UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

LICENCIATURA EN DESARROLLO DE SOFTWARE

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

TERCER SEGUIMIENTO DEL PROYECTO SEMESTRAL

SEGURIDAD EN CORREO ELECTRÓNICO

Prof.ª Isabel Leguias Integrantes:

Alsola, José

Cheung, Buddy

Mendoza, Jesús

Navarro, Abdias

Grupo: 1LS – 242

**10 de julio de 2018**

Contenido

[Introducción 3](#_Toc518477385)

[Capítulo I 4](#_Toc518477386)

[1.1 Planteamiento del problema 4](#_Toc518477387)

[1.2 Preguntas de investigación 4](#_Toc518477388)

[1.3 Objetivo General 5](#_Toc518477389)

[1.4 Objetivo Específicos 5](#_Toc518477390)

[1.5 Motivación 6](#_Toc518477391)

[1.6 Alcance o limitación 6](#_Toc518477392)

[Capítulo II 7](#_Toc518477393)

[2. Marco teórico 7](#_Toc518477394)

[2.1 Antecedentes y situación actual 7](#_Toc518477395)

[2.2 Enfoque empresarial 9](#_Toc518477396)

[2.3 Ataques y virus 10](#_Toc518477397)

[2.3.1 Melissa 10](#_Toc518477398)

[2.3.2 Ransonware 11](#_Toc518477399)

[2.3.3 Spam 12](#_Toc518477400)

[Capítulo III 13](#_Toc518477401)

[3. Marco metodológico 13](#_Toc518477402)

[3.1 Modalidad de la investigación 13](#_Toc518477403)

[3.2 Recolección de información 13](#_Toc518477404)

[3.3 Procesamiento y análisis de datos 13](#_Toc518477405)

[3.4 Desarrollo del proyecto 13](#_Toc518477406)

[Capítulo IV 14](#_Toc518477407)

[4. Desarrollo de la propuesta 14](#_Toc518477408)

[4.1 Análisis de resultado 14](#_Toc518477409)

[4.1.1 Resultado de la encuesta 14](#_Toc518477410)

[4.1.2 Resumen de la encuesta 18](#_Toc518477411)

[4.2 Propuesta de solución 18](#_Toc518477412)

[Conclusión 19](#_Toc518477413)

[Referencias bibliográficas 20](#_Toc518477414)

# **Introducción**

En esta investigación hablaremos de la seguridad en correos electrónicos en la cual abordaremos cuestiones como la utilización del correo electrónico por Internet o por otras redes que no sean de confianza supone riesgos de seguridad para su sistema, aunque este esté protegido por un cortafuego.

El correo electrónico es similar a otras formas de comunicación. Es importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos sistemas antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, convendrá que emplee medidas de seguridad para proteger la confidencialidad del correo electrónico.

También se hablará de spam, Phishing, estafas de todo tipo, cadenas de mensajes falsos ¿Cuáles son las amenazas más habituales asociadas al uso de los correos electrónicos? ¿Alternativas de seguridad en los correos electrónicos? ¿Cómo evitar un malware atreves de un correo electrónico? ¿Cómo evitar un correo electrónico fraudulento? Consejos de seguridad en el uso del correo web (web mail). Firmas digitales, certificados digitales, S/MIME y cifrados conceptos básicos y en acción.

# **Capítulo I**

## **1.1 Planteamiento del problema**

Actualmente, según estudios estadísticos, existen más de 500 millones de usuarios con al menos una dirección de correo electrónico activa; lo que en consecuencia supone un mercado para personas u organizaciones con fines maliciosos. En cualquier contexto que implique el uso de una dirección de correo electrónica, se deben implementar las medidas necesarias o regulatorias para asegurar el correcto uso de este servicio y evitar ser un blanco potencial o víctima de las distintas modalidades o ataques utilizados para vulnerabilizar la integridad de la información o datos, a través de este servicio. Medidas correctivas, buenas prácticas, entre otros puntos importantes se desarrollarán para plasmar de positivamente el correcto uso de este servicio crítico e importante, para estar preparado ante cualquier situación que pueda perjudicar el valor de este.

## **1.2 Preguntas de investigación**

* ¿Se adoptan las medidas necesarias en la actualidad para manejar adecuadamente la seguridad en los correos electrónicos?
* ¿Conocen los usuarios los distintos riesgos a los que están expuestos al utilizar correo electrónico?

## **1.3 Objetivo General**

El objetivo principal consiste en realizar un estudio específico acerca de las medidas de seguridad que se deben mantener y practicar para conservar y obtener un ámbito seguro en los correos electrónicos.

## **1.4 Objetivo Específicos**

* Evitar las malas prácticas en la seguridad implementada en los correos electrónicos.
* Conocer los riegos a los que están expuestos los usuarios que utilizan correo electrónico y cómo prevenirlos.
* Determinar las buenas prácticas que deben realizarse para mejorar la seguridad en el ámbito de los correos electrónicos.

## **1.5 Motivación**

El tema seleccionado es importante para el individuo debido a que en las ultimas 2 décadas ha ido evolucionando la tecnología más que en los últimos 40 años. El tema se seguridad en correos electrónicos es un tema muy delicado ya que se han ido desarrollando tecnologías o procesos en que l validaciones de usuario se dan por medio de este. Las últimas tendencias para el ingreso de aplicaciones se hacen mayormente a un clic enlazando datos vía correo electrónico y facilitando el ingreso al usuario. Por esto el tema seleccionado es necesario hacer una profunda investigación para asegurar datos en los correos o medidas para evitar el robo de estos.

El correo electrónico es similar a otras formas de comunicación. Es importante ser prudente a la hora de enviar información confidencial por correo electrónico. El correo electrónico viaja a través de numerosos sistemas antes de llegar a su destino, por lo que es posible que alguien lo intercepte y lo lea. Por lo tanto, convendrá que emplee medidas de seguridad para proteger la confidencialidad del correo electrónico.

## **1.6 Alcance o limitación**

En este tema abarcaremos todo lo referente a seguridad en los correos electrónicos, las medidas universalmente empleadas para el debido uso de un correo electrónico, las opciones de seguridad que se pueden integrar o habilitar para mantener seguro un correo electrónico, los riegos o amenazas más comunes que comprometen a los correos electrónicos, consejos, y cuáles son las mejores prácticas a seguir.

# **Capítulo II**

## **2. Marco teórico**

## **2.1 Antecedentes y situación actual**

Durante los últimos 20 años, el correo electrónico ha dejado de ser una herramienta que utilizaban principalmente los técnicos y los investigadores para convertirse en la red troncal de las comunicaciones corporativas. Cada día se intercambian más de 100 000 millones de mensajes de correo electrónico corporativos. A medida que crece el uso del correo electrónico, la seguridad cobra mayor importancia. Efectivamente, las campañas de spam masivo han dejado de ser el único foco de preocupación. En la actualidad, el spam y el malware son simplemente piezas de un complejo panorama que incluye tanto amenazas que entran como riesgos que salen. **[1]**

El servicio de correo electrónico es el más amplio e históricamente empleado en la red de redes, Internet. La mensajería electrónica posee enorme popularidad y utilidad. Una gran parte de nuestras entidades potencian la gestión administrativa y muchas otras de sus tareas empleando este servicio. Los programas servidores de correo usados en las diversas redes de computadoras, poseen varias debilidades en lo que se refiere a la seguridad que son, en muchos casos, herencia del frágil protocolo SMTP (Simple Mail Transfer Protocol). Estas vulnerabilidades comprometen el servicio de correo y los recursos que las diferentes instituciones exponen a través del mismo. **[2]**

La seguridad del correo electrónico depende del cifrado. En pocas palabras, el cifrado crea un correo electrónico seguro codificando los datos para que solo alguien con la contraseña correcta u otra autenticación pueda descifrar el mensaje. En muchos casos, este proceso de cifrado y descifrado se lleva a cabo sin que los usuarios lo sepan.

Para la seguridad del correo electrónico, los mensajes pueden encriptarse, o toda su conexión de red puede encriptarse a través de TLS, lo que protege el correo electrónico de la lectura mientras está en movimiento. **[3]**

Son pocas las personas o instituciones que actualmente no cuentan con una dirección de correo electrónico, y no es para menos, ya que el e-mail es uno de los servicios más populares y útiles que se nos ofrecen en el amplio mundo de la red. Gracias a éste servicio podemos comunicarnos con cualquier persona alrededor del mundo, compartir todo tipo de información y evitar los diversos inconvenientes del correo ordinario y todo de manera prácticamente gratuita. Pero, si hay millones de personas haciendo uso legítimo de un servicio, entonces también debe haber una forma de aprovecharlo para fines ilegítimos, y eso es lo que ha ocurrido con el correo electrónico, donde existe un gran número de amenazas ocultas, mismas que se han incrementado debido, entre otras cosas, a que la gente no presta el suficiente cuidado al abrir su correo, menospreciando o desconociendo los riesgos que existen. Amenazas como los virus, gusanos, troyanos y demás fauna cibernética conocida como malware, o ataques de spam, pharming y Phishing, han encontrado un verdadero nicho de acción en el correo electrónico. Por lo que a continuación se presenta una serie de recomendaciones para mitigar el riesgo y poder estar tranquilos al revisar nuestra bandeja de entrada. **[4]**

Los usuarios que se toman el tiempo para pensar en la seguridad son quienes por lo general usan contraseñas difíciles. Sin embargo, existen personas que prestan poca atención a su cuenta de correo electrónico principal, que muchas veces funciona como llave maestra para acceder a otras. La cuenta de correo electrónico principal es la que te permite recuperar los datos de cuentas que hayan sido secuestradas o ayudarte a recordar la contraseña. Desde este punto de vista, el correo electrónico principal es mucho más sensible que la de PayPal o la bancaria. Pero más allá de eso, si un criminal se apodera de tu correo electrónico podría recopilar información de tus otras cuentas y, así, comprometerlas. Por tanto, un correo electrónico robado equivale, en la mayoría de los casos, a que alguien robe toda tu vida digital completa. **[5]**

Es evidente que, con la masificación en el uso del correo electrónico, se convirtió en un elemento socorrido por los cibercriminales, que, con el afán de sacar ventaja sobre los usuarios, comenzaron a utilizarlo con fines maliciosos. A partir de entonces, fue posible identificar un sinnúmero de campañas que, a partir de los mensajes y los archivos adjuntos, buscaban afectar a las potenciales víctimas. Luego de conocerse el alcance del correo electrónico, aparecieron las primeras estafas en torno a esta útil herramienta. Muchas de ellas estaban totalmente orientadas a crear emociones entre los usuarios, haciendo alusión, por ejemplo, a supuestas fortunas, loterías o herencias a las cuales podían ser acreedores. Por último y no menos importante, el correo electrónico sigue siendo utilizado con uno de los principales métodos para propagar amenazas informáticas como el malware. Continuamente se observan campañas completamente orientadas a diseminar códigos maliciosos a través de archivos adjuntos a los mensajes. **[6]**

## **2.2 Enfoque empresarial**

Hoy en día la mayoría de entidades públicas o privadas que operan en internet, exigen como requisito proveer datos personales como un número de teléfono obligatorio o una dirección de correo principal y/o alternativa obligatoria para así impedir las altas anónimas o por “seguridad”, etc. Además estas entidades se suelen asegurar de que pueden “traficar” con nuestros datos y cederlos a terceros; Inevitablemente, al igual que en el caso anterior, cuantos más sitios en internet tengan nuestros datos de correo electrónico y demás, más fácil es que nos lleguen correos no deseados y que la bola de nieve siga creciendo. Es muy difícil que después de unos años de uso de una dirección de mail, no tengamos una cantidad considerable de correo basura. **[7]**

Como es conocido hoy día ya la seguridad en los correos electrónicos no son tan eficaces por la cantidad de nuevas formas de ataques hacia ellos. Es por esto que a su vez está surgiendo nuevas formas de seguridad contras estos ataques también como protecciones poderosas e identificaciones de amenazas en tiempo real. **[8]**

La investigación de Cisco Talos sugiere que es posible que las organizaciones no puedan impedir toda infiltración de malware en sus redes. Sin embargo, las soluciones modernas de seguridad de correo electrónico pueden ayudar a reducir la posibilidad de que los datos críticos salgan de la red, ya sea de forma accidental o intencionalmente. Las organizaciones necesitan detectar, bloquear y administrar riesgos en el correo electrónico saliente. Las soluciones con prevención de pérdida de datos (DLP) sensibles al contexto y basada en políticas, así como las funcionalidades de cifrado, pueden ofrecer dicha protección. El control antivirus y antispam saliente, junto con la limitación de velocidad de salida, permiten que las organizaciones eviten que las máquinas o las cuentas comprometidas aparezcan en una lista negra de correo electrónico. **[9]**

Tal como se pudo investigar algunas empresas de correo electrónicos te ofrecen muchas maneras de proteger tu correo electrónico es ahí donde entran algunas maneras de proteger y mantener seguro tu bandeja de entrar y evitar el acceso a virus, spam y otros. **[10]**

La seguridad web moderna debe tener la capacidad de bloquear malware de sitios sospechosos y legítimos antes de que llegue al usuario. Las herramientas empresariales que aumentan la productividad pueden incrementar significativamente la probabilidad de que los usuarios se encuentren con malware. Incluso los sitios web legítimos pueden representar una amenaza debido al malware diseñado para ocultarse a simple vista. La seguridad web en este entorno debe ser capaz de contar con un análisis basado en la reputación y en el comportamiento. También debe tener suficientes opciones para respaldar políticas que otorguen a los empleados acceso a los sitios que necesitan. Al mismo tiempo, deben denegar de manera selectiva el uso de sitios y funciones que no se deseen, como el intercambio de archivos en línea. **[11]**

Uno de los casos más emblemáticos es el del “virus Melissa”, el cual hizo su primer asalto el 26 de marzo de 1999, y que pasó desapercibido en miles de correos electrónicos por su nombre de mujer e innovadora estrategia.

El email, que empezaba diciendo algo así como “Aquí tienes lo que me pediste, no se lo muestres a nadie”, tenía unos archivos de Microsoft Word adjuntos, y logró ser tan desastroso que se estima que los daños que causaron ascendieron a los 80 millones de dólares solo en Estados Unidos.

## **2.3 Ataques y virus**

Desde que Internet es Internet han existido toda clase de virus informáticos. Sin embargo, “Melissa” destaca por ser el primero en donde utilizaba el servicio de email con datos adjuntos como plataforma de propagación. **[12]**

### 2.3.1 Melissa

Uno de los casos más emblemáticos es el del **virus melissa**, el cual hizo su primer asalto el 26 de marzo de 1999, y que pasó desapercibido en miles de correos electrónicos por su nombre de mujer e innovadora estrategia.

Especialistas en informática aseguran que su diseño, basado en las más sofisticadas técnicas de ingeniería social de entonces, hizo que este mensaje “maligno” calara dentro de tantas personas.

El email, que empezaba diciendo algo así como **“Aquí tienes lo que me pediste, no se lo muestres a nadie”**, tenía unos archivos de **Word** adjuntos, y logró ser tan desastroso que se estima que los daños que causaron ascendieron a los 80 millones de dólares solo en Estados Unidos.

De hecho, los entonces magnates de Internet y la informática como **Microsoft**  e **Intel** decidieron bloquear sus accesos al mundo digital para que este malware no siguiera penetrando dentro de sus sistemas.

Uno de los últimos métodos es el correo electrónico no deseado tipo raqueta, llamado así porque al igual que una raqueta de nieve, que deja huellas grandes, pero leves, el atacante propaga un montón de pequeños mensajes en una gran área para evitar que las defensas tradicionales lo detecten.

Los piratas informáticos de correo electrónico no deseado tipo raqueta rápidamente cambian el cuerpo de los mensajes, los enlaces y las direcciones IP utilizados para enviar correo electrónico no deseado, y nunca repiten la misma combinación. Las posibilidades son, al parecer, infinitas. Estos diferentes tipos de ataques son exitosos porque están bien disfrazados, combinan técnicas diferentes y evolucionan en forma constante. **[13]**

Más del 90% de los ataques aún comienzan por medio del correo electrónico y la naturaleza de las amenazas cambia constantemente. La tecnología de seguridad con la que usted cuente tiene que mantenerse a la par. Proofpoint Targeted Attack Protection (TAP) emplea un innovador sistema para detectar, analizar y bloquear amenazas avanzadas antes de que lleguen a la bandeja de entrada. TAP se incorpora en la plataforma de seguridad Proofpoint de siguiente generación. Le brinda una clara visibilidad en todas las comunicaciones por correo electrónico para que tenga una vista sin igual del panorama de amenazas, desde caballos de Troya bancarios y ransomware. **[14]**

El correo Electrónico al ser una herramienta tan utilizada es también una de las fuentes más comunes de ataques y de introducción de malware en la empresa por parte de los ciberdelincuentes. En un correo electrónico se pueden enviar todo tipo de documentos, videos, audio,… La tendencia natural es leer todos los correos y abrir todos adjuntos que nos llegan, pero este el primer error de los muchos que podemos cometer al trabajar con el correo electrónico. Quienes nos envían correo basura, spam, con malas intenciones, saben que la gran mayoría de los adjuntos con virus son detectados y eliminados por las aplicaciones antivirus, así que utilizan una segunda técnica consistente en el envío de enlaces al malware en el cuerpo del correo. **[15]**

### 2.3.2 Ransonware

El ransomware (secuestro de información) es el término genérico para referirse a todo tipo de software malicioso que le exige al usuario del equipo el pago de un rescate.

Hay al menos dos **tipos de ransomware**, aunque con diversas variantes.

* **Cifrado de archivos**. Tus archivos han sido cifrados con una clave que sólo el cibercriminal conoce. No puedes acceder a ningún fichero del sistema.
* **Pantalla de bloqueo**. Otra posibilidad es que te salga una pantalla de bloqueo y no puedas entrar en tu ordenador.

En ambos casos, te suelen pedir el pago de un rescate o supuesta multa para poner fin al bloqueo de tu ordenador. Cuando pagas el rescate, en teoría te dan una clave para descifrar tus archivos, o bien desaparece dicha pantalla de bloqueo.

El ransomware viene a través de un troyano o gusano que hemos podido descargar por diferentes vías.

* **Por un correo electrónico** con un archivo adjunto que descargaste. Ese correo aparentemente puede ser de correos o de un banco, pero no lo es.
* A través de una red P2P.
* Al hacer clic en un archivo ejecutable de algún programa para descargar.

### 2.3.3 Spam

El spam es el correo electrónico no solicitado que es enviado en cantidades masivas a un número muy amplio de usuarios generalmente con el fin de comercializar, ofertar o tratar de despertar el interés con respecto a algún producto o servicio.

Con respecto a los tipos de spam, partiendo de diferentes clasificaciones, se puede distinguir diferentes modalidades en función del contenido de los mismos:

* **El spam con fines comerciales.** Es el pionero de todos los tipos. Trata de difundir la posibilidad de adquirir algún producto o servicio a un precio inferior al de mercado. En algunos casos este tipo de mensajes está relacionado con tipos delictivos ya que viola leyes de propiedad intelectual, patentes o normativas sanitarias al vender joyas, fármacos o música.
* **El bulo (en inglés hoax).** Son mensajes de correo con contenido falso o engañoso. Este tipo de mensajes es enviado de forma encadenada y se solicita al receptor que prosiga la cadena de envíos. Su contenido son historias inverosímiles relativas a injusticias sociales o formulas para conseguir éxito. Este tipo de mensajes busca captar direcciones de correo electrónico (que se acumulan durante el proceso de reenvío) para utilizarlas posteriormente como objeto de spam.

El spam llega por **correo electrónico** y si bien en sus comienzos llegaba en formato de texto, la eficacia de los programas antivirus ha hecho a los spammer ingeniárselas para tratar de engañar a estos filtros.

# 

# **Capítulo III**

## **3. Marco metodológico**

## **3.1 Modalidad de la investigación**

La presente investigación se contextualiza en la modalidad de investigación descriptiva debida a que se detallara el nivel de seguridad que tiene en la actualidad los correos electrónicos y también conocer sus riesgos.

## **3.2 Recolección de información**

Para la recolección de la información se llevara a cabo una encuesta en internet a los estudiantes de la Facultad de Ingeniería en Sistemas sobre sus experiencias y conocimientos de los correos electrónicos para determinar el nivel de seguridad que tiene el correo electrónico en la actualidad.

## **3.3 Procesamiento y análisis de datos**

Las técnicas de análisis de datos se refieren a los procedimientos o formas particulares de obtener los datos o información necesaria para llevar a cabo la investigación.

* Control de datos
* Procesamiento de datos
* Captura de datos
* Análisis de datos
* Cuadro de presentación de la información recolectada

## **3.4 Desarrollo del proyecto**

* Analizar lenguajes de programación para el desarrollo del aplicativo.
* Realizar búsqueda y análisis de librerías en el lenguaje de programación seleccionado que permitan aplicar la seguridad en los mensajes de correo electrónico.
* Desarrollar el aplicativo
* Realizar pruebas al aplicativo.
* Documentar código.
* Presentar análisis de proyecto finalizado.

# **Capítulo IV**

## **4. Desarrollo de la propuesta**

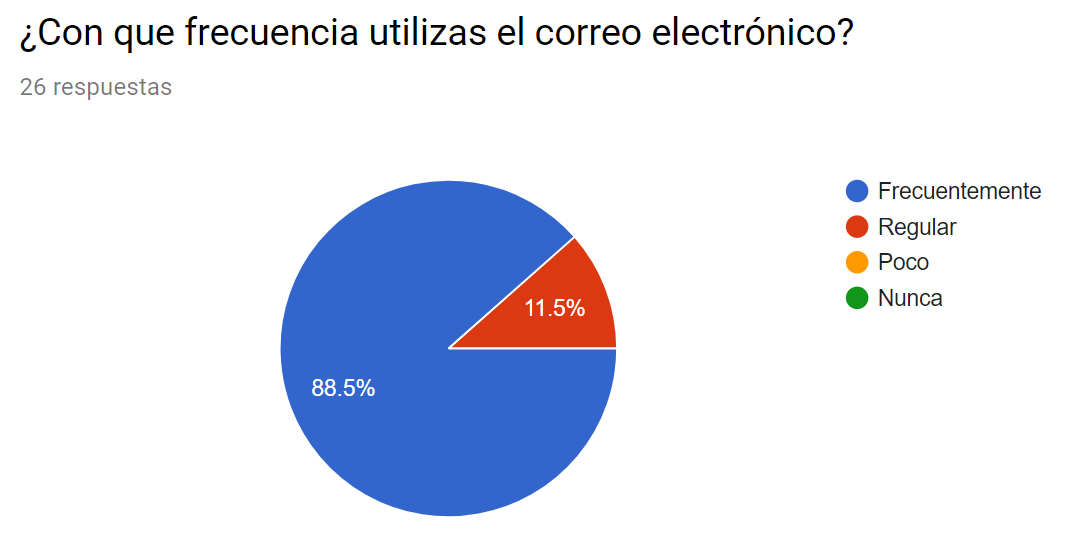
## **4.1 Análisis de resultado**

Para el análisis se establece una Encuesta de 7 preguntas con respuestas múltiples realizadas por los integrantes de este proyecto de investigación para determinar la medida de seguridad que implementan los estudiantes de la Facultad de Sistemas en la actualidad.

### 4.1.1 Resultado de la encuesta

**Pregunta 1:** ¿Con que frecuencia utilizas el correo electrónico?

**Objetivo:** Determinar si la mayoría de los estudiantes utilizan el correo electrónico y el nivel de frecuencia que se usa.



**Análisis:** Todo los estudiantes de la Facultad de Sistemas usan el correo electrónico y la mayoría de ellos lo usan con mucha frecuencia.

**Pregunta 2:** ¿Con que frecuencia recibes correos desconocidos?

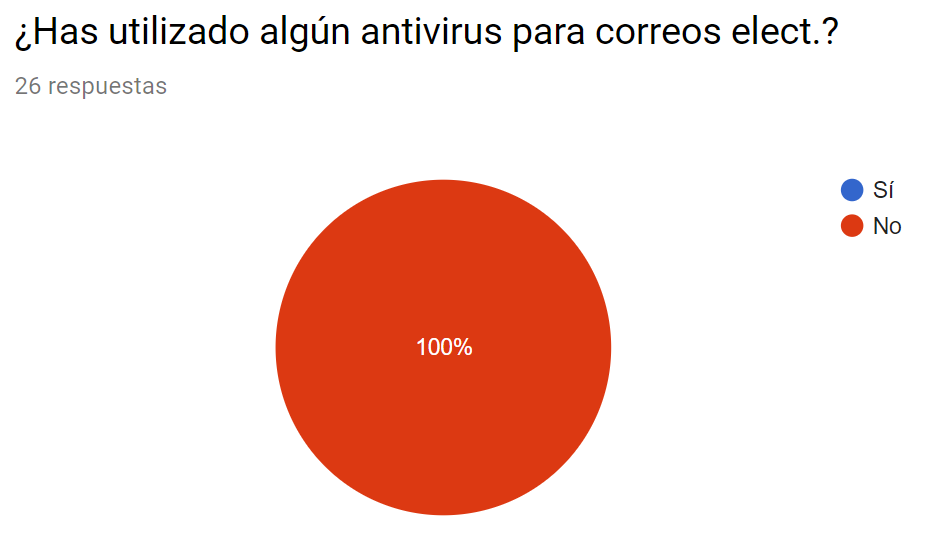
**Objetivo:** Determinar el nivel de frecuencia que los estudiantes reciben correos de dudosa procedencia.



**Análisis:** Según la investigación realizada, se determino que los estudiantes reciben correos desconocidos regularmente y que todos han recibido al menos uno de estos correos.

**Pregunta 3:** ¿Has utilizado algún antivirus para correos electrónicos?

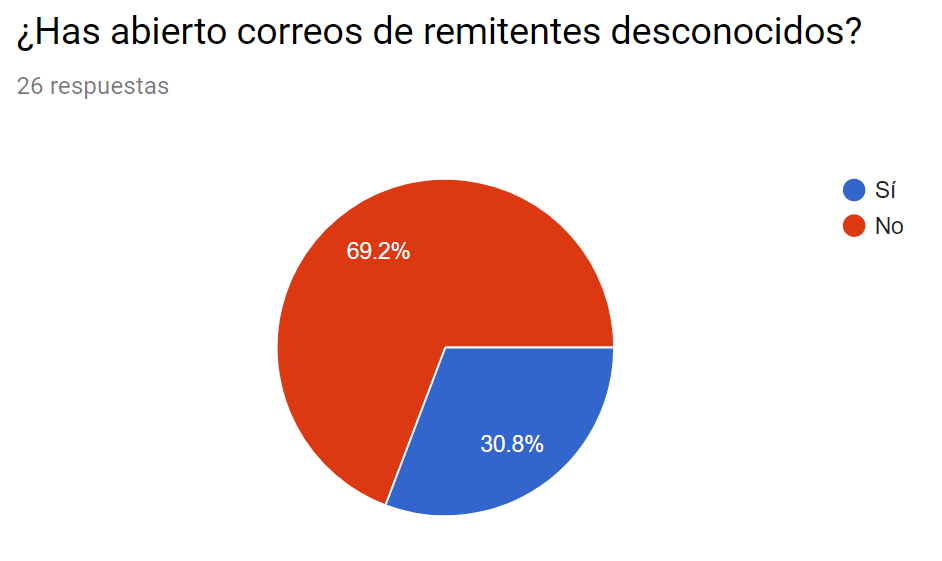
**Objetivo:** Determinar el porcentaje de estudiante que usan antivirus para proteger su correo electrónico.



**Análisis:** De acuerdo a la gráfica, ningún estudiante utiliza algún antivirus para proteger sus correos.

**Pregunta 4:** ¿Has abierto correos de remitentes desconocidos?

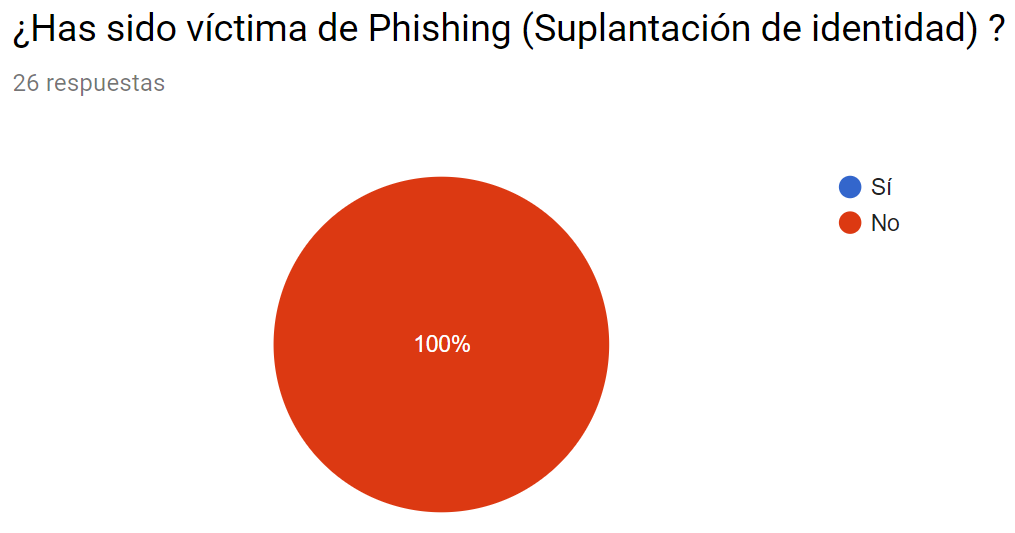
**Objetivo:** Determinar el porcentaje de cuantos estudiantes han abierto al menos un correo desconocido.



**Análisis:** A pesar que todos los estudiantes reconocen que es peligroso abrir un correo desconocido, el 30.8% han abierto un correo de remitente desconocido por curiosidad o por error.

**Pregunta 5:** ¿Has sido víctima de Phishing? (Suplantación de identidad)

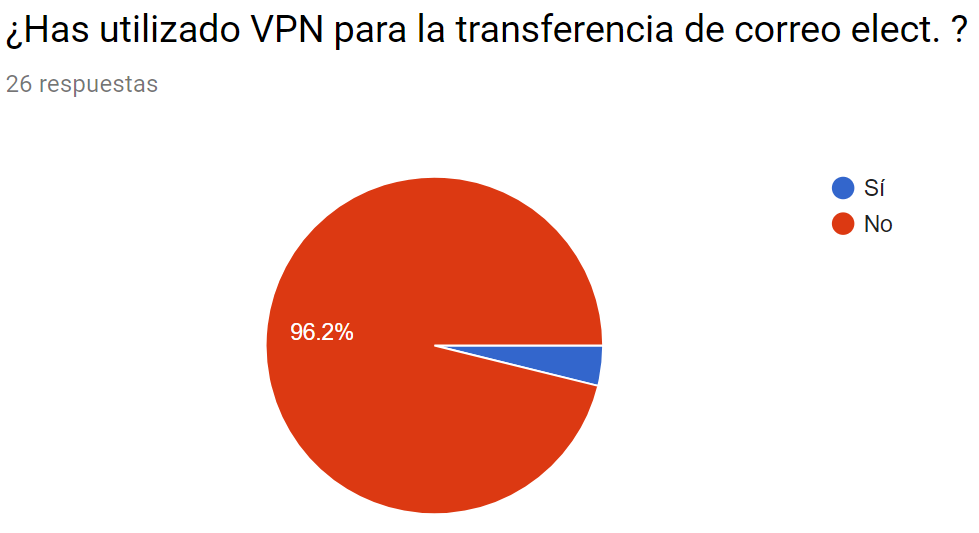
**Objetivo:** Determinar el porcentaje de victimas por Phishing.



**Análisis:** A pesar que ningún estudiante implementa una medida de seguridad para su correo electrónico, podemos ver que ninguno de ellos fueron víctima de Phishing.

**Pregunta 6:** ¿Has utilizado VPN para la transferencia de correos electrónicos?

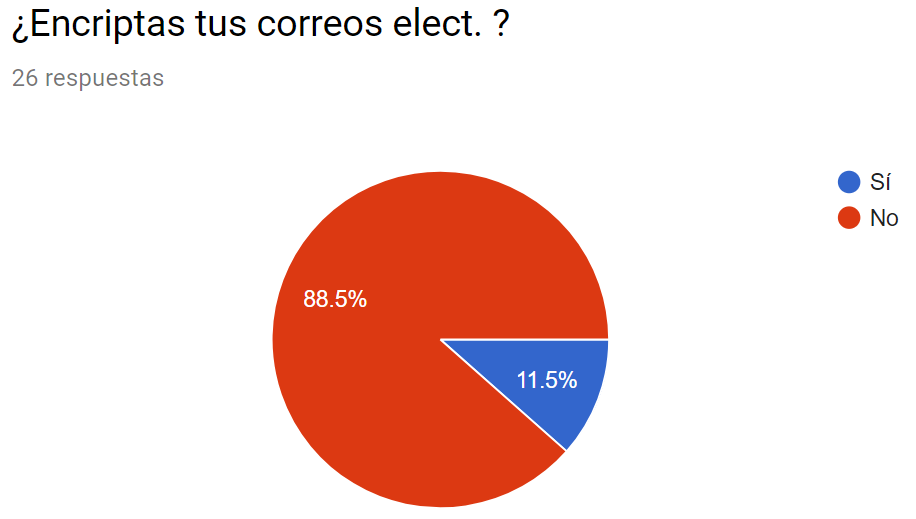
**Objetivo:** Determinar cuánto estudiantes utiliza VPN para transferir sus correos.



**Análisis:** Como podemos apreciar en la grafica solo un 4% de 26 estudiantes utilizan VPN como medida de seguridad para transferir sus correos.

**Pregunta 7:** ¿Encriptas tus correos electrónicos?

**Objetivo:** Determinar el porcentaje que los estudiantes encriptan sus correos electrónicos.



**Análisis:** Como se puede apreciar en los resultados obtenidos, el 88.5% de los encuestados no utilizan una encriptación para proteger sus correos electrónicos.

### 4.1.2 Resumen de la encuesta

Se ha determinado que de acuerdo a las estadísticas obtenidas en esta encuesta, se pudo concluir que la mayoría de los estudiantes de la Facultad de Sistemas tienen conocimientos acerca de las medidas necesarias de seguridad al utilizar un servicio de correo electrónico, además de los riesgos a los que están expuestos, más no adoptan estas medidas de prevención y seguridad.

## **4.2 Propuesta de solución**

En la elaboración del aplicativo como herramienta para sustentar como se puede garantizar seguridad en mensajes que se envíen por correo electrónico, se emplean librerías de encriptación / desencriptación desarrollados por usuarios expertos en el tema de la criptografía, estas ofrecen distintos métodos de encriptación como MAC, Encriptación Híbrida, Firmas digitales, etc. Estas librerías permiten que los mensajes cumplan con todos los parámetros de seguridad como confidencialidad, integridad o autenticidad, esto garantiza confianza al usuario aplicaciones para el envió de información por correo electrónico. El aplicativo emplea interfaces sencillas donde se insertara mensajes de texto y se procederá por medio de botones encriptar el mensaje.

Este proyecto por ser de ámbito para trabajar en un curso, no llega a tener un gran alcance por falta de tiempo pero se tiene pensado mejorar en un futuro.

# **Conclusión**

Al finalizar este proyecto de investigación, después de haber analizado los resultados obtenidos y relacionar toda la información, teniendo bien definida la situación actual propuesta en las preguntas de investigación, es así como se establece los resultados para cada una de estas interrogantes, las cuales están fundamentada en los resultados obtenidos en la encuesta de la investigación.

Como es inevitable que nos van a llegar correos no deseados, la primera y más importante medida a tomar siempre debe ser **utilizar el sentido común y no bajar la guardia:**

Sospechar de cualquier mail enviado con un asunto raro o inesperado, con un fichero adjunto de un tipo que no se espere, de un remitente del cual no esperemos un mail **aunque sea un contacto conocido**, en un idioma no habitual, con faltas de ortografía graves, o cualquier otro indicio de “no normalidad”.

# **Referencias bibliográficas**

**[1]** W. Hindriks. (2014, Ene.). Dispositivos de seguridad Cisco Email Security Appliance. Cisco. [En línea]. Disponible:https://www.cisco.com/c/dam/global/es\_es/pdfs/SEC17Q4Dispositivos-de-seguridad-Cisco-Email-Security-Appliance.pdf

**[2]** W. García. (2005, May.). Política de Seguridad en el Servicio de Correo Electrónico. Instituto Superior Politécnico José Antonio Echeverría. [En línea]. Disponible: http://www.criptored.upm.es/guiateoria/gt\_m189c.htm

**[3]** [H. Greevy](https://www.paubox.com/blog/author/hoalagreevy). (2016, Sep.). How Secure Email Works. Paubox. [En línea]. Disponible: https://www.paubox.com/blog/how-secure-email-works

**[4]** J. P. Corona. “.Seguridad”. Volumen 3, pp 1, Oct. 2009.

**[5]** D. Bergmingham. (2014, Oct.). Kapersky lab daily. Kapersky. [En línea]. Disponible: https://latam.kaspersky.com/blog/dar-prioridad-a-la-proteccion-de-cuentas-de-email-principales/4060/

**[6]** M. A. Mendoza. (2015, Oct.). welivesecurity. eset. [En línea]. Disponible: https://www.welivesecurity.com/la-es/2015/10/09/amenazas-frecuentes-correo-electronico/

**[7]** ANERR. (2015, Oct.). Amenazasporcorreo electrónico [En línea]. Disponible: http://www.anerr.es/2015/11/03/amenazas-por-correo-electronico/

**[8] Multicomp S.A.** (2017, Sept.). Seguridad de Correo electrónico altamente escalable y potente. [En línea].Disponible: http://multicomp.com.mx/seguridad-informatica/correo-electronico/

**[9]** globalsign (2016, Marzo.). Seguridad en el correo electrónico y el uso de firmas y cifrado [En línea]. Disponible: https://globalsign.seguridadamerica.com/docs/eBook.pdf

**[10]** Microsoft office (2016, Oct.). Protección contra amenazas [En línea]. Disponible: https://support.office.com/es-es/article/protecci%C3%B3n-contra-amenazas-en-office-365-b10023f6-f30f-45d3-b3ad-b71aa4aa0d58

**[11]** IBM knowledge center (2016, Oct.). Seguridad del correo electrónico [En línea]. Disponible: https://www.ibm.com/support/knowledgecenter/es/ssw\_ibm\_i\_61/rzaj4/rzaj45zoemail.htm

**[12]** teenvio. (2016, Dic.). Melissa el primer virus transmitido por el correo electrónico [En línea]. Disponible: https://www.teenvio.com/es/noticias/melissa-el-primer-virus-transmitido-por-correo-electronico/

**[13]** Universidad de Jaén. (2014, Oct.). Seguridad en el correo electrónico [En línea]. Disponible: https://www.uja.es/servicios/sinformatica/sites/servicio\_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%204.%20Seguridad%20en%20el%20correo%20electronico.pdf

**[14]** proofpoint. (2016, Oct.). Soluciones de seguridad de correo electrónico de la siguiente generación [En línea]. Disponible: https://www.proofpoint.com/es/solutions/next-generation-email-security

**[15]** Instituto Nacional de Ciber-Seguridad. (2015, Oct.). Medidas de seguridad de correo electrónico [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-correo-electronico