priorización y Documentación

Finalmente, los activos se priorizaron según el impacto potencial de su pérdida, alteración o divulgación. Se documentó la información en matrices, facilitando la visualización de los activos críticos y las relaciones entre ellos. Este inventario y valoración servirán de base para las siguientes fases de MAGERIT, donde se analizarán amenazas, vulnerabilidades y se definirán controles de seguridad adecuados.

Área	**Activo de Información**	**Descripción**	**Propietario/Responsable**	**Ubicación**	**Valoración (Conf/Int/Disp3)**	**Observaciones**
Gerencia	Documentos estratégicos	Planes, actas de reuniones, reportes de gestión	Gerente General	Oficina de gerencia	Alta/Alta/Media	Acceso restringido
Contabilidad	Libros contables	Registros de ingresos, egresos y balances	Contador	Oficina de contabilidad	Alta/Alta/Alta	Copias de seguridad diarias
Tesorería	Comprobantes y registros de pago	Recibos, transferencias, movimientos bancarios	Jefe de Tesorería	Oficina de tesorería	Alta/Media/Alta	Respaldo mensual
Talento Humano	Expedientes de personal	Contratos, evaluaciones, datos personales	Jefe de RRHH	Archivo físico/digital	Alta/Alta/Media	Confidencialidad estricta
Tecnología de la Información	Servidores y respaldos	Hardware, software y copias de seguridad	Administrador de TI	Sala de servidores	Alta/Alta/Alta	Monitoreo permanente
Seguridad de la Información	Políticas y procedimientos	Manuales, protocolos y registros de incidentes	Responsable de Seguridad	Oficina de seguridad	Alta/Alta/Media	Actualización periódica

[3] **Conf**: Confidencial
Int: Integridad
Disp: Disponibilidad

Riesgos	Matriz de riesgos	Identificación y evaluación de riesgos	Analista de Riesgos	Oficina de riesgos	Alta/Alta/Media	Revisión trimestral
Captaciones	Base de datos de captaciones	Información de depósitos a plazo fijo	Jefe de Captaciones	Sistema de gestión	Alta/Alta/Alta	Acceso restringido
Control Interno	Informes de control	Reportes de auditoría y cumplimiento	Responsable de Control Interno	Oficina de control	Alta/Alta/Media	Acceso por perfil
Crédito	Expedientes de crédito	Solicitudes, análisis y pagares	Jefe de Crédito	Archivo físico/digital	Alta/Alta/Media	Actualización mensual
Auditoría Interna	Informes de auditoría	Resultados de auditorías internas y externas	Auditor Interno	Oficina de auditoría	Alta/Alta/Media	Confidencialidad estricta

Tabla 11. Priorización y Documentación de activos (Fuente Propia)

Todos los activos listados en la Tabla 11, al contener información crítica o confidencial, deben ser transmitidos por correo electrónico únicamente bajo mecanismos de cifrado robusto, garantizando así la protección de la información y el cumplimiento de las obligaciones legales y regulatorias de la cooperativa.

Área	**Activo de Información**	**Motivo de cifrado obligatorio**
Gerencia	Documentos estratégicos	Contienen información confidencial y decisiones clave institucionales
Contabilidad	Libros contables	Incluyen datos financieros sensibles y registros de operaciones
Tesorería	Comprobantes y registros de pago	Manejan información bancaria y transaccional de socios y la cooperativa
Talento Humano	Expedientes de personal	Contienen datos personales, contratos y evaluaciones (protección de datos personales)
Tecnología de la Información	Servidores y respaldos	Información sobre infraestructura crítica y copias de seguridad

Área	Activo de Información	Motivo de cifrado obligatorio
Seguridad de la Información	Políticas y procedimientos	Manuales y registros de incidentes pueden revelar vulnerabilidades
Riesgos	Matriz de riesgos	Identificación y evaluación de riesgos internos y externos
Captaciones	Base de datos de captaciones	Información de cuentas de ahorro y depósitos de socios
Control Interno	Informes de control	Reportes de auditoría y cumplimiento con hallazgos sensibles
Crédito	Expedientes de crédito	Solicitudes, análisis y contratos con datos personales y financieros
Auditoría Interna	Informes de auditoría	Resultados de auditorías internas y externas, hallazgos críticos

Tabla 12. Información que debe viajar cifrada por correo. (Fuente Propia)

Todos los activos mencionados contienen información sensible de socios, empleados y operaciones financieras, cuya divulgación podría causar daños económicos, legales y reputacionales de acuerdo a la Ley Orgánica de Protección de Datos Personales y la normativa de la SEPS exigen la protección de datos personales y financieros, especialmente durante su transmisión electrónica.

4.1 Análisis de la encuesta para conocer el estado de la seguridad de la información dentro de la Cooperativa.

Para el desarrollo del presente proyecto de tesis, se diseñó y aplicó una encuesta interna en la Cooperativa con el objetivo de evaluar la percepción y comprensión sobre la seguridad de la información entre los empleados de las distintas áreas, bajo el título "Seguridad de la Información". La encuesta consideró factores específicos relacionados con la seguridad de la información, enfocándose particularmente en el uso del correo electrónico como medio de comunicación y posible vector de riesgo. Se optó por un formato digital utilizando Google Forms, lo que facilitó el acceso a la encuesta y permitió la obtención de análisis gráficos mediante las herramientas integradas de Google.

Para la difusión de la encuesta, se empleó el grupo interno de WhatsApp, a través del cual se compartió el enlace con la población objetivo, compuesta por ocho (8) jefaturas de

área. Posteriormente, se realizó un análisis detallado de cada pregunta, así como una conclusión general que permitió establecer un enfoque orientador sobre la seguridad de la información dentro de la Cooperativa, destacando los conceptos básicos que deben ser comprendidos por todo el personal.

A continuación, se presentan los resultados obtenidos por cada pregunta y la conclusión inicial derivada de la encuesta.

Preguntas a ejecutarse:

Pregunta 1. ¿Conoce usted si los correos electrónicos enviados desde la Cooperativa utilizan algún tipo de cifrado durante su transmisión (por ejemplo, TLS en SMTP)?

Se puede observar en el Anexo 3, que un 52,2% de empleados supone tener algún tipo de cifrado al enviar los mensajes por correo, haciendo de esta manera pensar que la información trasmitida por el canal SMTP es seguro y podría incurrir en envío de información confidencial por este medio sin tomar en cuenta el riesgo que existe si no está cifrado el canal.

Pregunta 2. ¿Está informado sobre los riesgos asociados al envío de correos electrónicos sin cifrado, como la posible interceptación o acceso no autorizado a la información?

Se observa en el Anexo 4, que de igual manera en relación a la pregunta anterior más de la mitad de empleados considera tener conocimiento y estar seguros de que la información trasmitida está cifrada y asegurada.

Pregunta 3. ¿Considera que la información enviada por correo electrónico actualmente es lo suficientemente segura para proteger datos sensibles?

Acá podemos determinar de acuerdo al Anexo 5, que no tiene correlación la respuesta de esta pregunta con las anteriores ya que se divide totalmente la ideología de que la información está segura al enviarse por correo, en relación a las dos anteriores en las que se tenía conocimiento de que la información que viaja por SMTP es segura y utiliza cifrado.

Pregunta 4. ¿Sabe si los archivos transferidos mediante SFTP en la Cooperativa están protegidos por mecanismos de cifrado durante su transmisión?

Se evidencia en el Anexo 6, que casi el 50% de los empleados están conscientes de que la información emitida por el canal SFTP contiene seguridad de extremo a extremo, pero

esto no es totalmente seguro ya que si la información que viaja puede ser remitida por error hacia otros usuarios y si no está cifrada puede ser utilizada sin ningún inconveniente, mientras que si se la cifra antes de enviarla se convierte en algo que únicamente el usuario definido podrá usar la información y los usuarios que la tengan y no sean autorizados no podrán usarla.

Pregunta 5. ¿Está familiarizado con la diferencia entre cifrado en tránsito (protección mientras la información viaja por la red) y cifrado en reposo (protección cuando la información está almacenada)?

Esta pregunta nos permite conocer el concepto que manejan los empleados dentro de la Cooperativa en razón de la información, en este sentido más de la mitad de los encuestados no entienden la diferencia de los dos conceptos, tal como se evidencia en el Anexo 7.

Pregunta 6. ¿Cree que la información almacenada en los servidores de la Cooperativa (correos electrónicos, archivos) cuenta con las medidas de cifrado adecuadas?

Se puede observar en el Anexo 8, que la mitad de encuestados considera que su información está totalmente segura y que cuenta con cifrado como medida de protección.

Pregunta 7. ¿Ha recibido capacitación o información sobre buenas prácticas para el manejo seguro de información confidencial utilizando correo electrónico (SMTP) o transferencia de archivos (SFTP)?

Se evidencia en el Anexo 9, que se debe contemplar capacitaciones regulares para poder tener un grupo de empleados totalmente capacitado en buenas prácticas de seguridad en la transmisión de información por medios como SMTP o SFTP.

Pregunta 8. ¿Está al tanto de la existencia de mecanismos de cifrado asimétrico, como PGP, para proteger la información que se envía o almacena?

Es muy importante conocer que más de la mitad de empelados está familiarizado con el concepto de cifrado PGP, ya que esto permitirá la implementación del mecanismo de cifrado PGP de una manera más rápida y efectiva dentro de la Cooperativa, de acuerdo al Anexo 10.

Pregunta 9. ¿Considera necesario implementar soluciones adicionales de cifrado, como PGP, para fortalecer la seguridad de la información?

Al tener personas que conocen conceptos de cifrado PGP hace que los procesos de

implementación y comprensión del funcionamiento del cifrado asimétrico será comprendido de manera correcta dentro de la implementación del mecanismo de cifrado para protección de la información en la Cooperativa, así lo muestra el Anexo 11.

Pregunta 10. ¿Cuál es su nivel de confianza en los actuales procedimientos de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información enviada y recibida a través de correo electrónico y SFTP?

Se evidencia en el Anexo 12, un nivel de confianza medio en los envíos de información por los canales SMTP y SFTP, haciendo entender que al incorporar el mecanismo de cifrado asimétrico para aseguramiento de la información estos índices aumentaran ya que se evidenciara la seguridad en los envíos.

4.5. Análisis de la solución para proteger las comunicaciones SMTP y SFTP dentro de la Cooperativa.

En la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., la gestión segura de las comunicaciones electrónicas es fundamental para proteger la confidencialidad, integridad y disponibilidad de la información institucional. Actualmente, se utiliza cPanel como servidor de correo electrónico, una plataforma ampliamente reconocida por su facilidad de administración y soporte para protocolos estándar como SMTP, IMAP y POP3, con configuraciones recomendadas para SSL/TLS que garantizan la encriptación en tránsito de los mensajes.

Sin embargo, aunque cPanel ofrece mecanismos robustos para la transmisión segura de correos mediante cifrado TLS, esta protección se limita al canal de comunicación entre el cliente y el servidor, sin asegurar la confidencialidad del contenido del correo una vez almacenado o en tránsito entre servidores. Por ello, la Cooperativa considera la implementación de un cliente de correo como Outlook, configurado para utilizar cifrado de extremo a extremo mediante PGP (Pretty Good Privacy), basado en criptografía asimétrica. Este enfoque permitirá que los correos electrónicos sean cifrados en el origen y solo descifrados por el destinatario final, garantizando que el contenido permanezca inaccesible para terceros, incluso en caso de compromisos en servidores intermedios.

La integración de PGP en Outlook, aunque requiere configuraciones adicionales y capacitación para los usuarios, representa una mejora significativa en la seguridad de las comunicaciones internas y externas. Además, el uso de claves públicas y privadas

proporciona un mecanismo confiable para la autenticación y la no repudio, aspectos críticos en el manejo de información sensible en el sector financiero.

Por otro lado, la administración de cPanel permite configurar restricciones SMTP para evitar conexiones no autorizadas y limitar el envío de correos a través de agentes confiables, lo que reduce el riesgo de abuso por parte de usuarios o scripts maliciosos. Complementar estas medidas con el cifrado de extremo a extremo en Outlook fortalece la estrategia de seguridad integral de la Cooperativa, mitigando riesgos asociados a ataques de phishing, interceptación y filtración de datos, la combinación de cPanel como servidor de correo con configuraciones SSL/TLS adecuadas y la implementación de Outlook con cifrado PGP de extremo a extremo constituye una solución robusta y escalable para proteger las comunicaciones electrónicas de la Cooperativa, alineándose con las mejores prácticas en seguridad informática y cumplimiento normativo del sector financiero popular y solidario.

La transferencia segura de archivos es un componente crítico para garantizar la protección de la información sensible y cumplir con los estándares normativos del sector financiero. La implementación del protocolo SFTP (SSH File Transfer Protocol) representa una solución robusta para la transmisión segura de datos, ya que utiliza el cifrado SSH para proteger la información durante el tránsito, evitando accesos no autorizados y posibles brechas de seguridad.

Para maximizar la seguridad de las transferencias SFTP, es fundamental adoptar prácticas esenciales como cifrado de datos en tránsito y en reposo utilizando algoritmos de cifrado fuertes, para proteger la confidencialidad e integridad de los datos en todo momento, tanto durante la transferencia como cuando están almacenados.

La adopción de estas medidas permitirá a la Cooperativa establecer un marco de seguridad SFTP sólido y resiliente, alineado con estándares internacionales como ISO/IEC 27001, y garantizará la protección de los activos digitales frente a amenazas cibernéticas cada vez más sofisticadas.

4.2 Instalación y uso del software Kleopatra y GpgOL, como mecanismo de cifrado para correos.

Kleopatra: Es un gestor de certificados PGP. Mediante esta herramienta es posible crear certificados, modificarlos, destruirlos, añadir identidades o modificar fechas de expiración, entre otros.

GpgOL: Es un plugin de Outlook que añade las funcionalidades de cifrar, descifrar, firmar y comprobar la autenticidad e integridad tanto de los correos, como de sus posibles archivos adjuntos.

GpgEX: una extensión del Explorador de Windows que le permite cifrar archivos mediante el menú contextual del botón derecho.

En primer lugar, debemos instalar el software Gpg4win que contiene tanto kleopatra como GpgOL y GpgEX, para poder usarlos en el cifrado, como lo indica la Figura 12.

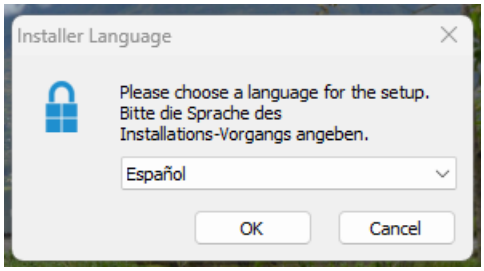


Figura 12. Instalación de Gpg4win. (Fuente Propia)

Luego de seleccionar el idioma a español, damos clic en Siguiente, como lo muestra la Figura 13.

Figura 13. Instalación de Gpg4win. (Fuente Propia)

Posterior a ello seleccionaremos las opciones de Kleopatra, GpgOL y GpgEX, y daremos clic en Siguiente, como lo muestra la Figura 14.

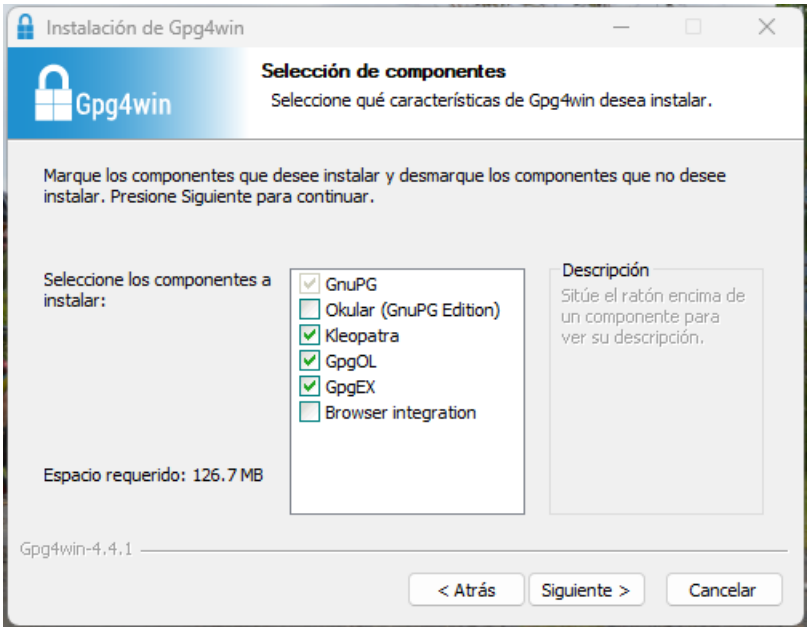


Figura 14. Instalación de Gpg4win. (Fuente Propia)

Seleccionamos la ubicación donde va a estar instalado el software, en este caso en el disco local C:\Program Files (x86)\Gpg4win, como lo muestra la Figura 15.

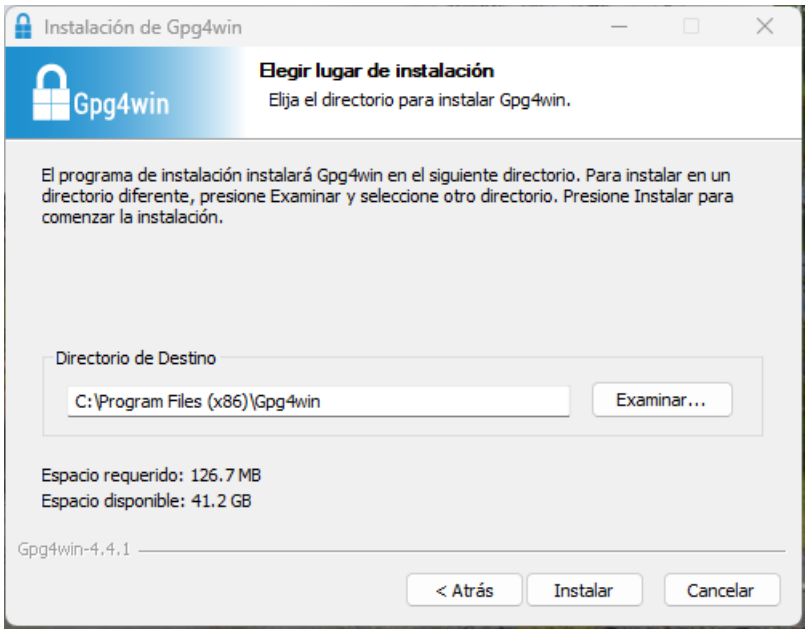


Figura 15. Instalación de Gpg4win. (Fuente Propia)

Esperamos a que se instale el programa, como lo muestra la Figura 16.

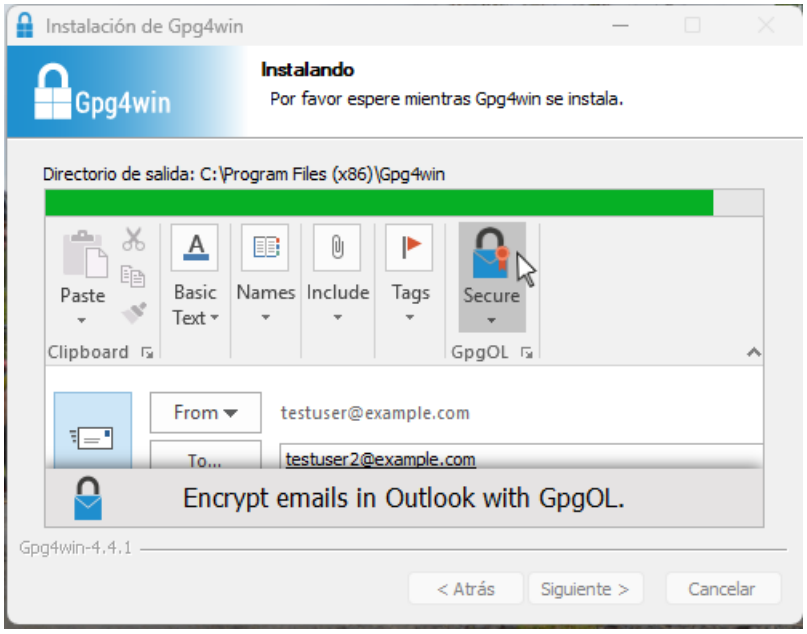


Figura 16. Instalación de Gpg4win. (Fuente Propia)

Dejamos seleccionado el check de kleopatra y damos clic en Terminar como lo muestra la Figura 17.

Figura 17. Instalación de Gpg4win. (Fuente Propia)

Una vez terminada la instalación se abrirá la ventana del programa kleopatra, en el cual podremos crear certificados para poder comenzar a utilizar PGP en el correo, como lo muestra la Figura 18.

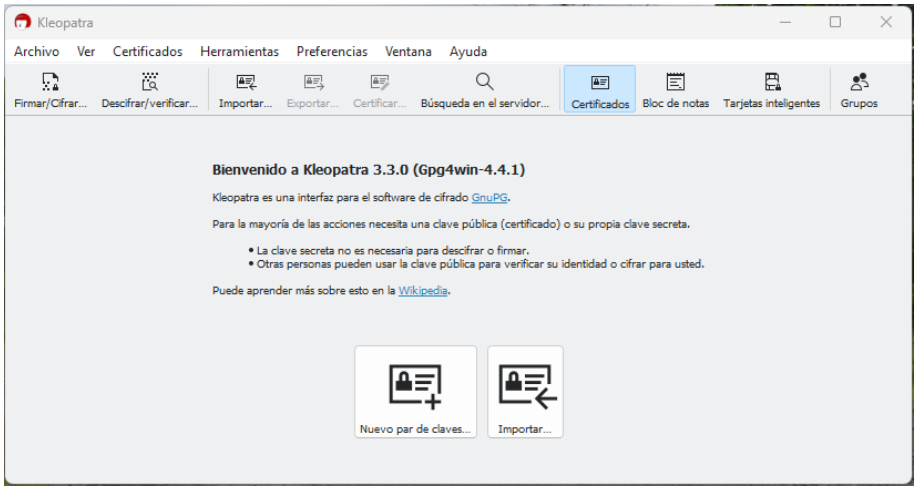


Figura 18. Ventana de creación de par de claves. (Fuente Propia)

4.3 Creación de certificados PGP.

Durante el proceso de creación del certificado, se procedió a definir una identificación única para el mismo. Para ello, se ingresó un nombre que permita identificar claramente al propietario del certificado, así como el correo electrónico asociado a dicho propietario. Esta información es fundamental, ya que se vincula directamente con el certificado y facilita su reconocimiento y validación dentro del sistema. Se debe tener en cuenta que tanto el nombre, como el comentario serán visibles para aquellos que vayan a usar nuestra clave pública para comunicarse con nosotros, como lo muestra la Figura 19.

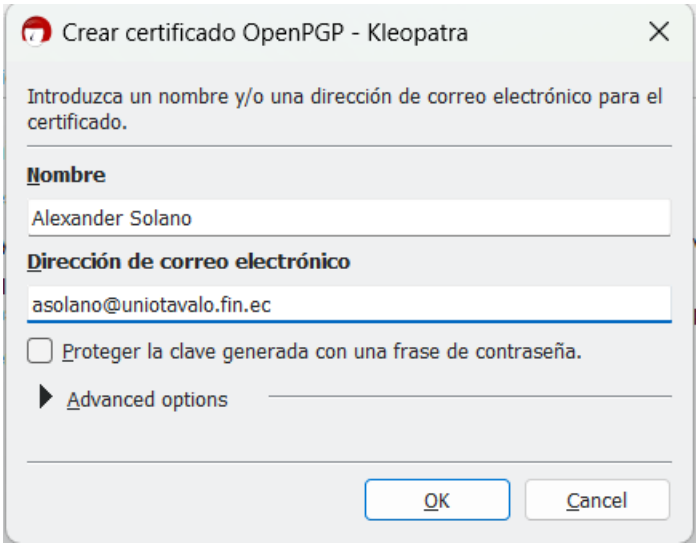


Figura 19. Introducción del nombre y correo del par de claves. (Fuente Propia)

En la pestaña **Advanced option** que se observa en la figura, se pueden definir características del certificado como son el algoritmo de cifrado (RSA, DSA y ECDSA), la

fecha de caducidad o para qué se utilizará (firma, cifrado, certificación o autenticación), como lo muestra la Figura 20.

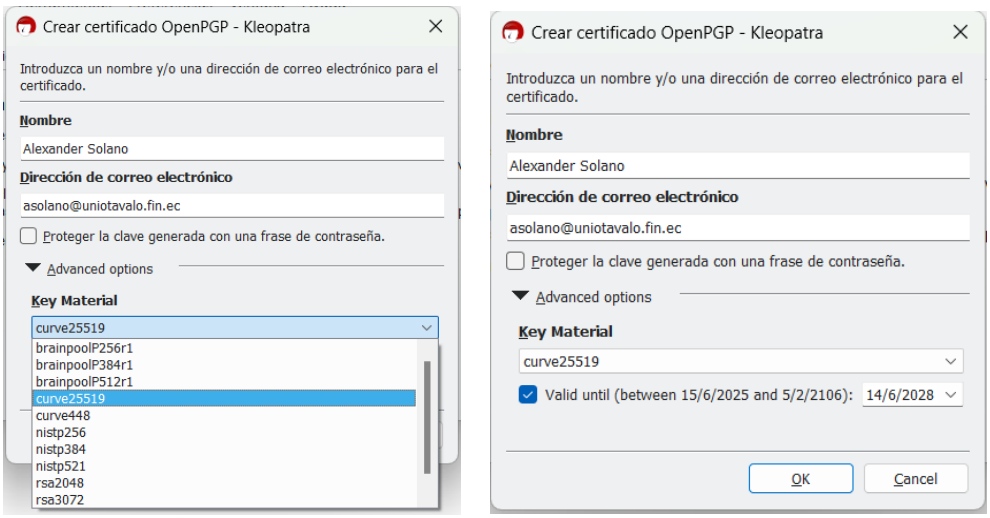


Figura 20. Selección de tipo de cifrado. (Fuente Propia)

Tras pulsar **OK** se mostrará otra ventana en la que se deberá colocar una clave segura para protección del certificado que se va a generar, como lo muestra la Figura 21.

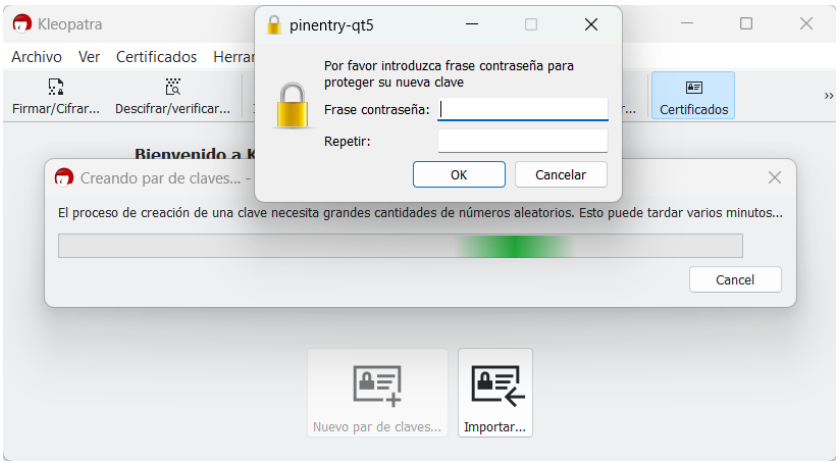


Figura 21. Introducción de la clave para el llavero de claves. (Fuente Propia)

Se debe introducir una clave de al menos 8 caracteres caso contrario dará un mensaje de advertencia indicando que la clave es insegura, como lo muestra la Figura 22.

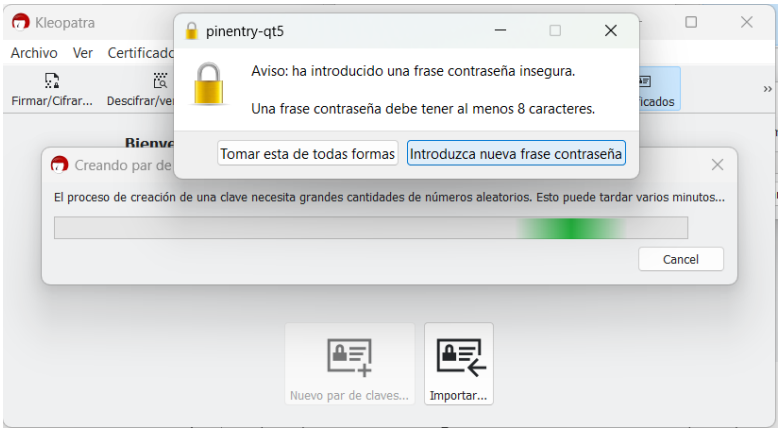


Figura 22.Ventana de advertencia de clave insegura. (Fuente Propia)

Una vez colocada la clave segura se genera el certificado con las credenciales suscritas, y se procede a dar clic en **OK**, como lo muestra la Figura 23.

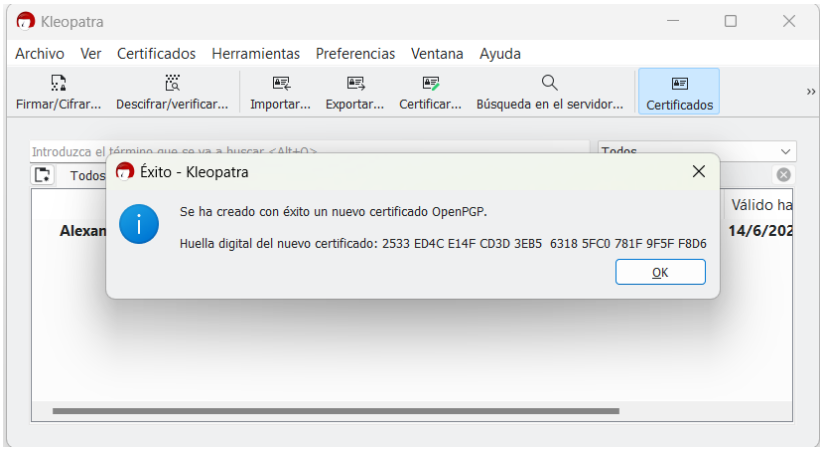


Figura 23. Certificado Generado satisfactoriamente. (Fuente Propia)

Una vez generado el certificado lo podremos observar ya generado con todas las características como son nombre, correo, estado su validez desde y hasta cuando es válido y el ID de la clave, como lo muestra la Figura 24.

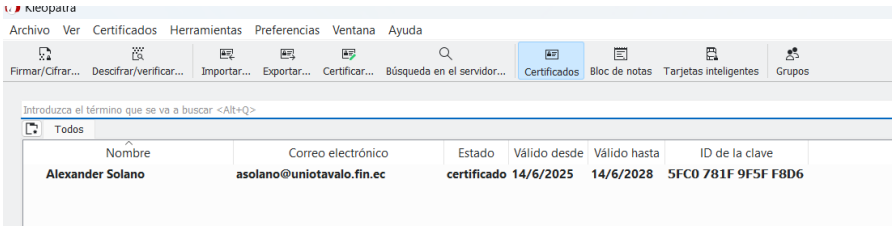


Figura 24. Almacén de certificados. (Fuente Propia)

Luego es importante CERTIFICAR el certificado para que tenga veracidad al momento de compartirlo públicamente, como lo muestra la Figura 25.

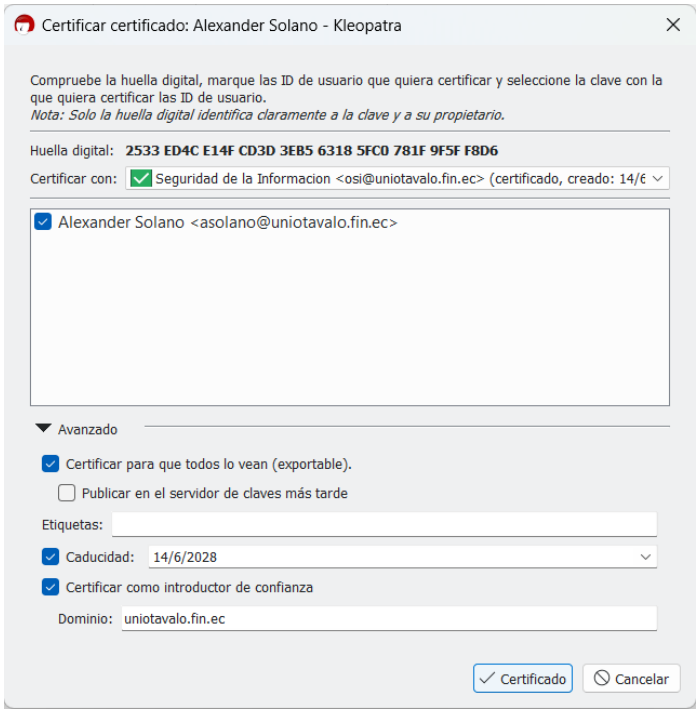


Figura 25. Certificación de certificado. (Fuente Propia)

Es importante mencionar que la certificación la realiza a través de un certificado adicional, no puede certificar un mismo certificado a sí mismo, por eso PGP genera una red de certificados de confianza de acuerdo a su metodología de seguridad, en este caso el área de seguridad de la información es el administrador de certificados y es el único que para la Cooperativa certificara su veracidad, como lo muestra la Figura 26.

Figura 26. Proceso correcto de certificación de certificado. (Fuente Propia)

4.4 Generar certificado de revocación.

Si en algún momento se sospecha que alguna de las claves ha sido comprometida o ha expirado, es posible crear un certificado de revocación. Este certificado permite cancelar

la clave pública afectada, lo cual es una medida recomendada para mantener la seguridad. Es importante generar este certificado y guardarlo en un lugar seguro para poder usarlo cuando sea necesario.

Para crear el certificado de revocación, basta con hacer clic derecho sobre el certificado en cuestión, seleccionar la opción DETALLES. Esto abrirá la ventana de detalles del certificado donde estará el botón **Generar certificado de revocación**. Al hacer clic en este botón, se generará un archivo con extensión .rev, que podrás guardar en la ubicación que prefieras, como lo muestra la Figura 27.

Figura 27. Generación de certificado de revocación. (Fuente Propia)

Esta acción es fundamental para proteger la integridad de las comunicaciones y asegurar que las claves comprometidas no puedan seguir siendo utilizadas, como lo muestra la Figura 28.

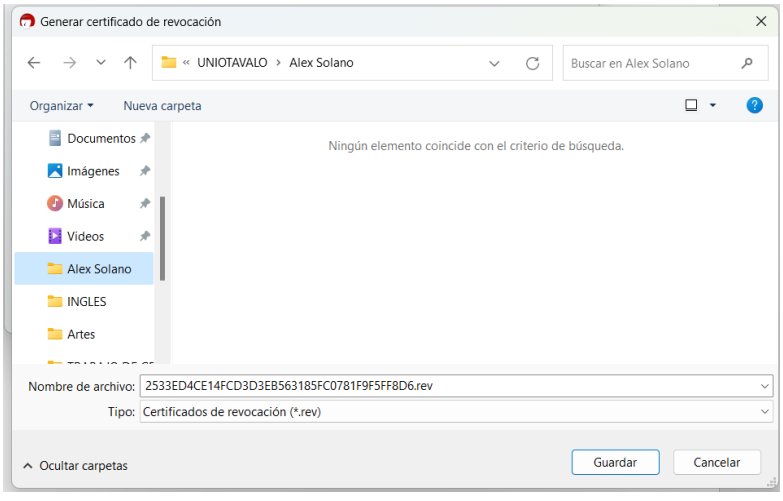


Figura 28. Almacenamiento de certificado de revocación. (Fuente Propia)

Para generar un certificado de revocación es necesario ingresar la clave asociada a nuestro certificado. Esta medida de seguridad evita que terceros no autorizados, que pudieran tener acceso físico o remoto a nuestro equipo, puedan generar un certificado de revocación de manera indebida. De este modo, se garantiza que solo el propietario legítimo del certificado pueda cancelar su validez en caso de compromiso o expiración, como lo muestra la Figura 29.

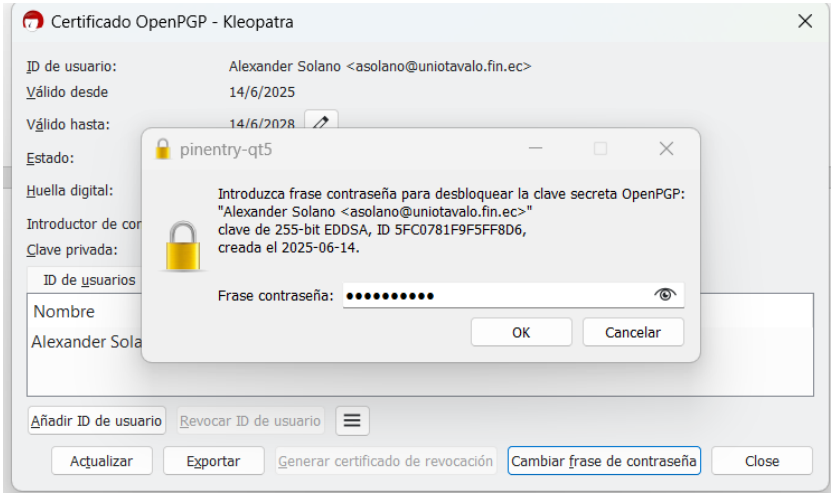


Figura 29. Ventana para la introducción de clave. (Fuente Propia)

Este paso es fundamental para mantener el control y la integridad sobre los certificados digitales, protegiendo la seguridad de las comunicaciones y evitando posibles usos fraudulentos, como lo muestra la Figura 30.

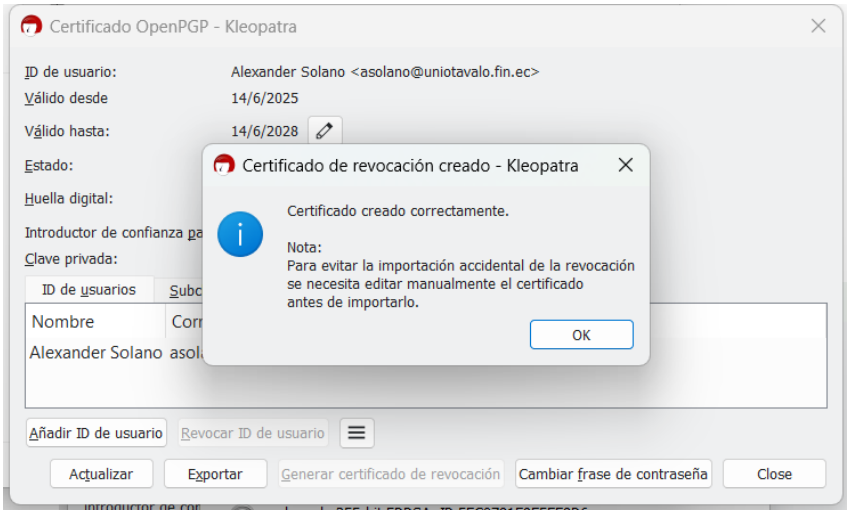


Figura 30. Ventana de certificado generado satisfactoriamente. (Fuente Propia)

4.5 Cambio de contraseña de un certificado.

Para cambiar la frase de contraseña de un certificado en Kleopatra, se debe iniciar haciendo clic con el botón derecho del ratón sobre el certificado al que se desea aplicar el cambio, desde la pantalla principal de la aplicación. En el menú desplegable, se selecciona la opción **Cambiar frase de contraseña**. Al hacerlo, se abrirá una ventana de diálogo en la que se solicitará ingresar primero la contraseña actual del certificado y, posteriormente, la nueva contraseña que se desea asignar.

Este procedimiento garantiza que solo el propietario legítimo del certificado pueda modificar la frase de contraseña, protegiendo así el acceso y uso adecuado de las claves asociadas. Además, permite mantener la seguridad y confidencialidad de las comunicaciones cifradas, asegurando que las claves privadas permanezcan protegidas frente a accesos no autorizados, como lo muestra la Figura 31.

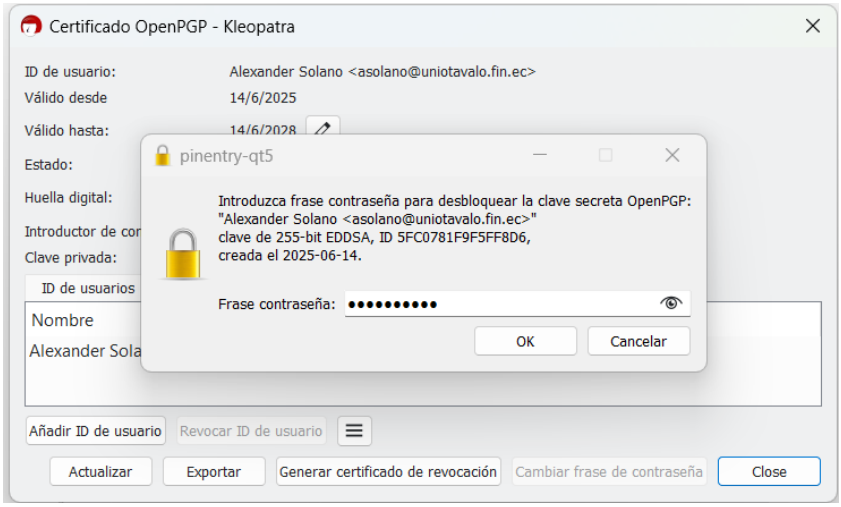


Figura 31. Ventana de cambio de contraseña de una clave PGP. (Fuente Propia)

4.6 Compartición de la clave pública de un certificado a través del correo electrónico.

Para compartir la clave pública de un certificado PGP es necesario exportarla previamente. Para ello, se debe hacer clic con el botón derecho del ratón sobre el certificado correspondiente, ubicado en la pantalla principal de Kleopatra, y seleccionar la opción **Exportar** en el menú desplegable.

Una vez seleccionada esta opción, se abrirá una ventana que permitirá elegir la

ubicación donde se guardará el archivo con la clave pública, generalmente con extensión .asc. Este archivo es el que se debe compartir con los destinatarios para que puedan cifrar los mensajes o archivos que le envíen de forma segura.

Este procedimiento es fundamental para garantizar que la clave pública se distribuya correctamente, facilitando la comunicación cifrada y protegiendo la confidencialidad de la información intercambiada. Además, es importante recordar que la clave pública puede compartirse libremente, ya que no compromete la seguridad del par de claves, a diferencia de la clave privada, que debe mantenerse siempre protegida y nunca compartirse, como se observa en la Figura 32.

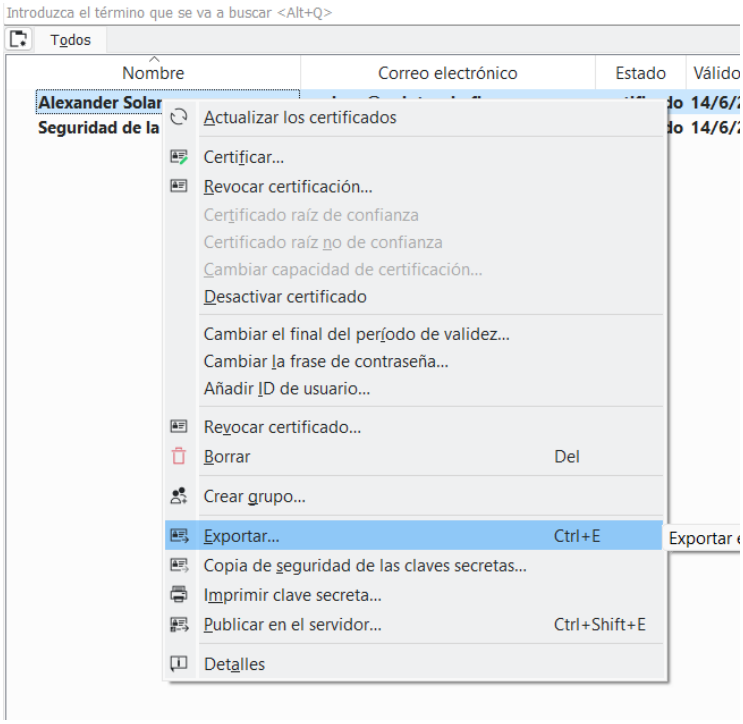


Figura 32. Ventana de exportar certificado. (Fuente Propia)

4.7 Firma y verificación de correos electrónicos.

4.7.1 Firma.

La acción de firmar un correo electrónico se realiza para que el receptor pueda verificar que la información recibida no ha sido alterada durante la transmisión, garantizando así la integridad de los datos. Para firmar un correo en Outlook, es necesario utilizar el complemento llamado GpgOL, que aparece como un icono en la interfaz del programa.

Para firmar un mensaje, se debe hacer clic en el icono de GpgOL y seleccionar la opción Sign en el menú desplegable. Por defecto, GpgOL firma automáticamente los correos

enviados; sin embargo, si se desea elegir manualmente el certificado PGP con el que se firmará cada correo, es necesario desactivar la opción **Automation** en la configuración de GpgOL, como lo muestra la Figura 33.

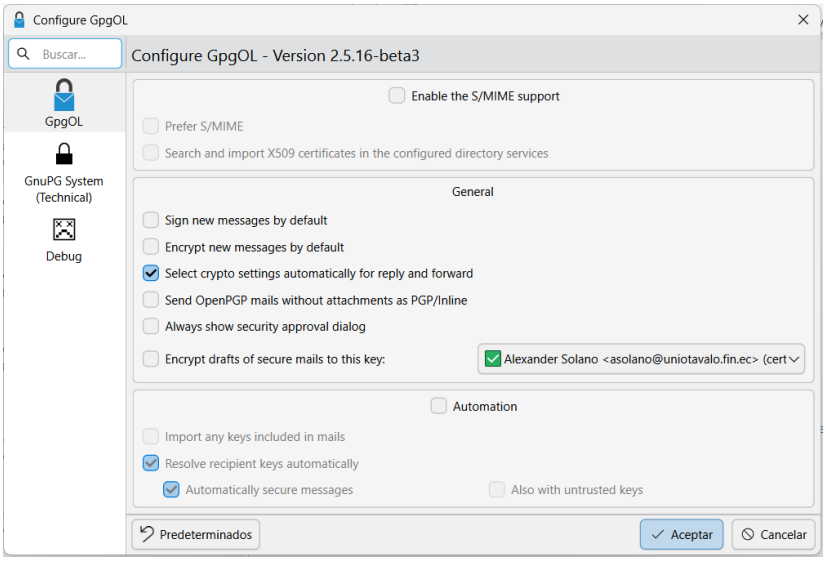


Figura 33. Configuración para la firma y cifrado de correos. (Fuente Propia)

Este procedimiento es esencial para asegurar que los correos electrónicos enviados desde la Cooperativa mantengan su autenticidad y que el destinatario pueda confiar en que el contenido no ha sido manipulado, fortaleciendo así la seguridad de las comunicaciones internas y externas.

Tras escribir el correo electrónico que se desea enviar, se pulsa «Enviar» y en la ventana que aparece se selecciona el certificado PGP que se utilizará para firmarlo, como se observa en la Figura 34.

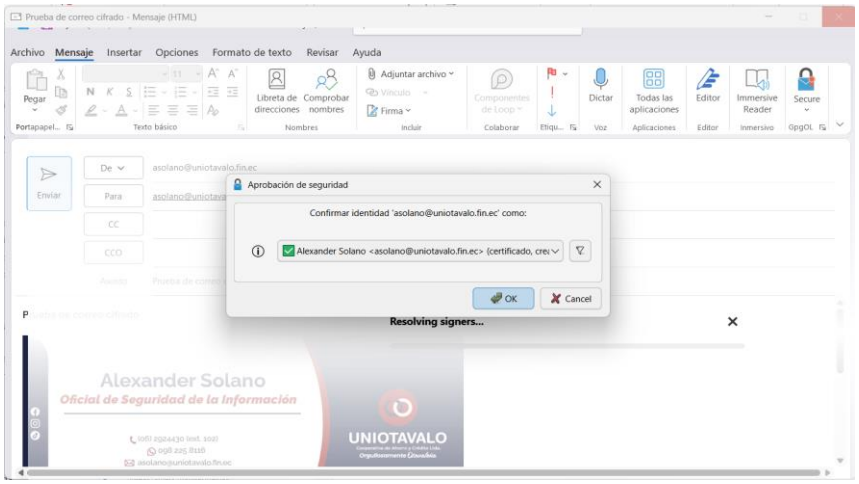


Figura 34. Firma de un correo electrónico en Outlook. (Fuente Propia)

4.7.2 Verificación.

Para verificar los correos electrónicos firmados por PGP es necesario disponer de la clave pública del usuario que ha enviado el correo electrónico- La verificación se hace de forma automática, y es posible comprobarlo viendo el icono de GpgOL y la etiqueta en el correo «GpgOL: Level 3 trust in ‘asolano@uniotavalo.fin.ec’», como se evidencia en la Figura 35.

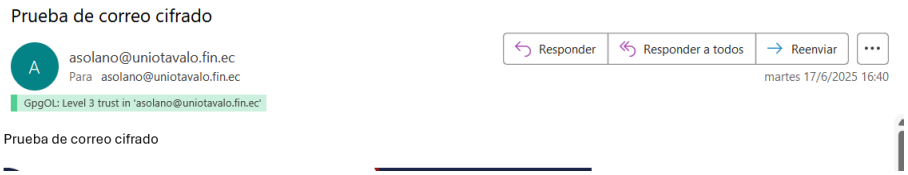


Figura 35. Verificación de la firma del correo electrónico. (Fuente Propia)

4.7.3 Cifrado.

Primeramente se debe disponer de la clave pública del certificado PGP del destinatario que se lo debe almacenar dentro de kleopatra para tenerlo dentro de la base de datos de certificados con los que se va a interactuar, luego se debe elaborar el respectivo contexto del correo a emitir y se deberá dar clic en el icono GpgOL ubicado en el menú superior de Outlook y dar clic en **Secure** y posterior activar **Encrypt**, una vez hecho este proceso damos clic en Enviar y tendremos un correo remitido de manera cifrada, como lo muestra la Figura 36.

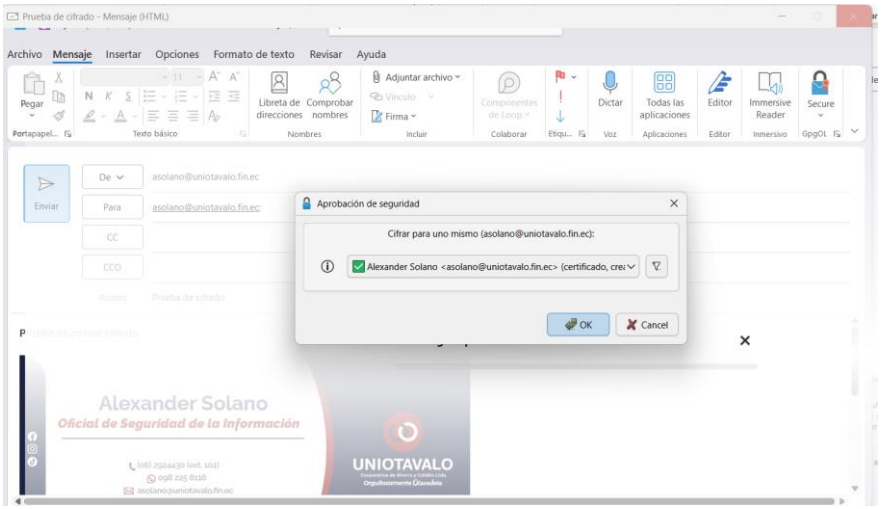


Figura 36. Aprobación de seguridad. (Fuente Propia)

4.7.4 Descifrado.

A la hora de recibir un correo electrónico cifrado, para su lectura antes será necesario descifrarlo. Para ello, en el momento de recibir el correo cifrado, GpgOL mostrará una ventana en la cual habrá que introducir la contraseña de nuestro certificado PGP, como lo muestra la Figura 37.

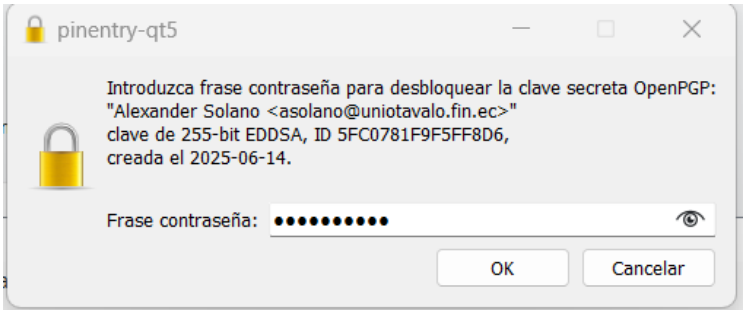


Figura 37. Ventana de inserción de la contraseña del llavero de claves para descifrar el correo. (Fuente Propia)

Una vez introducida, se mostrará el mensaje descifrado, y en el icono de GpgOL aparecerá un aviso para informar que el mensaje está cifrado, como se observa en la Figura 38.

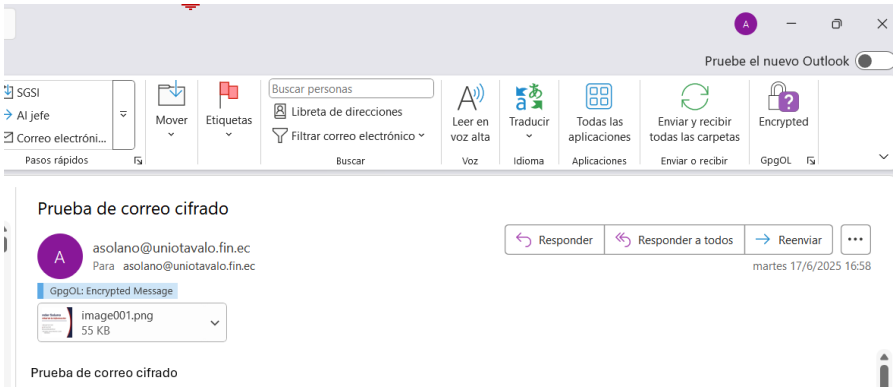


Figura 38. Verificación de mensaje cifrado. (Fuente Propia)

4.7.5 Modelo de arquitectura de integración del mecanismo criptográfico asimétrico de correo electrónico y SFTP.

A continuación, se muestra la Figura 39. Donde se representa gráficamente la arquitectura de integración del mecanismo criptográfico.

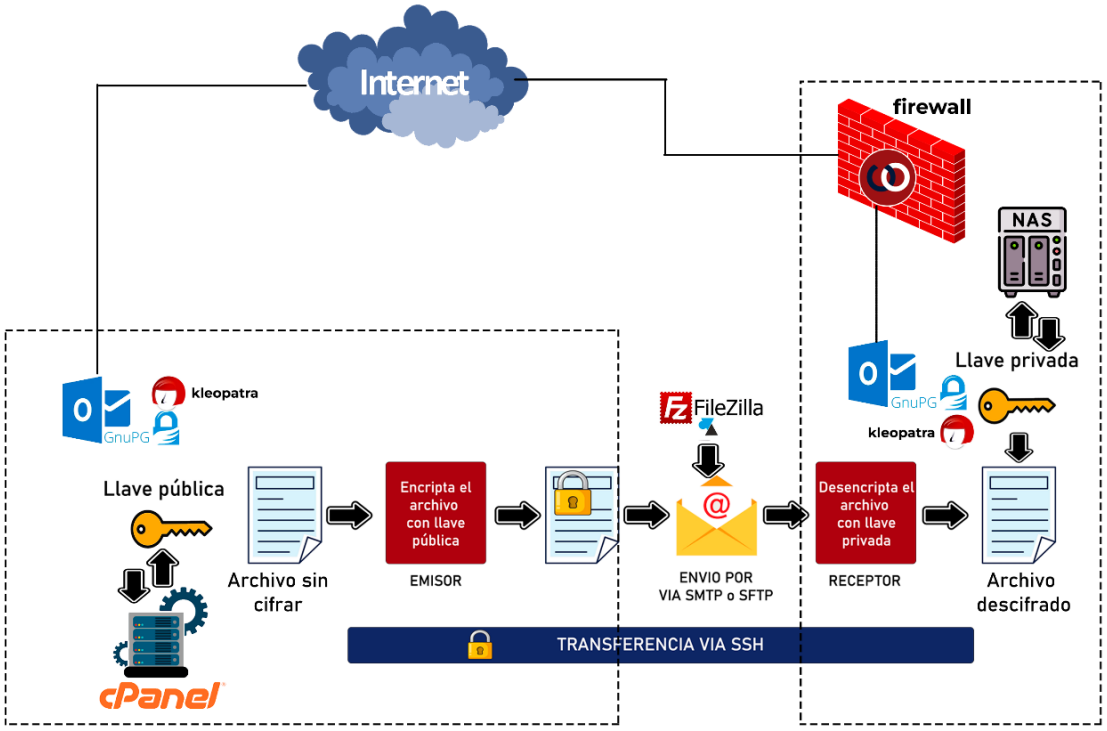


Figura 39. Modelo de arquitectura de integración del mecanismo criptográfico asimétrico de SMTP y SFTP. (Fuente Propia)

4.7.6 Componentes del diagrama de arquitectura del mecanismo criptográfico asimétrico de SMTP y SFTP.

FIREWALL. - El firewall es el componente encargado de examinar cada uno de los mensajes tanto de entrada como de salida hacia y desde la Cooperativa, en este sentido obstruye el ingreso de aquellos mensajes que no cumplen con las políticas dentro del firewall.

COMUNICACIONES SSH. - Las comunicaciones internas o externas por tema de capacidad de envío que no se las puede realizar por medio de correo serán realizadas a través de SSH utilizando un cliente como es el caso de FileZilla.

NAS. - Para el alojamiento de las claves privadas, es de vital importancia ya que será el lugar seguro de administración que no tendrá salida fuera de la LAN, por seguridad de la información que se maneja.

CPANEL. - Permite el alojamiento de las claves públicas a través del acceso a la web institucional, en donde por medio de un desarrollo dentro de la página web se podrá

almacenar y descargar las claves públicas para el uso del cifrado.

INTERCAMBIO DE LLAVES. - Las llaves serán intercambiadas mediante dos tipos de servidores, las públicas lo harán a través de un servidor en la nube de acceso libre, mientras que las privadas serán compartidas a través del servidor de almacenamiento interno NAS, para proteger el acceso y evitar posibles vulnerabilidades.

DEFINICION DE LOS ALGORITMOS DE CIFRADO Y FIRMA. - Se deberá definir primeramente los algoritmos a ser usados para el cifrado y firma digital, tanto para la información emitida por correo, SFTP, archivos en reposo y en tránsito, esto pues para cubrir lo establecido en el capítulo I de este proyecto.

Para la implementación del algoritmo RSA en cifrado y firmas digitales, se opta generalmente por claves de 2048 bits, ya que ofrecen un balance adecuado entre seguridad y eficiencia computacional. Aunque las claves de 3072 bits proporcionan mayor seguridad, su uso implica un considerable aumento en el tiempo de procesamiento. Por otro lado, rangos de claves menores, como los de 256 a 383 bits, mejoran la seguridad en comparación con claves más cortas, pero a costa de una reducción en la velocidad del proceso criptográfico. Claves inferiores a 224 bits presentan riesgos de seguridad y no se recomiendan. En consecuencia, el uso de claves RSA de 2048 bits es la opción más adecuada para garantizar un rendimiento óptimo sin comprometer la seguridad, según lo muestra la Figura 40.

Algoritmo	Tamaño de archivo(KB)	Tiempo de encriptado (segundos)	Tiempo de desencriptado(segundos)
AES	2048	0.562	0.815
DES		0.620	0.997
RSA		2.636	30.779
AES	4096	1.006	1.293
DES		1.238	1.561
RSA		4.508	64.319
AES	6144	1.658	1.971
DES		1.863	2.107
RSA		6.785	95.254
AES	8192	2.137	2.417
DES		4.476	2.768
RSA		9.032	126.594
AES	10240	2.819	3.096
DES		3.002	3.289
RSA		11.294	160.164

Figura 40. Análisis de rendimiento de los algoritmos DES, AES y RSA, (B. Padmavathi)

4.7.7 Compatibilidad con certificados PGP.

El estándar de criptografía de clave pública PGP, es el que será usado para el cifrado

y firma de los mensajes enviados a través de correo electrónico por medio del servicio de GnuPG, la emisión de los certificados cumplirá los requerimientos establecidos en el capítulo I de este proyecto. La solución GnuPG debe seguir las especificaciones recomendadas por el estándar PGP que especifica en el IETF RFC 4880 (Formato de mensaje PGP), por lo tanto, los algoritmos anteriormente mencionados son los que están dentro de los especificados para esta solución del proyecto. De esta manera, se puede determinar que el conjunto de algoritmos óptimos para los cifrados sería el RSA-2048 junto a SHA-256. Por otro lado, el estándar define que el algoritmo de cifrado de intercambio de llaves asimétricas óptimo para un firmado es el RSA y para cifrar el contenido de los mensajes de correo electrónico el algoritmo óptimo es el AES-128 o superior. (Fernández, Benjamín, 2021).

4.7.8 Aspectos de seguridad para generación de claves.

La longitud de clave a usar debe ser considerada teniendo en cuenta ciertos aspectos de seguridad. Cada uno de los niveles de confidencialidad o jerarquía va a tener un tipo de longitud de clave tal como se muestra en la Tabla 13.

Nivel de correo	Longitud de clave	Descripción
Nivel 1	2048 bits	Gerencia General, se maneja información con alta confidencialidad
Nivel 2	2048 bits	Esto se debe a que los usuarios de este nivel no envían gran cantidad de tráfico de correos y se requiere un nivel de seguridad superior.
Nivel 3	1024 bits	Esto se debe a que los usuarios de este nivel de tráfico de correos que generan son bajos.

Tabla 123. Niveles de generación de clave. (Fuente Propia)

4.7.9 Ciclo de vida de las llaves.

Es fundamental establecer el ciclo de vida de cada clave de cifrado considerando dos aspectos principales: la longitud de la clave y el nivel de confianza en el usuario. Estos elementos permiten estimar el periodo de validez adecuado para cada tipo de clave, facilitando así la elaboración de un cronograma para su renovación conforme a su ciclo de vida, como lo muestra la Tabla 14.

Nivel de correo	Longitud de clave	Confiabilidad del usuario	Ciclo de vida	Descripción
Nivel 1	2048 bits	Alta	24 meses	Para el área de gerencia, se propone un periodo de vigencia de dos años. Esto se debe a que la clave utilizada tiene una longitud de 2048 bits, lo que la hace difícil de descifrar. Además, los usuarios asignados a esta plantilla cuentan con un alto nivel de confianza, por lo que es poco probable que compartan su clave privada.
Nivel 2	2048 bits	Media	12 meses	Para los jefes de área y supervisores, se establece un ciclo de vida de un año para sus claves. Esta decisión se basa en que, aunque la clave es de 2048 bits y, por lo tanto, difícil de descifrar, el nivel de confianza en estos usuarios es moderado. Por ello, se recomienda limitar la validez de sus claves a un máximo de un año.
Nivel 3	1024 bits	Baja	6 meses	Para los usuarios comunes de correo electrónico, se establece un ciclo de vida de seis meses para sus claves. Esto se debe a que la longitud de sus claves es de 1024 bits, lo que las hace relativamente complejas de descifrar. Sin embargo, dado que el nivel de confianza en estos usuarios es bajo, se recomienda que la validez de sus claves sea limitada a medio año.

Tabla 134. Ciclo de vida de los certificados. (Fuente Propia)

Como se muestra en el cuadro, no todas las claves deben tener el mismo ciclo de vida; para reforzar la seguridad, es necesario limitar su periodo de validez. La forma más adecuada de definir esta duración es considerando factores clave, como la longitud de la clave y el nivel de confianza en el usuario. Aunque pueden existir otros elementos adicionales que las organizaciones podrían evaluar, en el caso de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., la definición se basa en estos criterios específicos. En conclusión, la configuración y gestión de las claves debe planificarse y analizarse cuidadosamente para establecer un estándar interno que facilite su administración. Asimismo, es fundamental definir claramente los parámetros temporales y los métodos criptográficos utilizados, asegurando así los niveles de seguridad necesarios para el servicio de correo electrónico en el que se aplicarán el cifrado y la firma digital. Finalmente, las mejores prácticas relacionadas con la gestión de claves deben documentarse en una política interna que detalle todos los aspectos de su configuración y manejo.

4.8 Prueba de concepto (POC).

La prueba de concepto POC de la implementación de cifrado PGP en la Cooperativa Uniotavalo es una demostración controlada que valida la viabilidad técnica y operativa de proteger comunicaciones vía SMTP (correos) y SFTP (transferencia de archivos) usando GNU Privacy Guard (GnuPG) con Outlook y FileZilla. Su objetivo es evidenciar cómo el cifrado asimétrico mitiga riesgos como interceptación de datos o ataques "hombre en el medio", mientras se mantiene la usabilidad en procesos diarios.

4.8.1 Escenario de prueba. (Tabla 6)

Rol	**Acción**	**Herramientas**
Remitente	Envía correo cifrado con PGP	Outlook + GpgOL (Gpg4win)
Destinatario	Recibe y descifra con clave privada	Kleopatra (Gpg4win)
Hacker	Intercepta el correo en tránsito	Wireshark

Tabla 145. Escenario de prueba (Fuente Propia)

Paso a paso para la POC:

1. Preparación del entorno

Instalar Gpg4win en equipos del remitente y destinatario:

Generar claves PGP RSA 2048 bits en ambos:

Abrir Kleopatra > "Nuevo par de claves" > RSA 2048 bits.

Exportar clave pública del destinatario (.asc) y compartirla con el remitente.

Este proceso se lo explico paso a paso en el apartado 4.3 de este proyecto.

2. Configurar Outlook para cifrado PGP

En el equipo del remitente:

Abrir Outlook y redactar correo, como lo muestra la Figura 41.

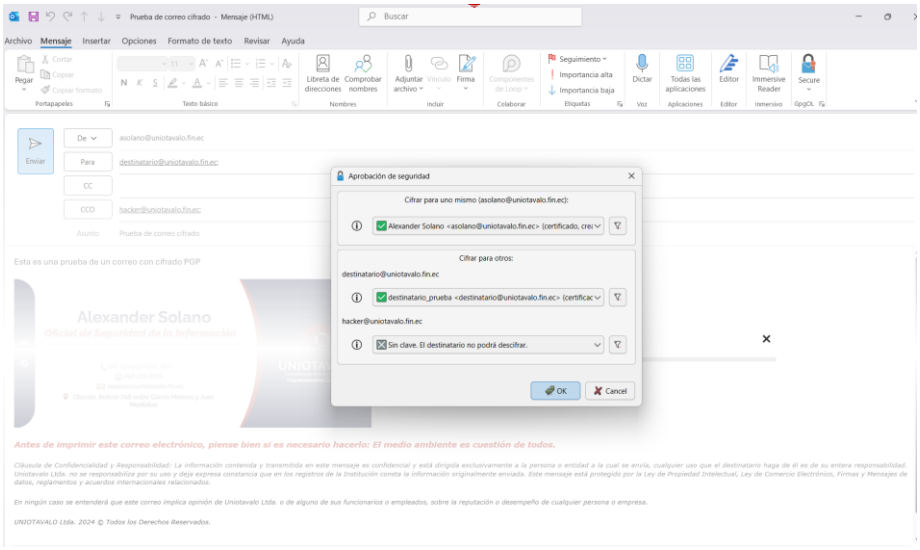


Figura 41. Configuración Outlook (Fuente Propia)

Clic en el icono GpgOL > Seleccionar "Encrypt".

Elegir la clave pública del destinatario.

Enviar correo (ejemplo: "Esto es una prueba de un correo con cifrado PGP").

3. Simular interceptación por hacker

Dentro del alcance del proyecto no contempla un proceso de ejecución de un ataque para demostrar la intercepción de canales SMTP y SFTP, en este sentido se emite un supuesto en el cual el hacker se apodera del correo y la información enviada, como se muestra en la Figura 42.

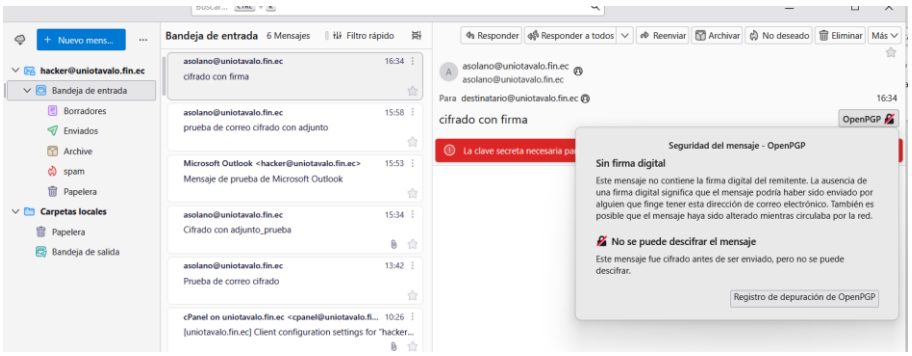


Figura 42. Simular interceptación por hacker (Fuente Propia)

Resultado:

Sin PGP: El hacker ve el contenido en texto claro.

Con PGP: Solo ve cifrado RSA 2048 bits (ilegible).

4. Verificación del destinatario

Destinatario:

Abre el correo en Outlook.

GpgOL solicita contraseña de su clave privada para descifrar, como se evidencia en la representación de la Figura 43.

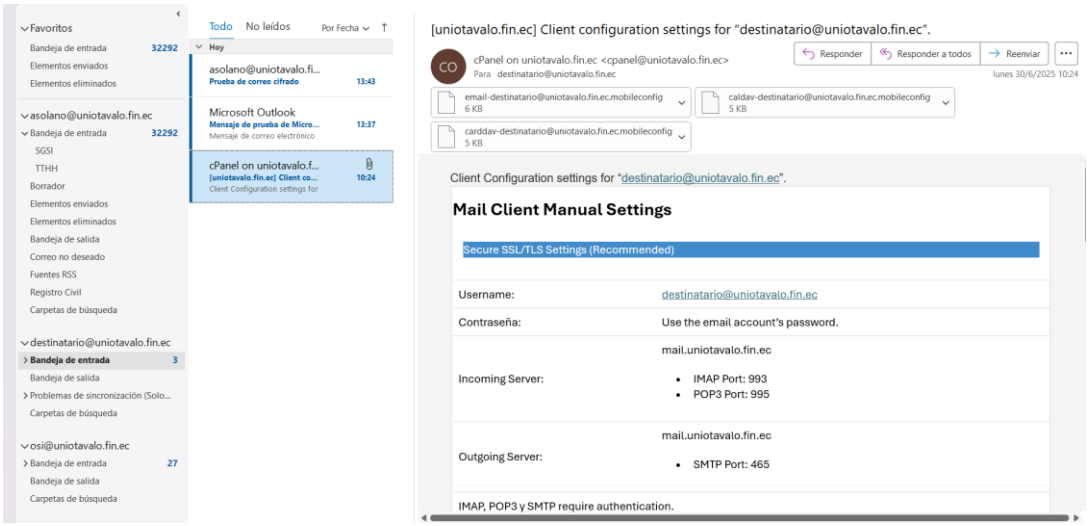


Figura 43. Verificación del destinatario (Fuente Propia)

Lee el mensaje original, como se muestra en la Figura 44.

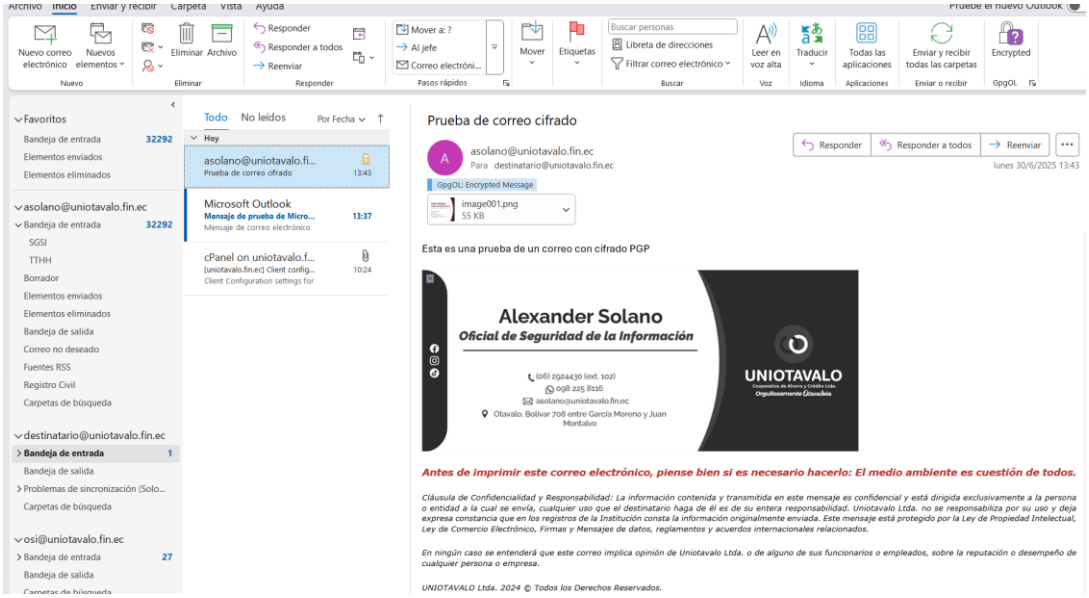


Figura 44. Lectura de mensaje (Fuente Propia)

Hacker:

Obtiene el correo, pero no lo puede abrir ni descifrar, según lo muestra la Figura 45.

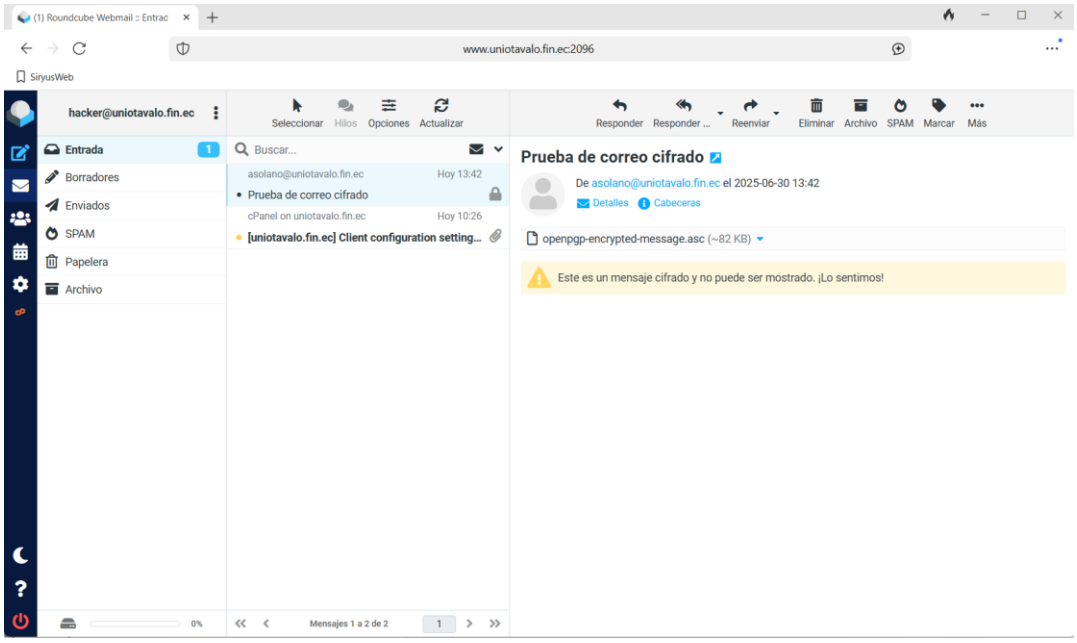


Figura 45. Recepción por parte del hacker (Fuente Propia)

Resultados de la POC: (Tabla 7)

Escenario	Destinatario	Hacker
Con PGP	✔ Lee el mensaje	✘ Cifrado ilegible
Sin PGP	✔ Lee el mensaje	✔ Lee el mensaje

Tabla 156. Resultados POC (Fuente Propia)

Evidencia técnica:

Cifrado PGP (RSA 2048 bits):

El hacker recibe un bloque cifrado, se lo evidencia en las Figuras 46 y 47.

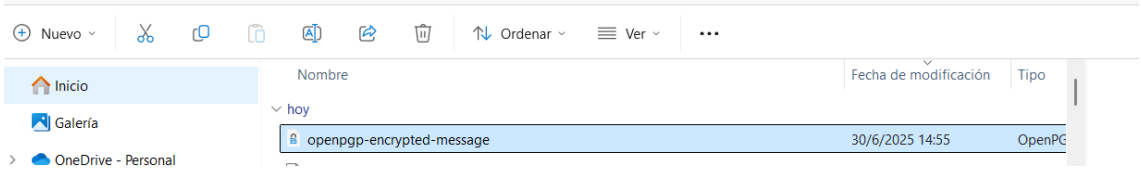


Figura 46. Cifrado PGP (RSA 2048 bits) (Fuente Propia)

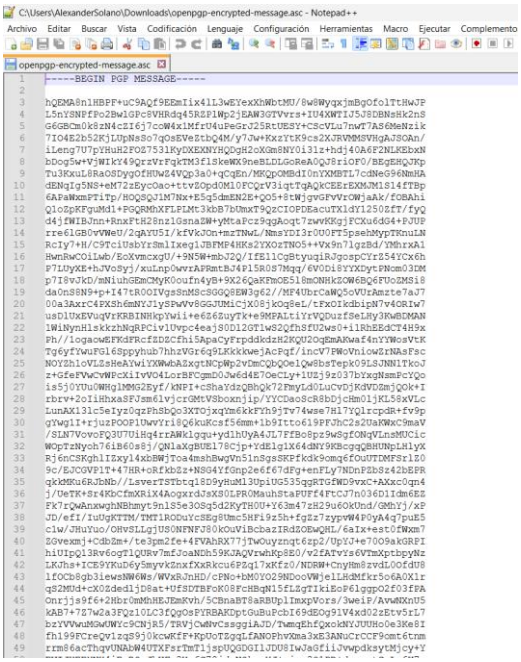


Figura 47. Cifrado PGP (RSA 2048 bits) (Fuente Propia)

Sin la clave privada, es computacionalmente inviable descifrarlo.

Sin cifrado:

El correo viaja en texto plano (SMTP no cifrado), expuesto a:

Ataques MITM en redes públicas.

Robo de datos sensibles, como se muestra en la Figura 48.

Figura 48. Descifrado de información (Fuente Propia)

Dentro del proceso de FileZilla.

Se deposita un archivo cifrado en la carpeta publica por error, y se ejecuta la prueba de concepto de que pasaría si personas no autorizadas obtiene el archivo, y se obtuvo lo que muestra la Figura 49.

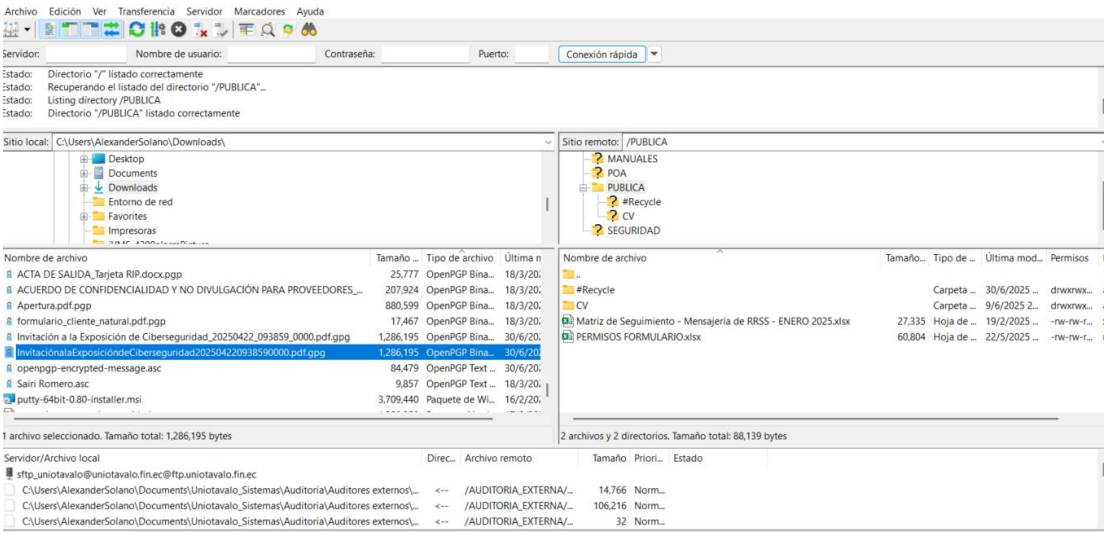


Figura 49. Proceso de envío de información por medio de FileZilla (Fuente Propia)

Usuarios con permisos: (Figura 50 y 51)

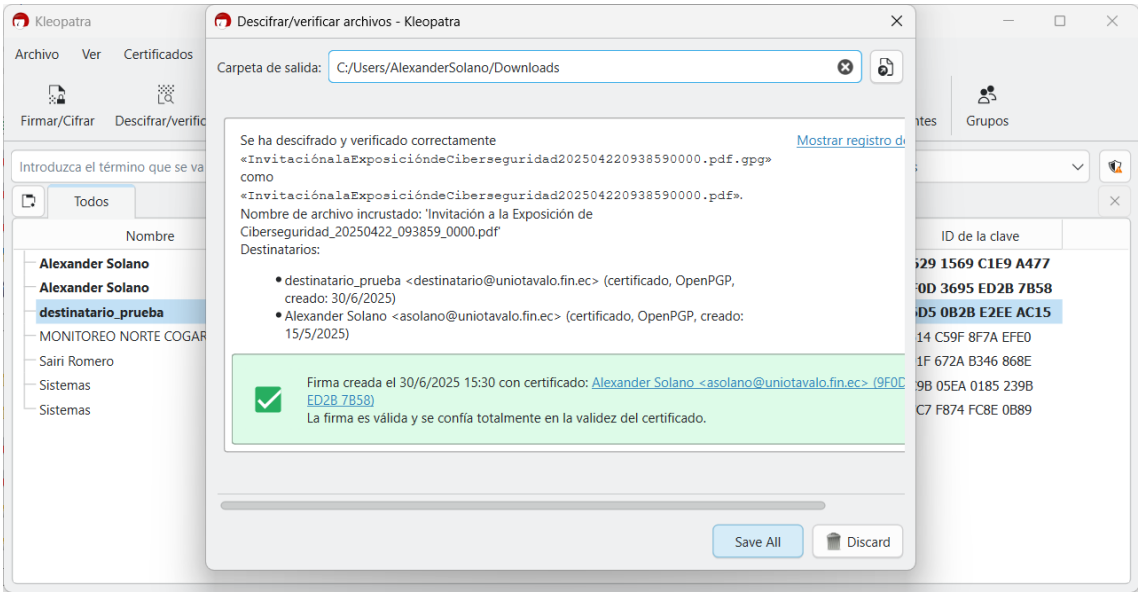


Figura 50. Certificación de permiso de usuario (Fuente Propia)

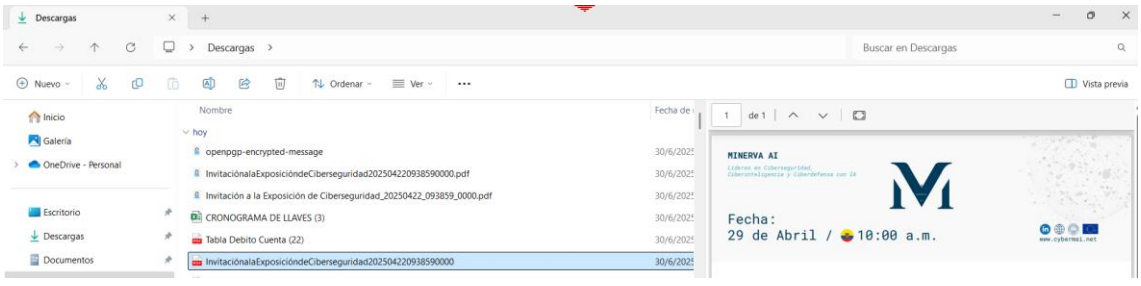


Figura 51. Descifrado por parte del usuario con permisos (Fuente Propia)

Usuarios sin permisos: (Figura 52 y 53)

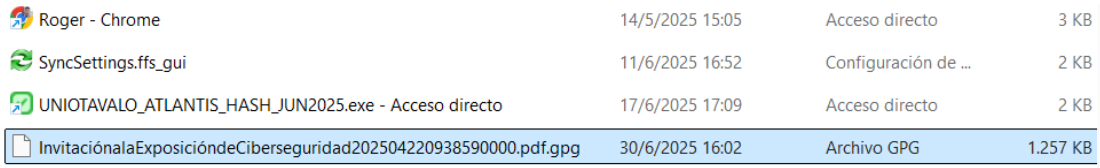


Figura 52. Descarga de información cifrada (Fuente Propia)

Figura 53. Información cifrada (Fuente Propia)

Conclusiones de la prueba:

Eficacia del PGP:

El cifrado asimétrico (RSA 2048 bits) garantiza confidencialidad e integridad y solo el destinatario con la clave privada puede acceder al contenido.

Riesgo sin cifrado:

Los correos en texto claro son vulnerables a interceptaciones en redes no seguras y los datos sensibles son expuestos violando las políticas de seguridad y regulaciones.

Recomendación para Uniotavalo:

Implementar PGP obligatorio para correos con datos confidenciales y capacitar al personal en uso de GpgOL y gestión de claves.

CAPITULO V

5 CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

La aplicación de la metodología MAGERIT permitió identificar y valorar de manera sistemática los riesgos asociados a los activos de información críticos de la Cooperativa, proporcionando una visión clara sobre las amenazas y vulnerabilidades que podrían afectar la continuidad y seguridad de las operaciones. La elección de PGP aseguró un alto nivel de seguridad mediante un estándar reconocido, protegiendo la confidencialidad e integridad de las comunicaciones dentro y fuera de la Cooperativa, al mismo tiempo que facilitó la integración técnica con los sistemas existentes y la capacitación del personal, lo que promovió una adopción eficiente y el cumplimiento normativo en el manejo de información sensible.

Gracias a MAGERIT, la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., obtuvo una base sólida y estructurada para priorizar acciones de mitigación y asignar recursos de manera eficiente, fortaleciendo su capacidad de prevención y respuesta ante incidentes que comprometan la seguridad de la información.

Para proteger el correo electrónico y la transferencia de archivos, se seleccionó la metodología de cifrado asimétrico GNUpg que permitió la integración de PGP (Pretty Good Privacy), un estándar ampliamente reconocido y utilizado para garantizar la seguridad, confidencialidad e integridad de la información. GNUpg utiliza un sistema de claves públicas y privadas que asegura que solo los destinatarios autorizados puedan acceder al contenido cifrado, además de validar la autenticidad mediante firmas digitales.

La implementación de PGP como solución de cifrado asimétrico demostró ser una estrategia efectiva para fortalecer la seguridad de la comunicación electrónica y la transferencia de archivos. Su adopción permitió garantizar la confidencialidad, integridad y autenticidad de la información, tanto en los procesos internos como en los intercambios con entidades externas. Además, su compatibilidad con estándares internacionales y su capacidad de adaptación a diferentes entornos tecnológicos la convierten en una herramienta sólida y sostenible para la protección de datos en contextos organizacionales exigentes.

5.2 Recomendaciones.

Se recomienda implementar la solución propuesta en la Cooperativa de Ahorro y

Crédito Uniotavalo Ltda., objeto de este estudio, ya que mejora significativamente la integridad y confidencialidad de la información transmitida mediante los protocolos analizados. Esto garantiza la fiabilidad de los usuarios involucrados y asegura la inmutabilidad de los datos, contribuyendo a preservar la reputación de la organización frente a posibles ataques tanto internos como externos.

El diseño contempla las aplicaciones necesarias para automatizar y facilitar la experiencia de los usuarios finales, incluyendo empleados internos, proveedores y clientes. La propuesta integra la tecnología basada en el estándar PGP, tal como se ha detallado en este proyecto de tesis.

Además, es aconsejable evaluar la viabilidad de esta solución en otros sectores empresariales distintos al financiero, extendiendo su aplicación a todo tipo de organizaciones. De hecho, se sugiere ampliar el alcance a instituciones que requieran proteger su información de extremo a extremo, ya sea en reposo o en tránsito, para asegurar el éxito de sus proyectos colaborativos con otras entidades.

REFERENCIAS

- Chicano Tejada, E. (2023). Auditoría de seguridad informática. IFCT0109: (2 ed.). Antequera, IC Editorial. Recuperado de https://elibro.net/es/ereader/utnorte/232692?
- Piattini Velthuis, M. (2015). Auditoría de tecnologías y sistemas de información: (ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial. Recuperado de https://elibro.net/es/ereader/utnorte/106490?
- Hernández Encinas, L. (2016). La criptografía: (ed.). Madrid, Spain: Editorial CSIC Consejo Superior de Investigaciones Científicas. Recuperado de https://elibro.net/es/ereader/utnorte/41843? .
- Piattini Velthuis, M. (2015). Auditoría de tecnologías y sistemas de información: (ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial. Recuperado de https://elibro.net/es/ereader/utnorte/106490?
- García, R. D. M. (2009). Criptografía clásica y moderna: (ed.). Oviedo, Septem Ediciones. Recuperado de https://elibro.net/es/ereader/utnorte/102985?.:
- Gómez Vieites, Á. (2010). Seguridad informática, básico: (ed.). Bogotá, Ecoe Ediciones. Recuperado de https://elibro.net/es/ereader/utnorte/130461
- Batten, L. M. (2013). Public Key Cryptography: Applications and Attacks. http://ieeexplore.ieee.org.upc.remotexs.xyz/xpl/ebooks/bookPdfWithBanner.jsp?fileName=6482702.pdf&bkn=6480474&pdfType=chapter
- Ecured. (2018). Curva elíptica. https://www.ecured.cu/Curva_elíptica
- Abdelkader, K. J. K. N. y T. (2019). Un esquema de cifrado eficiente y liviano netamente autenticado para la seguridad del correo electrónico. http://ieeexplore.ieee.org.upc.remotexs.xyz/stamp/stamp.jsp?tp=&arnumber=8935
- Barker, E. (2016). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. https://doi.org/10.6028/NIST.SP.800
- Dolmatov. (2010). RFC 5830 - GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms. https://tools.ietf.org/html/rfc5830 Ecured. (2018). Curva elíptica. https://www.ecured.cu/Curva_elíptica
- Gartner. (2016). Productos comerciales de encriptación asimétrica para correos electrónicos. https://www.gartner.com/doc/reprints?id=12XU816T&ct=160203&st=sb

- Gilchrist. (1999). The https://tools.ietf.org/rfc/rfc2612.txt
- Edigital, (2024). Smuggling SMTP, una amenaza emergente en la seguridad de correos electrónicos https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1815/
- Buckbee, Michael. (2023). ¿Qué es el Cifrado PGP y Cómo Funciona?. https://www.varonis.com/blog/pgp-encryption
- Gómez Fernández, L. y Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad: (ed.). Madrid, Spain: AENOR - Asociación Española de Normalización y Certificación. Recuperado de https://elibro.net/es/ereader/utnorte/
- Maillo Fernández, J. A. (2017). Sistemas seguros de acceso y transmisión de datos: (ed.). Paracuellos de Jarama, Madrid, RA-MA Editorial. Recuperado de https://elibro.net/es/ereader/utnorte/106503?
- Mendoza, C. (2015). METODOS DE ATAQUE INFORMATICOS". https://dspace.ups.edu.ec/bitstream/123456789/8185/1/Demostración de cifrado simétrico y asimétrico.pdf
- Gartner EPP (2024), tecnozero / Blog /, https://www.tecnozero.com/blog/cuadrante-gartner-epp-2024/
- INCIBE,(2021), Guía para el uso de PGP en clientes de correo electrónicohttps://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_cert_guia_para_el_uso_de_pgp_en_clientes_de_correo_electronico.pdf
- JSCAPE,(2025), PGP vs GPG: Las Diferencias Clave Explicadas, https://www.jscape.com/blog/pgp-vs-gpg-the-key-differences-explained.
- semana. (2017). Ataque informático en Ucrania más fuerte que el WannaCry. https://www.semana.com/mundo/articulo/ataque-informatico-en-ucrania-mas fuerte-que-el-wannacry/530605.
- Chaiwut, N., & Rueangsirarak, W. (2022). An online gap analysis on cyber security principles for Thailand organizations based on ISO/IEC 27001:2013 standard. 2022 6th International Conference on Information Technology (InCIT).

- Dickenson, Aidan (2023), Seguridad del correo electrónico, ¿Cómo elegir entre S/MIME y PGP para el cifrado de correo electrónico?

https://www.linkedin.com/advice/0/how-do-you-choose-between-smime-pgp-email.

- Parra, A. (n.d.). Características de la investigación documental. QuestionPro. Retrieved September 21, 2024, from https://www.questionpro.com/blog/es/investigacion-documental/

- QuestionPro. (2023, August 16). ¿Qué es la investigación de campo? Características y ejemplos. QuestionPro. https://www.questionpro.com/es/investigacion-de-campo.html

ANEXOS

Anexo 1. Solicitud de autorización de ejecución del proyecto de tesis.

UNIOTAVALO
Cooperativa de Ahorro y Crédito Ltda
Acuerdo Ministerial N°. 206 del 26 de Enero 2009

Otavalo, 29 de mayo de 2025

MSc. Anita Catucuago
GERENTE GENERAL
COOPERATIVA DE AHORRO Y CREDITO UNIOTAVALO LTDA

De mi consideración

Junto a un cordial saludo me dirijo a su persona, para informarle que actualmente egrese de la maestría en computación mención en seguridad informática en la Universidad Técnica del Norte, por lo cual solicito su debida autorización para poder ejecutar el proyecto de investigación denominado **"IMPLEMENTACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA PGP PARA LA PROTECCIÓN DE DATOS EN COMUNICACIONES SMTP Y SFTP DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIOTAVALO LTDA."**

Con el desarrollo de este tema planteado se fortalecerá la seguridad de la información tanto en reposo como en tránsito, a través de los medios digitales como son los correos y herramientas SFTP que se utilizan para compartir información de la Cooperativa.
Con estos antecedentes, solicito a usted su autorización para gestionar el tema de tesis en mención; el mismo que beneficiara a la Cooperativa en el ámbito de la seguridad informática.

Con sentimiento de distinguida consideración.

Atentamente,

UNIOTAVALO
Cooperativa de Ahorro y Crédito Ltda.
Ing. Alexander Solano

Ing. Jaime Alexander Solano Santacruz
OFICIAL DE SEGURIDAD DE LA INFORMACION
COOPERATIVA DE AHORRO Y CREDITO UNIOTAVALO LTDA.

OTAVALO
Bolívar 708 entre García Moreno y Juan Montalvo

IBARRA
Chica Narváez 6-11 y Juan José Flores

(06)2 924 430

Anexo 2. Aprobación de ejecución del proyecto de tesis.

UNIOTAVALO
Cooperativa de Ahorro y Crédito Ltda
Acuerdo Ministerial Nº. 206 del 26 de Enero 2009

Oficio Nro. GG-010-23-06-2025

Ibarra, 23 de junio de 2025

Ingeniero
Jaime Alexander Solano Santacruz
Maestrante Universidad Técnica del Norte
Oficial de Seguridad de la Información COAC Uniotavalo
Presente.-

De mi consideración:

Reciban un cordial saludo de parte de la Cooperativa de Ahorro y Crédito Uniotavalo Ltda., institución comprometida con el desarrollo social y económico de nuestra comunidad.

Por medio de la presente me dirijo a usted con la finalidad de dar contestación al oficio con fecha 29/05/2025 e informarle la aceptación de su solicitud para la realización de su proyecto de investigación denominado "IMPLEMENTACIÓN DE CRIPTOGRAFÍA ASIMÉTRICA PGP PARA LA PROTECCIÓN DE DATOS EN COMUNICACIONES SMTP Y SFTP DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIOTAVALO LTDA.", con el acceso a información con fines educativos y bajo la norma de confidencialidad.

Agradeciendo su atención, me suscribo con la mayor consideración.

Atentamente,

Mgs. Anita Catucuago
Gerente General
COAC UNIOTAVALO LTDA.

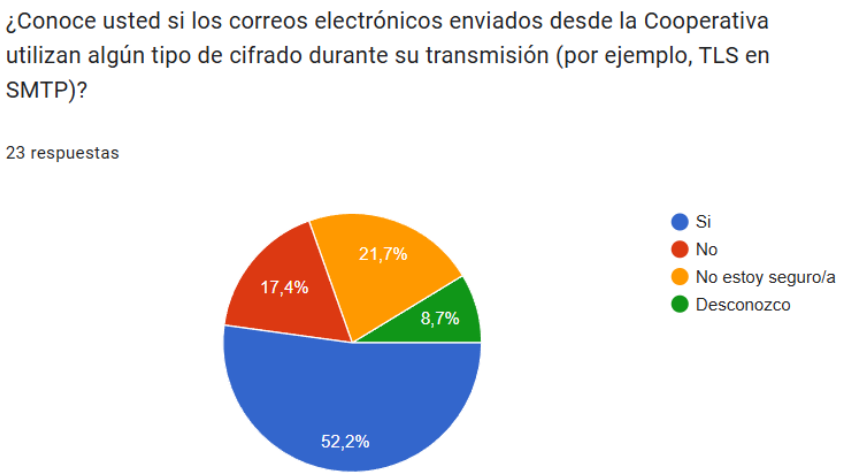
OTAVALO
Bolívar 708 entre García Moreno y Juan Montalvo

IBARRA
Chica Narváez 6-11 y Juan José Flores

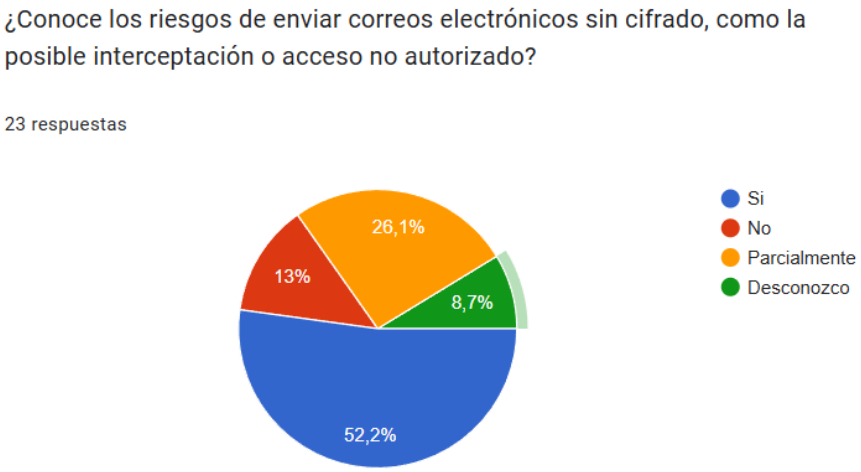
(06)2 924 430

Anexo 3. Pregunta 1. ¿Conoce usted si los correos electrónicos enviados desde la

Cooperativa utilizan algún tipo de cifrado durante su transmisión (por ejemplo, TLS en SMTP)?



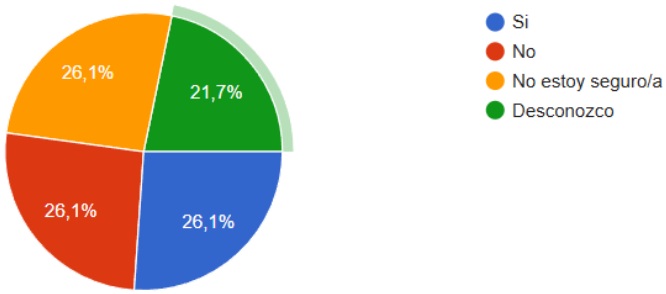
Anexo 4. Pregunta 2. ¿Está informado sobre los riesgos asociados al envío de correos electrónicos sin cifrado, como la posible interceptación o acceso no autorizado a la información?



Anexo 5. Pregunta 3. ¿Considera que la información enviada por correo electrónico actualmente es lo suficientemente segura para proteger datos sensibles?

¿Considera que la información enviada actualmente por correo electrónico es lo suficientemente segura para proteger datos sensibles?

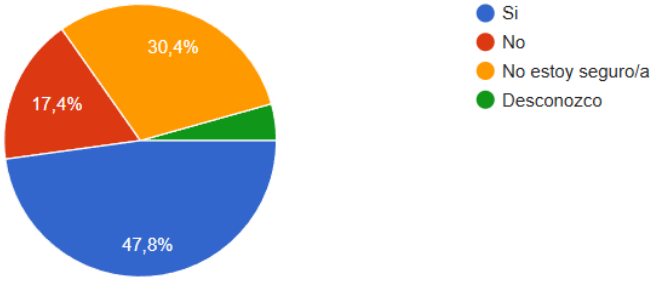
23 respuestas



Anexo 6. Pregunta 4. ¿Sabe si los archivos transferidos mediante SFTP en la Cooperativa están protegidos por mecanismos de cifrado durante su transmisión?

¿Sabe si los archivos transferidos mediante SFTP están protegidos por mecanismos de cifrado durante la transmisión?

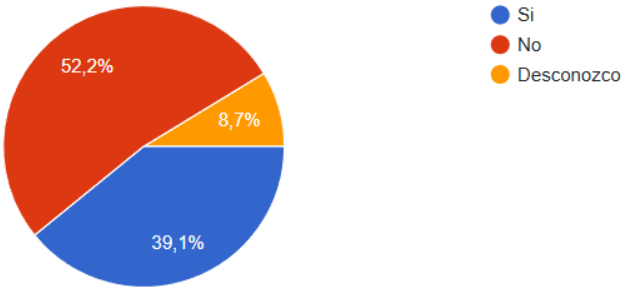
23 respuestas



Anexo 7. Pregunta 5. ¿Está familiarizado con la diferencia entre cifrado en tránsito (protección mientras la información viaja por la red) y cifrado en reposo (protección cuando la información está almacenada)?

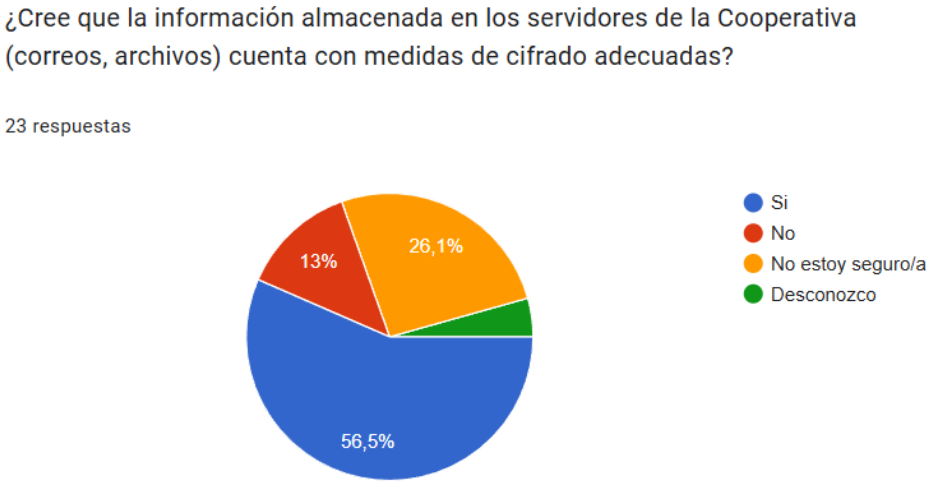
¿Distingue la diferencia entre cifrado en tránsito (protección mientras viaja por la red) y cifrado en reposo (protección mientras está almacenada)?

23 respuestas

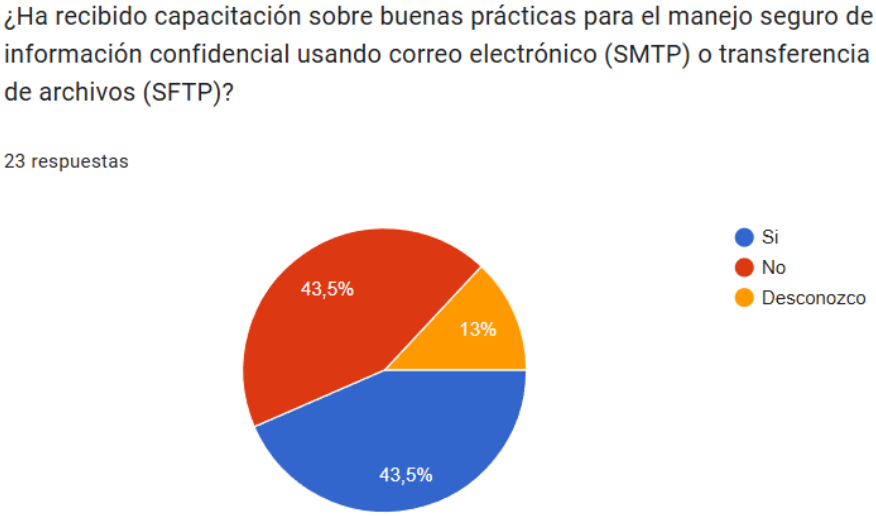


Anexo 8. Pregunta 6. ¿Cree que la información almacenada en los servidores de la

Cooperativa (correos electrónicos, archivos) cuenta con las medidas de cifrado adecuadas?



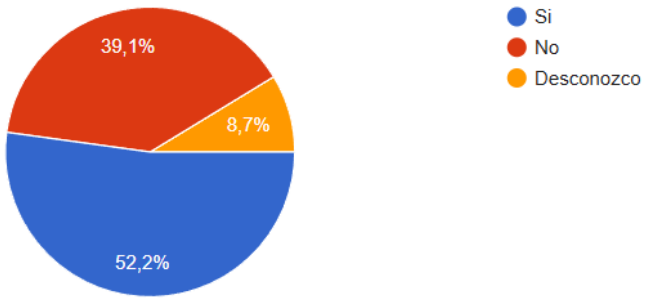
Anexo 9. Pregunta 7. ¿Ha recibido capacitación o información sobre buenas prácticas para el manejo seguro de información confidencial utilizando correo electrónico (SMTP) o transferencia de archivos (SFTP)?



Anexo 10. Pregunta 8. ¿Está al tanto de la existencia de mecanismos de cifrado asimétrico, como PGP, para proteger la información que se envía o almacena?

¿Está familiarizado/a con mecanismos de cifrado asimétrico, como PGP, para proteger la información enviada o almacenada?

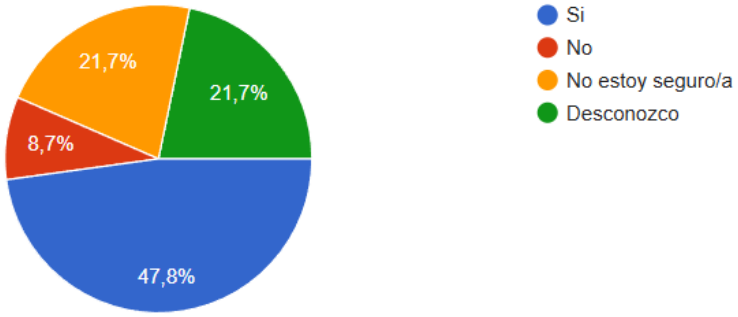
23 respuestas



Anexo 11. Pregunta 9. ¿Considera necesario implementar soluciones adicionales de cifrado, como PGP, para fortalecer la seguridad de la información?

¿Considera necesario implementar soluciones adicionales de cifrado, como PGP, para fortalecer la seguridad de la información?

23 respuestas



Anexo 12. Pregunta 10. ¿Cuál es su nivel de confianza en los actuales procedimientos de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información enviada y recibida a través de correo electrónico y SFTP?

¿Qué nivel de confianza tiene en los actuales procedimientos de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información enviada y recibida por correo electrónico y SFTP?

23 respuestas