REPUBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

NIVEL DE LA SEGURIDAD QUE PERCIBEN LOS USUARIOS EN EL USO DE LOS SERVICIOS OFRECIDOS POR LA NUBE DE G-SUITE EN PANAMÁ

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Tutor: Erick A. Ramos Sánchez

Autor: Fernando Alfredo King Bernal

Ciudad de Panamá, enero de 2020

REPUBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

NIVEL DE LA SEGURIDAD QUE PERCIBEN LOS USUARIOS EN EL USO DE LOS SERVICIOS OFRECIDOS POR LA NUBE DE G-SUITE EN PANAMÁ

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Autor: Fernando Alfredo King Bernal

Ciudad de Panamá, enero de 2020

Ciudad de Panamá, 20 de noviembre de 2019

Profesor:

Nagib Yassir

Coordinador Comité de Titulación de Estudios de Licenciatura.

Presente.

En mi carácter de Tutor del Trabajo de Grado presentado por el Bachiller, Fernando Alfredo King Bernal, Cedula de identidad N.º [illegible], para optar al grado de Licenciado en Ingeniería de Redes de Comunicación, con énfasis en seguridad, considero que el trabajo: "**NIVELES DE SEGURIDAD QUE PERCIBEN LOS USUARIOS EN EL USO DE LOS SERVICIOS OFRECIDOS POR LA NUBE DE G-SUITE** en Panamá", reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

Erick A. Ramos Sánchez

Documento de identidad (Pasaporte), No.

Línea de Investigación: Ingeniería y sistemas de comunicación.

1) Agradecimiento

Primero que todo agradezco a Dios por permitirme estar aquí en este lugar culminando este escalón de mi vida ansiado por mucho tiempo.

A mis padres Zoraida de King y Alfredo King por inculcar en mí la educación y guiarme en el buen camino.

Mi hermana Muriel que indirectamente a hecho que yo siga adelante demostrando le el buen camino y las ganas de superación que una persona puede tener para mejorar su vida sin importar la edad.

Al profesor y rector de la UNICYT Williams Núñez que en algún momento de mi transcurrir por la Universidad llegue a él, el cual me apoyo incondicionalmente. También agradezco el potencial que vieron 2 profesores en mí, El profesor Erick Ramos, Buena persona, excelente Docente y lo principal que cree en sus estudiantes Hoy profesor le Digo Gracias…

El Profesor Nagib Yassir, sí, también tengo estas líneas para usted y le digo Gracias por su tiempo sus consejos de Vida personal que pudimos conversar en algún momento.

Por último y no menos Importante a esas personas que hicieron más divertida esta trayectoria a mis Compañeros de clase esos que aguantaron mis loqueras que soportaron que les pidiera alguna tarea y que también vieron en mi a una persona o profesional que les podía dar la mano cuando ellos más lo necesitaran gracias, chicos esto también es por ustedes.

Hay muchas personas a quien también debo darle gracias, pero ellos saben quiénes son y si menciono nunca terminare mi lista a todos Gracias…

ÍNDICE GENERAL

Contenido

INDICE DE FIGURAS

REPUBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

NIVEL DE LA SEGURIDAD QUE PERCIBEN LOS USUARIOS EN EL USO DE LOS SERVICIOS OFRECIDOS POR LA NUBE DE G-SUITE EN PANAMÁ

Autor: Fernando Alfredo King Bernal
Tutor: Erick A. Ramos Sánchez
Año: 2020

2) RESUMEN

La sociedad viene adoptando gradualmente las tecnologías de la información y la comunicación, así, la brecha digital tiende a disminuir. La seguridad informática ocupa un lugar importante de atención en el proceso e inspira el propósito fundamental de esta investigación: determinar el nivel de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá. Otros sistemas y aplicaciones, que aparte de la seguridad propia de la plataforma, brindan una protección adicional para disminuir los riesgos del tratamiento de la información, también son considerados. Enmarcada en un paradigma Cuantitativo, ésta es una investigación descriptiva con un modelo de investigación de campo, donde se determinaron los diferentes niveles de seguridad y delimitaron falencias que presentan los usuarios en el manejo de la información que se sube a la nube, sin un nivel de protección (texto plano). La teoría adoptada es la racional tecnológica, también denominada hipotético-deductiva. Para ello se tomó una muestra aleatoria y se utilizó como técnica de investigación la encuesta y como instrumento el cuestionario, el cual fue aplicado en línea a los usuarios. Finalmente se organizó y analizó la información recabada y se llegó a la conclusión de que muchos desconocen el tipo de tecnología

en la que están almacenando su información, es decir, la nube, pero las características de seguridad dependen en gran medida de las decisiones que tomen los usuarios. Asi mismo, es necesario impulsar el reconocimiento de las tecnologías basadas en la nube como un motor del desarrollo social y económico del país.

Descriptores: Computación en la Nube, Nube G Suite, Seguridad informática, Percepción de la seguridad, Complementos de seguridad en la Nube.

REPUBLIC OF PANAMA
INTERNATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF COMPUTATION AND TECHNOLOGY SCIENCES

LEVEL OF SECURITY PERCEIVED BY USERS IN THE USE OF THE SERVICES OFFERED BY THE CLOUD OF G-SUITE IN PANAMA

Author: Fernando Alfredo King Bernal
Tutor: Erick A. Ramos Sánchez
Year: 2020

3) ABSTRACT

Society has been gradually adopting information and communication technologies, so the digital divide marks a tendency to diminish. Computer security occupies an important place of attention in the process and inspires the fundamental purpose of this research: to determine the level of security that users perceive in the use of the services offered by the G Suite cloud in Panama. Other systems and applications, which apart from the platform's own security, provide additional protection to reduce the risks of information processing are also considered. Framed in a Quantitative paradigm, this is a descriptive investigation with a field research model, where the different levels of security were determined and defined shortcomings that users present in the management of information that is uploaded to the cloud, without a level of protection (plain text). The theory adopted is the rational technology, also called hypothetical-deductive. For this, a random sample was taken and the survey was used as a research technique and as an instrument the questionnaire, which was applied online to users. Finally, the information collected was organized and analyzed and it was concluded that many are unaware of the type of technology in which they are storing their information, that is, the cloud, but the security features depend largely on the decisions

they make. the users. Likewise, it is necessary to boost the recognition of cloud-based technologies as an engine of the country's social and economic development.

Descriptors: Cloud Computing, Cloud G Suite, Computer Security, Security Perception, Cloud Security Add-ons.

4) INTRODUCCIÓN.

En la última década, la seguridad se ha convertido en uno de los grandes problemas en el uso de las tecnologías, y es uno de los aspectos más relevantes y críticos actuales. A pesar de que se invierten cuantiosas sumas de dinero, la fragilidad en la seguridad de la información, va en aumento cada día en las diferentes fuentes de comunicación e información. Sin embargo, a pesar de la seguridad de estos sistemas, los datos, aplicaciones y servicios que se implantan en ellos no siempre están seguros y siguen siendo un objetivo atractivo para individuos y hasta organizaciones con intereses ocultos, desde curiosos, ciber terroristas y hasta organizaciones tanto públicas como privadas.

En este estudio, se analizó la percepción de los usuarios, tanto los comunes como los corporativos, con respecto a los niveles de seguridad en el uso de los servicios que se ofrecen a través de la nube de G-suite, en Panamá. En entornos de Servicios en la nube o aplicación de redes sociales, muchas de estas utilizadas a diario. El problema radica en la seguridad y ciberseguridad, en las clases de servicios y tipos de seguridad en las aplicaciones, como también sobre las mejores prácticas de cómo generar contraseñas seguras, validar bien lo que se postea en las redes o Drive de G-suite. La información se organizó en cuatro capítulos distribuidos de la manera siguiente:

En el Capítulo I se describe la problemática que motivo este trabajo relacionado con la seguridad en la nube y particularmente con la Nube de G-suite. También, se formula la pregunta de investigación y se presentan los objetivos de esta pesquisa, dirigidos a determinar los niveles de seguridad percibidos y de qué forma los usuarios utilizan las diferentes aplicaciones, dispositivos y procedimientos para resguardar y preservar la información, así mismo, se justifica la relevancia del desarrollo de esta investigación.

En el Capítulo II se presentan los antecedentes de la investigación, así como las bases teorías relacionadas con el problema planteado. Se incluyen los problemas relacionados con la ciberseguridad, las características en el uso de la nube, los niveles de seguridad, algunas de las aplicaciones virtuales que se utilizan con más frecuencia para disminuir los riesgos y herramientas para incrementar la seguridad.

El capítulo III, se describen los elementos de la metodología empleada para el desarrollo de esta investigación, el tipo de investigación en la que está enmarcado el trabajo, las técnicas utilizadas, instrumento y los procedimientos para recabar, tabular y analizar la información.

En el Capítulo IV se detallan los resultados y se analizan los mismos para llegar a las conclusiones. También se presentan recomendaciones que podrían coadyuvar favorablemente en la seguridad de la información en la nube y en los distintitos dispositivos a los cuales se tiene acceso.

5) CAPITULO 1. PLANTEAMIENTO DEL PROBLEMA

1) 1.1 El problema.

La seguridad es uno de los aspectos más relevantes y críticos para las tecnologías dependientes de las redes de comunicación y en la que los proveedores de servicios en la nube o cloud service providers más han hecho énfasis. Compañías como IBM, Amazon, Oracle, Google, o Microsoft dedican enormes sumas de dinero para proteger las infraestructuras con las que prestan sus servicios o las que las empresas contratan a terceros en plataformas en la nube como Azure, Google Cloud o AWS. Sin embargo, a pesar de la seguridad de estos sistemas, los datos, aplicaciones y servicios que se implantan en ellos no siempre están seguros y siguen siendo un objetivo atractivo para los atacantes, desde curiosos hasta ciber terroristas y gobiernos con intereses diversos.

Panamá es un polo de desarrollo regional, con un importante centro bancario y un gran potencial para liderar el progreso en la región de Centroamérica y el Caribe, por lo tanto, es de gran interés el estudiar el nivel de seguridad en el uso de la computación en la nube en Panamá, para garantizar en la mayor medida posible la estabilidad de las operaciones.

La computación en la nube es un servicio de valor agregado novedoso, basado en las tecnologías de la información y la comunicación (TIC) que permite a los usuarios acceder a un conjunto de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma escalable, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado, o incluso gratuitamente.

La Cloud Security Alliance (CSA), De Blas (2018), ha expuesto que existen al menos 12 vulnerabilidades muy importantes a las que siguen expuestas las organizaciones que hacen uso de la computación en la nube como plataforma de trabajo y a las que hay que tomar previsiones: Violaciones de datos; Gestión de la identidad y los accesos deficientes; APIs inseguras; Vulnerabilidades de los sistemas; Robo de cuentas; Ataques desde el interior; Amenazas persistentes avanzadas (APT); Pérdida de datos; Análisis de riesgos insuficiente; Abuso y uso nefasto de servicios. Cloud; Ataques de

denegación de servicio (DoS); Vulnerabilidades por tecnologías compartida. CSA citado por De Blas (04/09/2018)

Es por ello que, a través de esta investigación se pretende abordar el estudio de Seguridad en el uso de la nube de G Suite en Panamá

2) **1.2 Formulación del Problema**

¿Cuál es el nivel de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá?

3) **1.3 Objetivos:**
4) **Objetivo General:**

Determinar el nivel de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá.

5) **Objetivos específicos.**

1. Identificar las aplicaciones utilizadas en la nube G Suite.
2. Describir aplicaciones virtuales que se utilizan para la disminución de riesgos de fuga de información y Acceso en la nube de G Suite a nivel de Empresas.
3. Desarrollar una encuesta que permita capturar el nivel de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá.
4. Analizar el nivel de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá.

6) 1.4 Justificación

La importancia de este trabajo radica en la pertinencia del tema en la actualidad, donde una considerable cantidad de información se maneja en la nube con algunos niveles de seguridad. Tanto las empresas, como los usuarios han tenido la necesidad de poner a su alcance información sin depender de un dispositivo (Móvil o Pc) único o lugar específico. Guardar o compartir sus datos a buen resguardo y manteniendo accesibilidad de estos en cualquier momento. Compartir contenido digital de forma rápida e instantánea, toda vez que, al mismo tiempo los soportes “físicos” están menos accesible o limitados en sus capacidades de Manejo de archivos.

El uso de la nube se ha convertido en una solución eficiente para compartir archivos sin necesidad de contacto físico entre las personas, aunque parezca una contradicción, la nube es una solución de almacenamiento en red muy social, tanto que incluso proveedores como Dropbox se han integrado totalmente en Facebook, la red social más popular. Además, su uso es una tendencia en crecimiento.

En tal sentido, Dropbox es uno de los servicios en la nube de uso habitual entre los usuarios de dispositivos móviles y PCs, con acceso a más de 5GB de almacenamiento gratuito para compartir fotografías y vídeos a distancia, ya sea a través de correo electrónico o Facebook. La nube da confianza a aquellas personas preocupadas por tener un sitio seguro donde poder almacenar información más susceptible de ser perdida o deteriorada.

La importancia, hoy por hoy, de las aplicaciones en la nube, como G Suite, es que su uso se ha convertido en una tendencia creciente, ya que brindan a los usuarios múltiples opciones, tanto en la parte de comunicación con herramientas para chats, meeting con otras personas en tiempo real, manejo de información compartida de forma segura entre las personas involucradas y la modificación de la misma en tiempo real sin tener presencia en un solo lugar, sino a través de la inmensa nube que es G Suite desde cualquier parte del mundo.

6) CAPÍTULO II. MARCO TEÓRICO

1) Antecedentes de Investigaciones.

Para Fernández, Pascal. (2018), en su resumen ejecutivo, señala que, “actualmente las TIC han producido un desarrollo exponencial en todos los campos a nivel nacional e internacional, las TIC hoy en día se ha convertido en una Herramienta eficaz en el desarrollo organizacional de todas las empresas.

Actualmente en el mercado mundial las empresas que no están preparadas para los cambios tecnológicos están destinadas a extinguirse en el ámbito empresarial.

El desarrollo del presente trabajo se enfoca en el análisis de la percepción de la Suite empresarial de Google “G Suite” como solución tecnológica en los negocios Empresariales. Con esta solución, las empresas no tienen que asumir los costos de mantener una infraestructura de comunicaciones y el esfuerzo que supone instalar y mantener una plataforma tecnológica en sus propias instalaciones reduciendo los costos de TI, obteniendo un gran ahorro económico para la empresa”.(http://repositorio.utp.edu.pe/handle/UTP/1486)

Antecedentes Históricos.

Según el trabajo de Larios, “La computación en la nube ha recorrido un largo camino desde que fue marcada por primera vez como una perspectiva de futuro por parte de algunos investigadores. La historia inicial de la computación en nube nos lleva a finales del siglo veinte, cuando la prestación de servicios de computación comenzó. Sin embargo, el concepto se remonta a J.C.R. Licklider y John McCarthy”.

El término “nube” se utiliza como una metáfora de Internet, basado en el dibujo de nubes utilizado en el pasado para representar a la red telefónica, y más tarde para representar a Internet en los diagramas de red de computadoras como una abstracción de la infraestructura subyacente que representa.

El cloud computing, o computo en la nube es una evolución natural de la adopción generalizada de la virtualización, la arquitectura orientada a servicios y utilidad del

cómputo. La idea básica es que los usuarios finales ya no necesitan tener conocimientos o el control sobre la infraestructura de tecnología “en la nube” que los apoya, sino que el usuario se dedica a su trabajo, a su negocio y otra organización (el proveedor de los servicios en la nube) se encarga de mantener la plataforma tecnológica y su actualización, disminuyendo los costos, que se comparten entre los distintos usuarios que contratan los servicios.

El concepto básico de la computación en nube o cloud computing se le atribuye a John McCarthy – responsable de introducir el término “inteligencia artificial”. En 1961, durante un discurso para celebrar el centenario del Massachusetts Institute of Technology (MIT), fue el primero en sugerir públicamente que la tecnología de tiempo compartido (Time-Sharing) de las computadoras podría conducir a un futuro donde el poder del cómputo e incluso aplicaciones específicas, podrían venderse como un servicio (tal como el agua o la electricidad). Esta idea de una computadora o utilidad de la información era muy popular en la década de 1960, incluso algunas empresas comenzaron a proporcionar recurso compartidos como oficina de servicios – donde se alquilaba tiempo y servicio de cómputo. Boxbyte (2012)

2) Historia de Google

(Febrero 11, 2017 por Historia y Biografía

“La historia de Google inicia en 1995 cuando Larry Page y Sergey Brin se conocen en la Universidad de Stanford, para aquellos días Larry tiene 22 años y ha finalizado sus estudios de Ingeniería Eléctrica en la Universidad de Michigan. Se plantea estudiar en Stanford, y Sergey, de 21 años, es el encargado de enseñarle el campus. Para este entonces Larry y Sergey no logran coincidir en nada”.

(**Febrero 11, 2017 por** Historia y Biografía) Un año después (1996) Larry y Sergey participan en un programa de posgrado en Informática en Stanford y empiezan a colaborar en el desarrollo de un motor de búsqueda para su tesis, a este buscador le dan el nombre de BackRub, este se utiliza en los servidores de Stanford durante más de un año, pero finalmente la Universidad deja de emplear este motor porque requiere demasiado ancho de banda.

Para 1997 Larry y Sergey descubren que el motor de búsqueda BackRub necesita renombrarse, es entonces donde luego de un «brainstormimg» se deciden por Google**.** El origen de la palabra Google se debe a un juego de palabras con el término matemático *«gúgol»***,** cuya pronunciación en inglés es similar a la de «Google» y que se refiere al número uno seguido de cien ceros. La elección del término se basa en el objetivo pretensioso de Larry y Sergey de organizar una cantidad aparentemente infinita de información en la Web.

Para agosto de 1998 Larry y Sergey presentaron ante Andy Bechtolsheim, cofundador de Sun Microsystems, su idea de motor de búsqueda, Andy se vio interesado, sin embargo, pronto les manifestó su necesidad de escabullirse para otra reunión, eso sí, les ofreció extender un cheque, en ese entonces no se veía dicha oferta como una promesa esperanzadora. Sin embargo, días después, Andy extiende un cheque por valor de 100.000 dólares para una entidad que aún no existe: una empresa llamada Google Inc.

«Los 25 millones de páginas actualmente catalogados parecen ser buenas opciones, el sitio tiene una extraña habilidad para devolver resultados muy relevantes. ¡Hay mucho más por venir en Google!, Pero incluso en su forma de prototipo es un gran motor de búsqueda.» (Pc Magazine-1998)

El crecimiento de Google era frenético, ya la oficina del garaje se queda pequeña y en febrero de 1999 Google se traslada a un nuevo local en el 165 de University Avenue en Palo Alto (California), con una plantilla compuesta únicamente por ocho empleados. En abril del mismo año llega un cálido miembro al grupo de Google, se trataba de Yoshka, el primer perro «de la empresa», el cual se incorpora junto con el vicepresidente sénior de operaciones, Urs Hoelzle**.**

Para mayo de 1999 Google incorpora a su primer empleado no ingeniero, Omid Kordestani, el cual ingresa a trabajar en el departamento de ventas. En su primer comunicado de prensa, Google anuncia una inyección de capital de 25 millones de

dólares procedente de Sequoia Capital y de Kleiner Perkins. John Doerr y Michael Moritz se incorporan a la junta directiva. En el comunicado se cita a Moritz, que utiliza el término «Googlers» para referirse a las personas que utilizan Google.

3) **Ciberseguridad en Panamá**

(Ciudad del saber noviembre 18, 2019) "La llegada de nuevas tecnologías ha contribuido al desarrollo de las organizaciones dentro del ecosistema digital. La información se intercambia cada vez más a través de medios digitales, y en un corto plazo miles de dispositivos tanto hogareños como corporativos se conectarán mediante Internet de las cosas (IoT), la nube, y la Inteligencia Artificial (IA)…Un Estudio sobre Tendencias en gestión de ciber riesgos y seguridad de la información en América Latina y Caribe 2019, de Deloitte, muestra que 4 de cada 10 organizaciones sufrieron un incidente de ciberseguridad en los últimos 24 meses. Solo el 31% de las empresas consultadas por la firma asegura contar con capacidades limitadas de monitoreo de ciberseguridad e inteligencia de amenazas.

"Con el avance de la conectividad de las personas y de las cosas (IoT) y el uso creciente de los datos se incrementan los ataques y vulnerabilidades, por lo que las organizaciones deben de seguir los pasos correctos para gestionar un camino seguro a su digitalización y que no cause riesgos para su información", expresó Eli Faskha, CEO de Soluciones Seguras.

Las amenazas se mantienen en constante evolución, sobre todo porque en los dispositivos se almacena información crítica que nos hace más vulnerables a los ciberataques, entre ellas se encuentran el malware, Ransomware, ataques de phishing (robo de información) y ataques DDoS."

En el marco de la celebración del Día Internacional de la Seguridad de la Información, que tendrá lugar el próximo 30 de noviembre, Soluciones Seguras brinda consejos prácticos que ayudarán a gestionar la información de forma segura y evitar que sea víctima de los ciberdelincuentes:

Para Alvarado, C. (2018). “En lo que respecta a Panamá, vocero de Frontera Security, advirtió que la mayoría de las empresas no cuentan con el personal y la tecnología adecuada para proteger su información en los diferentes estados donde se procesa y se utiliza. Según el especialista, “en Panamá nos encontramos en un nivel de madurez muy básico en temas de ciberseguridad”. En el 2017 Se incrementaron en un 35% los ataques de malware en el mundo. “Panamá necesita tomar medidas drásticas y urgentes para garantizar la seguridad de la información tanto en la empresa privada como en el Gobierno”.

En recientes estudios realizados sobre el uso y los servicios de la nube, se ha venido observando algunas ventajas y desventajas que debe tener presente al momento de ingresar: Google Apps for Works. (2017)

Para Sonia Duro Limia (enero, 2018). El almacenamiento en la nube es una traducción que hacemos directamente en inglés “cloud storage”, con esto se refiere, que mediante el permite guardar y gestionar datos en internet, proveniente de dispositivos no conectados. En ellos se pueden almacenar, varios tipos de archivos, tales como:

- Fotografías.
- Documentos.
- Copias de seguridad de correos electrónicos.
- Datos confidenciales de empresas, etc.

4) **Características del almacenamiento en la nube.**

- Subcontratados por empresas o particulares, es decir, gestionados por terceros.
- Son escalables, para poder adaptarse a las necesidades particulares de la empresa o particular en cada momento de su evolución.
- Accesibles desde cualquier lugar, con usuario y password
- Algunos proveedores de cloud storage, disponen de una de una versión gratuita y otra de pago.

Entre los diferentes tipos de cloud storage, encontramos tres (3) tipos:

1.- Nube pública

Esta opción suele ser gratuita por parte de los proveedores y está pensada para aquellos que no disponen de presupuesto.

2.- Nube privada

Está opción no está abierta al público en general y detrás de ella hay un sistema de seguridad más fuerte que en la pública.

3.- Nube híbrida

Es una mezcla de las dos anteriores, por lo que es más flexible y puede ser una buena opción si no requieres de demasiado espacio.

Durante la mayor parte del siglo XX, se utilizaban para guardar información, música, por ejemplo, el vinilo, el video cassette y el cassette para grabar y almacenar música, estos ocupan espacios y debías tenerla de manera física, para poder verlas y oírlas. Por otra parte, estas cintas, tienen enormes desventajas, comparadas al almacenamiento actual, algunas de ellas:

- Tiene una limitada capacidad de información.
- Ocupan espacio en tu PC.
- Pueden corromperse y son vulnerables ante los virus.
- La limitación de la memoria de tu PC ralentiza tu acceso a ellos.

El almacenamiento en la nube se convirtió en una panacea, ya que se puede:

- Contratar tanto espacio como requieras.
- Liberar más espacio en el PC o en los servidores.
- Mejores antivirus que el PC personal o el de la empresa.
- La memoria del PC puede trabajar más rápido, si así se desea.

El almacenamiento en Internet y las redes inalámbricas dan respuesta a las necesidades actuales de empresas y usuarios particulares. Trabajar en remoto y poder acceder a tus contenidos en cualquier momento y en cualquier lugar, ofrece una libertad y autonomía de trabajo de la que no hemos dispuesto antes.

Otras ventajas del almacenamiento en la nube:

1.- Es un sistema muy social

Aunque parezca una contradicción, poder subir tus contenidos a Dropbox, por ejemplo, sin necesidad de tener delante a la persona con quién quieres compartirlo.

2.- Permite la conciliación familiar

Si eres una empresa, el almacenamiento en la nube te permite eliminar los tiempos muertos de tus empleados, así como los desplazamientos o mañanas desaprovechadas con idas y venidas por enfermedades en la familia.

3.- Mejora la seguridad de tus documentos

Un proveedor de almacenamiento en la nube tiene mejores sistemas de seguridad y además, más actualizados.

La ciberseguridad es cada vez más importante para las personas y empresas, este sistema permite eliminar un esfuerzo que no es productivo en la actividad profesional o empresarial.

5) **4.- El almacenamiento en la nube no se daña.**

El uso de los USB, los discos duros se desactualizan, los PCS se tienen que renovar en un tiempo corto y los servidores se saturan. En cambio, la nube, siempre está disponible, ya que el proveedor se encarga de actualizar el software y/o el antivirus.

5.- Los contenidos disponibles para acezar cuando y desde donde se desee. Para su funcionamiento, lo que se necesita es una conexión a internet, y se puede trabajar fuera de la oficina o mientras se viaja.

6.- Facilita el trabajo en equipo

La facilidad de poder compartir un mismo documento entre un grupo de personas facilita la cooperación y ayuda a la creación de contenidos.

7.- Evita la dispersión de contenidos

Tener un único lugar en el que almacenar todos los contenidos que manejas, ahorra tiempo en buscarlo y ayuda a organizarlos.

7) Niveles de servicios que ofrece al proveedor.

El cómputo en la nube se puede dividir en tres niveles en función de los servicios que ofrecen los proveedores. Desde el nivel más interno hasta el más externo se encuentran: Infraestructura como Servicio, Plataforma como Servicio y Software como Servicio.

Según Conde Graphics. (Jul 5, 2017), el Ahorro en costos ha sido comprobado, Las aplicaciones web de colaboración y mensajería de Google no requieren la instalación de ningún hardware ni software y, además, solo necesitan un mantenimiento mínimo. Gracias a eso, las empresas pueden ahorrar mucho tiempo, además de costos de equipamientos técnicos.

A medida que los usuarios finales realizan la transición a Gmail y a Google Calendar, podrán usar la interfaz de Microsoft Outlook que ya conocen para las funciones de correo electrónico, contactos y calendario.

Capacidad de almacenamiento 50 veces mayor al valor promedio del mercado. Cada empleado cuenta con hasta 30 GB para almacenar mensajes de correo electrónico, lo que les permite conservar los mensajes importantes y encontrarlos inmediatamente gracias a la incorporación de la búsqueda de Google.

Gmail está diseñado para que los empleados dediquen menos tiempo a la administración de sus bandejas de entrada y puedan ser así más productivos. Gracias a las funciones disponibles para ahorrar tiempo, como el agrupamiento de mensajes en conversaciones, las etiquetas de los mensajes, la opción de búsqueda rápida de mensajes y el potente filtro antispam, los empleados pueden trabajar en forma eficiente con un gran volumen de correo electrónico.

Acceso a aplicaciones de Mensajería, calendario y correo electrónico para Smartphone.

Gracias a la variedad de opciones que tienen los empleados para acceder a la información cuando están fuera de la oficina, su productividad no disminuye con G Suite a pesar de que no se encuentren en su lugar de trabajo.

G Suite admite el acceso inalámbrico para Smartphone en los dispositivos BlackBerry, iPhone, Windows Mobile, Android y en teléfonos de menor potencia. Conde Graphics. (Jul 5, 2017)

(Gallego, 2019)**"**Panda Security recomienda a las empresas que adopten un enfoque integral de protección IoT que contemple actualizaciones, redes cifradas y soluciones de seguridad avanzada en las plataformas y software"**.**

(Mónica Gallego 28 agosto, 2019) "La gran mayoría de las empresas (93%) considera que no están lo suficientemente preparadas para afrontar los desafíos de ciberataques que plantea el Internet de las Cosas (IoT). Además, un 46% considera que necesita formación o talento complementario para abordar todos los aspectos de ciberseguridad. Prueba de ello, es que ocho de cada 10 organizaciones habrían recibido algún tipo de ciberataque en sus dispositivos IoT en el último año.

Estos son algunas de las principales conclusiones del informe Global Connected Industries Cybersecurity Survey de la compañía Irdeto, que refleja la preocupación de muchas empresas con esta tecnología, en especial en sectores como el industrial, el sanitario y el de transporte.

En este sentido, el IoT es un factor más de la digitalización que hace que las organizaciones sean cada vez más distribuidas: los dispositivos IoT forman parte de un nuevo ecosistema que, junto con otras tendencias entre las organizaciones como el teletrabajo y el BYOD, pueden ir más allá del perímetro de la empresa y aumentan la superficie de ataque, haciéndolas más vulnerables."

8) Aplicaciones virtuales de seguridad en la nube.

Algunas aplicaciones virtuales que nos permiten tener más protegido nuestros servicios en la nube o disminuir el riesgo de ellos en la Internet

Netskope: Herramienta que permite Asegurar la nube, permite obtener información y Visibilidad de todo lo referente a Políticas de Archivos adjunto dentro de Gsuite y Office 365.

Absolute: le brinda un enfoque radicalmente nuevo a la ciberseguridad mediante la habilitación de la seguridad de autor recuperación de terminales, permite cifrar el equipo no solo los discos desde cualquier parte del mundo donde se encuentre y con la Geolocalización se pueden encontrar la ubicación del mismo.

Stegano safe: (Juan Manuel Muñoz 25 mayo, 2016) "Es una herramienta que precisamente nos ayuda a cifrar nuestros datos y a prevenir su acceso no autorizado si llegamos a ser víctimas robos o pérdidas de información".

9) Herramientas para aumentar la seguridad y privacidad en Google Drive

La seguridad y privacidad, para **Jiménez, Javier (2018),** son dos aspectos vitales para los usuarios de Internet. Constantemente estamos expuestos a posibles problemas que pongan en riesgo estos dos pilares. Son muchos los servicios online, páginas, registros, que visitamos cada día. Poner hincapié en preservar nuestros datos es muy importante. En relación a Google Drive, es una plataforma que cuenta con muchos usuarios en todo el mundo y donde nuestros datos pueden sufrir algún tipo de ataque si no tenemos cuidado. Vamos a nombrar 3 herramientas interesantes para aumentar la seguridad y privacidad en este servicio de Google.

Google Drive utiliza su propio sistema de cifrado para proteger los archivos. Usa AES-256 para las transferencias y AES-128 para cifrar los archivos subidos. AES es un estándar bastante seguro y extendido, sin ataques en la actualidad. Esto significa que nuestros archivos, al menos sobre el papel, van a estar seguros.

Esto significa que ciframos los archivos en nuestro equipo, antes de enviarlos, y de esta manera la seguridad aumenta. Hay herramientas interesantes que pasamos a explicar.

Cryptomator es una de las herramientas más populares. Cuenta con versión gratuita y es de código abierto. Es muy sencillo de utilizar y funciona para los principales sistemas

operativos como Windows, macOS, Linux y también para dispositivos móviles, aunque en este caso el programa no es gratuito (iOS y Android).

Boxcryptor

Javier Jiménez (27 de junio, 2018) Otra herramienta para cifrar archivos en Google Drive es Boxcryptor. Nuevamente estamos ante un servicio gratuito, aunque tiene limitaciones a no ser que adquiramos la versión Premium. En este caso no estamos ante un software de código abierto.

Javier Jiménez (27 de junio, 2018) Boxcryptor crea una unidad virtual en el sistema. Una vez hecho esto agrega automáticamente cualquier proveedor de la nube a la unidad. La unidad Boxcryptor actúa como una capa adicional sobre los archivos que tengan los usuarios. Nos permite ver, editar y guardar los archivos cifrados sobre la marcha.

El programa cifra los archivos que se encuentren dentro de la unidad de manera automática. También los futuros que se agreguen.

Rclone with Crypt

Rclone with Crypt es la tercera de las herramientas para aumentar la seguridad y privacidad en Google Drive de las que hablamos. Se trata en esta ocasión de un programa de línea de comando que sincroniza archivos y directorios desde Google Drive, aunque también una larga lista de otros servicios.

Se trata de una herramienta de código abierto y permite a los usuarios tener un gran control y personalización al sincronizar los archivos en la nube. Nos permite cifrar los archivos en el equipo antes de subirlos a Drive. Javier Jiménez. (27 de junio, 2018)

10) Niveles de seguridad en plataformas como Gmail. ¿Cuáles son las medidas de seguridad que ofrece Gmail?

11)Medida 1: Una buena contraseña

Una contraseña de acceso a un Sistema en este caso Gmail debe ser robusta con una combinación de letras y números con símbolos estas contraseñas son más robustas a la hora de un ataque de fuerza bruta.

"En general, usa siempre estas pautas:

1. Tu contraseña debe tener al menos 8 caracteres
2. Debe tener letras y números mezclados
3. Debe tener minúsculas y mayúsculas mezclados
4. No debe hacer relación a tu nombre, el nombre de tus familiares o a fechas de nacimiento etc.
5. Nunca la escribas en un papel, libreta, pizarra o programa de computadora, siempre debe estar en tu cabeza" (Alejandro Águila S/F)

Medida 2: Colocar un número telefónico, ayuda a validar o detectar cuando traten de robar tus credenciales como segunda medida sería validación oral con el usuario.

Medida 3: Una o varias direcciones de otros correos donde puedan contactarte La opción es suministrar 1 o varias casillas de correo adicionales a tu Gmail que permitirán verificar tu identidad y volver a tener acceso a tu cuenta de Gmail. En este sentido Google te acepta que coloques otras direcciones de Gmail o direcciones de otros proveedores para que sean usadas como mecanismo de validación.

Medida 4: Una pregunta secreta. Finalmente, Gmail te permite escoger entre muchas preguntas personales predefinidas o crear una propia y llenar la respuesta correcta, de esta manera, sabiendo la respuesta a la pregunta secreta podrán confirmar que se trata de tu persona y no de un hacker.

12) Seguridad informática para la empresa con Google Drive

Publicado el (24 de octubre, 2018) “La información es poder. Eso es algo que toda empresa debe tener como un principio básico y la empresa no debe ser la excepción. Todo el tiempo trabajas con información tanto interna como de tus clientes para las actividades cotidianas de la empresa, por lo que un pequeño error en el flujo de información puede ser perjudicial para toda la organización.

Es por ello que invertir en seguridad informática que proteja los datos que se almacenan constantemente y que garantice que estarán disponibles para cualquier movimiento que se realice. "Seguridad Informática" se refiere a todo el conjunto de medidas que se toman para conservar la integridad de la información. En este caso, es sumamente necesario que se conozcan todos los posibles riesgos a los que está sujeta la información de la empresa para poder adoptar las medidas pertinentes.

Optar por una Solución en la nube. Como Google Drive, permite tener Disponibilidad e integra 2 de los Pilares importantes en la Seguridad de la información.

(Anónimo, 2019) “Las nuevas tecnologías le permiten almacenar grandes cantidades de información. Esto es una gran ventaja debido al crecimiento que puede experimentar su empresa”.

Es aquí donde es necesario considerar herramientas de seguridad informática que puedan brindar la posibilidad de respaldar su información, que se almacene en sitios libre de riesgos. Así, la información empresarial estará disponible en todo momento y contarás con la certeza de que t datos y la información de la misma, estarán seguras”.

13)Beneficios para la empresa.

El principal beneficio es la tranquilidad de que la información no se perderá y se mantendrá de forma íntegra todo el tiempo. Y por eso es importante saber cuáles son las herramientas de seguridad informática disponibles en el mercado y las características principales de estas.

1) **Google Drive**

“Es una herramienta útil para el almacenamiento de datos en grandes cantidades. Al ser un servicio de **Google**, toda la plataforma de **G Suite** estará integrada, por lo que será conveniente a la hora de almacenar archivos que estén igualmente pensados para esta plataforma, lo que permitirá trabajar desde la misma entre varios colaboradores”. Publicado el (24 de octubre, 2018)

Google Drive Business y Enterprise Brinda espacios ilimitados para el alojamiento de la información y su dominio empresarial.

Google tiene una infraestructura grande y poderosa, con varios centros de datos (datacenters) a nivel global propiedad de **Google** y servidores diseñados Para garantizar la seguridad de esta.

2) **Transferencias y envíos de datos seguros**

La transferencia de datos en G-suite puede ser controlado por herramientas externas bajo sus propias reglas y lineamientos de acceso. Una de esta es el Netskope, herramienta que te permite editar las políticas de envió de información a través de las cuentas de correo de Gsuite esto es una de las principales ventajas que pueden tener al colocar sus servicios en la nube.

En este sentido, la seguridad informática que ofrece G Suite está basada en políticas estrictas y sistemas de verificación de la identidad para que solo el usuario y sus colaboradores puedan acceder a la información. Para los contenidos empresariales se pueden agregar sistemas externos como Access Manager, que controlan y autentican los login con los servidores internos de Active Directory.

Adicionalmente, Permite trabajo colaborativo ya que contiene la herramienta de Google Docs. Que le permite en tiempo real desde cualquier parte del mundo interactuar con el documento, ya sea en una reunión y desee cambiar algo a la presentación en vivo puede realizarlo y se muestra en el documento la modificación que realiza.

Sin embargo, existen otros servicios y herramientas para utilizar al momento de transferir archivos, como las redes sociales o las intranets. Mientras que las redes sociales también ofrecen la ventaja de que los archivos pueden ser consultados en cualquier lugar, las intranets solo funcionarán dentro de las instalaciones de la empresa. La ventaja de las intranets es que solo el usuario tendrá acceso y control sobre toda la información.

También, Google Drive, a pesar de ser un servicio en línea, le permite la administración de la información, Google solo coloca el servicio y asegura la disponibilidad de la misma, pero le otorga al usuario la potestad de la administración, es decir que el usuario es el que indica quien tiene acceso a la información y puede colocar horas de visualización y parámetros que minimicen el riesgo de la misma. Muchas veces le permite, para dispositivos móviles, crear perfiles de trabajo donde puedes acceder a la información, procesarla, pero no transferirla a otro correo que no sea del mismo dominio o incluso hacer en el dispositivo móvil una captura de pantalla.

3) Desarrollo de aplicaciones para flujos de trabajo

“Finalmente, otra de las ventajas de utilizar **G Suite** en las versiones **Enterprise** y **Business** es la incorporación de las herramientas Google App Maker y Google Apps Script, las cuales te permitirán desarrollar sencillas aplicaciones para optimizar el trabajo de tu equipo dentro de la empresa.

Gracias a la utilización de plantillas y un entorno visual amigable, Google App Maker permite que, con conocimientos básicos, puedas crear aplicaciones de flujos de trabajo y de información con las que los recursos de tu empresa se aprovecharán de manera más eficiente, y siempre de forma segura”.(19 de agosto, 2019) Recuperado de https://arrobasystem.com/blogs/seguridad-informatica/seguridad-informatica-para-tu-empresa-con-google-drive

14)Herramientas en la nube para su empresa

De manera similar a la percepción, la seguridad informática debe de ser una prioridad en la empresa. No sólo importa el almacenamiento de la información, sino que es necesario que se piense en todos los riesgos a los que esta puede estar sujeta. Por ello, las herramientas de G Suite son una opción, si se quiere además de seguridad, tener, disponible la información, optimizar el trabajo y acceder a muchos otros beneficios.

La transformación digital está haciendo que los procesos de información de las empresas cambien. Es de suponer, entonces, que deben cambiar la manera de manejar la información y voltear a ver las grandes cualidades de servicios como **G Suite**, cuyos atributos han sido más que comprobados y recomendados.

La herramienta de **G Suite** ofrece alternativas que se adecúan a la empresa, además de que el servicio de soporte siempre está disponible para resolver todas las dudas sobre sus servicios. En este sentido, se tendrá las herramientas mejor calificadas del mercado que harán que la empresa logre alcanzar sus objetivos, siempre con la confianza de que la información. **Publicado el (24 de octubre, 2018)**

15)CAPÍTULO III. MARCO METODOLÓGICO

Este estudio, está enmarcado en la investigación descriptiva, la cual, Comprende para Tamayo y Tamayo (2003- pág. 47) la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente.", en este sentido, está referida a las características de la población a ser analizadas. Dicho estudio se centra en el "qué", en vez del "por qué" del sujeto de investigación, siendo su norte describir la naturaleza de un segmento demográfico.

1) Población y Muestra.

La población, se define como el número de individuos sometidos a análisis de acuerdo con las características de la misma. Esta población está caracterizada por usuarios finales que utilizan la herramienta como medio de comunicación que utilizan la aplicación de G suite (Gmail) y empresas que utilizan G Suite.

La Muestra es un segmento representativo de la población al cual se le aplicaron los instrumentos elaborados para obtener la información requerida, dicha muestra al momento de recaudar las respuestas se analizó para generar las conclusiones y recomendaciones.

2) Técnicas e Instrumentos

Las técnicas implementadas en la investigación fueron de carácter documental y de campo (encuesta), la cual consiste en la técnica que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recolectan y se analizan los datos como muestra representativa de la población explorada.

El instrumento a utilizar en esta investigación es un cuestionario constituido por 10 preguntas mixtas entre preguntas dicotómicas (selección entre verdadero y falso) y

preguntas de selección múltiple. Un cuestionario es un instrumento de investigación que a base de una serie de preguntas e instrucciones busca obtener un resultado de campo, es este caso se analiza las respuestas obtenidas de un Mínimo de 100 personas.

Diseño de Campo: Consiste en recoger información de la realidad, donde se realiza el estudio; en este caso se utilizó un instrumento el cual fue caracterizado anteriormente. Esta investigación se inscribe en el paradigma cuantitativo, ya que se manejan datos de información de la muestra seleccionada.

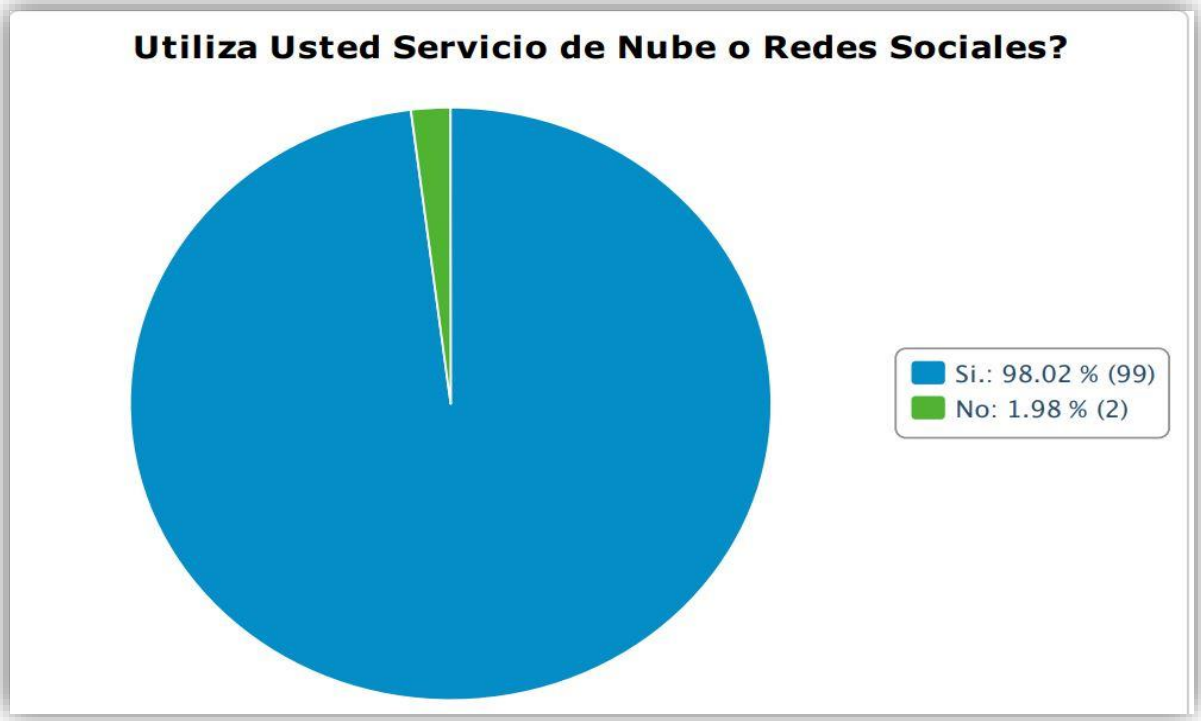
Procedimientos: Después de la investigación documental, donde se identificaron fuentes de información infográfica y se encontró información pertinente al tema objeto de estudio. Luego se elaboró una versión del Cuestionario, se validó con expertos en metodología y con conocimientos en el objeto de estudio, una vez que fue validado, se aplicó a la muestra seleccionada en línea. Se enviaron los Cuestionarios y se dio un tiempo para su respuesta y recepción. Se tabulo la información proveniente de todos los cuestionarios y posterior se graficaron sus resultados.

Obtenidas las respuestas de las encuestas, se llevó a efecto el procesamiento de los datos para su análisis de resultados y vinculación con los objetivos específicos, definidos en la investigación.

16)CAPÍTULO IV RESULTADOS, ANÁLISIS Y CONCLUSIONES

4.1 RESULTADOS

Figura 1. Grafica circular con el porcentaje de la muestra que utiliza los servicios de la nube o Redes Sociales.

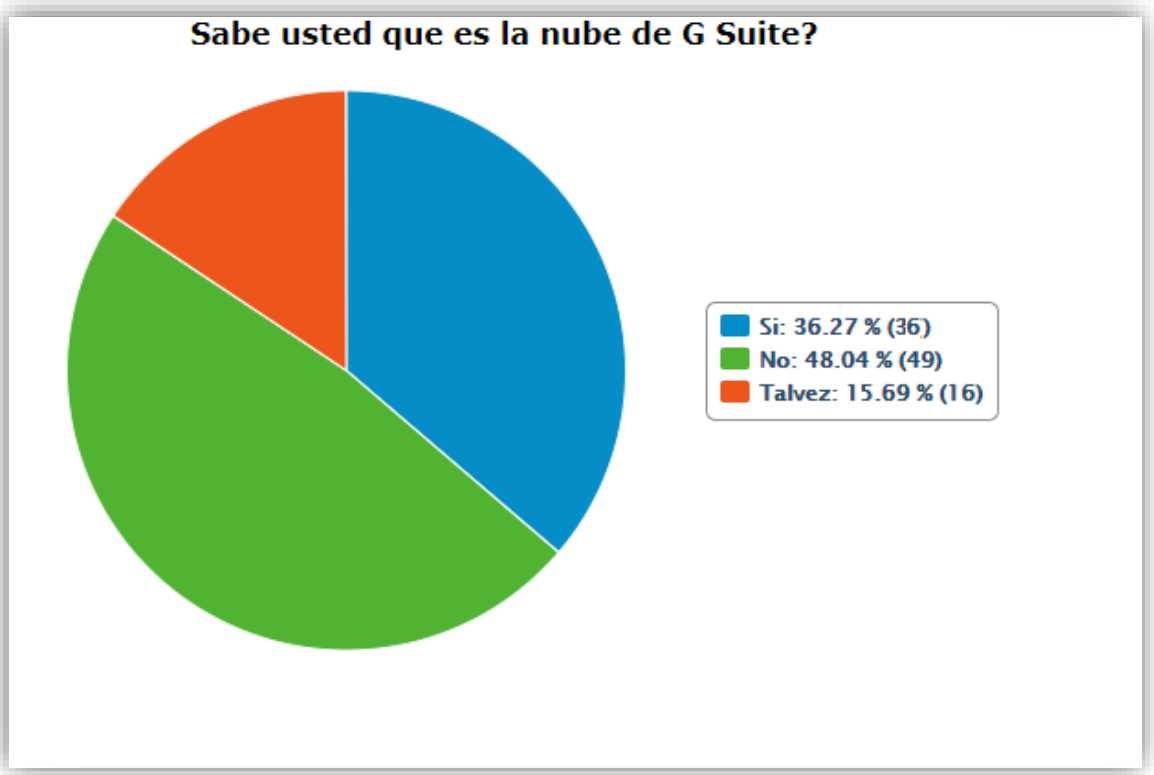


Fuente: Fernando King (2019).

Luego de aplicar el instrumento (la encuesta) a los participantes de la muestra establecida, se obtuvieron los siguientes resultados:

Con relación al primer ítem ¿Utiliza Usted Servicio de Nube o Redes Sociales? Los resultados obtenidos muestran que el 98.02% de los participantes de la muestra manifiesta que hace uso de los servicios de la nube o redes sociales.

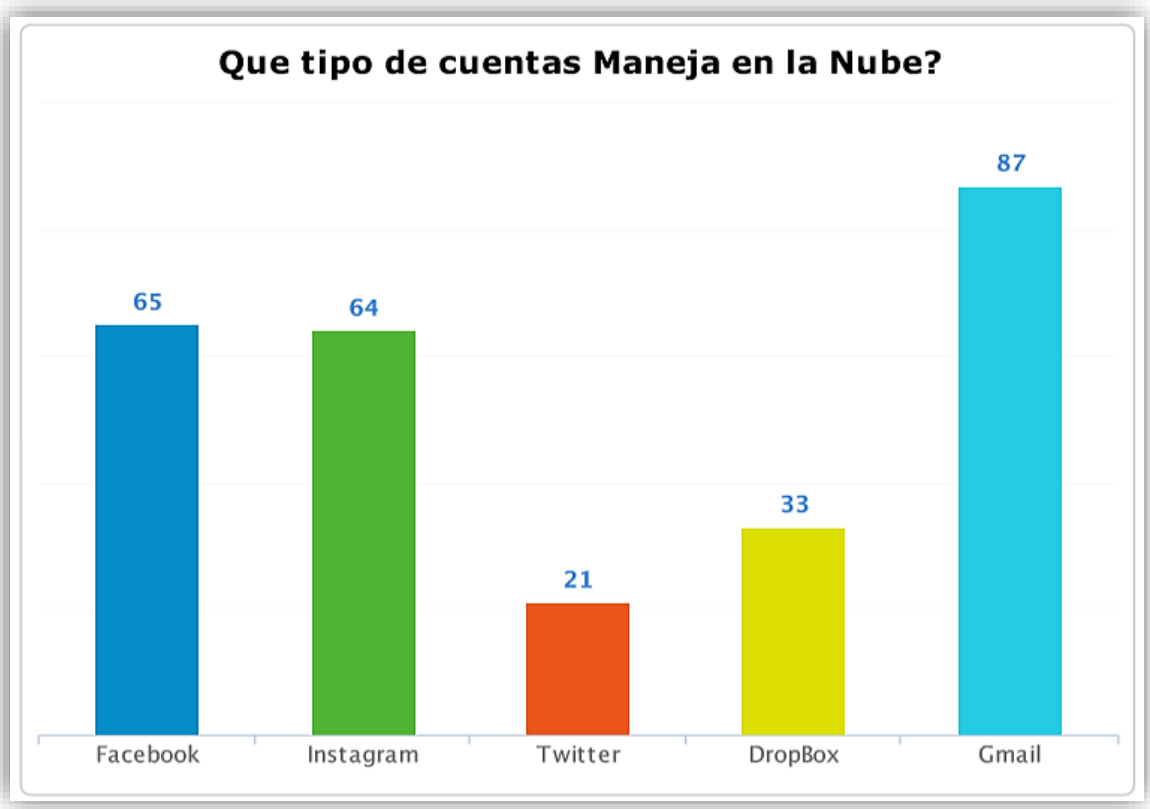
Figura 2. Grafica circular con el porcentaje de la muestra que sabe, desconoce o tiene dudas sobre que es la nube de G Suite.



Fuente: Fernando King (2019).

En el segundo ítem ¿Sabe usted que es la nube de G Suite? se observó que poco menos de la mitad de los participantes de la muestra no conoce la nube de G Suite y solo el 36.27% manifiesta conocerla. Por otra parte, el 15.69% manifestó tener dudas con relación a conocer que es la nube de G Suite.

Figura 3. Grafica de barras que muestran el porcentaje de uso por parte de la muestra que maneja alguna o varias cuentas de: em la nube, Gmail, Facebook, Instagram, Dropbox o Twitter.



Fuente: Fernando King (2019).

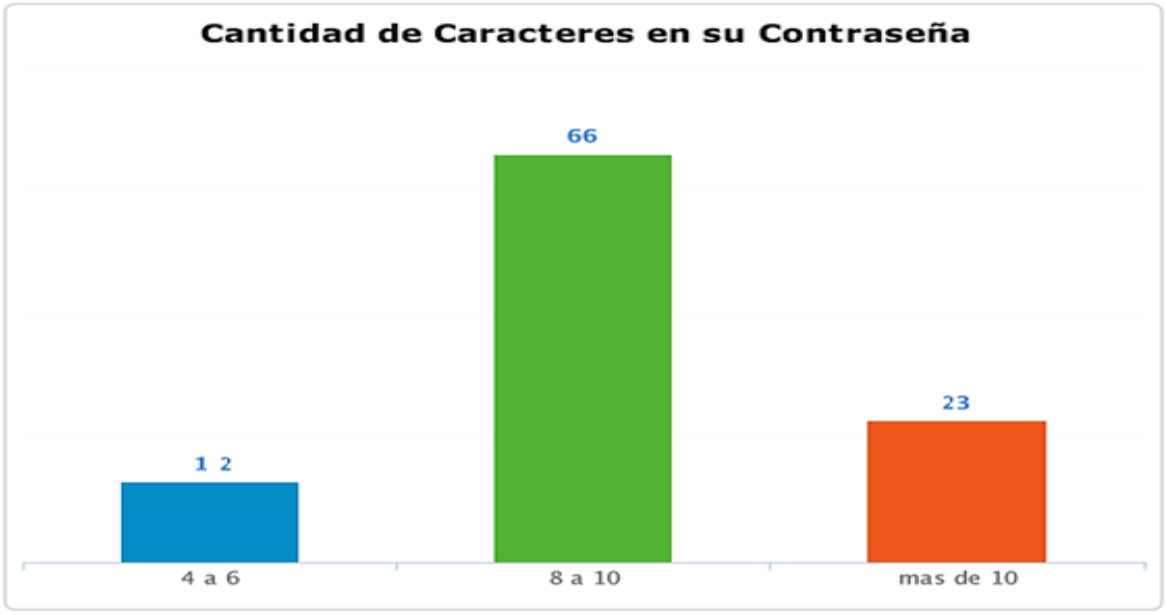
Con relación al tercer ítem ¿Qué tipo de cuentas maneja en la nube? Los resultados obtenidos muestran que 87 de los participantes de la muestra manifiesta que usa correo electrónico Gmail, 65 Facebook, 64 Instagram, 33 Dropbox y 21 Twitter, de entre distintos servicios en la nube.

Figura 4. Grafica Pastel donde se muestran los porcentajes de las preferencias de seguridad en cuanto a la complejidad de uso de contraseñas por parte de los participantes de la muestra.

Fuente: Fernando King (2019).

Del cuarto ítem: ¿Cuál es la complejidad de sus Contraseñas? las respuestas obtenidas de este ítem permiten observar que el 48% de los participantes de la muestra utiliza contraseñas alfanuméricas, mientras el 44.55% hace uso de contraseñas alfanumérica + Símbolos y solo un 8% utiliza contraseñas numéricas.

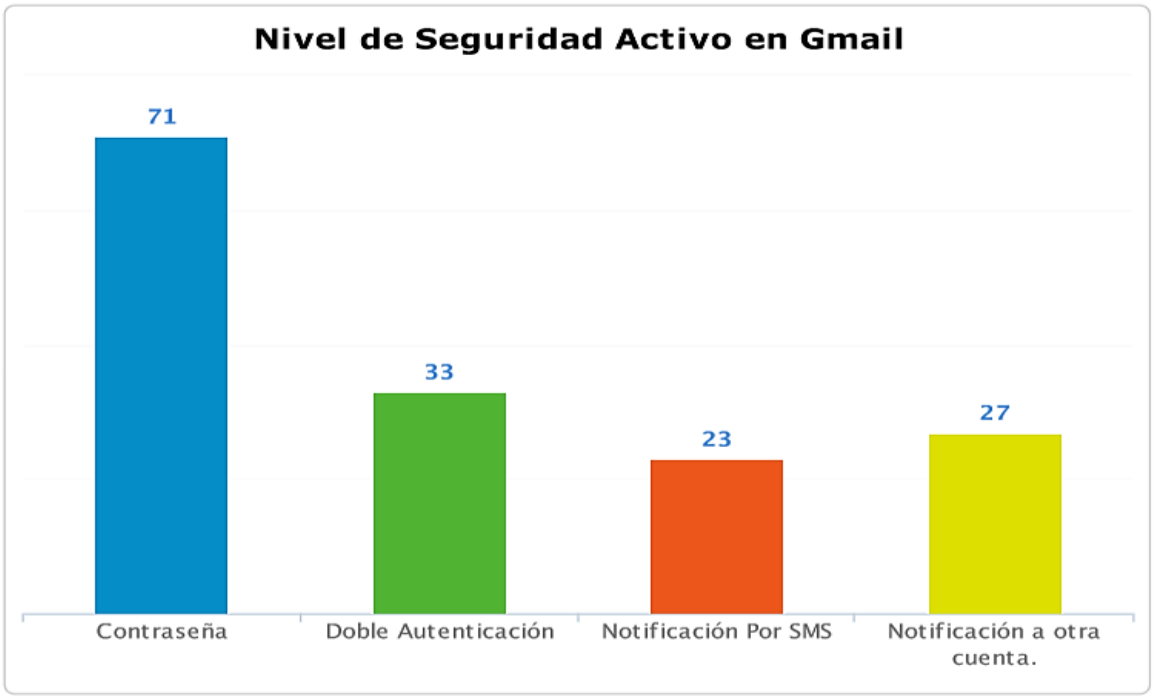
Figura 5. Grafica de barras que muestran los porcentajes de uso de diferentes intervalos de cantidades de caracteres en una contraseña (entre 4 y 6; entre 8 y 10; y más de 10), por parte de los individuos de la muestra.



Fuente: Fernando King (2019). Encuesta de opinión.

Con relación al quinto ítem ¿Cantidad de caracteres en su contraseña? Los resultados arrojan que 66% de los individuos de la muestra utilizan entre 8 y 10 caracteres, 23% utilizan más de 10 caracteres y solo 12% de las personas encuestadas utilizan entre 4 y 6 caracteres en sus contraseñas.

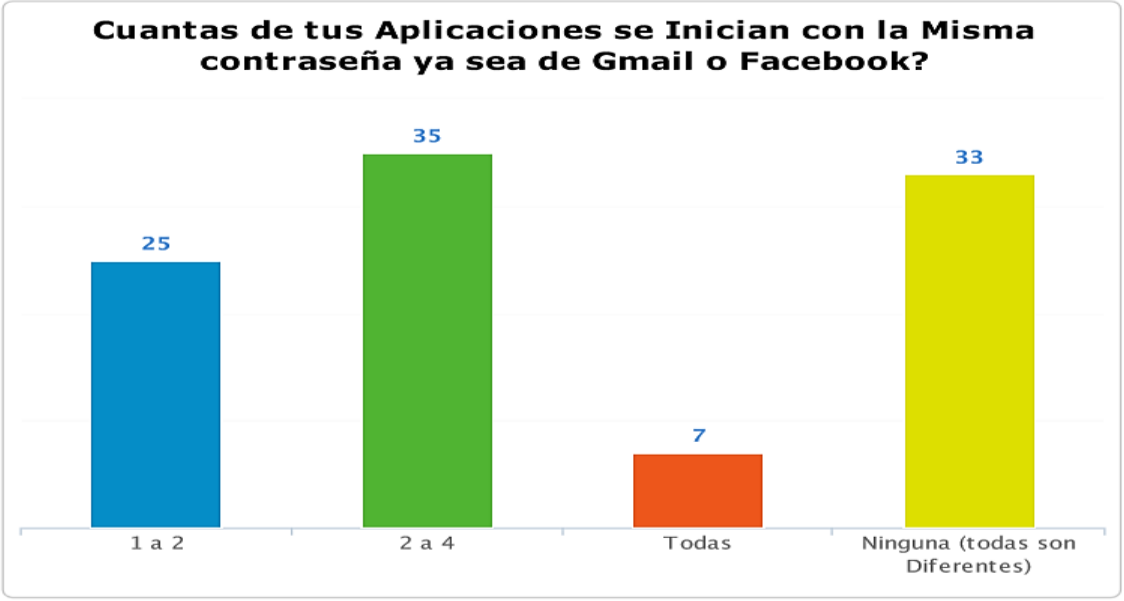
Figura 6. Grafica de barras que muestran los porcentajes de uso de diferentes mecanismos de seguridad activos para proteger las cuentas en Gmail, por parte de los individuos de la muestra.



Fuente: Fernando King (2019).

Continuando con la cuantificación de resultados, en el sexto ítem ¿Nivel de seguridad activo en Gmail? Los resultados obtenidos muestran que 71 de los participantes de la muestra posee un nivel de seguridad activo en Gmail basado en contraseña, en cambio un 33 utiliza la doble autenticación, un 27 hace uso del mecanismo de notificación a otra cuenta y 23 de las personas hace uso del mecanismo de notificación por SMS.

Figura 7. Grafica de barras que muestran los porcentajes de uso de la misma contraseña al iniciar distintas aplicaciones por parte de los participantes de la muestra, en cuatro categorías: entre 1 y 2 aplicaciones; entre 2 y 4 aplicaciones; Todas o ninguna (contraseñas diferentes para cada aplicación).



Fuente: Fernando King (2019).

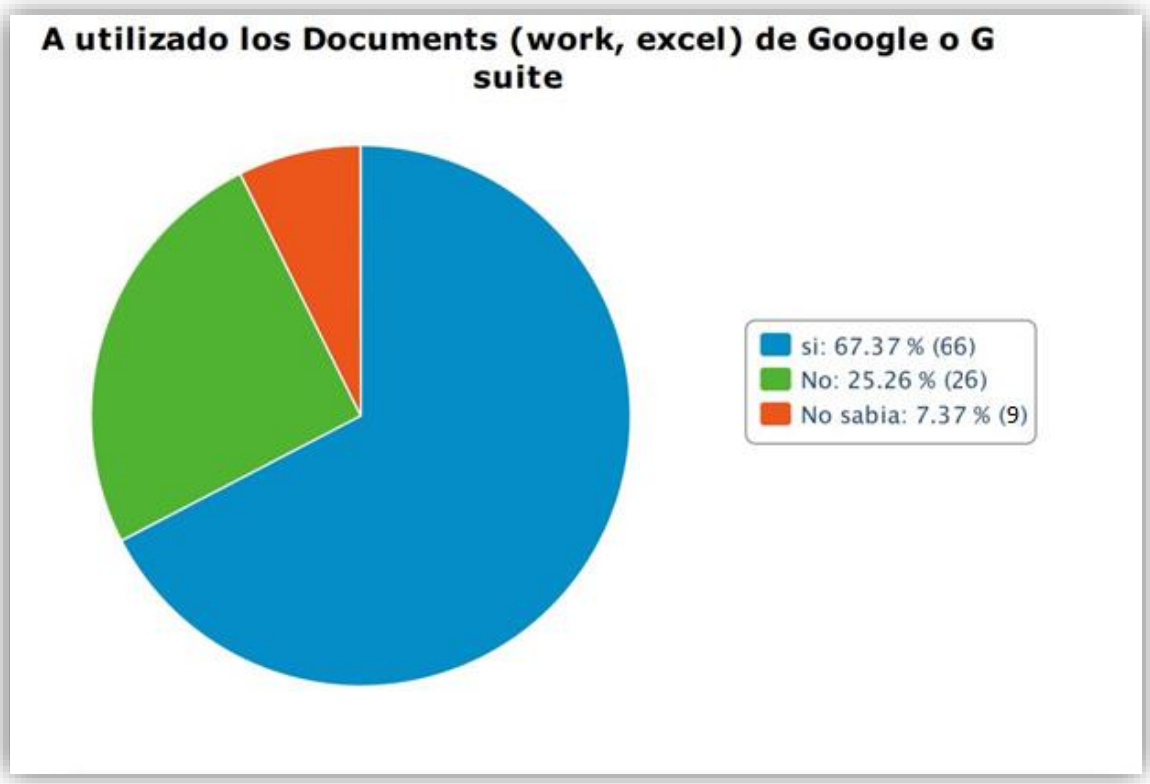
Del séptimo ítem: ¿Cuántas de tus aplicaciones se Inician con la misma contraseña ya sea de Gmail o Facebook? las respuestas obtenidas de este ítem muestran que los participantes de la muestra prefieren (35%) mantener la misma contraseña para iniciar sus aplicaciones (entre 2 y 4 aplicaciones), mientras que el 33% prefiere que cada aplicación tenga su propia contraseña. También, los resultados muestran que un 25% de los participantes de la muestra inician sus aplicaciones con una contraseña repetida y solo el 7% de los participantes de la muestra inician todas sus aplicaciones con una misma contraseña.

Figura 8. Grafica circular donde se muestran los porcentajes de individuos de la muestra que creen que toda la información que tiene en Google Drive si está segura y aquellos que no.

Fuente: Fernando King (2019).

Del octavo ítem: ¿Cree usted que toda la Información que tiene en Google Drive está segura? las respuestas obtenidas de este ítem permiten observar que el 44.68% de los participantes de la muestra opinan que toda la información que tiene en Google Drive no está segura. Por el contrario, el 24.47% de los participantes de la muestra confían que toda la información que tiene en Google Drive si está segura.

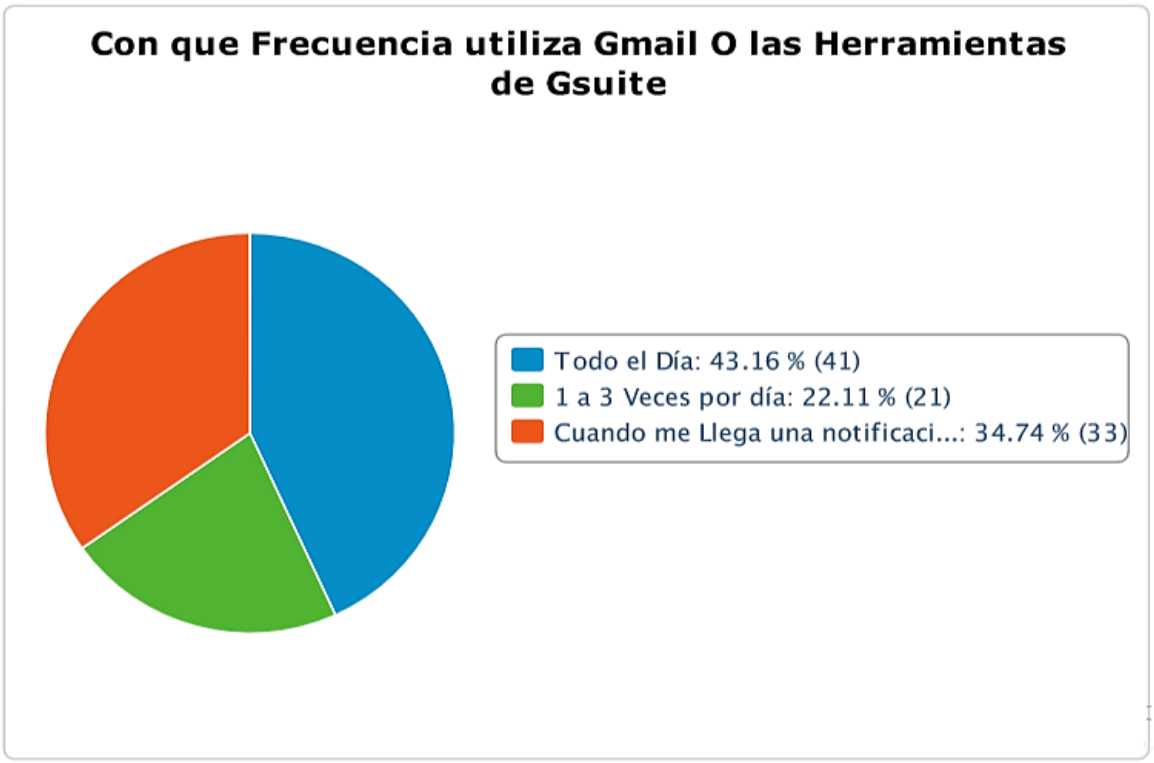
Figura 9. Grafica circular donde se muestran los porcentajes de individuos de la muestra que han utilizado los documentos de Google o Gsuite.



Fuente: Fernando King (2019).

Continuando con la cuantificación de resultados, en el noveno ítem ¿Ha utilizado los documentos (Word, Excel) de Google o G suite? Los resultados obtenidos muestran que el 67.37% de los participantes de la muestra han utilizado los documentos de Google o de Gsuite. En cambio, un 25.26% no los ha utilizado.

Figura 10. Grafica circular donde se muestra la frecuencia de uso de Gmail o las herramientas de Gsuite por parte de los participantes de la muestra en forma porcentual.



Fuente: Fernando King (2019).

Con relación al décimo ítem ¿Con que frecuencia utiliza Gmail o las herramientas de Gsuite? Los resultados arrojan que el 43.16% de los individuos de la muestra hacen uso de Gmail o las herramientas de Gsuite con una frecuencia de todo el día. Por otra parte, el 22.11% de los individuos de la muestra hacen uso de Gmail o las herramientas de Gsuite con frecuencia de entre 1 y 3 veces al día. También un 34.74 % de los individuos de la muestra hacen uso de Gmail o las herramientas de Gsuite solo cuando les llega una notificación.

4.2 ANÁLISIS DE RESULTADOS

A partir de los resultados obtenidos se pudo inferir lo siguiente:

Con relación al primer ítem ¿Utiliza Usted Servicio de Nube o Redes Sociales?, con este ítem se pretendió diferenciar y cuantificar los usuarios de los servicios ofrecidos por la nube de G Suite y aquellos usuarios que no los utilizan, aspecto importante para cumplir con el objetivo principal de esta investigación. El resultado obtenido permite inferir que la población estudiada maneja mayoritariamente aplicaciones en la nube y está consciente de ello.

En tal sentido, esto es consistente con los resultados de otros estudios y es pertinente para esta investigación, sin dejar de lado el reconocimiento de que existen otras plataformas que no utilizan la nube y de la “Brecha Digital” que representa el que algunas personas no utilizan aun o utilizan muy poco los recursos tecnológicos, ya que, para los efectos de esta investigación, lo más relevante fue investigar el nivel de la seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite en Panamá y para ello es importante que los usuarios no solo hagan uso de los recursos ofrecidos por la nube de G Suite, sino, que estén conscientes de su uso.

En el mismo orden de ideas, Con relación al segundo ítem ¿Sabe usted que es la nube de G Suite?, este ítem también pretendió diferenciar y cuantificar los usuarios de los servicios ofrecidos por la nube de G Suite y aquellos usuarios que no los conocen, un aspecto también importante para cumplir con el objetivo principal de esta investigación El resultado obtenido permite afirmar que existe un desconocimiento del nombre de los servicios de la nube de G Suite por parte de la mayoría de los participantes de la muestra, ya que del primer ítem se despende que los mismos manifestaron ser usuarios de servicio de Nube o de Redes Sociales.

Por otra parte, del análisis de los resultados del tercer ítem, ¿Qué tipo de cuentas maneja en la nube?, este ítem está relacionado con el primer objetivo específico y de

él se infiere que la mayoría de los usuarios (87 %) hace uso del correo electrónico de Gmail. Esto es especialmente interesante ya que varios de los otros servicios son dependientes desde el punto de vista de la seguridad, de la contraseña de un correo electrónico, por ello, la contraseña de Gmail se hace más crítica. Es asi como, las cuentas como las de Facebook, Twitter, Dropbox y otros servicios en la nube, dependen para su acceso del acceso al correo electrónico. ¨Por ello, el porcentaje de uso de Gmail, se hace muy importante para esta investigación.

En otro orden de ideas, en cuanto al cuarto ítem ¿Cuál es la complejidad de sus Contraseñas?, este ítem está relacionado con el segundo objetivo específico, sobre los niveles de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite. Del análisis de los resultados obtenidos y particularmente de este ítem se desprende que menos de la mitad de los participantes de la muestra (47.52%) utiliza contraseñas alfanuméricas, mientras el 52% no. De ello podemos deducir que el nivel de seguridad en cuanto al uso de contraseñas seguras no es mayor al 50%, lo cual representa un riesgo muy alto.

Con respecto al quinto ítem ¿Cantidad de caracteres en su contraseña?, este ítem también está relacionado con el segundo y con el tercer objetivo específico, sobre los niveles de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite. Se esperaría que la mayoría de los individuos seleccionaran una contraseña de más de 10 caracteres por seguridad, sin embargo, el análisis de resultados permite concluir que la mayoría de los individuos de la muestra (64.7%) hace uso de contraseñas con, entre 8 y 10 caracteres, y solo un 12.75% utiliza entre 4 y 6 caracteres, lo cual es un porcentaje bajo pero que indica que permite establecer acciones para obtener una mejora.

Asi mismo, del análisis de los resultados del sexto ítem, ¿Nivel de seguridad activo en Gmail?, este aspecto también está relacionado con el segundo y tercer objetivo específico, sobre los niveles de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G Suite. Se infiere a que la mayoría de los usuarios (71 %) posee un nivel activo de seguridad bajo en Gmail, basado solo en una

contraseña, en comparación con un porcentaje dos veces más bajo (23%) que hace uso de algún otro mecanismo de seguridad más elevado de notificación, como los mensajes por SMS o las notificaciones a otras cuentas con el 27%.

Asi, es claro que los tiempos de respuesta y la necesidad de contar con otros servicios necesarios como la solvencia del servicio de Internet, hacen que los niveles de seguridad activa, más altos sean menos atractivos para el usuario común, en particular aquellos que no han sufrido algún ataque a su seguridad. Sin embargo, para quienes la seguridad es una necesidad imperativa, como aquellos que utilizan Gmail para actividades laborales de misión crítica, el uso de niveles superiores de seguridad activa es la opción apropiada.

Por otra parte, del análisis de los resultados del séptimo ítem, ¿Cuántas de tus aplicaciones se Inician con la misma contraseña ya sea de Gmail o Facebook?, este ítem está vinculado tanto con el primero como con el segundo y tercer objetivo específico. Con relación al primer objetivo, permite reconocer aplicaciones virtuales ofrecidas por la nube de G Suite y de uso preferente por los individuos de la muestra.

También, en cuanto a los objetivos específicos segundo y tercero, sobre los niveles de seguridad que perciben los usuarios. Las respuestas obtenidas permiten deducir que solo el 7% de los participantes de la muestra inician todas sus aplicaciones con una misma contraseña, siendo esta práctica poco recomendable por su inseguridad. Por otra parte, el 33% de los individuos de la muestra inician todas sus aplicaciones con una contraseña diferente para cada aplicación, que es el caso más seguro considerado en el ítem.

Asi mismo, se determinó que el 60% de los individuos de la muestra inician sus aplicaciones con las mismas contraseñas en 2 y hasta 4 aplicaciones, Esto no indica si hacen uso de 2 o más contraseñas distintas por la forma en la que se construyó el ítem, dejando una duda sobre la inconveniencia o no de esta práctica.

En otro orden de ideas, Con relación al octavo ítem ¿Cree usted que toda la Información que tiene en Google Drive está segura?, este aspecto está relacionado con el segundo y tercer objetivo específico, sobre los niveles de seguridad que perciben los usuarios. El examen de los resultados indica que la mayoría de los participantes (44.09%) de la muestra no cree que toda la información que tiene en Google Drive está segura.

También, se deduce que un 30.85% desconoce el grado de seguridad de su información en Google Drive, con lo cual se puede afirmar que más de un 70% de los usuarios encuestados tiene serias dudas sobre la seguridad de sus datos en Google Drive, mientras que apenas un 24.73% si cree que toda la información que tiene en Google Drive está segura. Estos resultados indican que existe un problema de percepción sobre la seguridad de la Información que tienen los usuarios en Google Drive.

Con respecto al noveno ítem ¿Ha utilizado los documentos (Word, Excel) de Google o G suite?, este ítem está vinculado tanto con el primero como con el segundo y tercer objetivo específico. Con relación al primer objetivo, permite reconocer aplicaciones virtuales ofrecidas por la nube de G Suite y de uso preferente por los participantes de la muestra. El análisis de los resultados obtenidos muestra que la mayoría de los participantes de la muestra (68.09%) han utilizado los documentos de Google o de G Suite, lo cual la convierte en una de las aplicaciones en la nube preferida por los usuarios.

Por otra parte, del análisis de los resultados del décimo ítem, ¿Con que frecuencia utiliza Gmail o las herramientas de G Suite?, este ítem está vinculado tanto con el primero como con el segundo y tercer objetivo específico. Con relación al primer objetivo, permite reconocer aplicaciones virtuales ofrecidas por la nube de G Suite y de uso preferente por los individuos de la muestra. Las respuestas obtenidas permiten deducir que la mayoría de los individuos de la muestra (43.16%) hacen uso de Gmail o las herramientas de G Suite con una frecuencia de todo el día, lo cual convierte a G Suite en una aplicación de alto índice de uso cotidiano. Así mismo el 22.11% de los

individuos de la muestra hacen uso de Gmail o las herramientas de G Suite con frecuencia de entre 1 y 3 veces al día, por lo que se puede intuir que más del 65% de los participantes de la muestra hacen uso de las herramientas de G Suite al menos una vez por día. Esto afianza el hecho de que G Suite es un conjunto de herramientas de uso diario y frecuente.

4.3 CONCLUSIONES

La seguridad informática es un factor muy importante en la sociedad contemporánea, impulsada por la penetración de las TICS en la población y la disminución de “la Brecha Digital”. Por otra parte, el surgimiento de nuevas actividades fuera de la ley, por medio del uso de las TICS, delitos informáticos, delitos cibernéticos y hasta el ciberterrorismo, hacen que la sociedad del conocimiento avance con cautela en la incorporación de las tecnologías y busque “refugio” en las regulaciones legales.

En tal sentido, en la medida en que aparecen nuevas tecnologías y otras mejoran sus versiones, las tecnologías basadas en “la nube” como plataforma, han alcanzado un favoritismo parcial y en crecimiento. La conveniencia de contratar en vez de adquirir, plataforma tecnológica, aplicaciones o una mezcla de plataforma y aplicaciones apropiada y hasta contingente hace de la opción en la nube una opción que no debe pasarse por alto. Sin embargo, la incertidumbre o falta de confianza en las tecnologías basadas en la nube atenta contra el mayor y más rápido crecimiento de estas tecnologías.

A partir de los resultados obtenidos se pudo inferir que muchos desconocen el tipo de tecnología en la que están dejando su información es decir la nube, manteniendo siempre la información disponible, integra y confidencial, pero estas características dependen en gran medida de las prácticas de los usuarios, el nivel de seguridad que emplean los usuarios.

Las gráficas y encuestas de campo ayudaron a tener una visión panorámica de la misma dando como resultado que la seguridad que se implementa en los medios de hoy en día no es robusta y se es vulnerable a los ataques cibernéticos e ingeniera social que han aparecido en los últimos años en donde, por ejemplo, se realizan llamadas dando nombre de familiares, hijos o nietos con temas relativos a delitos. Aquí es donde se debe emplear la seguridad.

También, se pudo determinar que el correo electrónico continúa siendo la aplicación mas popular en la nube de G Suit, seguida de Facebook e Instagram, reafirmando el

carácter social de las redes. Asi mismo, existe conciencia entre los usuarios sobre el uso de contraseñas fuertes, alfanuméricas e incluso alfanuméricas con símbolos especiales, de más de siete caracteres, lo cual demuestra la evolución en las prácticas de seguridad por contraseña entre los usuarios.

Otro aspecto importante tiene que ver con el nivel de seguridad activo en Gmail, del cual se concluye que, aun cuando ha habido un avance en el uso de estas técnicas de seguridad, aún hay una mayoría de usuarios (más del 66 %) que no utilizan estos procedimientos que fortalecen la seguridad de acceso. Asi mismo, un alto número de usuarios (más del 66 %) utiliza la misma contraseña en varias aplicaciones, con lo que se infiere que aún hay mucho trabajo por realizar en cuanto a impulsar la seguridad por parte de los usuarios.

Finalmente, en la República de Panamá, se requiere mantener el crecimiento sostenido de la eficiencia para lo cual, el uso de las tecnologías más avanzadas y eficientes es una necesidad imperiosa. Es por ello que se concluye en esta investigación que es necesario impulsar el reconocimiento de las tecnologías basadas en la nube como un motor del desarrollo social y económico del país, con sus ventajas y debilidades, pero, sobre todo, con una sociedad preparada para afrontar los retos de cara al siglo XXI.

1) 4.4 RECOMENDACIONES

Entre las recomendaciones se destacan las siguientes:

- Los usuarios deben obtener capacitación en el ámbito de seguridad, en el manejo de las aplicaciones y recordar que son su propio “primer anillo de seguridad”, deben buscar ayuda.
- Los usuarios deben utilizar siempre varias formas de autenticación obteniendo más seguridad para su información como, por ejemplo, doble autenticación, notificación a otra cuenta de correo, otras formas.
- Es importante colocar contraseñas diferentes en cada cuenta que se tenga en internet, que no sean nombres ni fechas de familiares.
- Los usuarios deben validar suficientemente que postean ya que en los drives de Gmail si no se tiene la configuración bien realizada o una estructura definida en las contraseñas, sus fotos, conversaciones y demás podrían quedar expuestas a terceros.
- A nivel de las empresas, estas deben establecer políticas de uso donde se exija a los colaboradores utilizar algunos de los programas mencionados en este trabajo, para robustecer o limitar los accesos de los terceros y tener un mayor control de la información que se envía por correo o se descarga del mismo, ya que los programas suelen mostrar una inspección total de la información adjunta.
- Los usuarios deben cambiar periódicamente las contraseñas con un lapso de 3 a 6 meses.
- Asi mismo, los usuarios deben mejorar sus criterios y ser más cuidadosos a la hora de compartir la información que se publica en las redes sociales, tales como en Facebook o LinkedIn, esta información muchas veces se utiliza para hacer ingeniería social.
- Tanto los usuarios como las empresas deben ocuparse de reducir el riesgo de ataques como (Phishing, Ingeniería Social, Vishing), mediante estrategias y políticas de seguridad más robustas.

- Se recomienda a otros estudiantes interesados en estos temas, desarrollar una investigación sobre el nivel de percepción de seguridad enfocado en el uso de otras herramientas en la nube, para corroborar o contrastar los resultados de esta investigación.
- Se recomienda a la Universidad Internacional de Ciencia y Tecnologia (UNICyT), incorporar los resultados de esta investigación en los cursos y talleres sobre alfabetización digital.

17)Referencia Bibliográfica

1. DANIEL DE BLAS *(4/9/2018) p.17 Globb Security* en línea en: https://globbsecurity.com/servicios-cloud-las-12-amenazas-de-seguridad-en-la-nube-que-no-se-deben-olvidar-43654/
2. Villavicencio Fernandez, Pascal (2018) Análisis e implementación de la plataforma tecnológica de Google Empresarial para pequeñas y medianas empresas, Lima Perú http://repositorio.utp.edu.pe/handle/UTP/1486
3. Boxbyte (2012) p.18. El origen del Cómputo en la Nube. https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/

- Historia y Biografía (2017). (p.18) Historia de Google https://historia-biografia.com/historia-de-google/

4. Ciudad del Saber (noviembre 18, 2019 p.21) https://ciudaddelsaber.org/prensa/los-nuevos-retos-de-hoy-en-dia-para-la-ciberseguridad/
5. Mónica Gallego**. (**28 agosto, 2019) p.27. https://cybersecuritynews.es/la-ciberseguridad-del-internet-de-las-cosas-uno-de-los-retos-que-afrontan-las-organizaciones/
6. Juan Manuel Muñoz. p.28 (25 mayo, 2016) Herramienta para proteger tu información en la nube http://www.headsem.com/herramienta-para-proteger-tu-informacion-en-la-nube/
7. Alejandro Aguila (S/F) p.29 Privacidad de la información en Redes informáticas https://en.calameo.com/read/00501200193d4a56f8783
8. Tamayo y Tamayo, M. (2003). El proceso de la investigación científica. Edición 4ta, México: Editorial Limusa. https://clea.edu.mx/biblioteca/Tamayo%20Mario%20-%20El%20Proceso%20De%20La%20Investigacion%20Cientifica.pdf

9. Sonia Limia, (2018) ventajas del almacenamiento en la nube para tus contenidos https://es.semrush.com/blog/ventajas-almacenamiento-nube-contenidos-digitales/?kw=83790125715&cmp=8044659774&label=dsa_blog&utm_source=google&utm_medium=cpc&utm_campaign=ohm:acc-latam:lan-es:dev-pc:sou-dsa:mtp-blog:stp-smm:aud-new:mt-all:ver-1&utm_term=cid-8044659774,agi-83790125715,adi-396095093228,tid-dsa-838022530058,dev-c,reg-9069751&gclid=EAIaIQobChMI6oPgr42g5wIVjoVaBR3PQwxHEAAYAiAAEgKnmvD_BwE

10. Conde Graphics. (Jul 5, 2017)

https://medium.com/@condegraphics/ventajas-y-beneficios-g-suite-8a2296c9c47e

11. Jimenez, Javier. (2018), herramientas para aumentar la seguridad y privacidad en Google Drive, Red Zone https://www.redeszone.net/2018/06/27/herramientas-aumentar-seguridad-privacidad-google-drive/

12. Anónimo (, 2018) Seguridad informática para tu empresa con Google Drive, Arroba System https://arrobasystem.com/blogs/seguridad-informatica/seguridad-informatica-para-tu-empresa-con-google-drive

Anexos

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN II

Estudante: Fernando Alfredo King Bernal, Cédula de identidad no. 8-796-602¸**Tutor**: Prof. Erick A. Ramos Sánchez. Pasaporte No. 134183826; **Correo electrónico del participante**: Fernando.king1386@gmail.com.pa Celular No. 6527-7317; **Título tentativo del trabajo de grado (TG).** Niveles de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G-Suite en Panamá.
Línea de Investigación: Ingeniería y sistemas de comunicación

SESIÓN	FECHA	HORA REUNIÓN.	ASPECTO TRATADO	OBSERVACIÓN
1.	14/09/2019	10:25 a.m.	Contacto inicial: Exploración de área de investigación; Aceptación de Tutoría	Se estableció la modalidad a distancia como método de asesoría de tesis. (del 21/09/2019 al 28/09/2019)
2.	05/10/2019	09:20 a.m.	Se exploraron posibles temas de tesis propuestas por el asesor y por el estudiante	Esta reunión fue presencial en la sede de UNICyT. Aula 8
3.	23/10/2019	04:04 p.m.	Selección del tema de investigación y se discutió un plan preliminar.	Intercambio de ideas (del 23/10/2019 al 25/10/2019). Vía WhatsApp y por email.
4.	29/10/2019	09:04 p.m.	Revisión de avances, bases teóricas, normas APA para citas y referencias,	Correcciones varias (del 28/10/2019 al 31/10/2019). Vía WhatsApp y por email.
5.	21/10/2019	09:48 a.m.	Revisión y aprobación de Anteproyecto	Observaciones y correcciones varias (del 21/10/2019 al 01/11/2019). Vía WhatsApp y por email.
6.	17/11/2019	03:00 p.m.	Aspectos metodológicos y revisión general del avance de la tesis, Delimitación y cambio de título. Población, Muestra, Resultados.	Sugerencias de beses teóricas; Observaciones y correcciones varias (del 17/11/2019 al 10/12/2019). Vía WhatsApp y por email.
7.	18/12/2019	12:00 m.	Revisión general del avance de la tesis, Análisis de Resultados.	Observaciones y correcciones varias (del 16/12/2019 al 27/12/2019). Vía WhatsApp y por email.
8.	04/01/2020	09:18 a.m.	Revisión general del avance de la tesis, Conclusiones y Recomendaciones.	Observaciones y correcciones varias (del 17/01/2020 al 20/01/2020). Vía email.
9.	20/01/22020	03:05 p.m.	Revisión de informe parcial de la tesis.	
10.	03/01/22020	03:05 p.m.	Revisión final de la tesis.	

Titulo definitivo: Niveles de seguridad que perciben los usuarios en el uso de los servicios ofrecidos por la nube de G-Suite en Panamá.
Comentarios finales acerca de la investigación: Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

_____ _____

Firma Firma