ANALISIS Y DISEÑO DE UN MECANISMO DE CIFRADO DE CORREO ELECTRONICO PARA GARANTIZAR Y PROTEGER LA INFORMACION ENVIADA DE LAS PYMES

YESID HERNANDEZ MARIN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2020

ANALISIS Y DISEÑO DE UN MECANISMO DE CIFRADO DE CORREO ELECTRONICO PARA GARANTIZAR Y PROTEGER LA INFORMACION ENVIADA DE LAS PYMES

YESID HERNANDEZ MARIN

Trabajo de grado para optar el título de:
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director
YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, Octubre 2020

Dedico este proyecto de grado a mi familia, especialmente a mi esposa e hija quienes han sido mi inspiración para salir adelante y continuar con mi formación profesional.

Yesid Hernandez Marin

AGRADECIMIENTOS

Agradezco a mi Esposa e Hija por ser mi gran motivación y orgullo, han sido parte fundamental para cumplir todos mis proyectos personales, laborales y académicos. No es fácil, eso lo sé, pero tal vez si no las tuviera, no habría obtenido tantos logros.

Le agradezco a Dios por darme la fortaleza y sabiduría necesaria para afrontar todas las adversidades. Por enseñarme que si algo se desea se debe luchar por ellos nunca darse por vencido.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: Es cualquier elemento que contenga información para el desarrollo de las actividades puede ser físico o digital.

AES: Advanced Encryption Standard, es un esquema de cifrado simétrico por bloques.

ADWARE: Es un programa que se instala de forma automática con el fin de presentar publicidad con el fin de beneficiar a su creador.

AGUJERO DE SEGURIDAD: Dícese de una falla que se puede tener en un sistema.

ALGORITMO DE CIFRADO: Operación o funciona matemática para generar una clave para garantizar la confidencialidad e integridad de la información.

AMENAZA: Es un evento que se puede materializar y generar afectación sobre los activos de información.

ANTIVIRUS: Programa diseñado para detectar, bloquear y eliminar código malicioso (programas no solicitados, virus, troyanos, gusanos, etc.).

ANALISIS DE RIESGO: Es un proceso donde se validan los activos de información y documentan todas las posibles amenazas y los controles que se tendrían que aplicar para asegurar estos activos.

ATAQUE DE FUERZA BRUTA: Es la acción de averiguar las claves por medio de combinación de contraseñas hasta conseguir la adecuada.

AUDITORIA DE SISTEMAS: Es una revisión de sobre la implementación de controles de Seguridad de sistemas y gestión sobre los mismo.

AUTORIDAD DE CERTIFICACION: Es el ente designado para garantizar la identidad de los titulares en cuento a sus certificados y firmas digitales.

BACKDOOR: Es un punto débil por donde ingresar una persona no autorizada.

BACKUP: Hace referencia al respaldo que se debe tener sobre cualquier sistema.

BIA: Se trata de un análisis de los posibles riesgos que puede tener si se materializan eventos o amenazas.

BIOMETRIA: Es un método de reconocimiento de características fisiológicas ((huellas dactilares, retinas, iris, cara).

BOMBA LÓGICA: Parte de código insertado que permanece oculto hasta el momento que se configuro para ejecutar alguna acción maliciosa.

CERTIFICADO DIGITAL: Es un fichero digital generado por una autoridad certificadora que asocia la información del titular.

CIBERDELINCUENTE: Son personas que utilizan su conocimiento para realizar actividades delictivas en internet como el robo de información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad en el ciberespacio.

CIBERESPACIO: Es un entorno virtual artificial, es decir, no físico e intangible, que se desarrolla mediante herramientas informáticas, que permite la interacción e intercambio de información.

CIFRADO: Acción de ocultar o codificar información para evitar que personas no autorizadas puedan acceder a la misma.

CLAVE PÚBLICA: Son claves de cifrado que se pueden compartir para descifrar la información.

CLAVE PRIVADA: Son las claves de cifrado que son exclusivas de los Titulares sobre su información.

CONDIFIDENCIALIDAD: Acción de garantizar la que la información sea accedida por las personas autorizadas.

COOKIE(S): Hace referencia a un pequeño conjunto de información enviada desde internet por parte de los sitios web y que es almacenada dentro del equipo.

CRIPTOGRAFIA: Es la técnica que consiste en cifrar un mensaje.

DISPONIBILIDAD: Se trata de capacidad de tener la información siempre disponible o accesible.

DES: Data Encryption Standard, esquema de encriptación simétrico.

DLP: Data Loss Prevention, herramienta o aplicación con la finalidad de prevenir fugas de información.

DSA: Digital Signature Algorithm, método de cifrado que utiliza un algoritmo de firma diferente al RSA.

ECDSA: Algoritmo de Firma Digital de Curva Elíptica.
EVENTO DE SEGURIDAD: Cualquier acción que pueda llegar a afectar la confidencialidad, integridad y disponibilidad de la información.

EXPLOIT: Secuencia de comandos para aprovecharse de una falla o puerta trasera (*backdoor*) de un sistema.

FIRMA ELECTRONICA: Conjunto de datos electrónicos que contiene la información del titular para garantizar su autenticidad.

FUGA DE DATOS: Es la perdida de confidencialidad de la información.

FTP: Protocolo para trasferencia de archivos.

GUSANO: Es un programa malicioso o malware que se propaga de forma rápida.

HASH: Es un algoritmo matemático que trasforma los datos en una nueva secuencia.

INCIDENTE DE SEGURIDAD: Cualquier evento o riesgo materializado que afecte de forma negativa la confidencialidad, integridad y disponibilidad de la información.

INGENIERIA SOCIAL: Técnica para sustraer información de naturaleza sensible.

INTEGRIDAD: Es la propiedad de garantizar la exactitud de la información.

MALWARE: Es un software que tiene como objetivo dañar o infiltrarse en un sistema.

MD5: Uno de los primeros métodos de cifrado.

NO REPUDIO: Es la capacidad de demostrar la identidad de la información de ser de quien dice ser.

PARCHE DE SEGURIDAD: Son los cambios para garantizar el cierre de errores sobre los sistemas.

PENTEST: Son pruebas controladas sobre el software o hardware para validar su seguridad.

PHISHING: Es una estafa a través de correo electrónico con el fin de sacar información confidencial o sensible.

PGP: Es un programa para proteger la información por medio del cifrado.

POLITICA DE SEGURIDAD: Son las decisiones y medidas de seguridad de una empresa.

PROTOCOLO: Se trata de una regla estándar.

RANSOMWARE: La acción por la que un ciberdelincuente toma control o secuestra la información haciéndola inaccesible, hasta recibir algo a cambio.

RSA: Se trata de un sistema criptográfico de clave pública para cifrar documentos o firmarlos digitalmente.

SGSI: Sistema de gestión de seguridad de información.

SHA1: Secure Hash Algorithm, algotitmo de cifrado seguro.

SMTP: Protocolo simple de trasferencia de correo.

SPEARPHISHING: Es una estafa a través de correo electrónico dirigida a un grupo u organización con el fin de sacar información confidencial o sensible.

SPOOFING: Es la técnica de suplantación de identidad llevada a cabo por ciberdelincuentes.

SPYWARE: Es un malware que recopila información de un computador y la envía de forma remota a los ciberdelincuentes.

TRIPLEDES: Realiza triple cifrado del DES

TROYANO: Se trata de un malware o programa malicioso con la capacidad de auto replicarse y expandirse en otros sistemas.

TWOFISH: Es un algoritmo de cifrado simétrico por bloques.

VIRUS: Programa que se instala de forma automática con el único propósito de infectar o dañar el sistema.

VULNERABILIDAD: Fallos o deficiencias de un sistema que permite acceder de forma no legítima.

RESUMEN

El presente proyecto aplicado tiene como propósito presentar un método de aplicación de prácticas adecuadas para el manejo de correo electrónico corporativo, aplicable a micro, pequeñas y medianas empresas. El método propuesto está basado en un análisis previo a los activos de información, los procesos y los riesgos de seguridad de la información de este tipo de organizaciones frente a las amenazas latentes en el ciberespacio y al cumplimiento de los requerimientos normativos a nivel nacional correspondientes a los delitos informáticos y la protección de datos personales. El documento pretende dar un listado de parámetros e instrucciones a seguir, sin la necesidad de realizar grandes inversiones económicas en la infraestructura y en los procesos organizacionales de este tipo de empresas.

Este documento se basa en una investigación deductiva que se desarrolla mediante la premisa: todas las empresas que reciben, procesen o trasmiten información clasificada como confidencial, requieren conocer toda la normatividad legal y la correcta gestión de los activos de información de su negocio.

Palabras clave: Correo electrónico, Phishing, Ramsonware, Cifrado, Ciberataque, Vulnerabilidades.

ABSTRACT

The purpose of this applied project is to present a method of appropriate applying practices for corporate email management, it is applicable to SMEs. The proposed method is based on a prior analysis of the information assets, processes and information security risks according to this type of organization in order to face not only the latent threats in cyberspace but also the compliance with the regulatory requirements at the national level corresponding to computer crimes and the personal data protection. The document aims to give a list of parameters and instructions to avoid large economic investments in infrastructure and in the organizational processes of SMEs.

This document is based on a deductive research that is carried out using the premise: all companies that receive, process or transmit classified information considered as confidential require to know all the legal regulations and the correct management of the information assets of their business.

Key words: Email, Phishing, Ramsonware, Encryption, Cyber attack, Vulnerabilities.

INTRODUCCION

En Colombia existe un alto número de empresas clasificadas como micro, pequeñas y medianas que cubren el 80% de plazas laborales en el país y cubren del 90% al 94% de los sectores productivos en el país, que aportan aproximadamente el 40% del Producto Interno Bruto (PIB) [1],[2] las cuales tienen requerimientos intrínsecos de transferencia de información entre empleados, clientes, proveedores, entidades públicas, entre otros, lo cual genera necesidades no evidentes de seguridad de la información a los ojos de los emprendedores y empresarios que dirigen dichos establecimientos. Actualmente las compañías suelen manejar volúmenes de información por medio de sistemas de información, navegación en internet y correos electrónicos para realizar parte del proceso de comunicación interna y externa de información del negocio, este flujo de datos puede contener información que sea sensible y tener repercusiones legales, comerciales, civiles y económicas si llegase a quedar en manos de personas ajenas a la empresa o en su defecto en quien no corresponde dentro de la misma, información que puede quedar expuesta de manera pública, por ende convirtiéndose en un activo importante para personas inescrupulosas que pueden tener diversas motivaciones y causar daño a las empresas, generando interrupción en los procesos que se llevan a cabo en el día a día y que pueden ir del acceso a un archivo en un computador infectado a la pérdida de toda la información.

Esta connotación se ha hecho evidente por múltiples empresas de servicios de tecnología y ciberseguridad, en una encuesta de Cisco realizada en 26 países, informa que el 53% de las pymes encuestadas (n=1816) recibió algún tipo de ciberataque y que los cinco principales tipos de ataques recibidos son: Suplantación de identidad (Phishing), Amenazas Avanzadas Persistentes (Advanced Persistent Threats APT), Secuestro de datos (Ransomware), Ataques distribuidos de Denegación de Servicios (Distributed Denial of Service DDoS) y el uso no controlado de dispositivos personales en el entorno empresarial (Bring your own device, BYOD) [3], según el análisis de Comparitech en 2019 de 60 países Colombia ocupa el puesto 39 con mayores riesgos de sufrir un ataque de

[1] El Tiempo, «Eltiempo.com,» 26 Diciembre 2019. [En línea]. Available: https://www.eltiempo.com/economia/sectores/competitividad-de-las-pymes-en-colombia-para-2020-446922. [Último acceso: 05 Enero 2020].

[2] H. Monterrosa, «La Republica.com,» 31 Agosto 2019. [En línea]. Available: https://www.larepublica.co/economia/mipymes-representan-96-del-tejido-empresarial-y-aportan-40-al-pib-2903247. [Último acceso: 05 Enero 2020].

[3] Colomboamericana, Cámara de Comercio, «https://www.amchamcolombia.co/,» 2019. [En línea]. Available: https://www.amchamcolombia.co/es/comunicaciones/noticias-afiliados/1767-cisco-la-ciberseguridad-tambi%C3%A9n-es-un-reto-para-las-pymes. [Último acceso: 05 Enero 2020].

Ciberseguridad [4], en el último informe de tendencias de la Cámara Colombia de Informática y Telecomunicaciones CCIT, el último año los delitos informáticos se enfocan a las pymes, entidades financieras y grandes empresas con una concentración importante en Bogotá, Cali, Medellín Barranquilla y Bucaramanga [5].

Uno de los vectores de ataque más conocidos y empleados por los ciber delincuentes es la suplantación de identidad o Phishing, el cual muchas veces se filtra por medio de correo electrónico, los diversos métodos de ataque por phishing siempre tienen como objetivo comprometer de alguna forma información privada, confidencial o sensible lo que implica el uso de métodos de protección tanto para la información y las credenciales de acceso como para los medios de transmisión, es por este motivo que muchas empresas tienen como prioridad implementar políticas o técnicas de cifrado en su información general incluyendo la transmitida por correo electrónico, existiendo aquí el mayor riesgo de vulnerabilidad o sensibilidad en los datos intercambiados, en este contexto entra la aplicación fundamental del cifrado (utilización de llaves públicas o privadas, firmas digitales, apertura biométrica, entre otros) lo que puede garantizar que la comunicación se realice de manera satisfactoria y sin obstáculos entre el emisor y receptor de la misma, manteniendo la integridad de los datos que se quieren transferir.

Con el propósito de ofrecer una herramienta documentada útil y práctica para los empresarios, el autor consideró necesario hacer un diagnóstico sencillo orientado al público de las pymes, que le permitiera conocer de forma general el nivel de incorporación de los conceptos de seguridad de la información relacionados con el uso de correo electrónico, que trabajadores y empresarios usan en su labor diaria en las actividades desarrolladas por este tipo de empresas. Esta encuesta permitió al autor comprender que, aunque actualmente la tecnología está incluida en casi todos los procesos de una empresa, no necesariamente los funcionarios y empresarios conocen o aplican varias de prácticas de aseguramiento recomendadas en la literatura técnica, en general la mitad o menos de los encuestados conocen los controles de seguridad aplicados relacionados con la protección de correo electrónicos e incluso de las configuraciones de los mismos en su empresa.

Al revisar los datos obtenidos por medio de la encuesta realizada, el autor decidió documentar de manera breve un conjunto de conceptos básicos, técnicos y jurídicos, orientados a la formación de un referente de uso fácil que dirija al lector al conocimiento de la infraestructura y funcionamiento básico de las herramientas de correo electrónico y los medios de protección de la información. Este conjunto

[4] A. A. Tous-Mulkay, «Finanzas Personales.co,» 06 10 2019. [En línea]. Available: https://www.finanzaspersonales.co/columnistas/articulo/principales-riesgos-de-ciberseguridad-en-las-pymes/79732. [Último acceso: 01 02 2020].

[5] CCIT, «TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020,» 29 10 2019. [En línea]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. [Último acceso: 03 02 2020].

de herramientas documentadas, están antecedidas por una descripción de ataques que son comunes a los elementos de correo electrónico, los objetivos de protección de la información y controles de referencia para asegurar este tipo de activos, posteriormente se dan a conocer conceptos de gestión de activos de la información, cifrado, lineamientos en la gestión de correos electrónicos y en el aseguramiento de plataformas.

El último capítulo de este documento describe de manera breve los impactos esperados de los conceptos y metodología descritos, también reporta las conclusiones producto del análisis de información, evaluación y comparación de los resultados obtenidos durante la investigación.

1. PLANTEAMIENTO DEL PROBLEMA

Para las empresas en general es de vital importancia dar un buen manejo a la información enviada por correo electrónico, el no contar con una metodología de protección de esta información (cifrado) puede llevar a la pérdida o manipulación de la misma por parte de terceros no autorizados violando los principios de confidencialidad e integridad.

1.1 DESCRIPCIÓN DEL PROBLEMA

Como la mayoría de empresas, las PYMES manejan información que se puede considerar sensible o de carácter privado, por eso deben contar con un sistema de seguridad de la información holístico a nivel de la dirección, procesos y en su infraestructura diseñado para cubrir sus necesidades específicas de negocio. Sin embargo, estas implementaciones tienen costos elevados a nivel económico, de implementación, conocimiento y formación siendo generalmente relegados por el impacto que generan en su diseño e implementación, por ello se surge la necesidad de desarrollar componentes de aseguramiento ajustados a cada empresa, así se debe realizar en primera medida una correcta identificación de activos de información con el objetivo de diseñar y aplicar controles específicos para proteger la información que se transmite interna y externamente y puede llegar a ser usada de forma incorrecta, si no se cuenta con la seguridad adecuada o mejor aún metodología adecuada para el manejo de esta información.

Con el fin de cumplir con la normatividad vigente y asegurar la información que se trasmita o recibe se procuró dar respuesta por medio del presente estudio a:

¿Cómo el análisis y diseño de un mecanismo de cifrado de correo electrónico puede ayudar a proteger los activos de información de las PYMES?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Proponer metodología de cifrado de correo electrónico basado en las mejores prácticas del mercado y en estándares internacionales de seguridad, para las PYMES.

2.2 OBJETIVOS ESPECÍFICOS

- Revisar el estado actual del servicio de correo electrónico y políticas de seguridad de las PYMES.
- Recolectar información conceptual de seguridad de la información y estado de arte del cifrado, metodologías y normatividad vigente.
- Determinar la mejor metodología de cifrado para el aseguramiento del correo electrónico.
- Elaborar la documentación de la metodología aplicada y los resultados del proyecto.

3. JUSTIFICACION

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.

En la experiencia del autor es válido describir que múltiples empresas 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 compañía (principalmente intrusos informáticos o ciberdelincuentes).

Es por esto que el presente proyecto busca dar a las PYMES una metodología de cifrado de correo electrónico que se pueda integrar a sus políticas de seguridad, con el fin de garantizar que la información que se maneja solo sea accesible a quien va dirigida, mitigando así la filtración o daño de los datos.

Con la entrega de una metodología de cifrado adecuada para las PYMES, se dará un paso en el proceso continuo de aseguramiento de los activos de información para aquellas personas que envían correos como parte de su labor en las empresas y se puede garantizar en algunos procesos, que su información no será víctima de manipulación indebida por ciberdelincuentes o incluso por parte de la misma competencia. Esta metodología también es un valor agregado para las empresas vinculadas con aquellas que la implementan y que también quieran o requieran mantener su información con un nivel de seguridad adecuado, dando tranquilidad en las actividades cotidianas entre las empresas.

4. MARCO REFERENCIAL

4.1 ANTECEDENTES O ESTADO DEL ARTE

Es indispensable hacer un breve repaso de las estructuras iniciales de intercambio electrónico de información que dieron forma a lo que se conoce como correo electrónico y a los protocolos tanto de correo como de cifrado que a lo largo de varias décadas se han implementado para ofrecer una diversidad de servicios de correo, representadas por marcas y por iniciativas de código abierto en uso por empresas y personas de manera pública y privada.

El intercambio de información tomó forma a través de una de varias iniciativas enfocadas al correo basado en host y al correo basado en redes de área local, entre las iniciativas basadas en host se destaca el Sistema de tiempo compartido compatible o CTSS (Compatible Time-Sharing System) en el cual un conjunto de usuarios podrían conectarse y compartir archivos a un sistema de cómputo [6], esto ocurrió para 1961 y posteriormente en 1965 se solicitó por un conjunto de investigadores el comando MAIL, con privilegios de envío de mensajes, se le concedió acceso a los usuarios del Michigan Institute of Technology MIT a este protocolo el 8 de Septiembre de 1965 [7]. A continuación se hace una breve lista de iniciativas relevantes hasta el año 1981 donde se publica por parte de la corporación Rand un manual de uso de manejo electrónico en sistemas UNIX [8], al cual se unieron diversas estrategias de diversas compañías para ofrecer este tipo de servicios.

- SNDMSG 1971, primer correo electrónico sobre un enlace de red punto a punto, utilizando la red ARPANET[9].
- Primer buzón de correo APL Mailbox creado por Larry Breed en 1971 de la Corporación Científica de Tiempo Compartido STSC (Scientific Time Sharing Corporation) usando el lenguaje de programación APL [10].
- 666BOX 1973, una implementación del APL Mailbox por parte de la compañía canadiense I. P. Sharp Associates[11].

[6] http://www.cis.usouthal.edu, «CTSS, Compatible Time-Sharing System,» 01 01 2019. [En línea]. Available: http://www.cis.usouthal.edu/faculty/daigle/project1/ctss.htm. [Último acceso: 10 Enero 2020].

[7] T. V. Vleck, «The History of Electronic Mail,» 01 Febrero 2001. [En línea]. Available: https://www.multicians.org/thvv/mail-history.html. [Último acceso: 10 Enero 2020].

[8] R. H. N. S. T. K. B. a. P. K. Anderson, «The Design of the MH Mail System,» 31 Diciembre 1978. [En línea]. Available: https://www.rand.org/pubs/notes/N3017.html. [Último acceso: 10 Enero 2020].

[9] R. Tomlinson, «Firstemailframe,» 06 Mayo 2006 . [En línea]. Available: http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html. [Último acceso: 10 Enero 2020].

[10] L. Goldsmith, «APL Quotations and Anecdotes,» 18 Septiembre 2010. [En línea]. Available: https://www.jsoftware.com/papers/APLQA.htm. [Último acceso: 10 Enero 2020].

- Mail. Cliente de correo desarrollado por Kurt Shoens [12].

Para la década de 1980, el uso de computadores en redes de área local requerían de soluciones de transferencia de correo, por lo cual surgieron iniciativas como:

- Cc:Mail. Década de los 80, desarrollado en MS-DOS, permitía el envío de datos almacenados en redes LAN, este sistema fue absorbido por Lotus e integrado a su plataforma de correo en 1991 y posteriormente por IBM en 1995, su última versión fue liberada en el año 2000 y retirada en Octubre del mismo año [13].
- Microsoft Mail: Basado en adquisiciones de software realizadas por Microsoft fue lanzado en 1980 para redes de AppleTalk en introducido al entorno de computadores de escritorio como Microsoft Mail for PC Networks v2.1 en 1991, ofreciendo arquitecturas de cliente y servidor [14].

A partir de este momento múltiples fabricantes de sistemas operativos empezaron a construir estructuras de clientes servidor para soportar entre otros servicios el correo electrónico, el cual por su parte hace uso de diversas tecnologías. Entre las herramientas actuales de correo se usan diversas configuraciones que son transparentes al usuario final, en cuanto a que no es necesaria la visualización de las interacciones que permiten el uso del correo ya sea mediante un programa cliente en su equipo de cómputo o en un navegador web, estas herramientas hacen uso de configuraciones de seguridad que han sido incluidas con el paso del tiempo en los protocolos base de los servicios de correo electrónico.

Existen en general para el público de este documento dos plataformas de uso de correo electrónico, los programas cliente de email y los clientes de servicios web. Las dos plataformas funcionan como agentes de usuario de correo (Mail User Agent, MUA), uno de los ejemplos más comunes de aplicaciones cliente para equipos de cómputo son: Outlook, mail, Exchange, Zimbra, Apple Mail, etc. Algunos ejemplos de clientes de correo web son: AOL mail, Gmail, Outlook.com (reemplazo de Hotmail.com), Yahoo! Mail, entre muchos otros.

En las transacciones realizadas para el envío o recepción de correos electrónicos se usan documentos de referencia conocidos como Request For Proposal o RFC las cuales se mencionarán según se hace la descripción de una función, sistema o protocolo. En el envío o recepción de un correo electrónico un cliente de correo

---

[11] Ibidem. L. Goldsmith, «APL Quotations and Anecdotes»

[12] K. Shoens, «MAIL REFERENCE MANUAL,» 25 Abril 1984. [En línea]. Available: http://reports-archive.adm.cs.cmu.edu/anon/itc/CMU-ITC-012.pdf. [Último acceso: 10 Enero 2020].

[13] L. o. C. USA, «cc:Mail Archive Email Format,» 18 Mayo 2018. [En línea]. Available: https://www.loc.gov/preservation/digital/formats/fdd/fdd000391.shtml. [Último acceso: 10 Enero 2020].

[14] Computerworld, «Microsoft Mail: Solid, less graphical,» *Computerworld,* vol. XXV, p. 38, 21 Agosto 1991.

electrónico hace un acuerdo con un servidor de Agente de Transferencia de Correo (Mail Transfer Agent MTA) cuyo uso se define en los documentos, rfc3798 [15], rfc2305 [16], rfc3804 [17], rfc8098 [18], rfc4496 [19], rfc5442 [20], rfc5429 [21], para la recepción y almacenamiento de los correos del cliente. El MTA usa un Agente de Envío de Correos (Mail Delivery Agent, MDA) que se encarga de enviar los correos electrónicos hacia el buzón de correo del destinatario a medida que llegan los mensajes. Finalmente el MTA descarga los mensajes cuando el MUA solicita las descargas de los mismos, lo cual normalmente es un parámetro configurable. Para la descargas de los correo existe un componente llamado Agente de Recuperación de Correo (Mail Retrieval Agent, MRA) el cual puede ser un programa externo instalado por el usuario o puede ser parte del MUA.

En relación a la función del MTA, es posible que unos servidores alojen la información temporalmente y otros la almacenen de forma indefinida, así entran en juego nuevos protocolos:

- POP3: El Protocolo de Oficina Postal (Post Office Protocol) en su versión 3 permite que una aplicación cliente acceda, a través del protocolo IP, a un buzón de mensajes alojado en un servidor de correo. El cliente POP3 se conecta, recupera los mensajes del buzón, los guarda en el almacenamiento local del cliente de correo del usuario y los borra del servidor [22], el puerto en uso es 101.
- IMAP: El Protocolo de Acceso a Mensajes de Internet (Internet Message Access Protocol) en su versión 4 revisión 1. Permite desde múltiples clientes la recuperación de correo electrónico desde el servidor mediante una conexión TCP/IP. Este protocolo permite almacenar los correos en el servidor hasta que el cliente explícitamente solicite borrarlos [23], el puerto en uso es 143.

[15] I. E. T. Force, «Message Disposition Notification,» Mayo 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3798. [Último acceso: 10 Enero 2020].
[16] I. E. T. Force, «A Simple Mode of Facsimile Using Internet Mail,» Marzo 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2305. [Último acceso: 10 Enero 2020].
[17] I. E. T. Force, «Voice Profile for Internet Mail (VPIM) Addressing,» Junio 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3804. [Último acceso: 10 Enero 2020].
[18] I. E. T. Force, «Message Disposition Notification,» Febrero 2017. [En línea]. Available: https://tools.ietf.org/html/rfc8098. [Último acceso: 10 Enero 2020].
[19] I. E. T. Force, «Open Pluggable Edge Services (OPES) SMTP Use Cases,» Mayo 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4496. [Último acceso: 10 Enero 2020].
[20] I. E. T. Force, «LEMONADE Architecture - Supporting Open Mobile Alliance (OMA),» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5442. [Último acceso: 10 Enero 2020].
[21] I. E. T. Force, «Sieve Email Filtering: Reject and Extended Reject Extensions,» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5429. [Último acceso: 10 Enero 2020].
[22] I. E. T. Force, «Post Office Protocol - Version 3,» Mayo 1996. [En línea]. Available: https://tools.ietf.org/html/rfc1939. [Último acceso: 12 Enero 2020].
[23] I. E. T. Force, «INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1,» Marzo 2003. [En línea]. Available: https://tools.ietf.org/html/rfc3501. [Último acceso: 11 Enero 2020].

- MAPI: Interfaz de Programa de Aplicación de Mensajería (Messaging Application Programming Interface) es una Interfaz de Programación de Aplicaciones (Application Programming Interface API) de Microsoft que se utiliza para conectar las aplicaciones de Microsoft a servidores de Exchange, Outlook o de Office y sus servicios de correo asociados [24], [25].
- SMTP: Protocolo Simple de Transferencia de Correo (Simple Mail Transfer Protocol) es un protocolo únicamente para envío de información basado en texto y orientado a las comunicaciones, en el cual un MUA o un MTA solicita el envío de correos, mediante la emisión de cadenas de comandos, agregando los datos necesarios por medio de un canal de datos (TCP) para que el MUA del cliente destino procese los datos y reciba el correo. Usa típicamente el puerto 25 [26].
- HTTP: Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol) es un protocolo de la capa de aplicaciones para sistemas de información distribuidos y es el canal de comunicaciones para la red informática mundial o World Wide Web (WWW). Actualmente cuenta con tres versiones de las cuales HHTP 1.1 Y HTTP/2 estan ampliamente soportadas por los navegadores, mucho servicios de correo electrónico utilizan páginas en internet para proveer acceso e inicialmente usaron el protocolo HTTP, hasta la inclusión de protocolos como Secure Sockets Layer SSL y Transport Layer Security TLS [27], [28], [29].
- TLS: Transport Layer Security, es un protocolo que provee integridad y seguridad a las comunicaciones entre aplicaciones como, navegadores, correo electrónico, mensajería instantánea entre otros, haciendo uso de criptografía simétrica [30].

Con el objetivo de asegurar las comunicaciones sobre estos protocolos la Internet Engineering Task Force (IETF), emitió un conjunto de documentos para estandarizar el uso de medidas de seguridad con controles criptográficos como el uso de TLS. Esta extensión se denomina STARTTLS, en la cual se hace una

[24] Microsoft, «Exchange Server Protocol Documents,» 24 Septiembre 2019. [En línea]. Available: https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxprotlp/30c90a39-9adf-472b-8b5b-03c282304a83?redirectedfrom=MSDN. [Último acceso: 11 Enero 2020].

[25] Microsoft, «Outlook Connectivity with MAPI over HTTP,» 9 Mayo 2014. [En línea]. Available: https://blogs.technet.microsoft.com/exchange/2014/05/09/outlook-connectivity-with-mapi-over-http/. [Último acceso: 11 Enero 2020].

[26] I. E. T. Force, «Simple Mail Transfer Protocol,» Octubre 2008. [En línea]. Available: https://tools.ietf.org/html/rfc5321. [Último acceso: 11 Enero 2020].

[27] I. E. T. Force, «Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,» Junio 2014. [En línea]. Available: https://tools.ietf.org/html/rfc7230. [Último acceso: 14 Enero 2020].

[28] I. E. T. Force, «Hypertext Transfer Protocol Version 2 (HTTP/2),» Mayo 2015. [En línea]. Available: https://tools.ietf.org/html/rfc7540. [Último acceso: 14 Enero 2020].

[29] I. E. T. Force, «The Secure Sockets Layer (SSL) Protocol Version 3.0,» Agosto 2011. [En línea]. Available: https://tools.ietf.org/html/rfc6101. [Último acceso: 15 Enero 2020].

[30] I. E. T. Force, «The Transport Layer Security (TLS) Protocol Version 1.3,» Agosto 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8446. [Último acceso: 14 Enero 2020].

negociación entre clientes para el uso de certificados TLS e iniciar la transmisión utilizando el comando STLS en el puerto 101 del protocolo POP3, otra alternativa es usar el puerto 995 POP3S, para IMAP se recomienda el uso del puerto 993. Las recomendaciones para estas implementaciones se recopilan en la tabla 1.

Tabla 1. Documentos RFC para el aseguramiento de protocolos en uso para gestión de correo electrónico

RFC	Descripción	Objetivo	Referencia
rfc2595	Using TLS with IMAP, POP3 and ACAP	"Existe un fuerte deseo en el IETF de eliminar la transmisión de contraseñas de texto sin cifrar a través de canales no cifrados. Si bien SASL se puede utilizar para este propósito, TLS proporciona una herramienta adicional con diferentes características de implementación. Es probable que un servidor que admita TLS con contraseñas simples y un mecanismo SASL de desafío / respuesta interopere con una amplia variedad de clientes sin recurrir a contraseñas de texto sin cifrar."	[31]
rfc3207	SMTP Service Extension for Secure SMTP over Transport Layer Security	"Este documento describe una extensión del SMTP (correo simple Servicio de Protocolo de transferencia) que permite que un servidor y un cliente SMTP utilicen TLS (Seguridad de la capa de transporte) para proporcionar autenticación privada y autenticada por internet. Esto le da a los agentes SMTP la capacidad de proteger algunas o todas sus comunicaciones de espías y atacantes."	[32]
rfc4616	The PLAIN Simple Authenticati	"Este documento define un mecanismo de autenticación simple y capa de seguridad de usuario / contraseña en	[33]

[31] I. E. T. Force, «Using TLS with IMAP, POP3 and ACAP,» Junio 1999. [En línea]. Available: https://tools.ietf.org/html/rfc2595. [Último acceso: 12 Enero 2020].
[32] I. E. T. Force, «SMTP Service Extension for Secure SMTP over Transport Layer Security,» Febrero 2002. [En línea]. Available: https://tools.ietf.org/html/rfc3207. [Último acceso: 12 Enero 2020].
[33] I. E. T. Force, «The PLAIN Simple Authentication and Security Layer (SASL) Mechanism,» Agosto 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4616. [Último acceso: 13 Enero 2020].

	on and Security Layer (SASL) Mechanism	texto claro llamado mecanismo PLAIN. El mecanismo PLAIN está destinado a ser utilizado, en combinación con servicios de confidencialidad de datos proporcionados por una capa inferior, en protocolos que carecen de un comando de autenticación de contraseña simple."	
rfc7817	Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols	"Este documento describe el procedimiento de verificación de identidad del servidor de Seguridad de la capa de transporte (TLS) para los clientes SMTP Submission, IMAP, POP y ManageSieve."	[34]
rfc8314	Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access	"Esta especificación describe las recomendaciones actuales para el uso de Transport Layer Security (TLS) para proporcionar confidencialidad del tráfico de correo electrónico entre un Agente de usuario de correo (MUA) y un Servidor de envío de correo o Servidor de acceso a correo."	[35]
rfc8460	SMTP TLS Reporting	"Este documento describe un mecanismo y un formato de informe mediante el cual los sistemas de envío pueden compartir estadísticas e información específica sobre posibles fallas con los dominios receptores. Los	[36]

[34] I. E. T. Force, «Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols,» Marzo 2016. [En línea]. Available: https://tools.ietf.org/html/rfc7817. [Último acceso: 13 Enero 2020].

[35] I. E. T. Force, «Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access,» Enero 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8314. [Último acceso: 13 Enero 2020].

[36] I. E. T. Force, «SMTP TLS Reporting,» Septiembre 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8460. [Último acceso: 14 Enero 2020].

		dominios de los destinatarios pueden usar esta información para detectar posibles ataques y diagnosticar configuraciones erróneas involuntarias.”	
rfc8461	SMTP MTA Strict Transport Security (MTA-STS)	“SMTP MTA Strict Transport Security (MTA-STS) es un mecanismo que permite a los proveedores de servicios de correo (SP) declarar su capacidad de recibir conexiones SMTP seguras con Transport Layer Security (TLS) y especificar si los servidores de envío SMTP deben negarse a entregar correos a los hosts MX que no ofrezcan TLS con un certificado de servidor de confianza.”	[37]

FUENTE: Autor.

Entendiendo que el uso de estas plataformas implica la transferencia de información entre varias personas o entidades, normalmente bajo mutuo acuerdo, se implica el uso de algún tipo de tecnología que permita asegurar que solo las personas que son originalmente destinatarias de la información sean quienes la reciben, esto permite introducir el concepto de privacidad en el correo electrónico. La privacidad en medios electrónicos surge de la necesidad de proteger la información y prevenir que actores no deseados tengan acceso a ella. Naturalmente por acuerdos entre diferentes países, acuerdos comerciales y eventos de pérdida o fuga de información se empezaron a establecer diversos métodos para proteger la información con un sustento legal, en Colombia existe un conjunto de normas orientadas a definir los niveles de protección y las medidas y acciones a tomar para quienes infrinjan las leyes con el objetivo de acceder a in formación privada, esto se explorará en el marco legal de este documento.

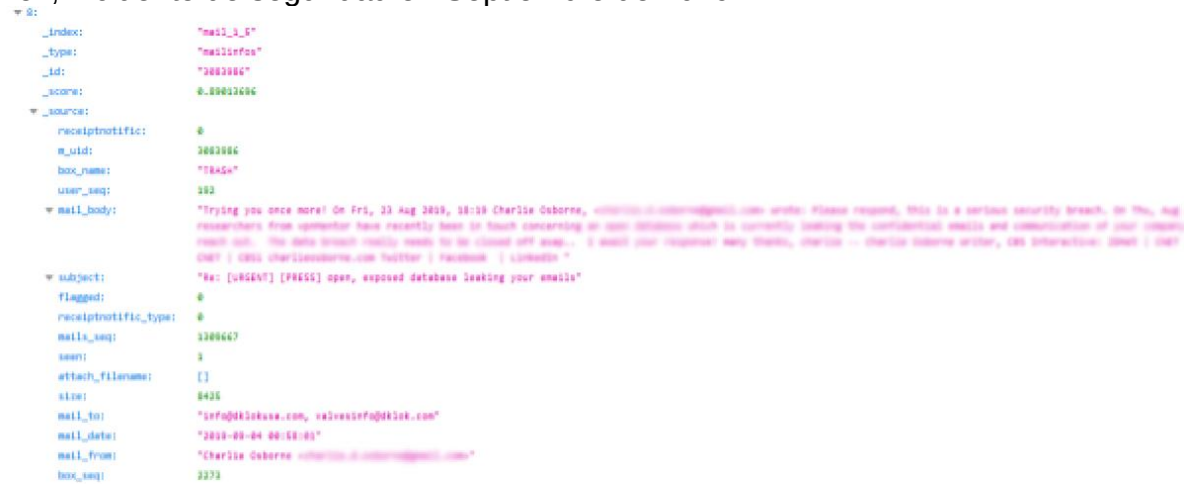
Pese a que ya existen un conjunto de normas, marcos de referencia y listados de buenas prácticas existe la posibilidad de que un sistema falle, no se configure adecuadamente, se dejen configuraciones de fábrica, no se realicen escaneos de vulnerabilidades, no se apliquen las actualizaciones emitidas por los fabricantes de software, no se utilicen conexiones protegidas con certificados digitales o que no se cifre la información entre muchas otras prácticas. La ocurrencia de uno o de varios de los eventos mencionados anteriormente, o incluso la falla en la definición de algún protocolo como los mencionados en la Tabla 1. o fallas en su implementación, pueden ser la causa de pérdida de información, escalamiento de privilegios, modificación no autorizada de la información o fuga de la misma.

[37] I. E. T. Force, «SMTP MTA Strict Transport Security (MTA-STS),» Septiembre 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8461. [Último acceso: 14 Enero 2020].

Existe un diverso y amplio conjunto de eventos o incidentes de ciberseguridad donde se afectan los principios de confidencialidad, integridad y/o disponibilidad (CID) de la información de una o varias empresas, sin embargo en este documento, el autor solo utilizará referencias de algunos eventos de seguridad relacionados con afectación del CID en casos específicamente relacionados al cifrado de correos electrónicos, aseguramiento de plataformas de correo, o fugas de información por medio de archivos, abuso de privilegios y ataques a servicios de correo.

Un incidente de seguridad de la información notable ocurrió en una empresa coreana de comercialización de insumos industriales, la cual tiene una base de negocios a nivel global. Se identificó que una plataforma de correo propia de la empresa permitía el acceso a registros de comunicaciones internas y externas de la compañía y la lectura de correos privado enviados a través de dicha plataforma. Esta empresa nunca reconoció la brecha aunque durante algunas semanas diferentes equipos y medios de comunicación los contactaron para informarles del incidente [38].

Figura 1 Texto del contenido de un correo electrónico de la empresa Coreana DK-Lok, incidente de seguridad en Septiembre de 2019.



FUENTE: https://www.zdnet.com/article/dklok-data-breach-leaked-global-enterprise-client-internal-emails/.[39]

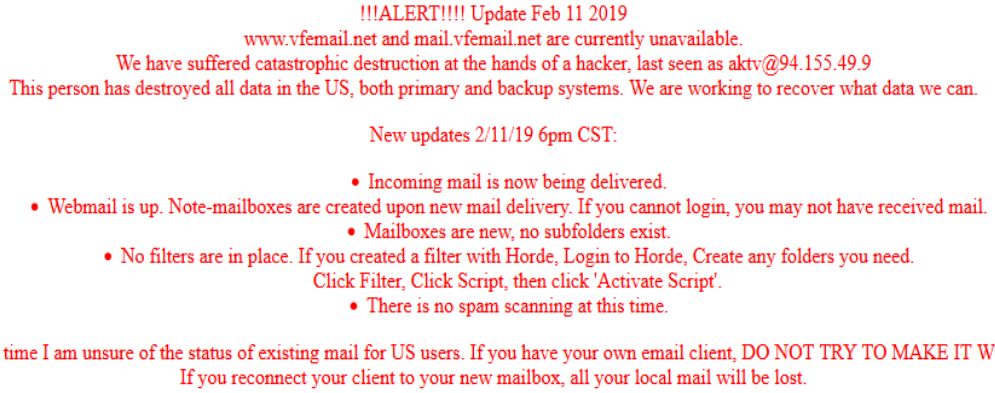
[38] C. Osborne, «zdnet.com,» 5 Septiembre 2019. [En línea]. Available: https://www.zdnet.com/article/dklok-data-breach-leaked-global-enterprise-client-internal-emails/. [Último acceso: 3 Febrero 2020].

[39] DK-Lok data breach exposes global enterprise client data, internal emails [En línea]. Disponible en: https://www.zdnet.com/article/dklok-data-breach-leaked-global-enterprise-client-internal-emails/

Este ejemplo es importante pues una configuración inadecuada de una plataforma permitió el acceso a información interna y privada, adicionalmente se identificó que los protocolos de envío de correo no contaban con contrales criptográficos que impidieran conocer los textos de los correos, información confidencial de la compañía, sus remitentes y datos de mil quinientas direcciones de correo electrónico.

En febrero de 2019 ocurrió un incidente de seguridad en el que se accedió ilegalmente a la configuración de un servicio de correo electrónico en el cual el atacante borró todos los sistemas que soportaban el servicio, incluyendo las máquinas virtuales y las copias de respaldo de los buzones de correo de los usuarios, en este caso aunque no hubo exposición de datos se configuró un ataque a la disponibilidad de la información contenida en correos electrónicos, pues los usuarios no podían sincronizar sus clientes correo con los buzones creados después del ataque, porque perdería (si las tenían) su copia local de correo electrónico [40].

Figura 2 Notificaciones de VFEmail después del ciberataque ocurrido el 11 de febrero de 2020



FUENTE: https://www.bleepingcomputer.com/news/security/hackers-wipe-vfemail-servers-may-shut-down-after-catastrophic-data-loss/.[41]

Es importante aclarar que aunque el sistema de correo afectado sigue funcionando y ofrece la posibilidad de usar cifrado con el protocolo Pretty Good Privacy o PGP [42] , la disponibilidad de la información es fundamental así se

[40] S. Gatlan, «Bleepingcomputer.com,» 12 Febrero 2019. [En línea]. Available: https://www.bleepingcomputer.com/news/security/hackers-wipe-vfemail-servers-may-shut-down-after-catastrophic-data-loss/. [Último acceso: 5 Febrero 2020].

[41] Hackers Wipe VFEmail Servers, May Shut Down After Catastrophic Data Loss [En línea]. Disponible en: https://www.bleepingcomputer.com/news/security/hackers-wipe-vfemail-servers-may-shut-down-after-catastrophic-data-loss/

[42] R. Walsh, «ProPrivacy,» 15 Noviembre 2019. [En línea]. Available: https://proprivacy.com/email/review/vfemail. [Último acceso: 5 Febrero 2020].

preserve la confidencialidad y la integridad, si no es posible acceder a ella o perder, como ocurrió en este caso, la totalidad de la información sin posibilidad de recuperarla.
En octubre de 2019 se reportó una brecha de seguridad en la información de un banco italiano, en efecto se reportaron dos brechas ocurridas entre septiembre y octubre de 2016 y entre junio y julio de 2017, en este caso la fuga de información ocurrió por el acceso indebido a información del banco por parte de un proveedor que ofrecía servicios tercerizados, por medio del cual se filtró un documento creado en 2015 con la información representada en tres millones de registros [43].

En noviembre de 2019 un empleado de la firma Trend Micro sustrajo información de aproximadamente 120.000 clientes de la firma, con el objetivo de suministrar información personal a terceras partes con el objetivo de realizar campañas de engaño a múltiples usuarios dueños de la información sustraída [44]. En este caso se evidencia que aun contando con estrategias complejas de ciberseguridad incluyendo el correo electrónico y controles criptográficos de una empresa de ciberseguridad, existen amenazas que van más allá de los controles técnicos implementados, y la materialización de estos riesgos yace fundamentalmente en la intencionalidad del actor que ejecuta el ciberataque.

Así como existen firmas que proveen servicios de correo electrónico a través de clientes y servicios web, existen organizaciones que suministran servicios para la gestión de la información alojada en estos servicios (correos electrónico, hipervínculos, reportes, correo no deseado), en 2017 la compañía Unroll.me fue acusada de presentar información falsa a usuarios de correos electrónicos para que se suscribieran a su plataforma y les concedieran acceso a sus buzones de correo para eliminar propagandas, y correos no deseados, sin embargo esta compañía vendía la información de los usuarios como nombres, facturas, direcciones de facturación e información de compras, esta información se sustrajo en el periodo comprendido entre noviembre de 2015 y septiembre de 2018. El objetivo final era comparar la información en correos recibidos en los buzones de los usuarios para validar las facturas recibidas de una firma de transporte Lyft y su competencia Uber [45]. En este caso sin importar las configuraciones de seguridad, los controles criptográficos y las medidas de seguridad implementadas en el servicio, el usuario final fue víctima de ataques de ingeniería social, concediendo acceso a un tercero sus credenciales de acceso para realizar gestión (término

[43] C. Osborne, «zdnet.com,» 28 Octubre 2019. [En línea]. Available: https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/. [Último acceso: 8 Febrero 2020].
[44] C. Osborne, «zdnet.com,» 6 noviembre 2019. [En línea]. Available: https://www.zdnet.com/article/trend-micro-reveals-insider-threat-exposing-customer-data/. [Último acceso: 12 febrero 2020].
[45] C. Osborne, «zdnet.com,» 18 Diciembre 2019. [En línea]. Available: https://www.zdnet.com/article/ftc-settles-with-unroll-me-over-allegedly-duping-users-over-email-data-collection-sale/. [Último acceso: 20 febrero 2020].

engañoso al no declarar los mecanismos, el objetivo y las actividades o tratamiento de la información a la que se concedió acceso) sobre su correo.

Por último se enuncia el que a la fecha es el incidente de fuga de información por correo electrónico o plataforma de correo más grande por el número de usuarios afectados, en 2016 la empresa Yahoo informó que fue víctima de dos ciberataques en 2013 y 2014, el total de víctimas alcanzó la totalidad de las 3000 millones de cuentas de usuarios de correo electrónico que para 2016 administraba Yahoo [46] , posteriormente se evidenció que el ataque duró hasta 2016.La compañía informó que las brechas obedecieron a ataques autorizados por el gobierno ruso, en efecto, cuatro personas fueron las responsables del ataque: dos funcionarios del gobierno ruso lograron que dos ciberdelincuentes accedieran a la herramienta de gestión de cuentas de Yahoo y lograran persistencia en sus servidores. Sin embargo, la pieza clave del ataque empezó por un correo engañoso dirigido (Spear Phishing) a un empleado de Yahoo, lo cual permitió el robo de sus contraseñas y la materialización del acceso no autorizado. En el desarrollo del ataque los ciberdelincuentes utilizaron valores criptográficos para crear COOKIES y suplantar sesiones de usuario sin necesidad de claves [47] . Esto causó graves pérdidas económicas a Yahoo y al holding que compró la empresa justo durante la materialización de los ataques, se cree que Yahoo disminuyó en US$350 millones su valor comercial; aunque se creó un fondo de restitución de más de US$117 millones y la socialización de los métodos de acceso al fondo, se considera que es imposible que la empresa restituya los daños causados a todos sus usuarios [48] . En este caso, es necesario aclarar que el uso de ataques de ingeniería social para convencer a un funcionario clave de acceder a un enlace malicioso, puede causar pérdidas masivas a nivel económico y una pérdida de imagen permanente para un negocio. Adicionalmente los controles criptográficos diseñados para individualizar las credenciales de acceso a un buzón de correo, se utilizaron para acceder sin necesidad de contraseñas a los buzones de usuarios específicos y la posibilidad de vulnerar la privacidad de la información de todos los usuarios de correo de Yahoo en un periodo de 3 años.

En este capítulo se describieron los orígenes del correo electrónico, una breve descripción técnica, diferentes escenarios de fuga de información y ciberataques que actualmente ocurren en plataformas percibidas como seguras por el público, que demuestran no solo la necesidad de implementar controles criptográficos en

[46] D. Swinhoe, «CSOonline,» 17 Abril 2020. [En línea]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Último acceso: 28 Abril 2020].

[47] M. Williams, «CSOonline,» 4 Octubre 2017. [En línea]. Available: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html. [Último acceso: 29 Abril 2020].

[48] C. Colby, «Cnet.com,» 15 Octubre 2019. [En línea]. Available: https://www.cnet.com/how-to/yahoo-data-breach-how-to-file-for-358-or-more-as-part-of-claim-settlement/?ftag=CMG-01-10aaa1b. [Último acceso: 1 Mayo 2020].

servicios de uso cotidiano como el correo electrónico, sino la obligatoria inclusión de capacitación en ciberseguridad para todos los funcionarios del sector de las Pymes y en general para todos los usuarios de sistemas informáticos.

4.2 MARCO TEORICO

4.2.1 LA CRIPTOGRAFÍA

Es una técnica para cifrar los mensajes que contiene información vital o sensible de una empresa. Según el artículo de la Universidad Externado de Colombia redactado por Jhonny Antonio Pabón. "Las tecnologías de la encriptación constituyen el avance tecnológico más importante de los últimos mil años. Ningún otro descubrimiento tecnológico - desde las armas nucleares (espero) hasta Internet- tendrá un impacto más significativo en la vida social y política de la humanidad. La criptografía va a cambiar absolutamente todo"[49]

Hay muchos métodos y teorías para realizar el proceso de criptografía, pero su máxima premisas es que la criptografía se basa en la aritmética. Lo anterior consiste en transformar el texto en números y luego usar cálculos para dejar esta información o texto en forma cifrada. De igual manera se debe contemplar que el receptor debe tener la forma de decodificar estos mensajes es acá donde se evidenciara la seguridad que se desea crear.

Para cualquier organización es de vital importancia métodos de criptografía para enviar o recibir información de forma segura. Los procesos de criptografía aplicada pueden ser simétricas y/o asimétricas depende del nivel de aseguramiento que se desee tener

CIFRADO: Es transformar información con el fin de protegerla de miradas ajenas. Al aplicar cifrado, un mensaje se altera hasta volverse irreconocible o incomprensible, pero la información no se pierde, sino que puede recuperarse más adelante.[50]

CIFRADO DE DATOS: Se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave. Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los equipos. El uso del cifrado de datos puede iniciarse en su equipo o en el servidor al que se conecta.[51]

---

[49] J. A. P. Cadavid, «Revitas Universidad Externado de Colombia,» 24 11 2010. [En línea]. Available: https://revistas.uexternado.edu.co/index.php/propin/article/download/2476/2112/. [Último acceso: 24 Abril 2020].

[50] F. FERRI-BENEDETTI, «¿QUÉ ES EL CIFRADO?,» 23 07 2013. [En línea]. Available: https://www.softonic.com/articulos/que-es-el-cifrado-encriptar. [Último acceso: 25 Abril 2020].

[51] J. O. Canizalez, «SEGURIDAD EN REDES,» SEGURIDAD EN REDES, 15 06 2011. [En línea]. Available: http://seguridad-deredes.blogspot.com/2011/06/cifrado-y-criptografia.html. [Último acceso: 01 05 2020].

CIFRADO SIMÉTRICO: Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave. Como ejemplo de sistema simétrico está «Enigma»; Éste es un sistema que fue usado por Alemania, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día. Algunos ejemplos actuales de algoritmos simétricos son 3DES, Blowfish e IDEA.[52]

CIFRADO ASIMÉTRICO: Para evitar estos inconvenientes, podemos utilizar lo que se conoce como cifrado asimétrico. A diferencia del cifrado simétrico, el asimétrico es un tipo de cifrado en el que no usamos una única clave sino dos. Una de ellas es privada y la otra es pública, de forma que la clave privada no se la entregamos a nadie mientras que la clave pública la dejamos a disposición de todo el mundo.[53]

ALGORITMO CRIPTOGRÁFICO: Es un método matemático que se emplea para cifrar y descifrar un mensaje. Generalmente funciona empleando una o más claves (números o cadenas de caracteres) como parámetros del algoritmo, de modo que sean necesarias para recuperar el mensaje a partir de la versión cifrada. El mensaje antes de cifrar se denomina texto en claro y una vez cifrado se denomina texto cifrado.[54]

ATAQUE CRIPTOGRÁFICO: El criptoanálisis se dedica a investigar los puntos débiles de las técnicas de cifrado. Es una disciplina fascinante, una combinación de lingüística, matemáticas, ingeniería inversa y espionaje. Las técnicas empleadas para un ataque criptográfico varían dependiendo de la cantidad de información disponible sobre el cifrado empleado y los datos protegidos. Conocer parte del contenido o la tecnología empleada resulta de gran ayuda. Sea cual sea el ataque empleado, son tres los recursos que todo atacante necesita: tiempo, información previa y recursos computacionales. La complejidad de los sistemas de cifrado actuales obliga a usar ordenadores a veces muy potentes.[55]

---

[52] The GnuPG Project, «The GNU Privacy Guard,» 07 01 2020. [En línea]. Available: https://www.gnupg.org/gph/es/manual/c190.html. [Último acceso: 15 Mayo 2020].

[53] Ibidem. The GnuPG Project, «The GNU Privacy Guard,»

[54] S. Talens-Oliag, «Introducción a la Criptología,» 14 04 2003. [En línea]. Available: https://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.html. [Último acceso: 14 Abril 2020].

[55] F. FERRI-BENEDETTI, «¿QUÉ ES EL CIFRADO?,» 23 07 2013. [En línea]. Available: https://www.softonic.com/articulos/que-es-el-cifrado-encriptar. [Último acceso: 25 Abril 2020].

CRIPTOGRAFÍA DE CLAVE PÚBLICA: Cuando hablamos de cifrar, se supone que quien envía y quien recibe el mensaje comparten una clave para cifrar y descifrar. Este es el método tradicional, que es el simétrico: ambos extremos conocen esa clave (share edkey), -como la del wifi- y esa es la que se usa. El problema de este método es que ambos extremos tienen que pasarse la clave en algún momento, con las complicaciones que eso supone (pasar por canales separados y asegurarse de que nadie la sabe).

Por eso se buscaron métodos alternativos y así surgió el cifrado de clave pública, que consiste en que una persona genera dos claves, una privada y una pública. La pública es, como su nombre lo indica, pública. De hecho debe ser publicada para que cualquiera pueda usarla para cifrar un mensaje que va a enviarte. Pero ese mensaje sólo puede ser descifrado con la clave privada asociada, que obviamente es la que tiene el receptor.[56]

OPENPGP: Es un estándar de código abierto basado en el método de cifrado PGP, nació con la finalidad de proteger la información que se distribuye a través de Internet.

El aseguramiento de la información es uno de los principales objetivos que se debe tener a la hora administrar un sistema de información. Es en este punto donde el uso de la criptografía se vuelve una herramienta clave que este proceso.[57]

4.2.2 ESTADARES DE SEGURIDAD DE LA INFORMACIÓN

ESTANDARES TRUSTED COMPUTER SECURITY EVALUATION CRITERIA. TCSEC.

El Departamento de Defensa de los Estados Unidos por los años 80's (1983-1985) publica una serie de documentos denominados Serie Arco iris (Rainbow Series). Dentro de esta serie se encuentra el Libro Naranja (Orange Book) el

[56] M. GONZALO, «Cómo cifrar tu correo de Gmail sin complicaciones con Mailvelope,» 23 07 2013. [En línea]. Available: https://www.eldiario.es/turing/como-cifrar-email-criptografia-Gmail-Mailvelope_0_156784455.html. [Último acceso: 14 Mayo 2020].

[57] INCIBE, «Utiliza el correo electrónico de forma segura con PGP,» 13 08 2019. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/utiliza-el-correo-electronico-forma-segura-pgp. [Último acceso: 15 Mayo 2020].

cual suministra especificaciones de seguridad. Se definen siete conjuntos de criterios de evaluación denominados clases (D, C1, C2, B1, B2, B3 y A1). Cada clase de criterios cubre cuatro aspectos de la evaluación: política de seguridad, imputabilidad, aseguramiento y documentación. Los criterios correspondientes a estas cuatro áreas van ganando en detalle de una clase a otra, constituyendo una jerarquía en la que D es el nivel más bajo y A1 él más elevado. Todas las clases incluyen requisitos tanto de funcionalidad como de confianza.[58]

ESTANDARES INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA.ITSEC.

Por su parte el InformationTechnology Security EvaluationCriteria (ITSEC), conformado principalmente por Francia, Alemania y Reino Unido, crearon su propio estándar de seguridad, al principio de los 90's, este se conoce como el Libro Blanco (White Book).

Se definen siete niveles de evaluación, denominados E0 a E6, que representan una confianza para alcanzar la meta u objetivo de seguridad. E0 representa una confianza inadecuada. E1, el punto de entrada por debajo del cual no cabe la confianza útil, y E6 el nivel de confianza más elevado.[59]

ESTÁNDAR BS 7799 (REINO UNIDO)

El estándar de seguridad de la información realizado por BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, la versión actual consta de dos partes:

- BS7799-1:1999 Es la guía de buenas prácticas. No es certificable
- BS7799-2:1999 Establece los requisitos de un sistema de seguridad de la información (SGSI) Lo certifica entidades independientes.[60]

[58] TUGURIUM, «TCSEC, el libro naranja de la seguridad informática,» 28 04 2017. [En línea]. Available: https://www.teknoplof.com/2017/04/28/tcsec-libro-naranja-la-seguridad-informatica/. [Último acceso: 20 Marzo 22].

[59] TUGURIUM, «Glosario Terminología Informática,» 23 Marzo 2009. [En línea]. Available: http://www.tugurium.com/gti/termino.php?Tr=Information%20Technology%20Security%20Evaluation%20Criteria&Tp=N&Or=0. [Último acceso: 20 Abril 2020].

[60] ISO.ORG, «STANDARDS,» 20 Febrero 2006. [En línea]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/info_security.pdf. [Último acceso: 24 Abril 2020].

ESTANDARES ISO / IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organizationfor Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El ISO / IEC -27000 se basa en la segunda parte del estándar británico BS7799 (BS7799:2). Está compuesta a grandes rasgos por:

- ISMS (Information Security Management System).
- Valoración de Riesgo.
- Controles.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

La Familia ISO 27000

Normas para Construir, Evaluar y Mejorar un SGSI

- 27000 Descripción general y vocabulario.
- 27001 Contiene los requisitos del SGSI: es un modelo certificable en seguridad de la información.
- 27002 Guía de Buenas prácticas en seguridad de la información que describe los objetivos de control y los controles recomendables en cuanto a seguridad de la información.
- 27003 Guía de implantación de un SGSI.
- 27004 Guía que determina la métrica y mediciones del SGSI y de sus controles para asegurar la eficacia del mismo.
- 27005 Guía para la gestión de riesgos de seguridad de la información.
- 27006 Requisitos para las entidades que realizan auditorias de certificación de un SGSI
- 27007 Guía para la realización de auditorías de SGSI
- 27008 Guía para la realización de las auditorias de los controles de seguridad de la información.
- 27035 Guía para la gestión de incidentes de seguridad de la información.

Principales Normas de Apoyo para Ampliar el Ámbito de un SGSI y adaptarlo a diferentes sectores

- 27010 Guía de controles de seguridad adicionales para organizaciones que comparten información.
- 27011 Guía para la aplicación de los controles de la ISO en el sector de telecomunicaciones.
- 27013 Guía para la implantación integrada de ISO 27001 e ISO 20000-1.
- 27014 Gobierno de la seguridad de la información.
- 27015 Guía para la aplicación de los controles de la ISO en servicios financieros.
- 27019 Guía para la aplicación de los controles de la ISO en el sector de industria energética.
- 27031 Guía para la continuidad del negocio en el sector TIC.
- 27032 Guía para la ciberseguridad.
- 27036-3 Guía para la seguridad en la cadena de suministro TIC.
- 27799 Guía para la aplicación de los controles de la ISO en el sector sanitario.[61]

[61] ISO27000.ES, «Serie "27000",» ISO27000.ES, 20 Septiembre 2019. [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 15 Marzo 2020].

4.3 MARCO CONCEPTUAL

El presente proyecto se basa en el cumplimiento de los tres pilares de la Seguridad de la Información, además de los conceptos claves para tener un mejor entendimiento del aseguramiento sobre el correo electrónico:

ACTIVO DE INFORMACIÓN: Es cualquier elemento que contenga información para el desarrollo de las actividades puede ser físico o digital.

ALGORITMO DE CIFRADO: Operación o funciona matemática para generar una clave para garantizar la confidencialidad e integridad de la información.

ANALISIS DE RIESGO: Es un proceso donde se validan los activos de información y documentan todas las posibles amenazas y los controles que se tendrían que aplicar para asegurar estos activos.

ATAQUE CRIPTOGRÁFICO: Es un método para sortear validar la seguridad de un sistema criptográfico.

CERTIFICADO DIGITAL: Es un fichero digital generado por una autoridad certificadora que asocia la información del titular.

CIFRADO: Acción de ocultar o codificar información para evitar que personas no autorizadas puedan acceder a la misma.

CIFRADO DE DATOS: se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave.

CIFRADO SIMÉTRICO: Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar.

CIFRADO ASIMÉTRICO: Para evitar estos inconvenientes, podemos utilizar lo que se conoce como cifrado asimétrico. A diferencia del cifrado simétrico, el asimétrico es un tipo de cifrado en el que no usamos una única clave sino dos.

CIFRADOR DE BLOQUE: Es un sistema criptográfico que cifra de bloques en bloque, usualmente cada bloque es de 128 bits. Algunos sistemas conocidos son, TDES, RC5, AES.

CIFRADOR DE FLUJO: Es un sistema criptográfico de cifra de bit en bit, los más conocidos son, RC4, SEAL, WAKE.

CRIPTOGRAFIA: Es la técnica que consiste en cifrar un mensaje.

CRIPTOGRAFÍA VISUAL: Es un esquema de compartición de secretos donde el secreto es una imagen y las partes son también varias imágenes. La ventaja de este tipo de criptografía es que no es necesaria una computadora para la reconstrucción del secreto.

CLAVE PÚBLICA: Son claves de cifrado que se pueden compartir para descifrar la información.

CLAVE PRIVADA: Son las claves de cifrado que son exclusivas de los Titulares sobre su información.

CORREO ELECTRÓNICO: Es un servicio o aplicativo que permite enviar y recibir información.

CONDIFIDENCIALIDAD: Acción de garantizar la que la información sea accedida por las personas autorizadas.

DISPONIBILIDAD: Se trata de capacidad de tener la información siempre disponible o accesible.

ESQUEMA CRIPTOGRÁFICO: Es un conjunto de primitivas que componen una aplicación criptográfica más completa, como el esquema de firma digital (compuesta de la primitiva de firma y la de verificación), el esquema de cifrado (compuesta con la primitiva de cifrado y la de descifrado) etc.

FAMILIA CRIPTOGRÁFICA: es el conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de Factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE, MQV)

FIRMA DIGITAL: es un método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento.

FIRMA DIGITAL CON APÉNDICE: método de firma digital que requiere al mensaje como entrada en el proceso de verificación.

FIRMA DIGITAL CON MENSAJE RECUPERABLE: método de firma digital que no requise real mensaje como entrada en el proceso de verificación. El mensaje se recupera después de que se ha verificado la firma.

FIRMA ELECTRONICA: Conjunto de datos electrónicos que contiene la información del titular.

FUGA DE DATOS: Es la perdida de confidencialidad de la información.

INTEGRIDAD: Es la propiedad de garantizar la exactitud de la información.

PHISHING: Es una estafa a través de correo electrónico con el fin de sacar información confidencial o sensible.

PGP: Es un programa para proteger la información por medio del cifrado.

POLITICA DE SEGURIDAD: Son las decisiones y medidas de seguridad de una empresa.

PROTOCOLO: Se trata de una regla estándar.

RSA: Se trata de un sistema criptográfico de clave pública para cifrar documentos o firmarlos digitalmente.

SEGURIDAD DE LA INFORMACIÓN: Tiene como objetivo proteger todos los activos de información de la empresa (Físicos y lógicos), basado en sus tres pilares confidencialidad, integridad y disponibilidad.

SEGURIDAD INFORMÁTICA: Hace referencia al aseguramiento de los activos de información (hardware y software), de todos sus controles y configuraciones que garanticen el correcto funcionamiento, disponibilidad y disminución de riesgos.

SEGURIDAD EN REDES: La seguridad en redes consiste en un conjunto de medidas preventivas, programadas para enfrentar riesgos de origen físico y lógico.

SGSI: Sistema de gestión de seguridad de información.

SPEARPHISHING: Es una estafa a través de correo electrónico dirigida a un grupo u organización con el fin de sacar información confidencial o sensible.

SPOOFING: Es la técnica de suplantación de identidad llevada a cabo por ciberdelincuentes.

VULNERABILIDAD: Fallos o deficiencias de un sistema que permite acceder de forma no legítima.

4.4 MARCO LEGAL

4.4.1 LEY 1273 DE 2009[62] (Delitos Informáticos en Colombia)

Establecida por el Congreso de Colombia agregando un bien jurídico para la protección de la información y los datos que se reciben, almacenan, procesan y/o trasmiten utilizado tecnologías de la información y las telecomunicaciones. Esta ley cuenta con dos capítulos con las siguientes notaciones:

Capítulo 1: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. En este capítulo encontramos la definición y acciones sobre los delitos:

- Es delito acceder a un sistema informático al que no se tenga un permiso previo. Aunque este no cuente con seguridad que deniegue este acceso.

- El delito bloquear el acceso a un sistema de información o alterar o no permitir que un sistema trabaje de acuerdo a lo establecido por su creador.

- Es delito sacar información de un sistema de información al que no se es dueño.

- Es delito borrar, modificar o eliminar un sistema de información sin autorización del creador o dueño del sistema.

- El delito usar para fines económicos o delictivos software malicioso.

- Es delito usar información privada o personal para usos delictivos o comerciales sin una previa autorización del dueño de la información.

- Es delito suplantar o crear sitios duplicados para captar información.

- Como delito agravante a los ítems antes nombrados es que se realice sobre los entes estatales u oficiales o del sector financiero nacional o extranjero.

[62] C. D. L. REPÚBLICA, «Ley 1273 DE 2009,» 05 Enero 2009. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. [Último acceso: 20 Enero 2020].

Capítulo 2: De los atentados informáticos y otras infracciones. En este capítulo encontramos la definición y acciones sobre los delitos:

- Es delito realizar robo o cometer delitos por medios informáticos.
- Es delito mover o realizar transferencia de activos por medios informáticos sin previa autorización .

4.4.2 LEY ESTATUTARIA 1581 DE 2012[63] (Protección de Datos Personales)

Establecida por el Congreso de Colombia y se encuentran consignadas las disposiciones generales para la protección de datos. Esta ley está dividida en nueve títulos en los que encontramos las siguientes notaciones:

Título I: Objeto, ámbito de aplicación y definiciones. Dentro de este numeral se encuentra regulado el manejo de la que se debe dar a los datos personales de todas las personas, además, de los derechos que cuentan para conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales.

Para el entendimiento de esta ley se cuenta con algunas definiciones entre las que encontramos:

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.
- Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

[63] C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1581 DE 2012,» 17 Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 21 Enero 2020].

- Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

- Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

- Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Título II: Principios Rectores. Dentro de este numeral se describen los principios que se deben tener sobre el uso, almacenamiento, manejo y protección de datos personales. Entre los principios que se describen en este ítem se encuentran:

- Principio de legalidad en materia de tratamiento de datos.
- Principio de finalidad.
- Principio de libertad.
- Principio de veracidad y calidad.
- Principio de transparencia.
- Principio de acceso y circulación restringida.
- Principio de Seguridad.
- Principio de confidencialidad.

Título III: Categorías Especiales de Datos. Dentro del presente numeral se define que los datos sensibles corresponden a aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar afectación sobre en el mismo. Solo esta excepcionado el uso de la información cuando es autorizada previamente o cuando es requerido por autoridades legítimas o en caso de mantener una finalidad histórica, estadística o científica.

También prevalecerá la protección de la información perteneciente a los derechos de los niños, niñas y adolescentes.

Título IV: Derechos y Condiciones de Legalidad para el Tratamiento de Datos. Se describe los derechos que tienen los Titulares sobre sus datos, de conocer el estado del almacenamiento y el uso que se da o la ubicación de los mismos además de siempre requerir a los Titulares autorización para el manejo que se quiera dar de forma adicional.

Título V: Procedimientos. En este numeral se describen las diferentes acciones que El Titular o sus causahabientes que consideren sean necesarios para consultar, reclamar, y que en caso de no ser posible realizar estas

acciones podrán escalar a ante la Superintendencia de Industria y Comercio un mal manejo de los datos.

Título VI: Deberes de los Responsables del Tratamiento y Encargados del Tratamiento. Se describen los deberes que deben tener con los Titulares de los datos y con los demás entes legales que la requieran además de mantener el cumplimiento del derecho del Habeas Data.

Título VII: De los Mecanismos de Vigilancia y Sanción. Este numeral cuenta con tres capítulos donde se describen los entes que regulan los Datos personales, las sanciones que se pueden presentar si se da un mal manejo y la obligación que tiene todos los entes que almacenen datos sensibles.

- Capítulo I: De la autoridad de protección de datos.
- Capítulo II: Procedimientos y sanciones.
- Capítulo III: Del Registro Nacional de Bases de Datos.

Título VIII: Transferencia de Datos a Terceros Países. En el numeral se indica que se encuentra prohibido llevar los datos por fuera del país, siempre y cuando no cuenten con la aprobación del titular o sean requeridos para fines específicos aprobados por esta norma.

Título IX: Otras disposiciones. Se indica que el Gobierno Nacional definirá las normas y buenas prácticas que se deben tener sobre la protección de datos personales.

4.4.3 LEY ESTATUTARIA 1266 DE 2008[64] (Habeas Data)

Establecida por el Congreso de Colombia y se encuentran consignadas las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Esta ley está dividida en siete títulos en los que encontramos las siguientes notaciones:

Título I: Objeto, ámbito de aplicación y definiciones. Se describen los derechos de todas las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos,

[64] C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1266 DE 2008,» 31 Diciembre 2008. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. [Último acceso: 22 Enero 2020].

libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales.

Para el entendimiento de esta ley se cuenta con algunas definiciones entre las que encontramos:

- Titular de la información: Persona a la que se refiere la información almacenada.

- Fuente de información: Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información.

- Operador de información: Es quien recibe la información y hace uso o retención de la información.

- Usuario: Es quien podrá consultar según los términos legales la información brindada por el Titular.

- Dato personal: Cualquier información relacionada a una persona.

- Dato público: Es información que se puede consultar de forma pública.

- Dato semiprivado: Información no solo puede ser de interés para el Titular sino también para otros.

- Dato privado: Información que solo es relevante al Titular.

- Agencia de Información Comercial: Es toda organización que tiene como actividad principal a recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes.

- Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Se describen además los principios que se deben tener sobre el uso, almacenamiento, manejo y protección de datos o derecho del Habeas Data. Entre los principios que se describen en este ítem se encuentran:

- Principio de veracidad o calidad de los registros o datos.
- Principio de finalidad.
- Principio de circulación restringida.
- Principio de temporalidad de la información.

- Principio de interpretación integral de derechos constitucionales.
- Principio de seguridad.
- Principio de confidencialidad.

Título II: Derechos de los titulares de la información. Se describe los derechos que tienen los Titulares sobre sus datos, de conocer el estado del almacenamiento y el uso que se da o la ubicación de los mismos además de siempre requerir a los Titulares autorización para el manejo que se quiera dar de forma adicional.

Título III: Deberes de los operadores, las fuentes y los usuarios de información. Se describen los deberes que deben tener con los Titulares de los datos y con los demás entes legales que la requieran además de mantener el cumplimiento del derecho del Habeas Data.

Título IV: De los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Título V: Peticiones de consultas y reclamos. En este numeral se describen las diferentes acciones que El Titular o sus causahabientes que consideren sean necesarios para consultar, reclamar, y que en caso de no ser posible realizar estas acciones podrán escalar a ante la Superintendencia de Industria y Comercio un mal manejo de los datos.

Título VI: Vigilancia de los destinatarios de la ley. Se describen los entes que regulan los derechos de Habeas Data, las sanciones que se pueden presentar si se da un mal manejo y la obligación que tiene todos los entes que almacenen estos datos.

Título VII: De Las disposiciones legales. Los entes que estén cubiertos bajo la administración de datos expuesta en esta ley tendrán un tiempo para implementar y alinearse a esta ley. Los Titulares deben actualizar de forma periódica esta información.

4.4.4 LEY 527 DE 1999[65] (Comercio Electrónico)

Establecida por el Congreso de Colombia y se encuentran consignadas las disposiciones generales el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de

[65] C. D. L. REPÚBLICA, «LEY 527 DE 1999,» 18 Agosto 1999. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html. [Último acceso: 24 Enero 2020].

certificación y se dictan otras disposiciones. Esta ley está dividida en 3 partes en los que encontramos las siguientes notaciones:

Parte I. Parte General

Capítulo I: Disposiciones generales.

Esta ley se aplica a todo tipo de información en forma de mensaje de datos salvo los comprendidos por temas legales o establecidos por disposición legal.

Para el entendimiento de esta ley se cuenta con algunas definiciones entre las que encontramos:

- Mensaje de datos. Es toda aquella información creada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

- Comercio electrónico. Referente a toda actividad de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.

- Firma digital. Es un valor numérico que se adhiere a un mensaje de datos. Este es utilizado como un identificador único.

- Entidad de Certificación. Es el ente que está autorizado por la ley para emitir certificados digitales.

- Intercambio Electrónico de Datos (EDI). Es la acción de trasmitir electrónicamente los datos de un sistema a otro.

- Sistema de Información. Se define como todo sistema utilizado para generar, enviar, recibir, archivar o procesar los mensajes de datos.

Capitulo II: Aplicación de los requisitos jurídicos de los mensajes de datos.

En el presente numeral se definen los usos y características de los mensajes de datos frente la utilidad de los mismos ante eventos jurídicos.

- Escrito: Se define al mensaje que expresa alguna información o aceptación.

- Firma: Cuando se requiere validar el origen de los mensajes o persona que envía.

- Original: Dice de aquel mensaje inicial.

- Integridad de un mensaje de datos: Es una de las características necesarias para tener validas de estos mensajes.

- Admisibilidad y fuerza probatoria de los mensajes de datos: Se dice cuando se tiene trazabilidad o log de seguimiento de correos.

- Criterio para valorar probatoriamente un mensaje de datos: Sera tomara como un activo si se puede garantizar la integridad del mensaje.

- Conservación de mensajes de datos y archivo de documentos a través de terceros: Solo si están autorizados y se tienen acuerdos para mantener estos mensajes de datos.

Capitulo III: Comunicación de los mensajes de datos.

Según la naturaleza de los mensajes de datos y acuerdos entre las partes que de cruzaran estos mensajes tendrán una valides y criticidad a tener cuenta. En este numeral se encuentra artículos que definen:

- Formación y validez de los contratos.
- Reconocimiento de los mensajes de datos por las partes.
- Atribución de un mensaje de datos.
- Presunción del origen de un mensaje de datos.
- Concordancia del mensaje de datos enviado con el mensaje de datos recibido.
- mensajes de datos duplicados.
- Acuse de recibo.
- Presunción de recepción de un mensaje de datos.
- Efectos jurídicos.
- Tiempo del envío de un mensaje de datos.
- Tiempo de la recepción de un mensaje de datos.
- Lugar del envío y recepción del mensaje de datos.

Parte II. Comercio Electrónico en Materia de Transporte de Mercancías

En este numeral se reglamenta los mensajes de datos relacionados con los actos relacionados con los contratos de transporte de mercancías y la valides de los documentos de trasporte enviados en estos mensajes.

Parte III. Firmas Digitales, Certificados Y Entidades De Certificación.

Capítulo I: Firmas digitales.

Indica cuando un suscriptor anexa la firma digital con la intención de acreditar el mensaje dato.

Capitulo II: Entidades de certificación.

Hace referencia a las entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que cumplan con los requerimientos que cumplen con los requisitos de ley para realizar esta actividad.

Capitulo III: Certificados.

Contiene la información digital del ente que desea der valido o garantizar la seguridad del mensaje

Capitulo IV: Suscriptores de firmas digitales.

Indica los deberes y responsabilidades de los suscriptores frente a las entidades públicas o privadas.

4.4.5 CIRCULAR EXTERNA 042 DE 2012[66] (Superintendencia Financiera)

Como agente regulador de las entidades financieras y en busca de mantener la seguridad de estas empresas y de todos sus clientes, la Superintendencia Financiera de Colombia reglamenta en su la circular externa 042 una serie de medidas encaminadas a fortalecer la seguridad y la calidad en el manejo de la información de los clientes y usuarios de las entidades y sus filiales, en lo referente a todas las operaciones.

Esta circular define los requerimientos mínimos de seguridad y calidad para la realización de operaciones. Entre los que encontramos:

- Obligaciones generales
- Seguridad y calidad
- Tercerización – Outsourcing
- Documentación
- Divulgación de información

[66] S. F. D. COLOMBIA, «CIRCULAR 042 DE 2012,» 05 Octubre 2012. [En línea]. Available: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf. [Último acceso: 26 Enero 2020].

- Obligaciones adicionales por tipo de canal
- Oficinas
- Cajeros Automáticos (ATM)
- Receptores de cheques
- Receptores de dinero en efectivo
- POS (incluye PIN Pad)
- Sistemas de Audio Respuesta (IVR)
- Centro de atención telefónica (Call Center, Contact Center)
- Sistemas de acceso remoto para clientes
- Internet
- Prestación de servicios a través de nuevos canales
- Banca Móvil.

4.4.6 CIRCULAR EXTERNA 007 DE 2018[67] (Superintendencia Financiera)

Como complemento de la circular 042 de la Superintendencia Financiera en esta circular se definen los requerimientos mínimos para la gestión de la seguridad de la Información y la Ciberseguridad.

Para este proceso se definen etapas que se debe tener en cuenta para cumplir con las necesidades de esta entidad, entre las que encontramos:

- Prevención
- Protección y Detección
- Respuesta y Comunicación
- Recuperación y Aprendizaje.

[67] S. F. D. COLOMBIA, «CIRCULAR 007 DE 2018,» 05 Junio 2018. [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20126/reAncha/1/c/00. [Último acceso: 27 Enero 2020].

5. ALCANCE Y DELIMITACION DEL PROYECTO

Se realizó un estudio de los elementos relevantes para la transmisión segura información, partiendo de la importancia de proteger y asegurar desde las herramientas que se utilizan hasta la forma de seleccionar y trasmitir esta información. Por tanto, se presentará un recorrido que abarca desde la conceptualización necesaria para entender el contexto, hasta su modelación frente a variados panoramas que las pymes pueden contemplar en su gestión. Se dará cuenta de una información efectiva, pertinente, y accesible que apunte al cómo implementar herramientas criptográficas, que garanticen la seguridad de la información, los archivos o datos que manejen las pymes.

El presente documento es viable para las pymes colombianas que requieran encontrar una forma sencilla y económica de mantener su información dentro de los parámetros legales y confidenciales; según el tipo de información que se determine en cada posible escenario que una pyme requiera. Por consiguiente, no sólo se expone el cifrado de información como la mejor herramienta para manipular la información, sino que también se presentan varias alternativas en las que dicho cifrado puede ser utilizado teniendo en cuenta los recursos y necesidades de cualquier pyme.

En definitiva, es indispensable resaltar del presente trabajo su enfoque guiado a tres puntos importantes, a saber: primero, la imperativa necesidad de un manejo adecuado de la información, teniendo en cuenta diferentes formas de acceder al proceso de cifrado. Segundo, la administración más apropiada para el uso del correo electrónico, apuntando a los posibles riesgos en que puede verse envuelta la información. Finalmente, cumplir y respetar los pilares de seguridad de la información: confidencialidad, disponibilidad e integridad de la información.

6. MARCO METODOLOGICO

El desarrollo de esta metodología se basó en una investigación de tipo deductiva partiendo de los diferentes estudios y documentación de la seguridad de la información para las PYMES, además de usar un enfoque basado en las de la norma ISO-IEC 27001 (SGSI) e ISO 27005 (Riesgos de Seguridad de la Información). También se basara en la recolección de información de procesos de aseguramiento de información disponibles en el mercado.

6.1 UNIVERSO Y MUESTRA

A través de una serie de encuestas a los empleados de algunas pymes, se obtuvo la información sobre los perfiles, recursos tecnológicos que maneja y el tipo de información que utiliza para desempeñar su cargo. A partir de estos datos, se logró definir el tipo de información que se debe tener en cuenta y enfocar dentro de la metodología que arrojara este proyecto.

6.2 FUENTES DE RECOLECCION DE INFORMACION

La investigación utilizó como fuentes de recolección de información diferentes monografías, estudios, informes estadísticos sobre el estado de seguridad de la información de las pymes y sus mayores retos en el mercado para salvaguardar la información que trasmite por correo electrónico. Además se tendrán en cuanta las leyes y normatividad vigente que aplica sobre las PYMES a para el manejo de la información.

6.3 TECNICAS E INTRUMENTOS

Para alcanzar el objetivo del presente documento, la investigación se apoyó en los siguientes instrumentos:

- Estudio del estado actual de la seguridad de la información en las PYMES.
- Encuestas, a los empleados de algunas PYMES que hagan envió o uso del correo electrónico para el desarrollo de sus actividades.
- Mediante observación se comprenderán los procesos y usos de la tecnología en su forma de trabajo diario.

7. METODOLOGÍA DE DESARROLLO

Para el desarrollo de la metodología anteriormente descrita se ejecutaron las actividades distribuidas en las siguientes fases:

- Fase I: Recolectar información conceptual de seguridad de la información y estado de arte del cifrado, metodologías y normatividad vigente.

  Se investigó en línea sobre la historia y evolución del correo electrónico, además los principales riesgos que se tienen al usar esta herramienta por las parte de las PYMES según el estudios previos realizados sobre estas. Se indago además por las normatividades vigentes para el manejo de información y datos personales, y que tipo de seguridad se aplica sobre los estos.

- Fase II: Revisar el estado actual del cumplimiento de estándares de seguridad de la información en el servicio de correo electrónico que utilizan las PYMES.

  Se listaron las principales normas como la ISO 27001, ISO27002, ISO27005, entre otras para definir la estructura de la metodología que se podría utilizar o seguir sus mejores prácticas.

- Fase III: Determinar e implementar metodología de cifrado para el aseguramiento del correo electrónico.

  Luego de conocer la mayoría de los riesgos y la identificación de las leyes que las pymes deberían cumplir se orientó el trabajo a la justificación y desarrollo de la metodología a implementar.

- Fase IV: Elaborar la documentación de la metodología aplicada y los resultados del proyecto.

  Se elabora el documento iniciando con la normatividad que la empresa debe conocer y entender. Continua con los temas a tener en cuenta como capacitación inicial desde la clasificación de los activos de información hasta la forma de mantenerlos seguros y transportarlos de forma segura por la red.

8. ANÁLISIS Y DISEÑO DE MECANISMO DE CIFRADO CORREO ELECTRONICO PARA PYMES

8.1 ANÁLISIS ENCUESTA PARA CONOCER ESTADO DE LA SEGURIDAD LA INFORMACIÓN EN LAS PYMES

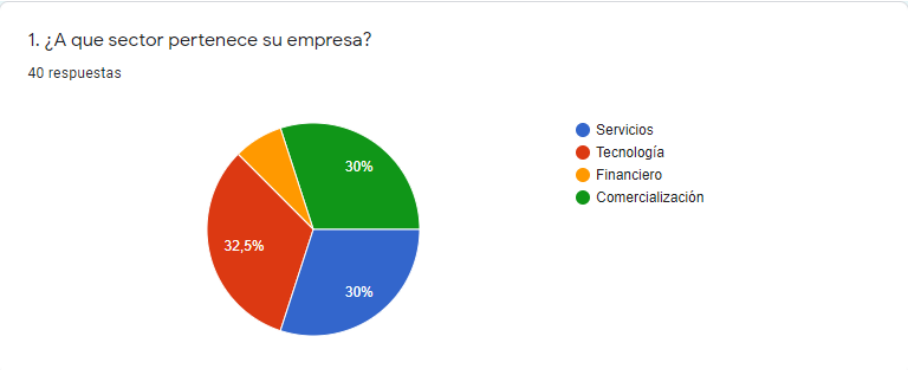
Para el desarrollo del presente trabajo aplicado, se desarrolló una encuesta aplicada a algunas PYMES de diferentes sectores económicos, denominada “Encuesta Para Conocer Estado De La Seguridad La Información En Las Pymes” (Ver Anexo 1). Para esta encuesta se tuvieron en cuenta factores específicos asociados a seguridad de la información desde la perspectiva de uso de correo electrónico. Se eligió un formato de encuesta digital basado en Google Forms, para facilitar el acceso a la encuesta y para obtener análisis gráfico de la misma haciendo uso de herramientas de Google. Se utilizó una aplicación de mensajería instantánea para hacer llegar la encuesta a la población a evaluar. Se envió el enlace y se alcanzó una población de cuarenta (40) encuestados, que hacen parte de empresas clasificadas como microempresas, pequeñas empresas o medianas empresas. Se realiza el análisis de cada pregunta y una conclusión general que permitió dar el enfoque orientador para las PYMES en los conceptos básicos de seguridad del a información que deben tener todas estas empresas.

A continuación se presentan los resultados obtenidos por cada pregunta y su conclusión inicial:

- Pregunta 1: ¿A qué sector pertenece su empresa’

  Para la encuesta se tuvieron en cuenta cuatro sectores de la economía geográficamente cercanos al autor.

Figura 3. Gráfico Encuesta Pregunta 1

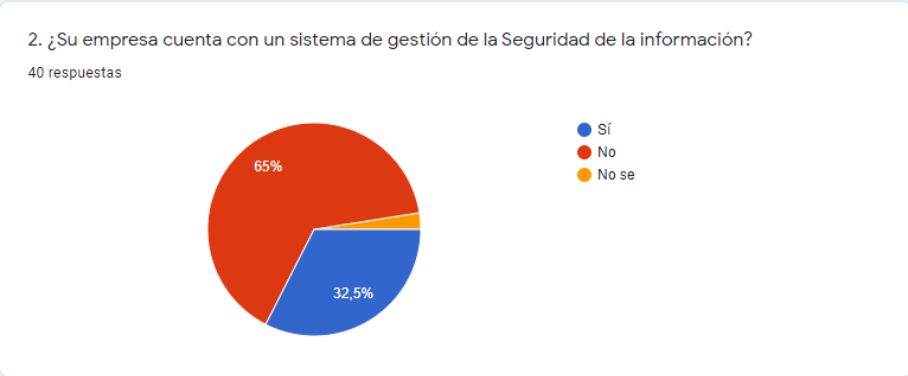


FUENTE: Autor.

- Pregunta 2: ¿Su empresa cuenta con un sistema de gestión de la Seguridad de la información?

  El 65% de los encuestados indican que no se ha implementado un sistema de gestión de seguridad de la información en la empresa donde laboran.

Figura 4. Gráfico Encuesta Pregunta 2

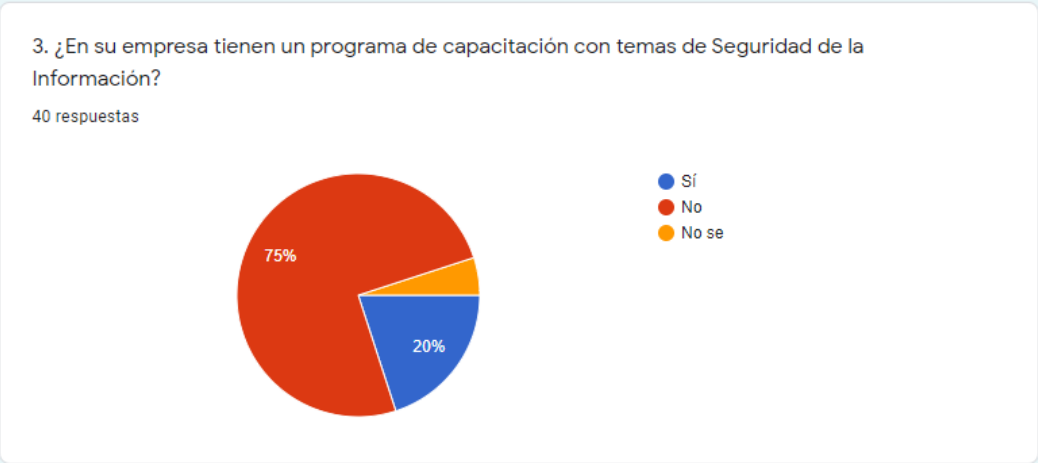


FUENTE: Autor.

- Pregunta 3: ¿En su empresa tienen un programa de capacitación con temas de Seguridad de la Información?

  A partir de los resultados, se puede observar que la mayoría de los encuestados indican no tener en la empresa una capacitación orientada a temas de seguridad de la información.

Figura 5. Gráfico Encuesta Pregunta 3

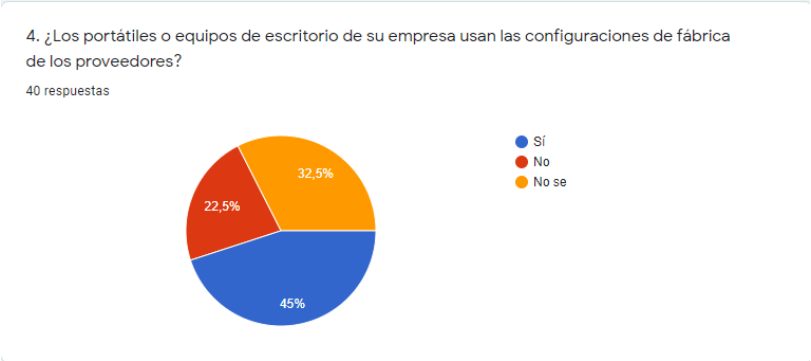


FUENTE: Autor.

- Pregunta 4: ¿Los portátiles o equipos de escritorio de su empresa usan las configuraciones de fábrica de los proveedores?

  A partir de los resultados, se encuentra que muchos de los equipos usados para el desarrollo de las actividades de la empresa, son equipos que se colocan en producción apenas se compran no tienen un alistamiento o aseguramiento previo.

Figura 6. Gráfico Encuesta Pregunta 4

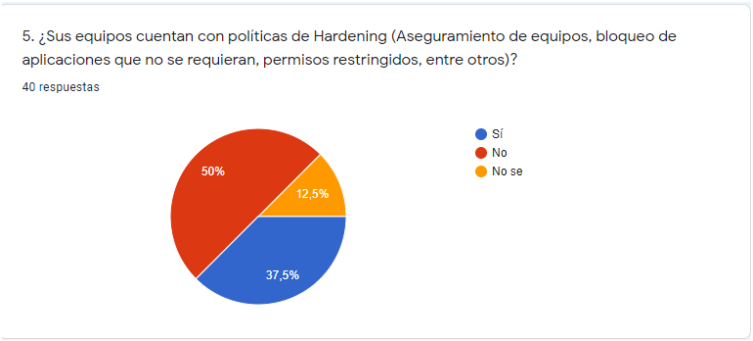


FUENTE: Autor.

- Pregunta 5: ¿Sus equipos cuentan con políticas de Hardening (Aseguramiento de equipos, bloqueo de aplicaciones que no se requieran, permisos restringidos, entre otros)?

  Se encuentra que un 45% de los equipos usados para el desarrollo de las actividades de la empresa, son equipos que se colocan en producción no tienen un alistamiento o aseguramiento previo. Y que solo el 22.5% de los encuestados conocen que de alguna forma los equipos de sus empresas son reconfigurados.

Figura 7. Gráfico Encuesta Pregunta 5

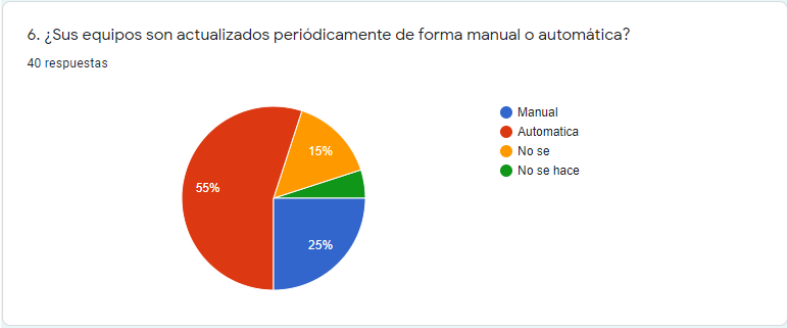


FUENTE: Autor.

- Pregunta 6: ¿Sus equipos son actualizados periódicamente de forma manual o automática?

  Se observa que el 5% de los equipos usados para el desarrollo de las actividades de las empresas no se actualizan, lo cual podría dar pie a que puedan explotar las vulnerabilidades que estos tengan. La cuarta parte de los encuestados saben que se hace de forma manual y el 55% informó que se hacen de mane automática sin embargo se hace necesaria una encuesta más específica para validar si realmente está configurada la actualización automática y si en realidad funciona.

Figura 8. Gráfico Encuesta Pregunta 6

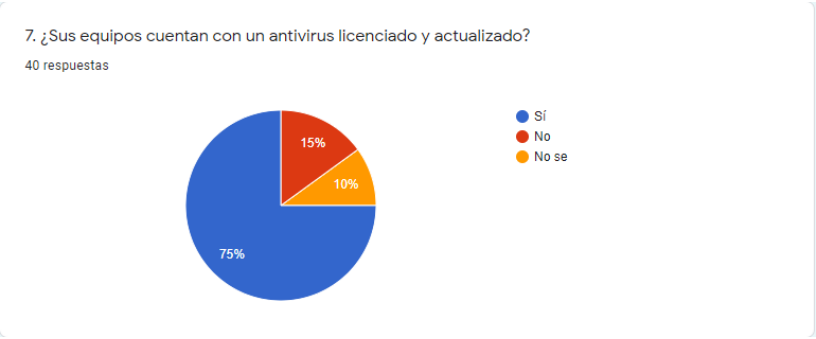


FUENTE: Autor.

- Pregunta 7: ¿Sus equipos cuentan con un antivirus licenciado y actualizado?

  A partir de los resultados, se observa que aunque no es un gran porcentaje varios de los equipos usados para el desarrollo de las actividades de las empresas no se usan antivirus o no usan antivirus licenciados, lo cual podría dar pie a que puedan explotar las vulnerabilidades que estos tengan.

Figura 9. Gráfico Encuesta Pregunta 7

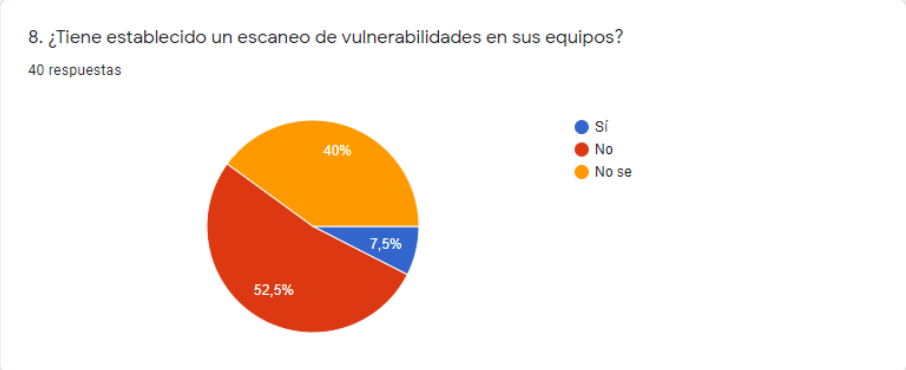


FUENTE: Autor.

- Pregunta 8: ¿Tiene establecido un escaneo de vulnerabilidades en sus equipos?

  A partir de los resultados, se observa que los equipos no cuentan con un análisis de vulnerabilidades por lo cual tampoco tendrá un aseguramiento que impida que puedan explotar las vulnerabilidades que estos tengan.

Figura 10. Gráfico Encuesta Pregunta 8

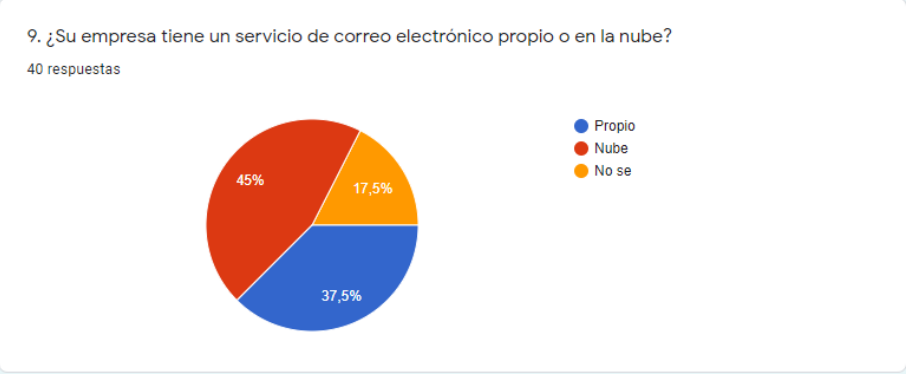


FUENTE: Autor.

- Pregunta 9: ¿Su empresa tiene un servicio de correo electrónico propio o en la nube?

  A partir de los resultados, se observa en un gran porcentaje utilizan servicios de correo electrónico en la nube, muy pocos son propios o están administrados.

Figura 11. Gráfico Encuesta Pregunta 9

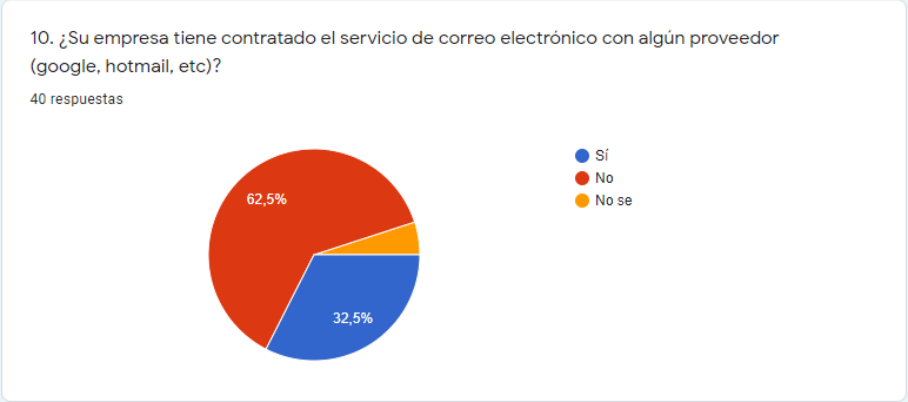


FUENTE: Autor.

- Pregunta 10: ¿Su empresa tiene contratado el servicio de correo electrónico con algún proveedor (google, hotmail, etc)?

  El 62.5% de los encuestados no conocen si en su empresa se usa alguna plataforma de correo en la nube, utilizando servicios de diversos proveedores. No se conoce con exactitud si desconocen la interrelación entre el concepto de nube, servicio de correo e internet.

Figura 12. Gráfico Encuesta Pregunta 10

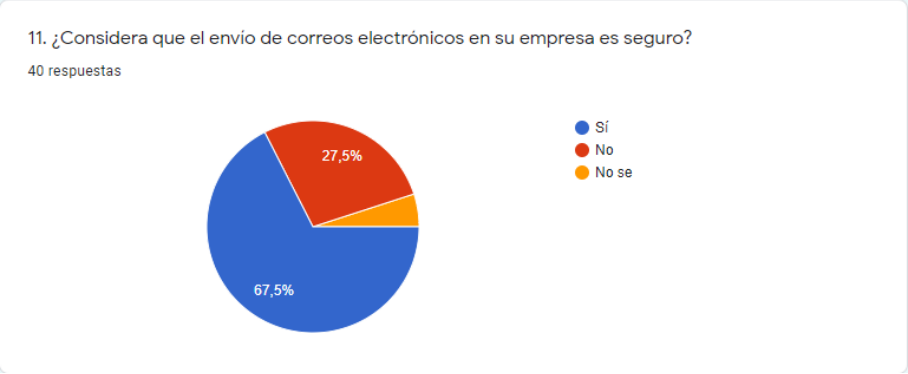


FUENTE: Autor.

- Pregunta 11: ¿Considera que el envío de correos electrónicos en su empresa es seguro?

  A partir de los resultados, se puede encontrar que no todos los encuestados tiene la certeza que el correo que se envía sea seguro.

Figura 13. Gráfico Encuesta Pregunta 11



FUENTE: Autor.

- Pregunta 12: ¿Realiza envío de información confidencial o privada para la empresa por correo electrónico?

  A partir de los resultados, se observa que mucha de la información que se envía o recibe de las empresas por los correos electrónicos es considerada confidencial o privada por cada encuestado.

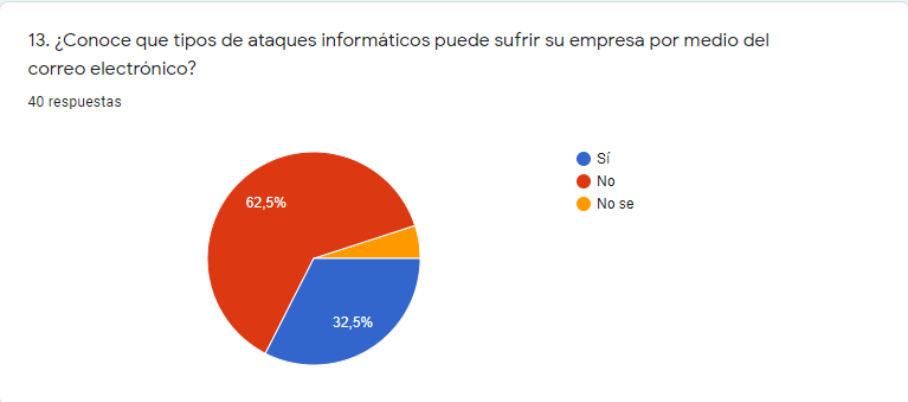
Figura 14. Gráfico Encuesta Pregunta 12

FUENTE: Autor.

- Pregunta 13: ¿Conoce que tipos de ataques informáticos puede sufrir su empresa por medio del correo electrónico?

  A partir de los resultados, se observa un porcentaje muy elevado de los encuestados no tienen conocimiento de los ataques informáticos que se pueden presentar por medio del correo electrónico.

Figura 15. Gráfico Encuesta Pregunta 13

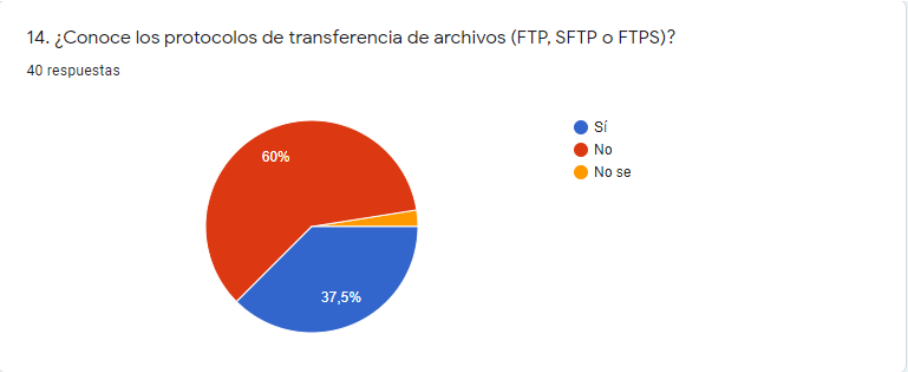


FUENTE: Autor.

- Pregunta 14: ¿Conoce los protocolos de transferencia de archivos (FTP, SFTP o FTPS)?

  A partir de los resultados, se observa un alto nivel de desconocimiento en otros medios de envío o recepción de la información.

Figura 16. Gráfico Encuesta Pregunta 14



FUENTE: Autor.

- Pregunta 15: ¿Tienen alguna política o restricción para enviar información por el correo electrónico (Tamaño o tipo de archivo)?

  A partir de los resultados, se observa que al no tener la administración de los correos no se pueden configurar para brindar seguridad en los correos electrónicos enviados o recibidos.

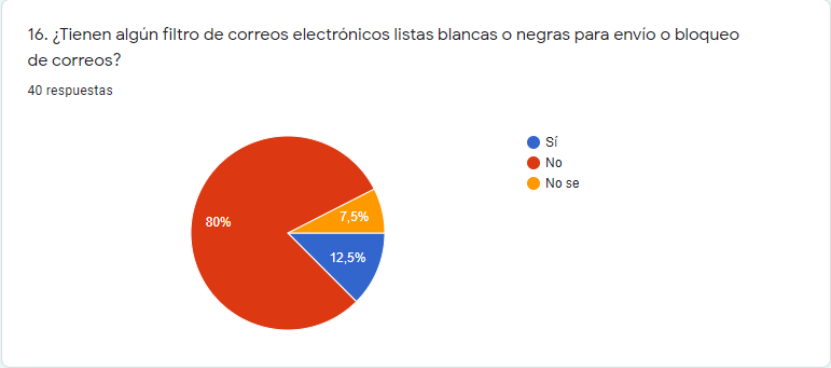
Figura 17. Gráfico Encuesta Pregunta 15

FUENTE: Autor.

- Pregunta 16: ¿Tienen algún filtro de correos electrónicos listas blancas o negras para envío o bloqueo de correos?

  El 80% de los encuestados desconoce si en su empresa se utilizan listas blancas o negras para los correos electrónicos, no se tiene certeza si la población encuestada, conoce el concepto de listas blancas o negras o su aplicación en los ámbitos de las tecnologías de la información.

Figura 18. Gráfico Encuesta Pregunta 16



FUENTE: Autor.

- Pregunta 17: ¿Se implementa alguna medida preventiva para el envío de correos electrónicos (cifrado)?

  A partir de los resultados, se observa no se tiene conocimiento del uso de cifrado en correo electrónico, teniendo en cuenta que un porcentaje de los encuestados afirmaron conocer el tipo de correo en uso, no se sabe si la población conoce formas de cifrar o asegurar la información que se envía o trasmite por medio del correo electrónico.

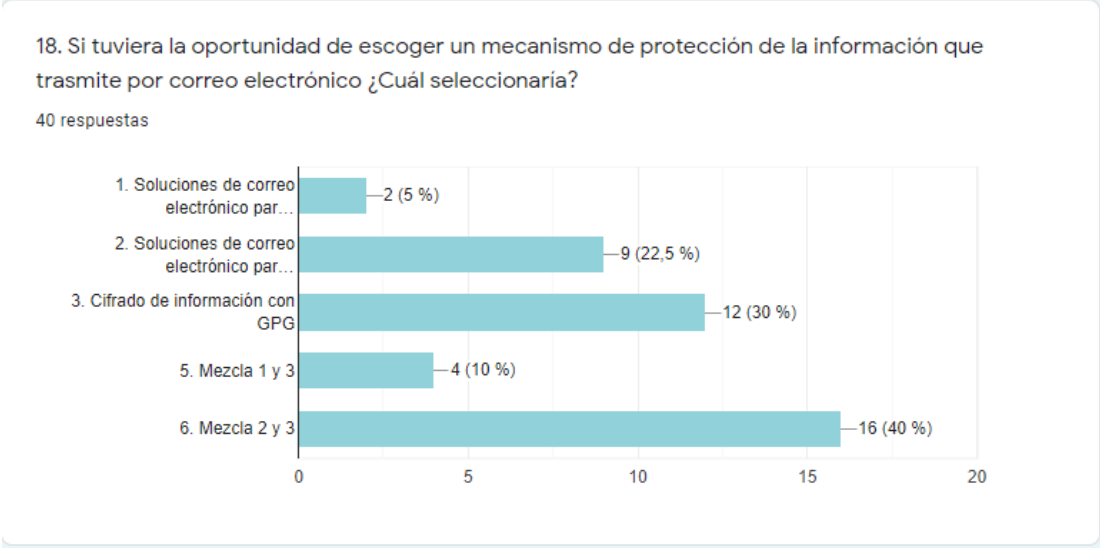
Figura 19. Gráfico Encuesta Pregunta 17

FUENTE: Autor.

- Pregunta 18: Si tuviera la oportunidad de escoger un mecanismo de protección de la información que trasmite por correo electrónico ¿Cuál seleccionaría?

  A partir de los resultados, se observa los encuestados desean conocer métodos de cifrado usando la nube como el servicio para almacenar la información. No se tiene mucho interés en tener una infraestructura que tengan que instalar y configurar en sus empresas para brindar seguridad en los correos electrónicos enviados o recibidos.

Figura 20. Gráfico Encuesta Pregunta 18



FUENTE: Autor.

Según lo observado en los resultados de las encuestas realizadas a algunas Pymes, se observa desconocimiento de la gestión que deberían realizar de la Seguridad de la Información tanto a nivel de la infraestructura interna como de los servicios utilizados por la empresa para el desarrollo de sus actividades. Además de la falta de controles que podrían tener para asegurar la información y del servicio utilizado para enviar la información por correo electrónico u otros medios.

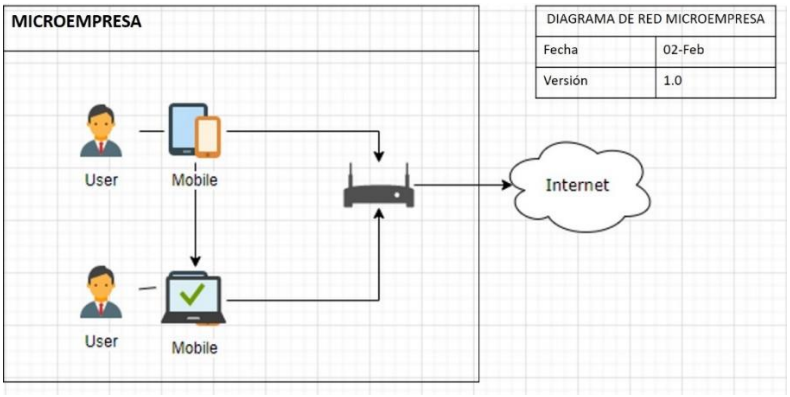
Otra conclusión que se logró obtener de la anterior encuesta es que para él envió de correo con información sensible no se cuenta con algún cifrado o seguridad aplicada y con ello poder garantizar la confidencialidad, integridad y disponibilidad de la información que se procesa por los correos electrónicos.

8.2 INFRAESTRUTURA TECNOLOGICA DE LAS EMPRESAS

Durante el levantamiento de información se identificaron diferentes infraestructuras o arquitecturas de red, en varios casos con una característica similar desde el punto de vista del tamaño o categoría de la empresa.

- Para las Microempresas donde la cantidad de empleados puede iniciar de 1 a 5 funcionarios, la conexión se realiza con un servicio de red casero donde solo se requiere tener un modem WIFI para realizar las actividades.

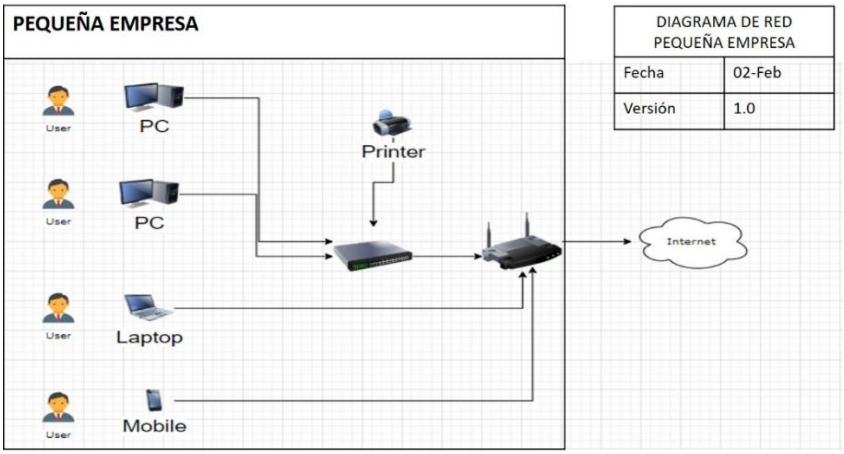
Figura 21. Diagrama de red Microempresa



FUENTE: Autor.

- Para las Pequeñas empresas donde la cantidad de empleados puede iniciar de 6 a 20 funcionarios, la conexión se realiza con un servicio de red compuesto por un modem WIFI y un switch para realizar las actividades.

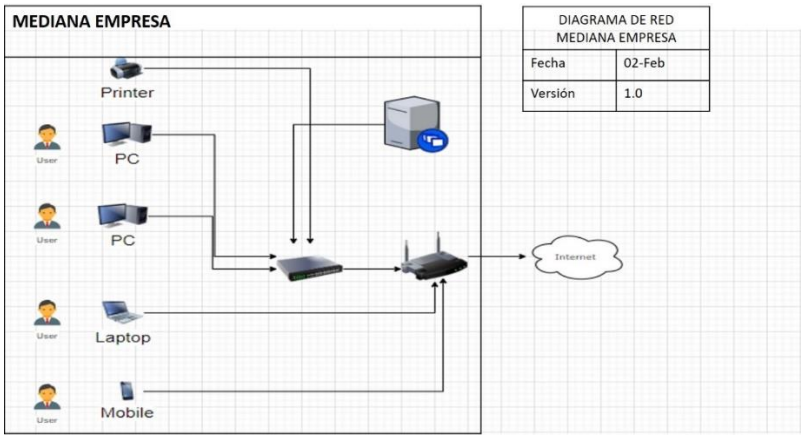
Figura 22. Diagrama de red Pequeña empresa



FUENTE: Autor.

- Para las Medianas empresas donde la cantidad de empleados puede iniciar de 21 a 40 funcionarios, la conexión se realiza con un servicio de red compuesto por un modem WIFI y un switch y en algunas ocasiones un servidor que brinda varios servicios (fileserver, Impresión , DCHP, etc.) para realizar las actividades.

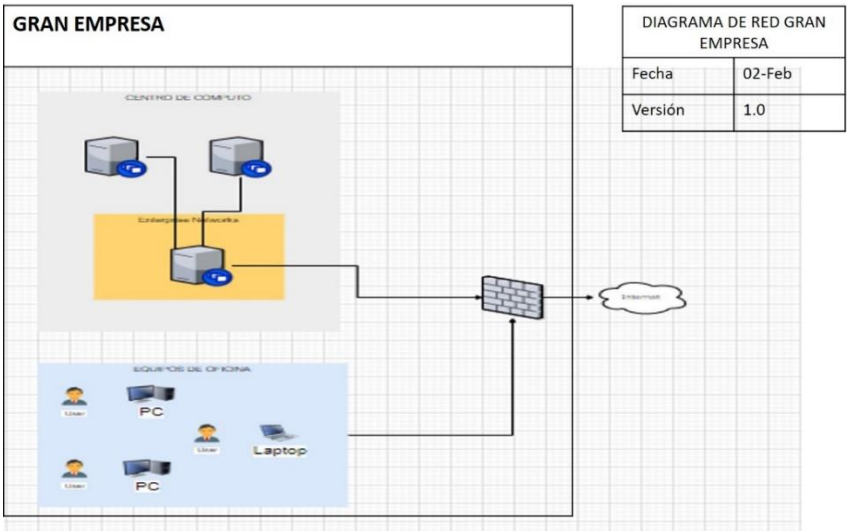
Figura 23. Diagrama de red Mediana empresa



FUENTE: Autor.

- En las grandes empresas donde la cantidad de empleados puede iniciar de 41 o más funcionarios, la conexión se realiza con un servicio de red compuesto por un firewall, router, uno o varios switch, WIFI servidores con varias funciones (fileserver, Impresión, DCHP, etc.) para realizar las actividades.

Figura 24. Diagrama de red Gran empresa



FUENTE: Autor.

Se identificó que según los diferentes tipos de infraestructura interna de las empresas cada una puede tener necesidades diferentes para el desarrollo de sus actividades. Sin embargo todos concuerdan que hay flujo de la información que va a internet o vía web al que es necesario garantizar una seguridad adecuada.

8.3 TIPOS DE INFRAESTRUTURA PARA EL CORREO ELECTRONICO

Dentro de la investigación realizada se observaron varios tipos de infraestructura usada para el manejo y administración de correo electrónico. Se identificaron que puede variar según el tamaño de la empresa, necesidades del negocio, experiencia e infraestructura utilizada para el desarrollo del negocio. Se logró identificar que de los tipos de infra estructura se encuentra: manejo de correos gratuitos, correos cloud corporativos con dominio propio o simplemente con instalaciones de servicios de correo local dentro de la empresa. A continuación se incluye una descripción de los servicios que brindan y qué condiciones se deben tener en cuenta.

8.3.1 SERVICIO DE CORREOS CLOUD GRATUITOS

En la Web se encuentran diversos proveedores que brindan servicios de correo electrónico gratuito, con diferentes características y condiciones en su uso, teniendo en cuenta que el medio por el cual las empresas se comunican con sus clientes y proveedores se debe tener algunos parámetros básicos al seleccionar un servicio de correo gratuito. Algunos de los requisitos que se deberían tener en cuenta son:

- Fácil uso: Al ser una herramienta que puede ser usada por todos los miembros de la empresa debe ser de fácil uso y acceso para cada empleado.

- Reputación: El proveedor del servicio del correo debe tener un reconocimiento en el mercado, es importante tener en cuenta que será utilizado para comunicarse con sus clientes volviéndose un activo valioso para le empresa.

- Filtros Spam: Con el crecimiento de los servicios en la web la necesidad de limitar o identificar los correos que llegan como Spam se vuelve una parte crucial en el manejo del tiempo que pueda requerir validar los correos realmente importantes.

- Disponibilidad: Al ser un servicio utilizado para las actividades diarias de las empresas, se requiere contar que este servicio siempre esté disponible.

- Capacidad de almacenamiento: Al ser una herramienta por la que se recibe y envía información de la empresa debe tener buena capacidad de almacenamiento.

- Respaldo y recuperación

Algunos de los proveedores de correo gratuito más usados por las empresas son:

- Gmail
- Outlook.com
- icloud.com
- yahoo.com
- zoho.com

El registrarse en cualquiera de estas plataformas es muy fácil ya que tienen ambientes amigables para todas las personas, sin embargo es importante tener en cuenta que aun cuando son de fácil acceso y cumplan con los requisitos básicos que buscan las empresas, es necesario considerar las ventajas y desventajas que esto gratuitos puedan tener.

- Ventajas: Una de las ventajas más claras que se tienen es no tiene costo acceder a estos correos. Además de la facilidad para envió de correos instantáneos y que es de fácil acceso para las personas.

- Desventajas: Aunque es un servicio que tiene un proveedor que lo soporte entre las principales desventajas podemos encontrar:

    - Es más fácil recibir correo con virus al no tener filtros de Spam ni DLP para el manejo del correo.
    - La identidad puede ser fácilmente robada.
    - No permite que el correo sea reconocido al no usar un dominio que identifique la empresa.
    - No es profesional no da buena imagen a la empresa.
    - Es más fácil que lo puedan clasificar como correo sospechoso.
    - No se cuenta con respaldo garantizado.

8.3.2 SERVICIO DE CORREOS CLOUD ADMINISTRABLES

Además de tener en cuenta los mismos parámetros de selección que el correo gratuito, a este servicio se agregan variables enfocadas tener mayor personalización, seguridad y monitoreo de los correos tal como se relaciona a continuación:

- Dirección de correo personalizada: Es un valor agregado para la empresa el poder desde un correo dar a conocer el nombre de la empresa, y dar la tranquilidad que el correo que se reciba sea un destinatario aprobado.

- Fácil uso: Al ser una herramienta que puede ser usada por todos los miembros de la empresa debe ser de fácil uso y acceso para cada empleado.

- Reputación: El proveedor del servicio del correo debe tener un reconocimiento en el mercado, es importante tener en cuenta que será utilizado para comunicarse con sus clientes volviéndose un activo valioso para le empresa.

- Filtros Spam inteligentes y/o administrables: Con el crecimiento de los servicios en la web la necesidad de limitar o identificar los correos que llegan como Spam se vuelve una parte crucial en el manejo del tiempo que pueda requerir validar los correos realmente importantes.

- Prevención contra Spam y virus: La mayoría de proveedores para garantizar las cuentas corporativas adicionan los módulos de seguridad que tiene como valor agregado de tener las cuentas de correos con ellos.

- Disponibilidad: Al ser un servicio utilizado para las actividades diarias de las empresas, se requiere contar que este servicio siempre esté disponible.

- Mayor capacidad de almacenamiento: Al ser una herramienta por la que se recibe y envía información de la empresa debe tener buena capacidad de almacenamiento.

- Monitoreo y soporte: Tal como se indica agregar a la empresa opciones de monitorear y/o control de los correos de la empresa se vuelve una opción valiosa para la empresa.

Algunos de los proveedores de correo más usados por las empresas son:

- Office 365
- G Suite
- Mail.com
- Zoho Workplace
- ProtonMail
- Rackspace
- Bluehost
- FastMail

- Mailbird
- Liquid Web

Adquirir un correo corporativo no es complicado la mayoría de estas plataformas dan soporte o plataformas amigables para configurar estos correos, a diferencia del correo gratuito son más las ventajas y que las desventajas que se tienen.

- Ventajas: De los principales beneficios es dar buen nombre a la compañía al dar la tranquilidad a otras empresas que los correos que salen son controlados y monitoreados.

    - Seguridad sobre los correos.
    - Personalización de los correos.
    - Recuperación y continuidad de correos.
    - Monitoreo y control.
    - Soporte y mantenimiento.

- Desventajas: La mayor desventaja es el costo que se puede tener según los servicios que se contraten o que desean agregar ya que el costo será dará vs la cantidad de empleados o cuentas de correo que se deseen.

8.3.3 SERVICIO DE CORREOS INFRAESTRUCTURA LOCAL

Cuando las empresas desean tener un mayor control sobre su información y más aún sobre los correos electrónicos, realizan implementaciones locales dentro de su infraestructura tecnológica para tal propósito.

Para realizar este proceso no es una tarea sencilla ya que deben empezar por asegurar la infraestructura sobre la que desean implementar el servicio de correos, otra parte fundamental es tener clara la capacidad que puede llegar a tener este servicio de forma local, ya que sobre el mismo tendrán que contemplar tener un Backups de toda esta infraestructura.

La definición y ejecución de controles sobre la infraestructura y servicio requiere tener, el conocimiento necesario para poder soportar y administrar la misma es uno de varios requisitos que puede requerir este tipo de infraestructura. También se va a necesitar:

- Adquirir un dominio para asignar sobre los correos.
- Comprar los certificados digitales para este servicio.
- Gestionar la publicación del servicio de correo con el proveedor de internet que tengan contratado.
- Adquirir soporte o personas que administren la plataforma.
- Definir e implementar reglas Spam.
- Configurar servicio DLP o bloqueo preventivo del contenido que ingresa o sale del correo.

Estos servidores pueden ser montados tanto en software libre como en licenciado. Lo primordial es estar dispuesto a dedicar a una persona responsable de este servicio y además, tener claro que al ser un servicio clave debe contar con una infraestructura que soporte o de la opción de mantener una continuidad del negocio.

Es claro que este tipo de infraestructura al igual de los servicios de correo en cloud también tiene sus ventajas o desventajas entre las que se encuentran:

- Ventajas: Uno de los principales beneficios tener mayor control sobre la ubicación y uso de los correos, aunque también se puede encontrar.
    - Seguridad sobre los correos.
    - Personalización de los correos.
    - Recuperación y continuidad de correos.
    - Monitoreo y control.
    - Soporte y mantenimiento.

- Desventajas: La mayor desventaja es el costo que se puede tener según los servicios que se contraten y de acuerdo al crecimiento o tamaño de la empresa. Otras desventajas que se deben contemplar son:
    - Tener una infraestructura adicional que soporte el correo.
    - La necesidad de monitoreo constante e implementación de rutinas de mantenimiento.

Según lo observado e investigado aunque existen diferentes estructuras para tener correos electrónicos y si se tiene la posibilidad de invertir costos sobre este servicio para obtener mayor seguridad y además incluir opciones de control y monitoreo sobre estas plataformas, se hace necesario garantizar el contenido dentro de estos correos.

8.4 ¿POR QUÉ PROTEGER LA INFORMACION QUE SE ENVIA POR EMAIL?

En la actualidad se observa que el acceso a la información es parte importante para el desarrollo de las actividades laborales o personales. Para el uso controlado y seguro de esta información se manejan infraestructuras informáticas que permitan que esta permanezca confiable, integra y que siempre esté disponible.

Estas infraestructuras no siempre son tan robustas, en algunas ocasiones suele manejarse esta información hasta en los PC personales. En muchas empresas suelen estar compuesta por varios equipos de comunicación almacenamiento y procesamiento que permiten la transmisión y acceso de la información. Sin importar cuál sea el medio que se use debe ser claro que es importante contar con la seguridad necesaria para proteger las mismas ya sea nivel personal o de la empresa.

Dada la importancia que tiene la información se hace indispensable que haya una protección de estos sistemas, no solo por lo útil para las personas sino también porque es propensa a ser utilizadas para otros fines. Por ejemplo en una empresa la información que contiene es útil para su crecimiento al igual que esta información en manos de la competencia podría darle fin a la misma empresa. Por consiguiente proteger la información es una de las primeras tareas que se deben tener en cuenta para llegar a nuestras metas.

En conclusión es necesario tener un sistema que asegure nuestra información, que de tranquilidad tanto a una persona como a las empresas que no va a tener riesgo en el manejo de la información. Debe ser un proceso que este en constante monitoreo y control.

8.5 CONTROLES NTC-ISO 27001:2013 A TENER EN CUENTA

La norma NTC-ISO 27001:2013 contiene los requisitos y controles necesarios para la implementación de un sistema de gestión de seguridad de la información SGSI. La adecuación o cumplimiento de esta norma es acorde en muchas ocasiones a las definiciones del CORE de negocio que exigen un total cumplimiento de estos requisitos.

Para las Pymes la utilización de la norma NTC-ISO 27001:2013 no es muy frecuente, dado que o se contempla que se pueden llegar a implementar o tomar como guía solo algunos de los requisitos expuestos en ella. Para el presente trabajo aplicado se utilizara como base para realizar o brindar las mejores prácticas de aseguramiento para las PYMES aun cuando no se apliquen todos los dominios que esta norma contiene.

Tomando como base la tabla de los dominios y controles de la norma correspondientes al Anexo A de la norma NTC-ISO 27001:2013 (**Ver Anexo 2**) para el presente proyecto se tuvieron en cuenta los siguientes numerales:

- A.7 Seguridad De Los Recursos Humanos
    - A.7.2 Durante la ejecución del empleo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
        - A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.
- A.8 Gestión De Activos
    - A.8.1 Responsabilidad por los activos: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
    - A.8.2 Clasificación de la información: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
- A.9 Control De Acceso
- A.10 Criptografía
- A.12 Seguridad De Las Operaciones

- A.13 Seguridad De Las Comunicaciones

    - A.13.2 Transferencia de información: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

- A.18 CUMPLIMIENTO

En el **Anexo 2** del presente trabajo se podrán consultar al detalle todos los controles que se encontraran dentro de la norma NTC-ISO 27001:2013. Se observaran cuatro columnas representan:

- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC-ISO 27001:2013.
- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- APLICA SI O NO: El listado de controles además debe ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la entidad tenga documentado y de fácil acceso el inventario de controles.
- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla.

9. METODOLOGÍA DE CIFRADO PARA EL ASEGURAMIENTO DEL CORREO ELECTRÓNICO.

Para el desarrollo de la metodología o pasos a seguir para asegurar la información se utilizó la norma NTC-ISO 27001 como una base de buenas prácticas a implementar dentro de las Pymes. Con el anterior propósito la implementación de la metodología propuesta para las Pymes se tuvo en cuenta una breve capacitación en temas legales o de normatividad aplicable a las empresas en general. Se prosigue con las diferentes opciones de cifrado que se pueden utilizar para asegurar la recepción, procesamiento, almacenamiento y trasmisión de información. Además se concluye con una serie re recomendación en la implementación de políticas, procedimientos o guías de aseguramiento sobre las plataformas donde se procesaran los correos.

9.1 CAPACITACION INICIAL

9.1.1 NORMATIVIDAD VIGENTE EN COLOMBIA APLICABLE A PYMES

Tal como es enunciado en la mayoría de documentos legales o jurídicos el desconocimiento de una ley no exime el cumplimiento de ellas. Con base en la anterior premisa es importante dar a conocer a los integrantes o empleados de una empresa las leyes que son aplicables al recibir, procesar, almacenar o trasmitir información interna, de clientes y/o proveedores.

LEY 1273 DE 2009[68] (Delitos Informáticos en Colombia): Ley que se encarga de la protección de la información y de los datos que circulan sobre las tecnologías de la información y las comunicaciones.

LEY ESTATUTARIA 1581 DE 2012[69] (Protección de Datos Personales): En esta ley se describen las disposiciones legales para la protección de los datos personales para salvaguardar la vida privada o familiar de los colombianos.

[68] C. D. L. REPÚBLICA, «Ley 1273 DE 2009,» 05 Enero 2009. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. [Último acceso: 20 Enero 2020].

[69] C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1581 DE 2012,» 17 Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 21 Enero 2020].

LEY ESTATUTARIA 1266 DE 2008[70] (Habeas Data): En esta ley se reglamenta la seguridad que se debe garantizar sobre las bases de datos que contenga información personal, financiera, comercial o sensible entre otras.

LEY 527 DE 1999[71] (Comercio Electrónico): Esta ley reglamenta las condiciones de seguridad que debe existir sobre el comercio o transacciones electrónicas que realizan las organizaciones.

CIRCULAR EXTERNA 042 DE 2012[72] Y CIRCULAR EXTERNA 007 DE 2018[73] (Superintendencia Financiera): Según se describe en estas circulares todas aquellas empresas que brindan algún servicio o soporte a entidades financieras deben implementar o alinearse a las buenas prácticas de seguridad de la información descritas en la norma NTC-ISO 27001.

9.1.2 CLASIFICACIÓN DE LA INFORMACIÓN

Es responsabilidad de los líderes o propietarios de las Pymes llevar un inventario y clasificación de activos de información con el fin de darle el correcto uso y aseguramiento a todos los activos de información de la compañía.

Los activos de información están agrupados en cuatro categorías:

- **Digitales**: Dentro de esta clasificación se encuentran las bases de datos y archivos de datos, Servidores de archivos, contratos y acuerdos, documentación del sistema, información sobre investigaciones de mercado, documentación de las áreas, manuales y procedimientos internos, informes de auditorías.

[70] C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1266 DE 2008,» 31 Diciembre 2008. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. [Último acceso: 22 Enero 2020].
[71] C. D. L. REPÚBLICA, «LEY 527 DE 1999,» 18 Agosto 1999. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html. [Último acceso: 24 Enero 2020].
[72] S. F. D. COLOMBIA, «CIRCULAR 042 DE 2012,» 05 Octubre 2012. [En línea]. Available: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf. [Último acceso: 26 Enero 2020].
[73] S. F. D. COLOMBIA, «CIRCULAR 007 DE 2018,» 05 Junio 2018. [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20126/reAncha/1/c/00. [Último acceso: 27 Enero 2020].

- **Físicos**: Son todos aquellos activos como documentos internos, de clientes y proveedores, registros personales, políticas, manuales de usuarios y/o técnicos de las empresas

- **Software**: Es todo el software utilizado por la compañía para el desarrollo de sus actividades como por ejemplo correo, aplicativos contables, sistemas financieros, aplicaciones de soporte o monitoreo entre otros.

- **Equipos**: Equipos de cómputo, equipos de comunicaciones, medios removibles, impresoras, scanner, tabletas, PDA, teléfonos corporativos teléfonos IP y otros equipos.

- **Redes**: VPN, FTP, SFTP, FTPS u otras conexiones.

Como actividad inicial de cualquier empresa, se debe realizar una clasificación de la información de acuerdo a la los tres pilares de la seguridad de la información.

- Según su confidencialidad se clasifican en:

    - **Confidencial:** Información estratégica sobre las operaciones de la compañía y las actividades de negocio que afecte a propietarios, inversionistas clientes, proveedores o genere desventaja frente a los competidores.

    - **Sensible o Personal:** La información que se puede utilizar para identificar, contactar o localizar a una persona, se denomina "información personal identificable" o PII.

    - **Uso interno:** Información que solo debe ser divulgada internamente, dirigida al personal interno.

    - **Publico:** Información que ha sido declarada de conocimiento público.

- Según su integridad se clasifican en:

    - **Modificación altamente restringida:** La modificación de esta información puede causar daño significativo al negocio.

- **Modificación restringida:** Información potencial para cambios moderados. La frecuencia con la que se realizan cambios sobre este tipo de activo de información no es frecuente.
- **Modificación controlada:** Información que puede ser modificada bajo circunstancias debidamente controladas.

- **Modificación Simple:** Información que puede ser modificada sin presentar ningún inconveniente para el negocio.

- Según su disponibilidad se clasifican en:

  - **Muy crítica:** Cuando la no disponibilidad de la información puede causar consecuencias serias para el negocio.

  - **Critica:** Cuando disponibilidad de la información necesaria para la continuidad del negocio.

  - **Importante:** Cuando la falta de disponibilidad de esta información puede llegar a no tener repercusiones negativas en la operación.

  - **Simple:** Cuando la disponibilidad de la información no afecta la operación normal.

9.1.3 RIESGOS ASOCIADOS AL USO DE CORREO ELECTRONICO

Es necesario al momento de capacitar a los usuarios buscar concientizar no solo de los riesgos sino los malos usos que pueden asociados al tener un correo electrónico que se pueden presentar al servicio de correo por ejemplo:

- Correo no deseado (spam): Son correos enviados de forma masiva casi siempre con publicidad o información no solicitada por los destinatarios, y cuyos contactos son obtenidos a través de internet.

Figura 25. Correo no deseado o Spam.

Fuente: Correo personal autor

- Suplantación de identidad (spoofing): Son correos falsos suplantando la identidad, nombres y dominios personas, socios comerciales o proveedores legítimos, por medio de estos intentan obtener información sensible o critica.

  ¿Cómo lo detecto?: Cuando el contenido del correo o dirección de remitente son diferentes al actual o tiene dudas de la información que se solicita.

  ¿Cómo evitarlo?: Si tienes dudas del correo comprueba la veracidad del mensaje, contacta por otro medio al remitente y confirma los datos.

- Phishing: Es un ataque informático que busca tener acceso a información personal para poder suplantar la información del usuario.

  ¿Cómo lo detecto?: Correos con links a encuestas sitios falsos donde solicitan información sensible.

  ¿Cómo evitarlo?: Nunca enviar datos sensibles por correo, no abrir ni responder link de correos electrónicos no solicitados, no abrir correos de información no solicitados, comprobar las URL y dominios de sitios a donde te re direcciona.

9.2 POLITICA Y PROCEDIMIENTO DE CIFRADO RECOMENDADO

Dentro de las Pymes que deseen asegurar la información deben seguir los siguientes lineamientos para la aplicación de controles criptográficos:

- Es necesario utilizar la herramienta una aplicación de sobre los archivos o información que por su clasificación de activos, criticidad y riesgo requieran niveles máximos de aseguramiento.

- Los algoritmos de cifrado aprobados son: AES, TripleDES, Twofish, DSA, RSA, ECDSA y SHA1, los cuales deben ser utilizados como base de la tecnología de cifrado.

- Los sistemas de criptografía simétricos deben utilizar llaves con 128 bits o más. Las llaves de los sistemas de criptografía asimétricos deben utilizar longitudes que ofrezcan una robustez similar.

- Debe ser definido quienes pueden conocer o tener acceso a las llaves criptográficas.

- Con el fin de controlar las claves tendrán fechas de inicio y caducidad de vigencia no mayor a un año.

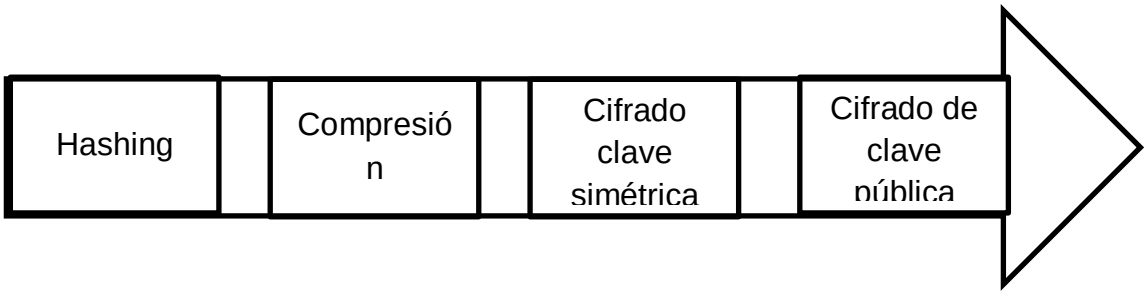
- Se implementará un sistema de administración de claves criptográficas para asegurar el correcto uso de las herramientas se podrá utilizar dos tipos de técnicas criptográficas:

    - Técnicas de clave secreta (criptografía simétrica), usada cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

    - Técnicas de clave pública (criptografía asimétrica), usada cuando cada usuario tiene un par de claves: una clave pública (que puede ser relevada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se usan para firmar digitalmente.

El cifrado que se presentará para el desarrollo del actual trabajo consiste en 4 pasos básicos para asegurar la información, tal como se observa a continuación:

Figura 26. Proceso de cifrado



FUENTE: Autor.

A continuación se presentaran las dos opciones de cifrado trabajadas con las Pymes para el desarrollo de este trabajo de grado aplicado.

9.2.1 INSTALACIÓN Y USO HERRAMIENTA GOANYWHERE OPEN PGP

Aunque en la actualidad existen varias formas de cifrar y aplicaciones que cumplen este proceso algunos desarrollados en software libre o comerciales, se basara en la experiencia del autor sobre la herramienta GoAnywhere Open PGP que es una aplicación con una interfaz muy amigable para el usuario final. A continuación se presenta todo el proceso que se debe seguir para su adquisición y utilización

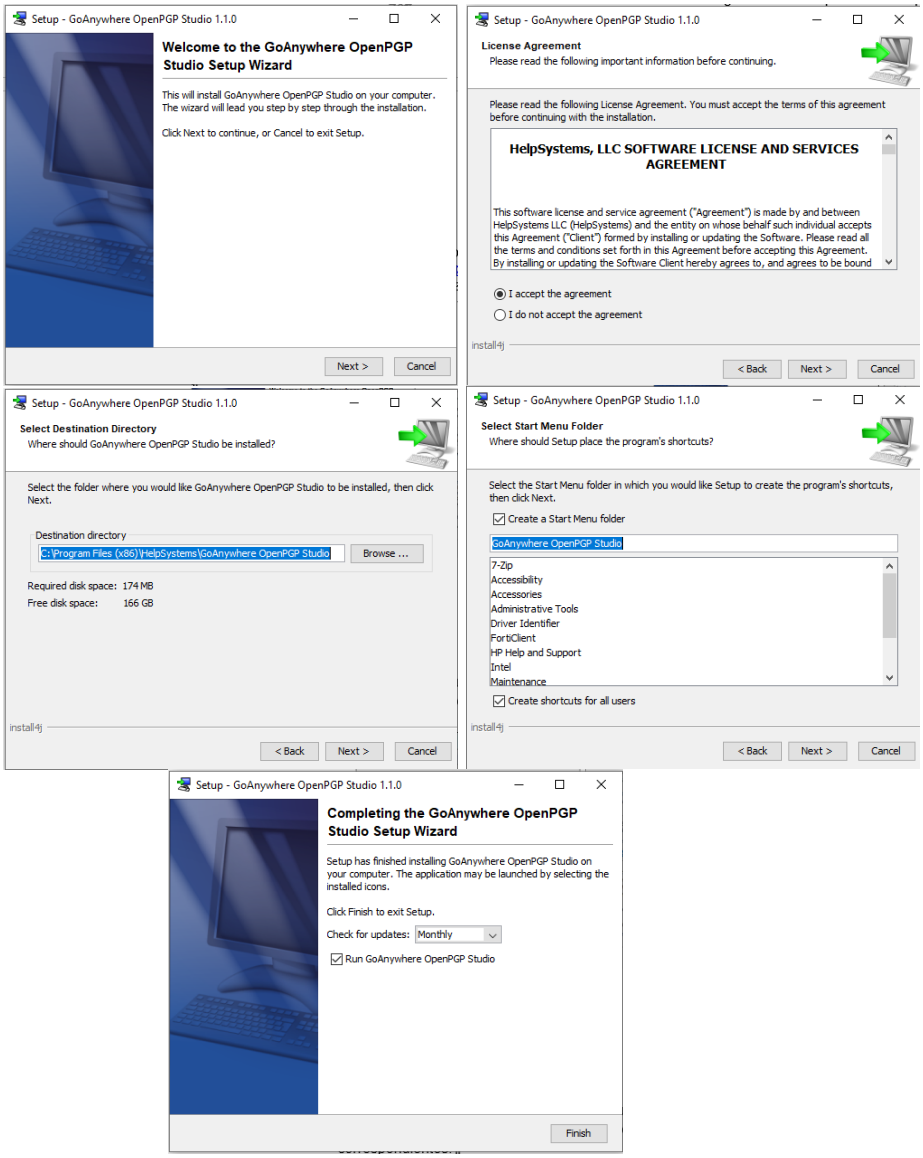
- Descarga: Se recomienda realizar la descarga de cualquier software desde el mismo sitio de su creador del aplicativo, esto garantizara que el software no sea alterado para otros fines. Para el presente trabajo se realizó desde la URL https://www.goanywhere.com/es/open-pgp-studio allí solicitara unos datos de la persona que desee descargar el aplicativo. Una vez diligenciado llegara al correo un link para descarga de mismo.

Figura 27. Correo que llegara indicando que se puede proceder con la descarga

FUENTE: Autor.

- Instalación: A continuación se adjuntan los pasos que se deben seguir para la correcta instalación del aplicativo descargado en el anterior Item.

Figura 28. Proceso de instalación aplicativo GoAnywhere Open PGP

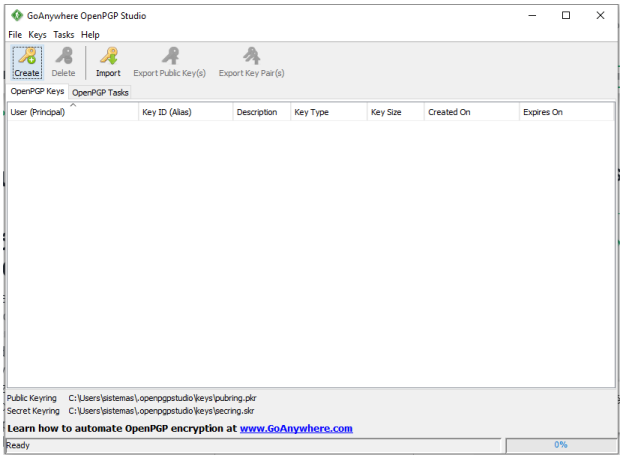


FUENTE: Autor.

- Creación de llaveros: En este proceso se dará a conocer tanto los llaveros donde almacenaran las llaves o claves criptográficas.

Al ingresar al aplicativo se debe validar que se encuentre ubicado en la pestaña “OpenPGP Keys” con el fin de poder crear el llavero y las llaves correspondientes.

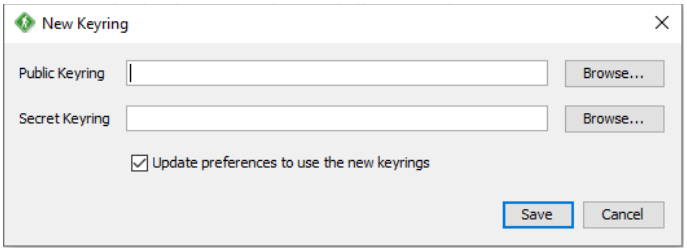
Figura 29. Aplicación GoAnywhere Open PGP instalada



FUENTE: Autor.

Para la creación de llaveros se debe ingresar al menú “Keys/New Keyring, deberá aparecer la ventana que se muestra en la siguiente imagen, allí se debe dar clic en el botón “Browse” para elegir la ruta en donde se guardara el llavero.

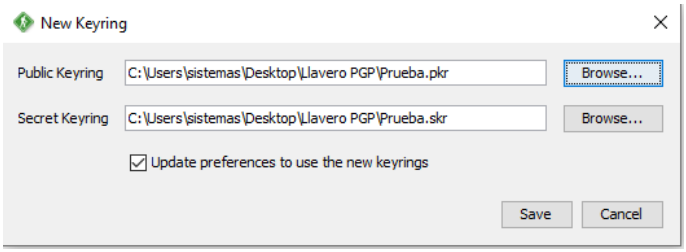
Figura 30. Opción donde se define la ruta donde quedara guardado el llavero



FUENTE: Autor.

Se elige la ruta en donde se desea guardar el llavero y se asigna el nombre que se desee y se da clic en el botón “Save” como se muestra en la siguiente imagen.

Figura 31. Ubicación seleccionada para el ejemplo.



FUENTE: Autor.

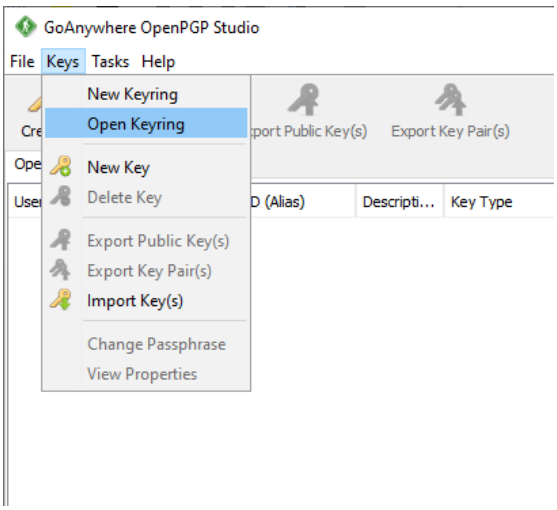
Cuando se ha creado el llavero la pantalla queda en blanco para comenzar a crear las llaves.

Nota: Los llaveros no se pueden exportar, en caso que se necesite trasladar un llavero se debe buscar la ruta en donde fue guardado y realizar la copia.

- Abrir llaveros:

  Para Abrir un llavero existente se debe ubicar en el menú “Keys/Open Keyring” como se muestra en la siguiente imagen.

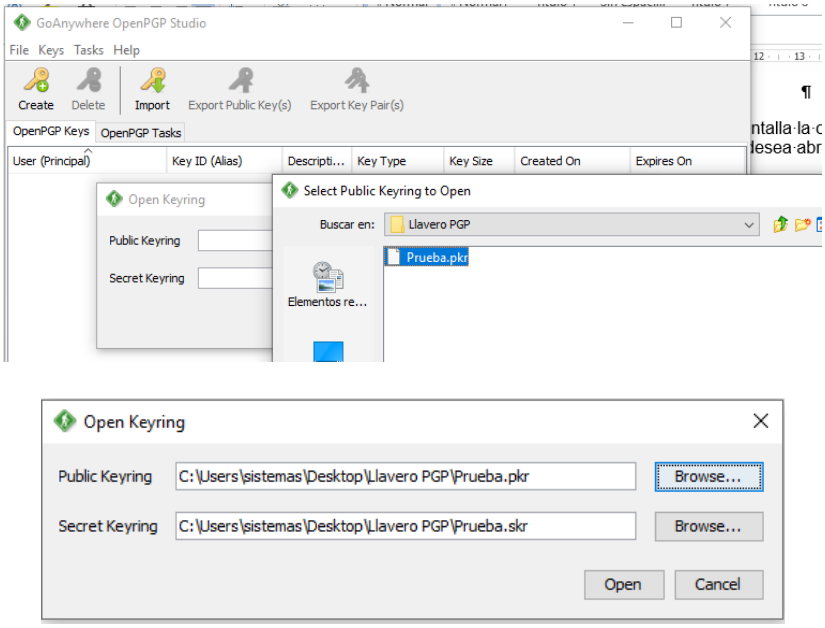
Figura 32. Opción para seleccionar o abrir un llavero existente.



FUENTE: Autor.

Luego de realizar la opcion anterior debe mostrar en pantalla la opcion para buscar la ruta en donde se encuentra el llavero que se desea abrir, como se muestra en las siguientes imagenes.

Figura 33. Proceso para seleccionar llavero existente.



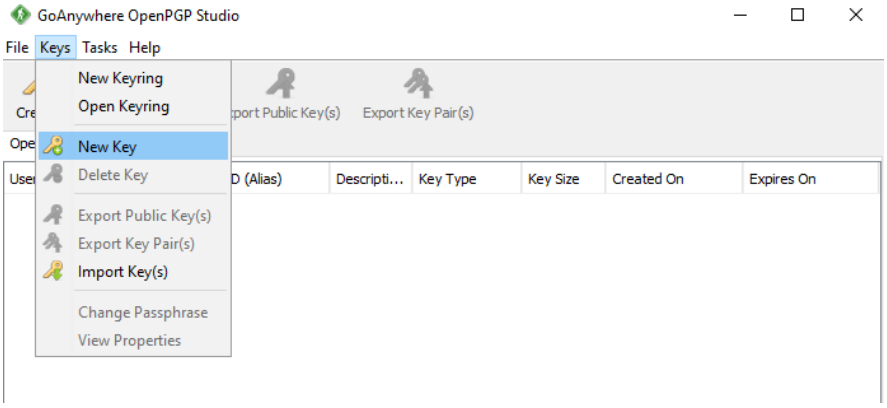
FUENTE: Autor.

Al dar clic en el boton “Open” de la imagen anterioir abrirá el llavero que fue seleccionado con todas las llaves que se encuentran creadas allí.

- Creación de llaves: Para empezar a crear llaves es necesario que antes se haya creado el llavero, de lo contrario va a generar error y no permitirá la creación de llaves.

  Para crear las llaves se debe ubicar en el menú “Keys/New Key” como se muestra a continuación.

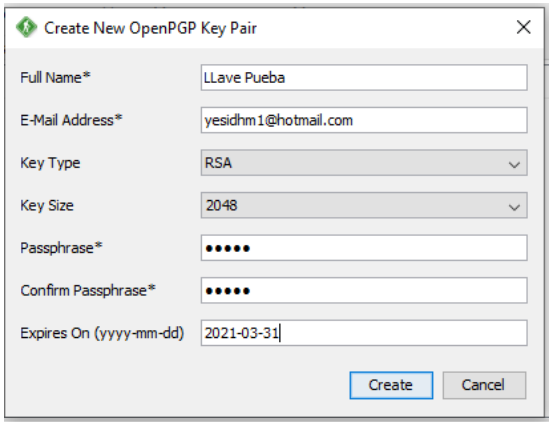
Figura 34. Selección de opción para crear llaves.



FUENTE: Autor.

Al realizar la acción anterior se mostrará la siguiente pantalla, en donde se deberán diligenciar los campos “Full name”, “E-mail Address”, “Passphrase”, “Confirm Passphrase” de acuerdo a lo que se requiera, en el campo “Key Type” se debe seleccionar la opción RSA, el campo “Key Size” se deja la opción que se encuentra predeterminada “2048” y en el campo “Expires On (yyy-mm-dd)” se debe digitar la fecha de caducidad de la llave, si no se requiere esta fecha no se debe ingresar ningún dato, para finalizar dar clic en el botón “Create”.

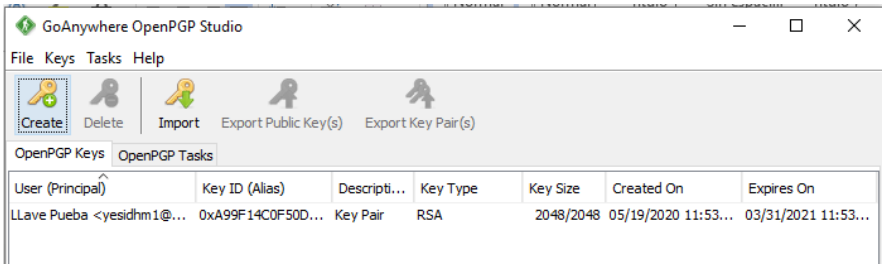
Figura 35. Campos que se deben crear para crear las llaves de cifrado.



FUENTE: Autor.

En la siguiente imagen se muestra la llave que se creó en el paso anterior.

Figura 36. Llaves de cifrado ya creadas.

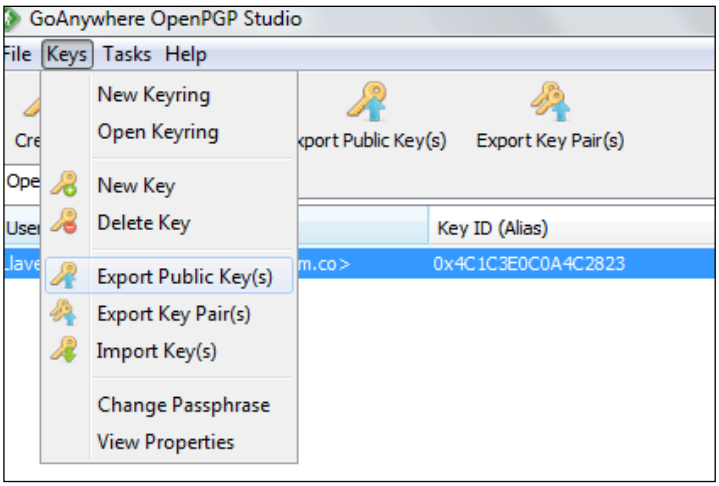


FUENTE: Autor.

- Exportar llaves: El proceso de exportación de llaves se realiza para poder dar a la persona que recibirá el archivo la opción de poder ver el mismo.

Para exportar las llaves creadas se deben ubicar en el menú “Keys/Export Public Key(s)” para la llave pública o “Keys/Export Key Pair(s)” para la llave privada, como se muestra a continuación:

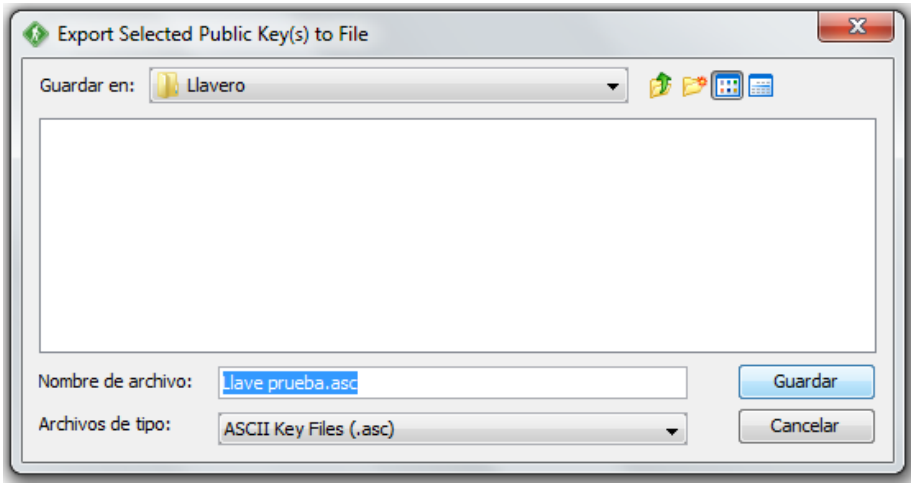
Figura 37. Proceso para exportar llaves.



FUENTE: Autor.

Luego del paso anterior se muestra en pantalla la opción para elegir la ruta en donde se va a exportar la llave pública o privada según sea el caso y se oprime el botón “Guardar”.

Figura 38. Ruta donde se exportaran las llaves.

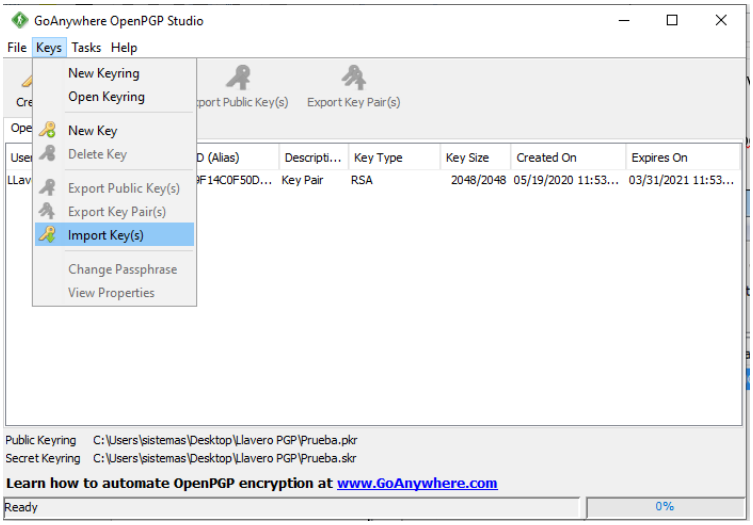


FUENTE: Autor.

- Importar llaves: En caso necesitar ver los archivos que llegan de otro destino, ellos deben compartir su clave pública y a su vez se debe guardar para poder ver los archivos que nos envíen.

Para importar llaves se debe ubicar en el menú “Import Key(s)” como se muestra en la imagen.

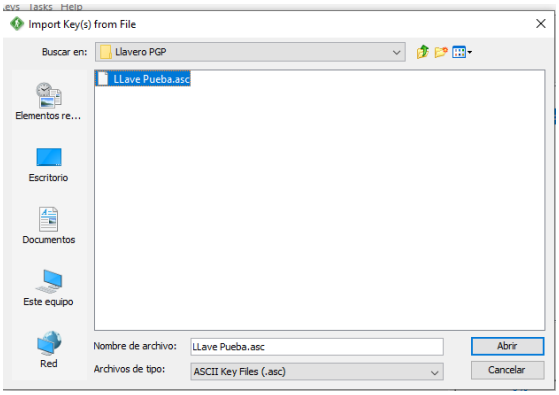
Figura 39. Proceso para importar llaves.



FUENTE: Autor.

Se debe seleccionar la ruta en donde se encuentran las llaves que se van a importar y clic en el botón abrir como se muestra en la siguiente imagen.

Figura 40. Selección de llave a importar.

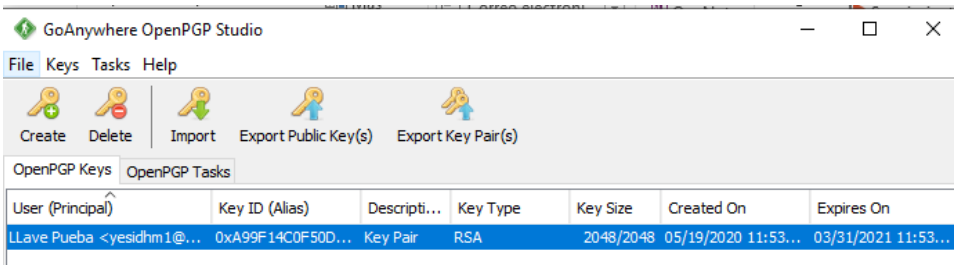


FUENTE: Autor.

- Cifrar archivos

Para cifrar archivos se debe verificar que se encuentre en la pestaña “OpenPGP Tasks” como se muestra en la siguiente imagen.

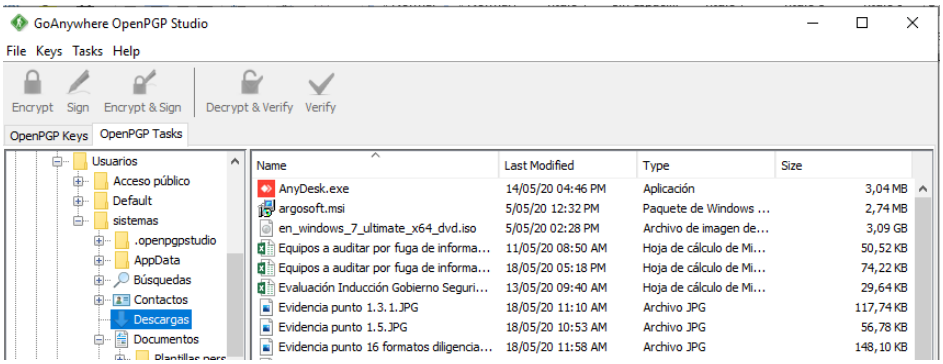
Figura 41. Inicio de proceso de cifrado archivos.



FUENTE: Autor.

Al lado izquierdo de la pantalla se muestran las carpetas del equipo, allí se debe ubicar el archivo que quiere cifrar, en este caso se encuentra en la carpeta “Llavero” como se muestra en la imagen.

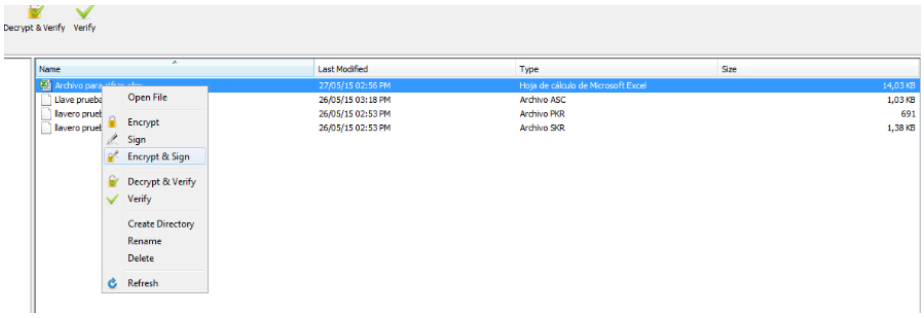
Figura 42. Selección de ruta de archivo a cifrar.



FUENTE: Autor.

Cuando se ha identificado el archivo que se quiere cifrar, se da clic derecho sobre el archivo (Pantalla derecha) y se selecciona la opción “Encrypt” como se muestra en la siguiente imagen.

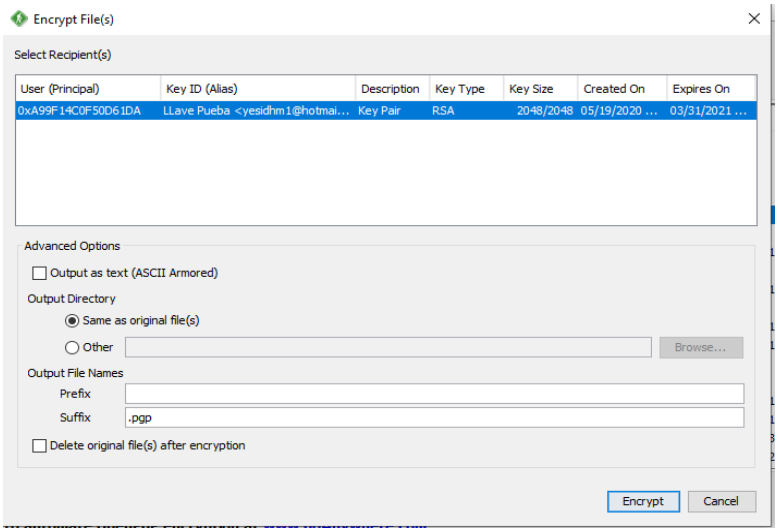
Figura 43. Selección archivo a cifrar.



FUENTE: Autor.

Al realizar la acción anterior debe mostrar la siguiente pantalla, allí se tiene la opción para seleccionar la llave con que se va a cifrar, una ruta diferente para guardar el archivo cifrado y para eliminar el archivo original después de cifrarlo como se muestra a continuación:

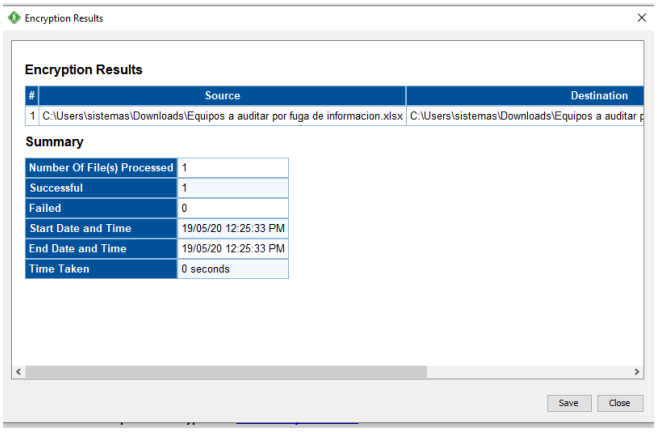
Figura 44. Selección de llave con la que se va a cifrar.



FUENTE: Autor.

A continuación debe mostrar la pantalla de confirmación de cifrado del archivo como se muestra en la siguiente imagen:

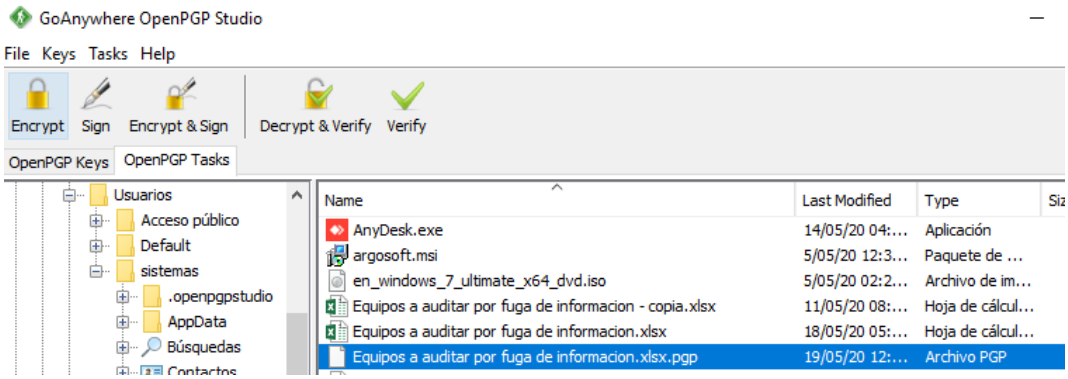
Figura 45. Resultado del proceso de cifrado del archivo.



FUENTE: Autor.

En la siguiente pantalla se puede observar el archivo cifrado:

Figura 46. Archivo cifrado y listo para envío.

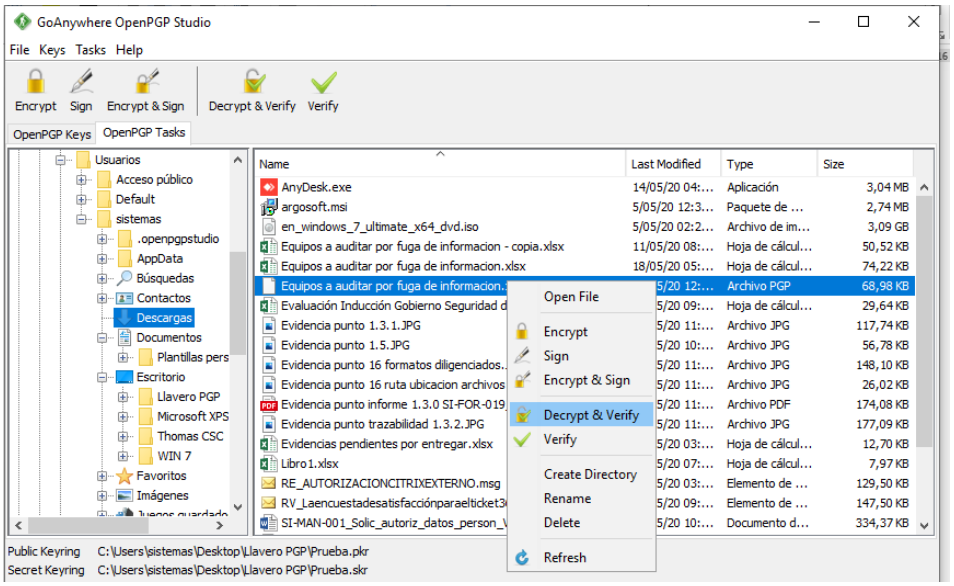


FUENTE: Autor.

- Descifrar Archivos

  Para descifrar archivos se debe ubicar el archivo en la parte izquierda de la pantalla, cuando se tenga identificado se debe dar clic derecho y elegir la opción “Decrypt & verify” como se muestra a continuación:

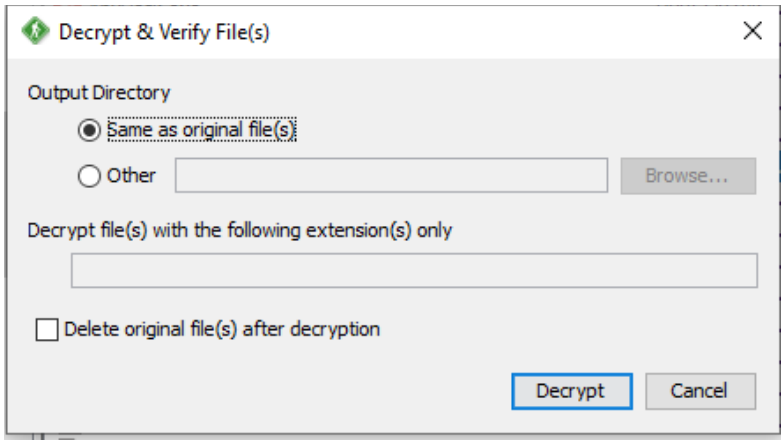
Figura 47. Selección de archivo a descifrar.



FUENTE: Autor.

Luego de realizar la acción anterior se debe visualizar la siguiente pantalla, se da clic en el botón “Decrypt”.

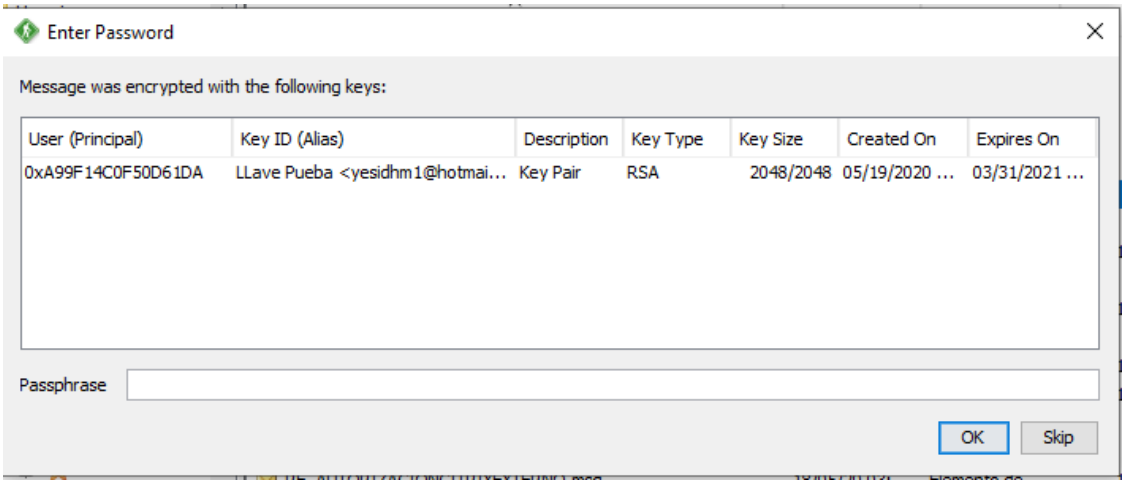
Figura 48. Selección de ruta para dejar archivo descifrado.



FUENTE: Autor.

Luego se debe mostrar la siguiente pantalla en donde se debe seleccionar la llave e ingresar la contraseña para descifrar el archivo como se observa a continuación:

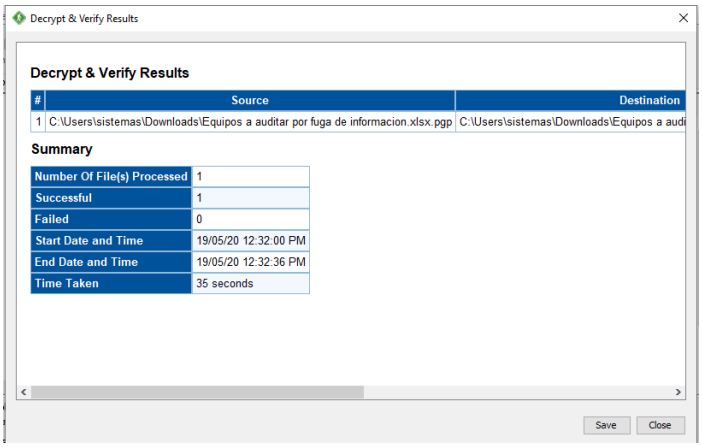
Figura 49. Selección de llave para descifrar.



FUENTE: Autor.

A continuación debe mostrar la pantalla de confirmación de descifrado del archivo como se muestra en la siguiente imagen:

Figura 50. Resultado del archivo descifrado.



FUENTE: Autor.

9.2.2 USO DE LA FIRMA DIGITAL EN EL CORREO ELECTRONICO

Es importante aclarar que una firma digital no es igual a una firma que se agrega al correo donde se indica normalmente una despedida y los datos del remitente. Es una actividad común que se copien estas firmas de correo y se personalicen. La diferencia es un mensaje firmado digitalmente puede provenir solo el propietario ya que contiene un identificador o huella digital que puede ser comprobada por el receptor del correo, esto brinda la tranquilidad de saber que el mensaje no sido manipulado.

Para poder configurar la firma digital uno de los requisitos es adquirir un certificado digital por uno de los entes autorizados para tal fin. Este certificado tendrá un costo con base en el tipo de certificado que se desee adquirir y de la organización que lo genere.

La firma digital aunque fue un proceso adicional presentado a las Pymes no tuvo gran acogida al cubrir la necesidad primaria de proteger los archivos que viajaban por el correo electrónico, además por implicar un registro y un costo adicional que no se deseó realizar. Por lo anterior no se abarco más es este ítem.

9.3 OTROS CONTROLES A TENER EN CUENTA

9.3.1 IMPLEMENTACIÓN NORMA O POLÍTICA DE USO DEL CORREO ELECTRÓNICO

Para las Pymes es importante tener entre sus políticas de seguridad y capacitación de usuarios, la documentación adecuada del manejo del correo electrónico al ser la principal herramienta para facilitar la comunicación entre funcionarios, clientes y proveedores. Por ser un insumo tan importante se debe cumplir con los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio. Se sugiere a las Pymes tener en su infraestructura u organigrama un grupo o comité se seguridad de la información para llevar este control. Entre las normas o políticas a implementar se sugiere:

- El grupo de seguridad debe establecer políticas, procedimientos y manuales permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

- Se debe generar capacitaciones y campañas para concientizar a todo el personal de la empresa, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

- La cuenta de correo electrónico asignada es de carácter individual e intransferible; por lo cual no debe utilizar ninguna cuenta diferente para el desarrollo de sus actividades.

- Los mensajes e información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada empleado. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la empresa y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas.

- No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la empresa y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

9.3.2 POLITICAS DE ALISTAMIENTO Y/O ASEGUAMIENTO EN INFRAESTRUCTURA.

Durante la validación de las diferentes Pymes se encontró que los equipos usados para el manejo de correo electrónico, no cuentan por políticas de aseguramiento o hardening sobre estos equipos, convirtiéndose en uno de los eslabones débiles para la empresa.

En el alistamiento de los equipos de escritorio y portátiles se deben implementar listas de chequeo que garanticen el cumplimiento de los controles de seguridad básicos de estos equipos. Algunas de las actividades que se deben tener en cuenta son:

- Uso de software licenciado: Tanto por cumplimiento legal Colombiano como por las vulnerabilidades que se crean al piratear o craquear cualquier sistema informático, se hace necesario trabajar con sistemas que estén legalmente adquiridos y permitan su correcta actualización y soporte.

- Actualizaciones automáticas: Si los sistemas con licenciados y están correctamente instalados, se debe siempre tener activa la opción para instalar las últimas actualizaciones de seguridad.

- Desactivación y/o eliminación de cuenta invitados: Como buena práctica se debe desactivar o eliminar las cuentas de invitado o genéricas que vienen sobre los sistemas informáticos.

- Cambio de usuario administrador por defecto: Se aconseja eliminar o cambiar el usuario administrador y que el uso de este usuario sea restringido y sea usado netamente para actividades de soporte sobre los equipos de cómputo.

- Implementación de políticas de claves seguras: La asignación de contraseñas debe ser personalizada y realizada de forma segura, garantizara que no cualquiera pueda acceder a los sistemas más que el que necesite hacerlo. Los parámetros que se deben tener en cuenta son:

    - Longitud mínima (8 caracteres).
    - La contraseña debe cumplir con al menos tres de las cuatro (3 de 4), de las siguientes características:
        - Utilización de mayúsculas (A, B, C, D, E, F…)
        - Utilización de minúsculas (a, b, c, d, e, f…)
        - Utilización de números (1, 2,3…)
        - Utilización de caracteres especiales (%,#,&,@)
    - Bloqueo de cuenta de inicio de sesión por intentos de ingreso fallidos (5 veces), posteriormente se reactivará después de 30 minutos.
    - La expiración periódica de la contraseña está definida en 60 días.

- Asignación de usuarios nombrados o personalizados: Cada empleado de la compañía debe contar con su propio usuario y ser responsable de uso. Permitirá tener trazabilidad de quien usa o manipula la información.

- Antivirus: Se debe contar con una solución de antivirus capaz de detectar y eliminar virus informáticos, esta debe contar con un soporte que garantice la actualización contante de la base de amenazas informáticas y así poder hacer gestión sobre las mismas.

- Bloqueo de puertos o implementación de DLP: Para prevenir fuga de información o acceso no autorizado por medios extraíbles, se debería implementar una solución de DLP o bloquear los puertos USB desde la BIOS o a nivel de registro de Windows.

- Cifrado de equipos: Para equipos que sean retirados de la compañía para el desarrollo o continuidad del negocio, se recomienda usar cifrado de disco duro sobre estos equipos, lo anterior para garantizar que en caso de pérdida o robo la información almacenada en ellos no sea de fácil acceso.

- Respaldos de información: Periódicamente se debe realizar un respaldo de la información en medios adicionales o una ubicación centralizada para poder recuperar la información ante cualquier evento.

10. RESULTADOS E IMPACTOS

Las pruebas realizadas dentro del trabajo de grado evaluaron el conocimiento de la población objetivo, sobre las herramientas de soporte, uso y aseguramiento de correo electrónico y algunas medidas de seguridad de la información implementadas en las pymes. Los controles criptográficos establecidos por los proveedores de correo electrónico para los servicios de transmisión de información en la mayoría de los casos no son visibles o se desconoce por parte de la población evaluada de si son adecuados o no para las necesidades de uso en su trabajo diario. El autor identificó que una de las principales deficiencias es la falta de conocimiento en la clasificación y gestión de los activos de información, las personas que trabajan o dirigen empresas pueden no conocer o estar conscientes del nivel de criticidad de la información, que en caso de fuga o de acceso no autorizado y controlado podría materializar riesgos al negocio en perspectiva de la información, el cumplimiento normativo y la estabilidad misma de cada empresa. Al leer este documento el lector identificará que una vez clasificados los activos de información, se hace necesario evaluar los controles que se pueden aplicar sobre estos para garantizar la confidencialidad, integridad y disponibilidad de la información.

También se logró evidenciar que en un alto porcentaje de la población evaluada asociada a Pymes, no se cuenta con conceptos sólidos sobre el funcionamiento y uso de buenas prácticas respecto del correo electrónico, ni se toman medidas de seguridad para el envío o recepción de correos, al que igual que se tiene un desconocimiento generalizado sobre los tipos de ciberataques que pueden ocurrir a una empresa y a su personal a través del correo electrónico. El lector de este documentó conocerá de manera fácil y recordable las herramientas de seguridad y podrá identificar los tipos de ciberataques en uso por los ciberdelincuentes, conceptos que son claves para configurar sus herramientas empresariales y operar con un nivel de tranquilidad suficiente, sabiendo que se han implementado controles de seguridad básicos y escalables que darán seguridad y estabilidad tanto a la empresa como a sus clientes y proveedores. Es de interés del autor que el lector pueda usar este documento para difundir este aporte al conocimiento y ayude en su entorno social a la construcción de una cultura de ciberseguridad.

Este documento tendrá un impacto a mediano plazo en las pymes y personas que lo tomen como referencia y que deseen asegurar sus activos de información, ya que podrán identificar las diferentes vulnerabilidades que se presentan y los controles que pueden aplicar para mitigarlas o compensarlas. Brindará opciones de aseguramiento que no implicaran grandes inversiones y que finalmente motivaran la curiosidad del lector en saber si hay algo adicional que aprender e implementar sobre la seguridad de la información en su labor o negocio. Los conceptos aprendidos darán la certeza de que las ofertas de negocio de pymes

que tengan un nivel al menos mínimo de aseguramiento, tendrán una mejor aceptación por otras empresas o personas que deseen establecer negocios e intercambios de información con niveles aceptables de aseguramiento en la transferencia de información. Este proceso se hará más robusto mediante procesos de auditoría de seguridad de la información entre las relaciones comerciales de las empresas

11. DIVULGACIÓN

Este documento estará al alcance de cualquier persona que haga parte de una pyme y que quiera optar por conocer los requisitos básicos para implementar seguridad en el correo electrónico. Estará disponible en el repositorio de la UNAD como “ANALISIS Y DISEÑO DE UN MECANISMO DE CIFRADO DE CORREO ELECTRONICO PARA GARANTIZAR Y PROTEGER LA INFORMACION ENVIADA DE LAS PYMES”.

12. CONCLUSIONES Y RECOMENDACIONES

La construcción del presente documento llevó al autor a comprender que se hace necesario conocer los resultados de otras investigaciones, las soluciones identificadas y exploradas junto con los conceptos técnicos aplicables a los grupos de enfoque, con el objetivo de producir un material de referencia fácil de interpretar. Adicionalmente para el desarrollo del presente trabajo de grado se encontraron obstáculos referentes al análisis de ciberseguridad en pymes en Colombia.

Para la consolidación del presente trabajo de grado se realizó una investigación del estado del arte de la seguridad de la información en las pymes, empezando por un enfoque externo a la realidad Colombiana, para identificar que se ha investigado y propuesto en otras culturas, por lo cual el autor reconoce que es clave conocer de primera mano cómo es el aseguramiento que implementan las empresas para el desarrollo del negocio, si se considera una necesidad o simplemente no se ve la utilidad que brinda proteger los activos de información de las compañías. Este documento se escribió de tal forma que permitirá el desarrollo de una conciencia en las personas que hacen parte de este tipo de empresas, en que el aseguramiento de sus sistemas ayudará a mitigar o minimizar el impacto de las acciones de aquellos ciberdelincuentes que están buscando obtener un beneficio económico, reputacional o egocéntrico a partir de una falla de seguridad.

Fue posible también observar que algunas pymes al no contar una guía o conocimiento claro de las leyes y marcos de referencia que pueden aplicar a sus negocios, pueden descuidar el cumplimiento de las mismas, sin saber que al estar alineadas con las leyes y las mejores prácticas de seguridad de la información se puede obtener un valor agregado que pueden utilizar para el crecimiento comercial de la empresa.

Es de vital importancia implementar políticas de seguridad enfocadas principalmente a la clasificación y al aseguramiento de la información dado que en las pymes se puede encontrar un alto número de activos considerados como confidenciales, sensibles o de uso interno y más cuando la misma puede llegar a ser trasmitida por correo electrónico u otros medios digitales. El principal objetivo es salvaguardar este conjunto de activos en este tipo de empresas mediante la aplicación de los conceptos y metodologías descritas en el presente documento.

Es posible para una pyme contar con este documento como una base que incluye los conceptos y procedimientos metódicos básicos sobre la gestión de seguridad de la información en el correo electrónico, es posible que se convierta en una herramienta fundamental para que el personal encargado pueda asegurar los activos de información de la empresa, pues al estar preparada y con el

conocimiento esencial, podrá mitigar o controlar los posibles riesgos que se pueden presentar en los flujos de la información a nivel interno y hacia otras empresas.

Se requiere de trabajos futuros que permitan validar la implementación de los conceptos descritos en el presente documento y que hagan un análisis posterior mediante herramientas estadísticas para validar el impacto del conocimiento aquí descrito en pymes en Colombia.

13. REFERENCIAS BIBLIOGRÁFICAS

A. A. Tous-Mulkay, «Finanzas Personales.co,» 06 10 2019. [En línea]. Available: https://www.finanzaspersonales.co/columnistas/articulo/principales-riesgos-de-ciberseguridad-en-las-pymes/79732. [Último acceso: 01 02 2020].

C. Colby, «Cnet.com,» 15 Octubre 2019. [En línea]. Available: https://www.cnet.com/how-to/yahoo-data-breach-how-to-file-for-358-or-more-as-part-of-claim-settlement/?ftag=CMG-01-10aaa1b. [Último acceso: 1 Mayo 2020].

C. D. L. REPÚBLICA, «Ley 1273 DE 2009,» 05 Enero 2009. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. [Último acceso: 20 Enero 2020].

C. D. L. REPÚBLICA, «LEY 527 DE 1999,» 18 Agosto 1999. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html. [Último acceso: 24 Enero 2020].

C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1266 DE 2008,» 31 Diciembre 2008. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. [Último acceso: 22 Enero 2020].

C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1581 DE 2012,» 17 Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 21 Enero 2020].

C. Osborne, «zdnet.com,» 18 Diciembre 2019. [En línea]. Available: https://www.zdnet.com/article/ftc-settles-with-unroll-me-over-allegedly-duping-users-over-email-data-collection-sale/. [Último acceso: 20 febrero 2020].

C. Osborne, «zdnet.com,» 28 Octubre 2019. [En línea]. Available: https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/. [Último acceso: 8 Febrero 2020].

C. Osborne, «zdnet.com,» 5 Septiembre 2019. [En línea]. Available: https://www.zdnet.com/article/dklok-data-breach-leaked-global-enterprise-client-internal-emails/. [Último acceso: 3 Febrero 2020].

C. Osborne, «zdnet.com,» 6 noviembre 2019. [En línea]. Available: https://www.zdnet.com/article/trend-micro-reveals-insider-threat-exposing-customer-data/. [Último acceso: 12 febrero 2020].

CCIT, «TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020,» 29 10 2019. [En línea]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. [Último acceso: 03 02 2020].

Colomboamericana, Cámara de Comercio, «https://www.amchamcolombia.co/,» 2019. [En línea]. Available: https://www.amchamcolombia.co/es/comunicaciones/noticias-afiliados/1767-cisco-la-ciberseguridad-tambi%C3%A9n-es-un-reto-para-las-pymes. [Último acceso: 05 Enero 2020].

Computerworld, «Microsoft Mail: Solid, less graphical,» Computerworld, vol. XXV, p. 38, 21 Agosto 1991.

D. Swinhoe, «CSOonline,» 17 Abril 2020. [En línea]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Último acceso: 28 Abril 2020].

El Tiempo, «Eltiempo.com,» 26 Diciembre 2019. [En línea]. Available: https://www.eltiempo.com/economia/sectores/competitividad-de-las-pymes-en-colombia-para-2020-446922. [Último acceso: 05 Enero 2020].

F. FERRI-BENEDETTI, «¿QUÉ ES EL CIFRADO?,» 23 07 2013. [En línea]. Available: https://www.softonic.com/articulos/que-es-el-cifrado-encriptar. [Último acceso: 25 Abril 2020].

H. Monterrosa, «La Republica.com,» 31 Agosto 2019. [En línea]. Available: https://www.larepublica.co/economia/mipymes-representan-96-del-tejido-empresarial-y-aportan-40-al-pib-2903247. [Último acceso: 05 Enero 2020].

http://www.cis.usouthal.edu, «CTSS, Compatible Time-Sharing System,» 01 01 2019. [En línea]. Available:

http://www.cis.usouthal.edu/faculty/daigle/project1/ctss.htm. [Último acceso: 10 Enero 2020].

I. E. T. Force, «A Simple Mode of Facsimile Using Internet Mail,» Marzo 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2305. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access,» Enero 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8314. [Último acceso: 13 Enero 2020].

I. E. T. Force, «Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,» Junio 2014. [En línea]. Available: https://tools.ietf.org/html/rfc7230. [Último acceso: 14 Enero 2020].

I. E. T. Force, «Hypertext Transfer Protocol Version 2 (HTTP/2),» Mayo 2015. [En línea]. Available: https://tools.ietf.org/html/rfc7540. [Último acceso: 14 Enero 2020].

I. E. T. Force, «INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1,» Marzo 2003. [En línea]. Available: https://tools.ietf.org/html/rfc3501. [Último acceso: 11 Enero 2020].

I. E. T. Force, «LEMONADE Architecture - Supporting Open Mobile Alliance (OMA),» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5442. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Message Disposition Notification,» Febrero 2017. [En línea]. Available: https://tools.ietf.org/html/rfc8098. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Message Disposition Notification,» Mayo 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3798. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Open Pluggable Edge Services (OPES) SMTP Use Cases,» Mayo 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4496. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Post Office Protocol - Version 3,» Mayo 1996. [En línea]. Available: https://tools.ietf.org/html/rfc1939. [Último acceso: 12 Enero 2020].

I. E. T. Force, «Sieve Email Filtering: Reject and Extended Reject Extensions,» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5429. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Simple Mail Transfer Protocol,» Octubre 2008. [En línea]. Available: https://tools.ietf.org/html/rfc5321. [Último acceso: 11 Enero 2020].

I. E. T. Force, «SMTP MTA Strict Transport Security (MTA-STS),» Septiembre 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8461. [Último acceso: 14 Enero 2020].

I. E. T. Force, «SMTP Service Extension for Secure SMTP over Transport Layer Security,» Febrero 2002. [En línea]. Available: https://tools.ietf.org/html/rfc3207. [Último acceso: 12 Enero 2020].

I. E. T. Force, «SMTP TLS Reporting,» Septiembre 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8460. [Último acceso: 14 Enero 2020].

I. E. T. Force, «The PLAIN Simple Authentication and Security Layer (SASL) Mechanism,» Agosto 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4616. [Último acceso: 13 Enero 2020].

I. E. T. Force, «The Secure Sockets Layer (SSL) Protocol Version 3.0,» Agosto 2011. [En línea]. Available: https://tools.ietf.org/html/rfc6101. [Último acceso: 15 Enero 2020].

I. E. T. Force, «The Transport Layer Security (TLS) Protocol Version 1.3,» Agosto 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8446. [Último acceso: 14 Enero 2020].

I. E. T. Force, «Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols,» Marzo 2016. [En línea]. Available: https://tools.ietf.org/html/rfc7817. [Último acceso: 13 Enero 2020].

I. E. T. Force, «Using TLS with IMAP, POP3 and ACAP,» Junio 1999. [En línea]. Available: https://tools.ietf.org/html/rfc2595. [Último acceso: 12 Enero 2020].

I. E. T. Force, «Voice Profile for Internet Mail (VPIM) Addressing,» Junio 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3804. [Último acceso: 10 Enero 2020].

INCIBE, «Utiliza el correo electrónico de forma segura con PGP,» 13 08 2019. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/utiliza-el-correo-electronico-forma-segura-pgp. [Último acceso: 15 Mayo 2020].

ISO.ORG, «STANDARDS,» 20 Febrero 2006. [En línea]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/info_security.pdf. [Último acceso: 24 Abril 2020].

ISO27000.ES, «Serie "27000",» ISO27000.ES, 20 Septiembre 2019. [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 15 Marzo 2020].

J. A. P. Cadavid, «Revitas Universidad Externado de Colombia,» 24 11 2010. [En línea]. Available: https://revistas.uexternado.edu.co/index.php/propin/article/download/2476/2112/. [Último acceso: 24 Abril 2020].

J. O. Canizalez, «SEGURIDAD EN REDES,» SEGURIDAD EN REDES, 15 06 2011. [En línea]. Available: http://seguridad-deredes.blogspot.com/2011/06/cifrado-y-criptografia.html. [Último acceso: 01 05 2020].

K. Shoens, «MAIL REFERENCE MANUAL,» 25 Abril 1984. [En línea]. Available: http://reports-archive.adm.cs.cmu.edu/anon/itc/CMU-ITC-012.pdf. [Último acceso: 10 Enero 2020].

L. Goldsmith, «APL Quotations and Anecdotes,» 18 Septiembre 2010. [En línea]. Available: https://www.jsoftware.com/papers/APLQA.htm. [Último acceso: 10 Enero 2020].

L. o. C. USA, «cc:Mail Archive Email Format,» 18 Mayo 2018. [En línea]. Available: https://www.loc.gov/preservation/digital/formats/fdd/fdd000391.shtml. [Último acceso: 10 Enero 2020].

M. GONZALO, «Cómo cifrar tu correo de Gmail sin complicaciones con Mailvelope,» 23 07 2013. [En línea]. Available: https://www.eldiario.es/turing/como-cifrar-email-criptografia-Gmail-Mailvelope_0_156784455.html. [Último acceso: 14 Mayo 2020].

M. Williams, «CSOonline,» 4 Octubre 2017. [En línea]. Available: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html. [Último acceso: 29 Abril 2020].

Microsoft, «Exchange Server Protocol Documents,» 24 Septiembre 2019. [En línea]. Available: https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxprotlp/30c90a39-9adf-472b-8b5b-03c282304a83?redirectedfrom=MSDN. [Último acceso: 11 Enero 2020].

Microsoft, «Outlook Connectivity with MAPI over HTTP,» 9 Mayo 2014. [En línea]. Available: https://blogs.technet.microsoft.com/exchange/2014/05/09/outlook-connectivity-with-mapi-over-http/. [Último acceso: 11 Enero 2020].

R. H. N. S. T. K. B. a. P. K. Anderson, «The Design of the MH Mail System,» 31 Diciembre 1978. [En línea]. Available: https://www.rand.org/pubs/notes/N3017.html. [Último acceso: 10 Enero 2020].

R. Tomlinson, «Firstemailframe,» 06 Mayo 2006 . [En línea]. Available: http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html. [Último acceso: 10 Enero 2020].

R. Walsh, «ProPrivacy,» 15 Noviembre 2019. [En línea]. Available: https://proprivacy.com/email/review/vfemail. [Último acceso: 5 Febrero 2020].

S. F. D. COLOMBIA, «CIRCULAR 007 DE 2018,» 05 Junio 2018. [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20126/reAncha/1/c/00. [Último acceso: 27 Enero 2020].

S. F. D. COLOMBIA, «CIRCULAR 042 DE 2012,» 05 Octubre 2012. [En línea]. Available: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf. [Último acceso: 26 Enero 2020].

S. Gatlan, «Bleepingcomputer.com,» 12 Febrero 2019. [En línea]. Available: https://www.bleepingcomputer.com/news/security/hackers-wipe-vfemail-servers-may-shut-down-after-catastrophic-data-loss/. [Último acceso: 5 Febrero 2020].

S. Talens-Oliag, «Introducción a la Criptología,» 14 04 2003. [En línea]. Available: https://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.html. [Último acceso: 14 Abril 2020].

T. V. Vleck, «The History of Electronic Mail,» 01 Febrero 2001. [En línea]. Available: https://www.multicians.org/thvv/mail-history.html. [Último acceso: 10 Enero 2020].

The GnuPG Project, «The GNU Privacy Guard,» 07 01 2020. [En línea]. Available: https://www.gnupg.org/gph/es/manual/c190.html. [Último acceso: 15 Mayo 2020].

TUGURIUM, «Glosario Terminología Informática,» 23 Marzo 2009. [En línea]. Available: http://www.tugurium.com/gti/termino.php?Tr=Information%20Technology%20Security%20Evaluation%20Criteria&Tp=N&Or=0. [Último acceso: 20 Abril 2020].

TUGURIUM, «TCSEC, el libro naranja de la seguridad informática,» 28 04 2017. [En línea]. Available: https://www.teknoplof.com/2017/04/28/tcsec-libro-naranja-la-seguridad-informatica/. [Último acceso: 20 Marzo 22].

14. ANEXOS

Anexo 1. Encuesta Online – Estado de la Seguridad de la Información en PYMES.

https://docs.google.com/forms/d/e/1FAIpQLSc2EKtdH3Ze9MUXLRdD9yvx5un5Xk2EOrthN14N8KKeA2nzdg/viewform?usp=sf_link

ENCUESTA PARA CONOCER ESTADO DE LA SEGURIDAD LA INFORMACIÓN EN LAS PYMES

EL OBJETIVO DE LA ENCUESTA ES CONOCER SI LA EMPRESA CUENTA CON POLÍTICAS DE SEGURIDAD APLICADA A SUS PROCESOS, ESPECÍFICAMENTE PARA EL ENVIÓ Y RECEPCIÓN DE CORREOS ELECTRÓNICOS DE FUENTES INTERNAS O EXTERNAS

La encuesta no tardará más de cinco minutos en completarla y será de gran ayuda para ofrecer una metodología segura para transmisión y recepción de correos de forma interna y externa.

Los datos que en ella se consignen se tratarán de forma anónima.

*Obligatorio

Nombre Completo

Tu respuesta

Cargo

Tu respuesta

1. ¿A que sector pertenece su empresa? *

Elige

2. ¿Su empresa cuenta con un sistema de gestión de la Seguridad de la información? *

- Sí
- No
- No se

3. ¿En su empresa tienen un programa de capacitación con temas de Seguridad de la Información? *

- Sí
- No
- No se

4. ¿Los portátiles o equipos de escritorio de su empresa usan las configuraciones de fábrica de los proveedores? *

- Sí
- No
- No se

5. ¿Sus equipos cuentan con políticas de Hardening (Aseguramiento de equipos, bloqueo de aplicaciones que no se requieran, permisos restringidos, entre otros)? *

- Sí
- No
- No se

6. ¿Sus equipos son actualizados periódicamente de forma manual o automática? *

- Manual
- Automatica
- No se
- No se hace

7. ¿Sus equipos cuentan con un antivirus licenciado y actualizado? *

- Sí
- No
- No se

8. ¿Tiene establecido un escaneo de vulnerabilidades en sus equipos? *

- Sí
- No
- No se

9. ¿Su empresa tiene un servicio de correo electrónico propio o en la nube? *

- Propio
- Nube
- No se

10. ¿Su empresa tiene contratado el servicio de correo electrónico con algún proveedor (google, hotmail, etc)? *

- Sí
- No
- No se

11. ¿Considera que el envío de correos electrónicos en su empresa es seguro? *

- Sí
- No
- No se

12. ¿Realiza envío de información confidencial o privada para la empresa por correo electrónico? *

- Sí
- No
- No se

13. ¿Conoce que tipos de ataques informáticos puede sufrir su empresa por medio del correo electrónico? *

- Sí
- No
- No se

14. ¿Conoce los protocolos de transferencia de archivos (FTP, SFTP o FTPS)? *

- Sí
- No
- No se

15. ¿Tienen alguna política o restricción para enviar información por el correo electrónico (Tamaño o tipo de archivo)? *

- Sí
- No
- No se

16. ¿Tienen algún filtro de correos electrónicos listas blancas o negras para envío o bloqueo de correos? *

- Sí
- No
- No se

17. ¿Se implementa alguna medida preventiva para el envío de correos electrónicos (cifrado)? *

- Sí
- No
- No se

18. Si tuviera la oportunidad de escoger un mecanismo de protección de la información que trasmite por correo electrónico ¿Cuál seleccionaría? *

- [ ] 1. Soluciones de correo electrónico para PYMES implementadas en equipos de la empresa
- [ ] 2. Soluciones de correo electrónico para PYMES basadas en la nube (google, hotmail, etc.)
- [ ] 3. Cifrado de información con GPG
- [ ] 5. Mezcla 1 y 3
- [ ] 6. Mezcla 2 y 3

Enviar

Página 1 de 1

Nunca envíes contraseñas a través de Formularios de Google.

Este contenido no ha sido creado ni aprobado por Google. Notificar uso inadecuado - Términos del Servicio - Política de Privacidad

Google Formularios

Anexo 2. Normas ISO 27000 aplicadas

NÚM.	NOMBRE	APLICA SI O NO	JUSTIFICACIÓN
1	Objeto y campo de aplicación	SI	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas	SI	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones	SI	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma	SI	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
5	Políticas de seguridad de la información		
5.1	Directrices establecidas por la dirección para la seguridad de la información		
5.1.1	Políticas para la seguridad de la información	SI	Se debe implementar políticas de información que deben ser publicadas y ser de conocimiento para la entidad.
5.1.2	Revisión de las políticas para seguridad de la información	SI	Se debe realizar validación de las políticas y ajustar si es el caso.
6	Organización de la seguridad de la información		
6.1	Organización interna		
6.1.1	Roles y responsabilidades para la seguridad de información	SI	Se debe definir y asignar las responsabilidades para el grupo de seguridad de información.
6.1.2	Separación de deberes	SI	Si hay áreas que compartan actividades se deberá separar las funciones para que entre en conflicto.
6.1.3	Contacto con las autoridades	SI	Se deberían mantener los contactos apropiados con las autoridades pertinentes.
6.1.4	Contacto con grupos de interés especial	NO	No se debe tener acceso a foros o redes donde se pueda divulgar información
6.1.5	Seguridad de la información en la gestión de proyectos	SI	La seguridad de la información se deberá tratar en todo proyecto no importa el tipo de proyecto
6.2	Dispositivos móviles y teletrabajo		
6.2.1	Política para dispositivos móviles	SI	No se permite acceso a los sistemas desde dispositivo móviles
6.2.2	Teletrabajo	SI	No se permite trabajo desde la casa o teletrabajo.
8	Gestión de activos		
8.1	Responsabilidad por los activos		
8.1.1	Inventario de activos	SI	Se debe tener un inventario claro.
8.1.2	Propiedad de los activos	SI	Los equipos deben tener un responsable o una persona a la que le sean asignados
8.1.3	Uso aceptable de los activos	SI	Se deberá contar con políticas para el manejo de los activos.
8.1.4	Devolución de activos	SI	Todos los activos deben ser devueltos una vez terminado el contrato.
8.2	Clasificación de la información		
8.2.1	Clasificación de la información	SI	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
8.2.2	Etiquetado de la información	SI	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.2.3	Manejo de activos	SI	Se deberían desarrollar e implementar procedimientos para el manejo

			de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.3.1	Gestión de medios removibles	SI	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.2	Disposición de los medios	SI	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
8.3.3	Transferencia de medios físicos	SI	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
9	Control de acceso		
9.1	Requisitos del negocio para control de acceso		
9.1.1	Política de control de acceso	SI	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
9.1.2	Política sobre el uso de los servicios de red	SI	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizado se específicamente.
9.2	Gestión de acceso de usuarios		
9.2.1	Registro y cancelación del registro de usuarios	SI	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2	Suministro de acceso de usuarios	SI	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
9.2.3	Gestión de derechos de acceso privilegiado	SI	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.2.4	Gestión de información de autenticación secreta de usuarios	SI	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
9.2.5	Revisión de los derechos de acceso de usuarios	SI	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
9.2.6	Retiro o ajuste de los derechos de acceso	SI	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
9.3	Responsabilidades de los usuarios		
9.3.1	Uso de la información de autenticación secreta	SI	Se debería exigir a los usuarios que cumplan las prácticas dela organización para el uso de información de autenticación secreta.
9.4	Control de acceso a sistemas y aplicaciones		
9.4.1	Restricción de acceso Información	SI	La información se debe restringir según el control de acceso
9.4.2	Procedimiento de ingreso seguro	SI	Si se requiere acceso se debe contar con método seguro
9.4.3	Sistema de gestión de contraseñas	SI	Deben contar con métodos que aseguren las seguridad de claves
9.4.4	Uso de programas utilitarios privilegiados	SI	Se deben restringir y controlar acceso a programas no autorizados.
9.4.5	Control de acceso a códigos fuente de programas	SI	Se debería restringir el acceso a los códigos fuente de los programas.
10	Criptografía		
10.1	Controles criptográficos		

10.1.1	Política sobre el uso de controles criptográficos	SI	Se debe implementar políticas que orienten al uso de controles criptográficos de la información para su protección.
10.1.2	Gestión de llaves	SI	SE debe implementar una política de uso de llaves criptográficas y que estas se renueven con una frecuencia definida.
11	Seguridad física y del entorno		
11.2	Equipos		
11.2.1	Ubicación y protección de los equipos	SI	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado
11.2.2	Servicios de suministro	SI	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro
11.2.3	Seguridad del cableado	SI	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño
11.2.4	Mantenimiento de equipos	SI	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas
11.2.5	Retiro de activos	SI	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
11.2.7	Disposición segura o reutilización de equipos	SI	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
11.2.8	Equipos de usuario desatendidos	SI	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
11.2.9	Política de escritorio limpio y pantalla limpia	SI	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información
12	Seguridad de las operaciones		
12.5	Control de software operacional		
12.5.1	Instalación de software en sistemas operativos	SI	Debe haber un procedimiento que no permita instalar software no permitido y si lo tiene poder detectar este software.
12.6	Gestión de la vulnerabilidad técnica		
12.6.1	Gestión de las vulnerabilidades técnicas	SI	Se Deben evaluar vulnerabilidades del sistema, se debe evaluar y llegar a la mejor solución de las mismas
12.6.2	Restricciones sobre la instalación de software	SI	Se deben tener una regla que no permita a los usuarios instalar software o se tenga una previa autorización
12.7	Consideraciones sobre auditorias de sistemas de información		
12.7.1	Información controles de auditoría de sistemas	SI	Las auditorías a los sistemas se deben planear para que no afecten a la operación.
13	Seguridad de las comunicaciones		
13.2	Transferencia de información		
13.2.1	Políticas y procedimientos de transferencia de información	SI	Se debe implementar control para la trasferencia de información dentro o fuera de la compañía.
13.2.2	Acuerdos sobre transferencia de información	SI	Se debe contemplar un método para trasferencia de archivos si el negocio lo requiere

13.2.3	Mensajería electrónica	SI	Se debe proteger la información enviada por correo electrónico.
13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Se debe crear una política que restrinja la divulgación de la información y mantener acuerdos de confidencialidad.
16	Gestión de incidentes de seguridad de la información		
16.1	Gestión de incidentes y mejoras en la seguridad de la información		
16.1.1	Responsabilidad y procedimientos	SI	Se deben generar procedimientos y asignar las responsabilidades para que generen respuestas oportunas
16.1.2	Reporte de eventos de seguridad de la información	SI	Todo evento se debe reportar siguiendo el conducto regular
16.1.3	Reporte de debilidades de seguridad de la información	SI	Se debe solicitar a todo el personal que reporte cualquier tipo de debilidad del sistema para realizar la mejoras del sistema
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	Todo evento se debe evaluar y clasificar si puede ser incidente de seguridad para dar el mejor manejo al mismo
16.1.5	Respuesta a incidentes de seguridad de la información	SI	Se debe informar todo evento de seguridad así como la respuesta dada al mismo.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Se debe analizar todos los eventos y soluciones dadas a problemas para así tener la mejor solución y disminuir el riesgo
16.1.7	Recolección de evidencia	SI	Se debe tener un procedimiento para recolectar fallas del sistema para que se tenga una evidencia para posteriores auditorias.
18	Cumplimiento		
18.1	Cumplimiento de requisitos legales y contractuales		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	Se debe identificar requisitos legales locales y nacionales y así poder dar un manejo adecuado de los mismos.
18.1.2	Derechos de propiedad intelectual	SI	Se deben proteger los derechos de propiedad intelectual.
18.1.3	Protección de registros	SI	Los registro se deben proteger ante fraude destrucción, acceso no autoriza o todo lo que pueda afectar los mismo.
18.1.4	Privacidad y protección de datos personales	SI	Se debe asegurar no divulgar información personal tal como lo dice la ley
18.1.5	Reglamentación de controles criptográficos	SI	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
18.2	Revisiones de seguridad de la información		
18.2.1	Revisión independiente de la seguridad de la información	SI	Se debe validar todos los procesos de la seguridad de la información de forma independientemente a intervalos planificados o cuando ocurran cambios significativos.
18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	Se debe validar con regularidad todas las normas de seguridad para hacer los ajustes necesarios para tener la mejor seguridad
18.2.3	Revisión del cumplimiento técnico	SI	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información

Anexo 3. Resumen Analítico Especializado – RAE

Fecha de Realización:	27/09/2020
Programa:	Especialización en Seguridad Informática.
Línea de Investigación:	Proyecto Aplicado.
Título:	ANALISIS Y DISEÑO DE UN MECANISMO DE CIFRADO DE CORREO ELECTRONICO PARA GARANTIZAR Y PROTEGER LA INFORMACION ENVIADA DE LAS PYMES.
Autor(es):	Hernandez Marin Yesid
Palabras Claves:	Correo electrónico, Phishing, Cifrado, Ciberataque, Vulnerabilidades.
Descripción:	El presente proyecto aplicado tiene como propósito presentar un método de aplicación de prácticas adecuadas para el manejo de correo electrónico corporativo, aplicable a micro, pequeñas y medianas empresas. El método propuesto está basado en un análisis previo a los activos de información, los procesos y los riesgos de seguridad de la información de este tipo de organizaciones frente a las amenazas latentes en el ciberespacio y al cumplimiento de los requerimientos normativos a nivel nacional correspondientes a los delitos informáticos y la protección de datos personales. El documento pretende dar un listado de parámetros e instrucciones a seguir, sin la necesidad de realizar grandes inversiones económicas en la infraestructura y en los procesos organizacionales de este tipo de empresas. Este documento se basa en una investigación deductiva que se desarrolla mediante la premisa: todas las empresas que reciben, procesen o trasmiten información clasificada como confidencial, requieren conocer toda la normatividad legal y la correcta gestión de los activos de información de su negocio.

Fuentes bibliográficas destacadas:

A. A. Tous-Mulkay, «Finanzas Personales.co,» 06 10 2019. [En línea]. Available: https://www.finanzaspersonales.co/columnistas/articulo/principales-riesgos-de-ciberseguridad-en-las-pymes/79732. [Último acceso: 01 02 2020].

C. Colby, «Cnet.com,» 15 Octubre 2019. [En línea]. Available:

https://www.cnet.com/how-to/yahoo-data-breach-how-to-file-for-358-or-more-as-part-of-claim-settlement/?ftag=CMG-01-10aaa1b. [Último acceso: 1 Mayo 2020].

C. D. L. REPÚBLICA, «Ley 1273 DE 2009,» 05 Enero 2009. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. [Último acceso: 20 Enero 2020].

C. D. L. REPÚBLICA, «LEY 527 DE 1999,» 18 Agosto 1999. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html. [Último acceso: 24 Enero 2020].

C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1266 DE 2008,» 31 Diciembre 2008. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html. [Último acceso: 22 Enero 2020].

C. D. L. REPÚBLICA, «LEY ESTATUTARIA 1581 DE 2012,» 17 Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 21 Enero 2020].

C. Osborne, «zdnet.com,» 18 Diciembre 2019. [En línea]. Available: https://www.zdnet.com/article/ftc-settles-with-unroll-me-over-allegedly-duping-users-over-email-data-collection-sale/. [Último acceso: 20 febrero 2020].

C. Osborne, «zdnet.com,» 28 Octubre 2019. [En línea]. Available: https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/. [Último acceso: 8 Febrero 2020].

C. Osborne, «zdnet.com,» 5 Septiembre 2019. [En línea]. Available: https://www.zdnet.com/article/dklok-data-breach-leaked-global-enterprise-client-internal-emails/. [Último acceso: 3 Febrero 2020].

C. Osborne, «zdnet.com,» 6 noviembre 2019. [En línea]. Available: https://www.zdnet.com/article/trend-micro-reveals-insider-threat-exposing-customer-data/. [Último acceso: 12 febrero 2020].

CCIT, «TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020,» 29 10 2019. [En línea]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. [Último acceso: 03 02 2020].

Colomboamericana, Cámara de Comercio, «https://www.amchamcolombia.co/,» 2019. [En línea]. Available: https://www.amchamcolombia.co/es/comunicaciones/noticias-afiliados/1767-cisco-la-ciberseguridad-tambi%C3%A9n-es-un-reto-para-las-pymes. [Último acceso: 05 Enero 2020].

Computerworld, «Microsoft Mail: Solid, less graphical,» Computerworld, vol. XXV, p. 38, 21 Agosto 1991.

D. Swinhoe, «CSOonline,» 17 Abril 2020. [En línea]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Último acceso: 28 Abril 2020].

El Tiempo, «Eltiempo.com,» 26 Diciembre 2019. [En línea]. Available: https://www.eltiempo.com/economia/sectores/competitividad-de-las-pymes-en-colombia-para-2020-446922. [Último acceso: 05 Enero 2020].

F. FERRI-BENEDETTI, «¿QUÉ ES EL CIFRADO?,» 23 07 2013. [En línea]. Available: https://www.softonic.com/articulos/que-es-el-cifrado-encriptar. [Último acceso: 25 Abril 2020].

H. Monterrosa, «La Republica.com,» 31 Agosto 2019. [En línea]. Available: https://www.larepublica.co/economia/mipymes-representan-96-del-tejido-empresarial-y-aportan-40-al-pib-2903247. [Último acceso: 05 Enero 2020].

http://www.cis.usouthal.edu, «CTSS, Compatible Time-Sharing System,» 01 01 2019. [En línea]. Available: http://www.cis.usouthal.edu/faculty/daigle/project1/ctss.htm. [Último acceso: 10 Enero 2020].

I. E. T. Force, «A Simple Mode of Facsimile Using Internet Mail,» Marzo 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2305. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Cleartext Considered Obsolete: Use of Transport Layer Security

(TLS) for Email Submission and Access,» Enero 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8314. [Último acceso: 13 Enero 2020].

I. E. T. Force, «Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing,» Junio 2014. [En línea]. Available: https://tools.ietf.org/html/rfc7230. [Último acceso: 14 Enero 2020].

I. E. T. Force, «Hypertext Transfer Protocol Version 2 (HTTP/2),» Mayo 2015. [En línea]. Available: https://tools.ietf.org/html/rfc7540. [Último acceso: 14 Enero 2020].

I. E. T. Force, «INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1,» Marzo 2003. [En línea]. Available: https://tools.ietf.org/html/rfc3501. [Último acceso: 11 Enero 2020].

I. E. T. Force, «LEMONADE Architecture - Supporting Open Mobile Alliance (OMA),» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5442. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Message Disposition Notification,» Febrero 2017. [En línea]. Available: https://tools.ietf.org/html/rfc8098. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Message Disposition Notification,» Mayo 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3798. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Open Pluggable Edge Services (OPES) SMTP Use Cases,» Mayo 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4496. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Post Office Protocol - Version 3,» Mayo 1996. [En línea]. Available: https://tools.ietf.org/html/rfc1939. [Último acceso: 12 Enero 2020].

I. E. T. Force, «Sieve Email Filtering: Reject and Extended Reject Extensions,» Marzo 2009. [En línea]. Available: https://tools.ietf.org/html/rfc5429. [Último acceso: 10 Enero 2020].

I. E. T. Force, «Simple Mail Transfer Protocol,» Octubre 2008. [En línea]. Available: https://tools.ietf.org/html/rfc5321. [Último acceso: 11 Enero 2020].
I. E. T. Force, «SMTP MTA Strict Transport Security (MTA-STS),» Septiembre

2018. [En línea]. Available: https://tools.ietf.org/html/rfc8461. [Último acceso: 14 Enero 2020].

I. E. T. Force, «SMTP Service Extension for Secure SMTP over Transport Layer Security,» Febrero 2002. [En línea]. Available: https://tools.ietf.org/html/rfc3207. [Último acceso: 12 Enero 2020].

I. E. T. Force, «SMTP TLS Reporting,» Septiembre 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8460. [Último acceso: 14 Enero 2020].

I. E. T. Force, «The PLAIN Simple Authentication and Security Layer (SASL) Mechanism,» Agosto 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4616. [Último acceso: 13 Enero 2020].

I. E. T. Force, «The Secure Sockets Layer (SSL) Protocol Version 3.0,» Agosto 2011. [En línea]. Available: https://tools.ietf.org/html/rfc6101. [Último acceso: 15 Enero 2020].

I. E. T. Force, «The Transport Layer Security (TLS) Protocol Version 1.3,» Agosto 2018. [En línea]. Available: https://tools.ietf.org/html/rfc8446. [Último acceso: 14 Enero 2020].

I. E. T. Force, «Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols,» Marzo 2016. [En línea]. Available: https://tools.ietf.org/html/rfc7817. [Último acceso: 13 Enero 2020].

I. E. T. Force, «Using TLS with IMAP, POP3 and ACAP,» Junio 1999. [En línea]. Available: https://tools.ietf.org/html/rfc2595. [Último acceso: 12 Enero 2020].

I. E. T. Force, «Voice Profile for Internet Mail (VPIM) Addressing,» Junio 2004. [En línea]. Available: https://tools.ietf.org/html/rfc3804. [Último acceso: 10 Enero 2020].

INCIBE, «Utiliza el correo electrónico de forma segura con PGP,» 13 08 2019. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/utiliza-el-correo-electronico-forma-segura-pgp. [Último acceso: 15 Mayo 2020].

ISO.ORG, «STANDARDS,» 20 Febrero 2006. [En línea]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/info_security.pdf.

[Último acceso: 24 Abril 2020].

ISO27000.ES, «Serie "27000",» ISO27000.ES, 20 Septiembre 2019. [En línea]. Available: http://www.iso27000.es/iso27000.html. [Último acceso: 15 Marzo 2020].

J. A. P. Cadavid, «Revitas Universidad Externado de Colombia,» 24 11 2010. [En línea]. Available: https://revistas.uexternado.edu.co/index.php/propin/article/download/2476/2112/. [Último acceso: 24 Abril 2020].

J. O. Canizalez, «SEGURIDAD EN REDES,» SEGURIDAD EN REDES, 15 06 2011. [En línea]. Available: http://seguridad-deredes.blogspot.com/2011/06/cifrado-y-criptografia.html. [Último acceso: 01 05 2020].

K. Shoens, «MAIL REFERENCE MANUAL,» 25 Abril 1984. [En línea]. Available: http://reports-archive.adm.cs.cmu.edu/anon/itc/CMU-ITC-012.pdf. [Último acceso: 10 Enero 2020].

L. Goldsmith, «APL Quotations and Anecdotes,» 18 Septiembre 2010. [En línea]. Available: https://www.jsoftware.com/papers/APLQA.htm. [Último acceso: 10 Enero 2020].

L. o. C. USA, «cc:Mail Archive Email Format,» 18 Mayo 2018. [En línea]. Available: https://www.loc.gov/preservation/digital/formats/fdd/fdd000391.shtml. [Último acceso: 10 Enero 2020].

M. GONZALO, «Cómo cifrar tu correo de Gmail sin complicaciones con Mailvelope,» 23 07 2013. [En línea]. Available: https://www.eldiario.es/turing/como-cifrar-email-criptografia-Gmail-Mailvelope_0_156784455.html. [Último acceso: 14 Mayo 2020].

M. Williams, «CSOonline,» 4 Octubre 2017. [En línea]. Available: https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html. [Último acceso: 29 Abril 2020].

Microsoft, «Exchange Server Protocol Documents,» 24 Septiembre 2019. [En línea]. Available: https://docs.microsoft.com/en-

us/openspecs/exchange_server_protocols/ms-oxprotlp/30c90a39-9adf-472b-8b5b-03c282304a83?redirectedfrom=MSDN. [Último acceso: 11 Enero 2020].

Microsoft, «Outlook Connectivity with MAPI over HTTP,» 9 Mayo 2014. [En línea]. Available: https://blogs.technet.microsoft.com/exchange/2014/05/09/outlook-connectivity-with-mapi-over-http/. [Último acceso: 11 Enero 2020].

R. H. N. S. T. K. B. a. P. K. Anderson, «The Design of the MH Mail System,» 31 Diciembre 1978. [En línea]. Available: https://www.rand.org/pubs/notes/N3017.html. [Último acceso: 10 Enero 2020].

R. Tomlinson, «Firstemailframe,» 06 Mayo 2006. [En línea]. Available: http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html. [Último acceso: 10 Enero 2020].

R. Walsh, «ProPrivacy,» 15 Noviembre 2019. [En línea]. Available: https://proprivacy.com/email/review/vfemail. [Último acceso: 5 Febrero 2020].

S. F. D. COLOMBIA, «CIRCULAR 007 DE 2018,» 05 Junio 2018. [En línea]. Available: https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/20126/reAncha/1/c/00. [Último acceso: 27 Enero 2020].

S. F. D. COLOMBIA, «CIRCULAR 042 DE 2012,» 05 Octubre 2012. [En línea]. Available: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf. [Último acceso: 26 Enero 2020].

S. Gatlan, «Bleepingcomputer.com,» 12 Febrero 2019. [En línea]. Available: https://www.bleepingcomputer.com/news/security/hackers-wipe-vfemail-servers-may-shut-down-after-catastrophic-data-loss/. [Último acceso: 5 Febrero 2020].

S. Talens-Oliag, «Introducción a la Criptología,» 14 04 2003. [En línea]. Available: https://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.html. [Último acceso: 14 Abril 2020].

T. V. Vleck, «The History of Electronic Mail,» 01 Febrero 2001. [En línea]. Available: https://www.multicians.org/thvv/mail-history.html. [Último acceso: 10

Enero 2020].

The GnuPG Project, «The GNU Privacy Guard,» 07 01 2020. [En línea]. Available: https://www.gnupg.org/gph/es/manual/c190.html. [Último acceso: 15 Mayo 2020].

TUGURIUM, «Glosario Terminología Informática,» 23 Marzo 2009. [En línea]. Available: http://www.tugurium.com/gti/termino.php?Tr=Information%20Technology%20Security%20Evaluation%20Criteria&Tp=N&Or=0. [Último acceso: 20 Abril 2020].

TUGURIUM, «TCSEC, el libro naranja de la seguridad informática,» 28 04 2017. [En línea]. Available: https://www.teknoplof.com/2017/04/28/tcsec-libro-naranja-la-seguridad-informatica/. [Último acceso: 20 Marzo 22].

Contenido del documento:

Marco Metodológico:	El desarrollo de esta metodología se basó en una investigación de tipo deductiva partiendo de los diferentes estudios y documentación de la seguridad de la información para las PYMES, además de usar un enfoque basado en las de la norma ISO-IEC 27001 (SGSI) e ISO 27005 (Riesgos de Seguridad de la Información). También se basara en la recolección de información de procesos de aseguramiento de información disponibles en el mercado. UNIVERSO Y MUESTRA A través de una serie de encuestas a los empleados de

	algunas pymes, se obtuvo la información sobre los perfiles, recursos tecnológicos que maneja y el tipo de información que utiliza para desempeñar su cargo. A partir de estos datos, se logró definir el tipo de información que se debe tener en cuenta y enfocar dentro de la metodología que arrojara este proyecto. FUENTES DE RECOLECCION DE INFORMACION La investigación utilizó como fuentes de recolección de información diferentes monografías, estudios, informes estadísticos sobre el estado de seguridad de la información de las pymes y sus mayores retos en el mercado para salvaguardar la información que trasmite por correo electrónico. Además se tendrán en cuanta las leyes y normatividad vigente que aplica sobre las PYMES a para el manejo de la información. TECNICAS E INTRUMENTOS Para alcanzar el objetivo del presente documento, la investigación se apoyó en los siguientes instrumentos: • Estudio del estado actual de la seguridad de la información en las PYMES. • Encuestas, a los empleados de algunas PYMES que hagan envió o uso del correo electrónico para el desarrollo de sus actividades. • Mediante observación se comprenderán los procesos y usos de la tecnología en su forma de trabajo diario.
Conceptos adquiridos :	ACTIVO DE INFORMACIÓN: Es cualquier elemento que contenga información para el desarrollo de las actividades puede ser físico o digital. ALGORITMO DE CIFRADO: Operación o funciona matemática para generar una clave para garantizar la confidencialidad e integridad de la información. ANALISIS DE RIESGO: Es un proceso donde se validan los activos de información y documentan todas las posibles amenazas y los controles que se tendrían que aplicar para asegurar estos activos.

	ATAQUE CRIPTOGRÁFICO: Es un método para sortear validar la seguridad de un sistema criptográfico. CERTIFICADO DIGITAL: Es un fichero digital generado por una autoridad certificadora que asocia la información del titular. CIFRADO: Acción de ocultar o codificar información para evitar que personas no autorizadas puedan acceder a la misma. CIFRADO DE DATOS: se puede entender como el hecho de guardar algo valioso dentro de una caja fuerte cerrada con llave. CIFRADO SIMÉTRICO: Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. CIFRADO ASIMÉTRICO: Para evitar estos inconvenientes, podemos utilizar lo que se conoce como cifrado asimétrico. A diferencia del cifrado simétrico, el asimétrico es un tipo de cifrado en el que no usamos una única clave sino dos. CIFRADOR DE BLOQUE: Es un sistema criptográfico que cifra de bloques en bloque, usualmente cada bloque es de 128 bits. Algunos sistemas conocidos son, TDES, RC5, AES. CIFRADOR DE FLUJO: Es un sistema criptográfico de cifra de bit en bit, los más conocidos son, RC4, SEAL, WAKE. CRIPTOGRAFIA: Es la técnica que consiste en cifrar un mensaje. CRIPTOGRAFÍA VISUAL: Es un esquema de compartición de secretos donde el secreto es una imagen y las partes son también varias imágenes. La ventaja de este tipo de criptografía es que no es necesaria una computadora para la reconstrucción del secreto. CLAVE PÚBLICA: Son claves de cifrado que se pueden compartir para descifrar la información. CLAVE PRIVADA: Son las claves de cifrado que son exclusivas de los Titulares sobre su información.

	CORREO ELECTRÓNICO: Es un servicio o aplicativo que permite enviar y recibir información. CONDIFIDENCIALIDAD: Acción de garantizar la que la información sea accedida por las personas autorizadas. DISPONIBILIDAD: Se trata de capacidad de tener la información siempre disponible o accesible. ESQUEMA CRIPTOGRÁFICO: Es un conjunto de primitivas que componen una aplicación criptográfica más completa, como el esquema de firma digital (compuesta de la primitiva de firma y la de verificación), el esquema de cifrado (compuesta con la primitiva de cifrado y la de descifrado) etc. FAMILIA CRIPTOGRÁFICA: es el conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de Factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE, MQV) FIRMA DIGITAL: es un método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento. FIRMA DIGITAL CON APÉNDICE: método de firma digital que requiere al mensaje como entrada en el proceso de verificación. FIRMA DIGITAL CON MENSAJE RECUPERABLE: método de firma digital que no requise real mensaje como entrada en el proceso de verificación. El mensaje se recupera después de que se ha verificado la firma. FIRMA ELECTRONICA: Conjunto de datos electrónicos que contiene la información del titular.

	FUGA DE DATOS: Es la perdida de confidencialidad de la información. INTEGRIDAD: Es la propiedad de garantizar la exactitud de la información. PHISHING: Es una estafa a través de correo electrónico con el fin de sacar información confidencial o sensible. PGP: Es un programa para proteger la información por medio del cifrado. POLITICA DE SEGURIDAD: Son las decisiones y medidas de seguridad de una empresa. PROTOCOLO: Se trata de una regla estándar. RSA: Se trata de un sistema criptográfico de clave pública para cifrar documentos o firmarlos digitalmente. SEGURIDAD DE LA INFORMACIÓN: Tiene como objetivo proteger todos los activos de información de la empresa (Físicos y lógicos), basado en sus tres pilares confidencialidad, integridad y disponibilidad. SEGURIDAD INFORMÁTICA: Hace referencia al aseguramiento de los activos de información (hardware y software), de todos sus controles y configuraciones que garanticen el correcto funcionamiento, disponibilidad y disminución de riesgos. SEGURIDAD EN REDES: La seguridad en redes consiste en un conjunto de medidas preventivas, programadas para enfrentar riesgos de origen físico y lógico. SGSI: Sistema de gestión de seguridad de información. SPEARPHISHING: Es una estafa a través de correo electrónico dirigida a un grupo u organización con el fin de sacar información confidencial o sensible. SPOOFING: Es la técnica de suplantación de identidad llevada a cabo por ciberdelincuentes.

	VULNERABILIDAD: Fallos o deficiencias de un sistema que permite acceder de forma no legítima.
Conclusiones:	La construcción del presente documento llevó al autor a comprender que se hace necesario conocer los resultados de otras investigaciones, las soluciones identificadas y exploradas junto con los conceptos técnicos aplicables a los grupos de enfoque, con el objetivo de producir un material de referencia fácil de interpretar. Adicionalmente para el desarrollo del presente trabajo de grado se encontraron obstáculos referentes al análisis de ciberseguridad en pymes en Colombia. Para la consolidación del presente trabajo de grado se realizó una investigación del estado del arte de la seguridad de la información en las pymes, empezando por un enfoque externo a la realidad Colombiana, para identificar que se ha investigado y propuesto en otras culturas, por lo cual el autor reconoce que es clave conocer de primera mano cómo es el aseguramiento que implementan las empresas para el desarrollo del negocio, si se considera una necesidad o simplemente no se ve la utilidad que brinda proteger los activos de información de las compañías. Este documento se escribió de tal forma que permitirá el desarrollo de una conciencia en las personas que hacen parte de este tipo de empresas, en que el aseguramiento de sus sistemas ayudará a mitigar o minimizar el impacto de las acciones de aquellos ciberdelincuentes que están buscando obtener un beneficio económico, reputacional o egocéntrico a partir de una falla de seguridad. Fue posible también observar que algunas pymes al no contar una guía o conocimiento claro de las leyes y marcos de referencia que pueden aplicar a sus negocios, pueden descuidar el cumplimiento de las mismas, sin saber que al estar alineadas con las leyes y las mejores prácticas de seguridad de la información se puede obtener un valor agregado que pueden utilizar para el crecimiento comercial de la empresa. Es de vital importancia implementar políticas de seguridad enfocadas principalmente a la clasificación y al aseguramiento de la información dado que en las pymes se puede encontrar un alto número de activos considerados como confidenciales, sensibles o de uso interno y más cuando la misma puede llegar a ser trasmitida por correo electrónico u otros medios digitales. El principal objetivo es salvaguardar este conjunto de activos

	en este tipo de empresas mediante la aplicación de los conceptos y metodologías descritas en el presente documento. Es posible para una pyme contar con este documento como una base que incluye los conceptos y procedimientos metódicos básicos sobre la gestión de seguridad de la información en el correo electrónico, es posible que se convierta en una herramienta fundamental para que el personal encargado pueda asegurar los activos de información de la empresa, pues al estar preparada y con el conocimiento esencial, podrá mitigar o controlar los posibles riesgos que se pueden presentar en los flujos de la información a nivel interno y hacia otras empresas. Se requiere de trabajos futuros que permitan validar la implementación de los conceptos descritos en el presente documento y que hagan un análisis posterior mediante herramientas estadísticas para validar el impacto del conocimiento aquí descrito en pymes en Colombia.