UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

DIFICULTADES TÉCNICAS DE SEGURIDAD DE LOS SERVICIOS EN LA NUBE

EGRESADO:

DENNY MIGUEL CONTRERAS JIMENEZ

TUTOR:

ING. LEON ACURIO

JOFFRE VICENTE

AÑO 2022

RESUMEN

El proyecto está dirigido a las dificultades técnicas de seguridad de los servicios de la nube. Basado en los conocimientos tecnológicos se analiza la plataforma como tal y dar con sus problemas de seguridad o posibles fallos de los usuarios a la hora de manejar los dispositivos.

Para obtener bases teóricas para innovar y resguardar la información de cada usuario, se procede a realizar una revisión bibliográfica en temas que tengan que ver con la presente investigación como Ciberseguridad, Computación en la nube, gestión, amenazas, etc.

Con las bases Teóricas, procedemos dar inicio al análisis a las posibles falencias que tiene la computación de la nube, y la capacidad personal se puede mejorar la seguridad y el bienestar de nuestra información ya que ahí se encuentra todos los datos personales.

En los tiempos de ahora se trabaja de forma manual, es necesario llevar un control de nuestras claves y que nuestra información no esté siendo visible en algún otro logar del mundo.

Para llegar a los problemas presentes de la investigación se utilizó la metodología de investigación cualitativa.

Dentro de los resultados obtenidos por la investigación que se realizó, es obtener la precaución y el cuidado de la información que subimos a la web, en este caso en cloud computing.

Finalmente se presentan las siguientes conclusiones, donde destacamos que la necesidad del cuidado de la información de la nube y de este modo fortalecer el control sobre nuestra información.

Palabras clave: información, precaución, seguridad, gestión.

ABSTRACT

The project addresses the technical security difficulties of cloud services. Based on the technological knowledge, the platform is analyzed as such and its security problems or possible user failures when managing the devices are found.

In order to obtain theoretical bases to innovate and protect the information of each user, a bibliographic review is carried out on topics that have to do with this research such as Cybersecurity, Cloud Computing, management, threats, etc.

With the Theoretical bases, we proceed to start the analysis of the possible shortcomings of cloud computing, and personal capacity can improve the security and well-being of our information since all personal data is found there.

Nowadays we work manually, it is necessary to keep track of our passwords and that our information is not being visible in any other place in the world.

To reach the present research problems, the qualitative research methodology was used.

Among the results obtained by the investigation that was carried out, it is to obtain the precaution and care of the information that we upload to the web, in this case in cloud computing.

Finally, the following conclusions are presented, where we highlight that the need to take care of cloud information and thus strengthen control over our information.

Keywords: information, precaution, safety, management.

INTRODUCCION

En el presente trabajo se trata de dificultades técnicas de seguridad de los servicios de la nube. Esto se da por ataques informáticos ya que hay mucha gente que se quiere aprovechar de la mínima vulnerabilidad que esta tiene.

Esto suele suceder por el mal manejo de las claves, archivos maliciosos, publicidad engañosa, entre otros. Pues es necesario tener muy en cuenta los detalles con respecto a la seguridad informática, ya que podemos prevenir estos ataques ilícitos. Estas actividades ilícitas se dan mucho en la web en general.

También se analizará el uso del proceso del uso del servicio para que no sufra alguna perdida de información, se le mostrara los beneficios de la nube tanto públicas como privadas.

Se le mostrara como está distribuido la información que beneficios tiene, quien nomas los usa y quienes tienen acceso a ellos ya que la información que los datos que se almacena en la nube es muy valiosa tanto para empresas como para los usuarios

El tema es relevante ya que actualmente existe un alto grado de ataques ilícitos informáticos en lo que es la web, sabiendo esto debemos tener precaución a la hora de confiar en algún archivo u enlaces desconocidos.

La línea de investigación del presente estudio de caso se relaciona con Sistemas de información y comunicación, emprendimiento e innovación y en la sub línea redes y tecnologías inteligentes de software y hardware.

DESARROLLO

El presente estudio de caso se lo realizó con base en investigaciones digitales, realizadas por profesionales en el área de sistemas, que se encuentran publicadas en la web, cómo libros, Documentos PDF y más. La metodología utilizada es de tipo cualitativa, ya que se ha utilizado información existente para realizar el presente trabajo y exponer las conclusiones del caso.

Seguridad Informática

Vivimos en una época tecnológica, la cual produce cambios de gran impacto en nuestra sociedad. Una de las herramientas más poderosas que ha producido este impacto es el internet, gracias a esta herramienta vivimos en lo que hoy en día se conoce como la era digital.

Tanto así, que en la actualidad el servicio del internet ya no se lo considera como un "lujo" que solo lo podían tener las personas "influyentes", "con dinero", ahora la mayoría de la población tiene acceso a él, se ha convertido en un servicio básico. Esto ha beneficiado grandemente a la economía digital, ya que las grandes y medianas empresas han podido brindar sus servicios a los clientes, sin la necesidad de estar físicamente en el establecimiento. No obstante, así como tiene sus ventajas, también tiene sus desventajas, en este caso, la vulnerabilidad de la seguridad. El uso de contraseñas es una de las medidas más empleadas al momento de querer proteger algún tipo de información, mismas que en muchas ocasiones han sido vulneradas por personas maliciosas con el fin de robar dinero o suplantar la identidad de los usuarios.

Frente a estas amenazas aparece la Seguridad informática o Ciberseguridad, que en el mundo digital se lo conoce como el proceso que detecta, previene y responde a las

dificultades técnicas de seguridad. Los términos de este proceso se detallan con más claridad, de la siguiente manera:

1. Prevenir: es recomendable que los cibernautas se eduquen y adquieran conocimientos de seguridad informática, con el objetivo de usar de manera optima y eficiente los recursos en internet.
2. Detectar: es posible que la detección se de en tiempo real, gracias a la intervención de un software informático, o después de que haya sucedido el ataque, siendo un problema mayor, ya que estas personas maliciosas pueden hacer de las suyas durante todo ese intervalo de tiempo.
3. Responder: en el hipotético caso que el ataque informático les haya resultado bien a los atacantes, se debe tener un plan de contingencia, un plan de respuesta, con enfoque técnico y legal. Una de las medidas técnicas, sería que se desconecte el router, ya que el virus no se seguiría esparciendo por la red. Además, es recomendable modificar las contraseñas y evitar robos de dinero y suplantación de identidad. En el ámbito legal, es importante denunciar el ataque cibernético.

La Seguridad Informática o Ciberseguridad se enfoca en la protección de los servidores, sistemas e información de los ataques cibernéticos.

Cloud Computing

Cloud Computing es la tecnología que mediante la red nos ayuda a conectarnos a diferentes servicios, sistemas y almacenamientos de archivos. (Cierco, 2019)

Estos servicios les permiten a los cibernautas, tener control y acceso a un grupo de recursos compartidos. Este grupo de recursos pueden ser: redes o servidores. El principal encanto de este servicio es su flexible acceso. (Cierco, 2019)

En la actualidad, varías de las grandes empresas utilizan estos servicios, tales como Google o EBAY. Estos proveedores se manejan con la misma estrategia, la cual es demostrar todos los beneficios de trabajar con computación en la nube, en varias ocasiones idealizándolas para atraer usuarios y ganar clientes. (Mell & Grance, 2017)

Desde hace tiempo, la computación en la nube se ha transformado en una herramienta de uso diario y a la vez la manera en que los cibernautas hacen uso de la misma. Este servicio se da a consecuencia de los avances tecnológicos y no se limita solo a la parte comercial, este puede acceder a centros de datos desde cualquier sitio. (Mell & Grance, 2017)

El Cloud Computing funciona en los presentes modelos de despliegue:

Nube Pública	Nube Privada
Sus recursos están disponibles para todo el público mediante una red abierta o pública. Esto quiere decir que los cibernautas compartirán el espacio disponible entre ellos mismos.	Su ventaja principal es dar exclusividad a una sola organización, brindarles el dominio total de sus servicios, asegurando mayor seguridad de los datos.
Nube Híbrida	**Nube Comunitaria**
Este modelo es uno de los más usados, ya que se trata de una fusión entre la Nube Pública y la Nube Privada, brindando la ventaja de que las organizaciones puedan ser propietarios de cierta parte de los servicios y a la vez comande con los servicios dados en la NPública.	Este modelo es usado de manera exclusiva en una comunidad de consumidores que tienen los mismos intereses.

Gráfico 1. Modelos de Despliegue en la nube – Autor: Denny Contreras

Nube Pública

La nube publica actuales no están implementados con una buena solución ya que independientemente no tiene una buena infraestructura, esta como un conjunto heterogéneo más de seguridad en sus entornos. Mejores niveles de rendimiento, costos menores y una disponibilidad mayor en la infraestructura, las aplicaciones y servicios.

Características de la nube publica:

- Asignación de recursos
- Acuerdos de uso
- Gestión

Uso de la nube publica

El uso de la nube publica es mas sencilla de utilizar ya que es uno de las plataformas de almacenamiento de información mas usado por las personas ya que el servicio que ofrece es gratuito y le ofrece al cliente 15GB de almacenamiento para que pueda subir todo tipo de respaldo sin costo alguno.

Casos comunes de uso de la nube:

- Escalamiento de infraestructura
- Recuperación ante desastres
- Almacenamiento de datos
- Desarrollo de aplicaciones
- Análisis de macrodatos

Las nubes públicas en los entornos híbridos

En la nube se ha disminuido el uso de distribución exclusiva de nube privada y pública, ahora optan por dar soluciones de entonos híbridos que incluyen infraestructura de nube pública y privada.

Nube privada

En la nube privada el usuario se hace responsable de todos los costos que esta cuenta para brindar su servicio. El usuario debe hacerse cargo de sus propios recursos como: maquinas, redes, almacenamiento, centro de datos, etc. La infraestructura de la nube privada permite tener una variedad de recursos basados en tecnologías de la información en tiempos determinados y alinea los costos en tiempo real.

Los servicios de la nube privada los usan especialmente, las entidades corporativas y entidades gubernamentales grandes o pequeñas.

A continuación, los beneficioso que esta ofrece:

- Mayor seguridad de la infromacion
- Muy pocos desperdicios de recursos
- Mayor productividad
- Costos accesibles
- Mayor manejo del software
- Mayor eficiencia del sistema

El Cloud Computing se distingue por sus servicios específicos, los cuales se dividen en tres diferentes niveles: SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service).

SaaS (Software as a Service)
Ofrece el despliegue de software y brinda la capacidad de utilizar las app de software dueñas del proveedor que se ofrecen como servicios. El usuario no posee el control de la infraestructura subyacente en la nube, solo de pocas opciones de configuración básicas. En este nivel, el proveedor es propietario de todos los recursos, esto quiere decir que el cliente se evita la realización de mantenimientos o actualizaciones. Todo el resguardo y seguridad es manejada por el proveedor.
PaaS (Platform as a Service)
Brinda un grupo de herramientas para desarrollar software y app web de manera que el usuario pueda hacer el despliegue de aplicaciones. El cliente no gestiona la infraestructura, no obstante, controla en su totalidad las app de esta. Este servicio les permite el sencillo acceso a los desarrolladores de software, para crear app por medio de internet, en cualquier lugar que se encuentre.
IaaS (Infraestructure as a Service)
Brinda gran capacidad para procesar y almacenar redes y varios recursos que permiten ejecutar software arbitrarios, permitiendo el libre control al cliente sobre sus app instaladas. Esta infraestructura soporta servicios que incluyen BD, un entorno para el desarrollo de aplicaciones y más. El cliente accede a todos estos recursos mediante la virtualización, esa es su ventaja principal.

Gráfico 2. Modelos de servicio de Cloud Computing – Autor: Denny Contreras

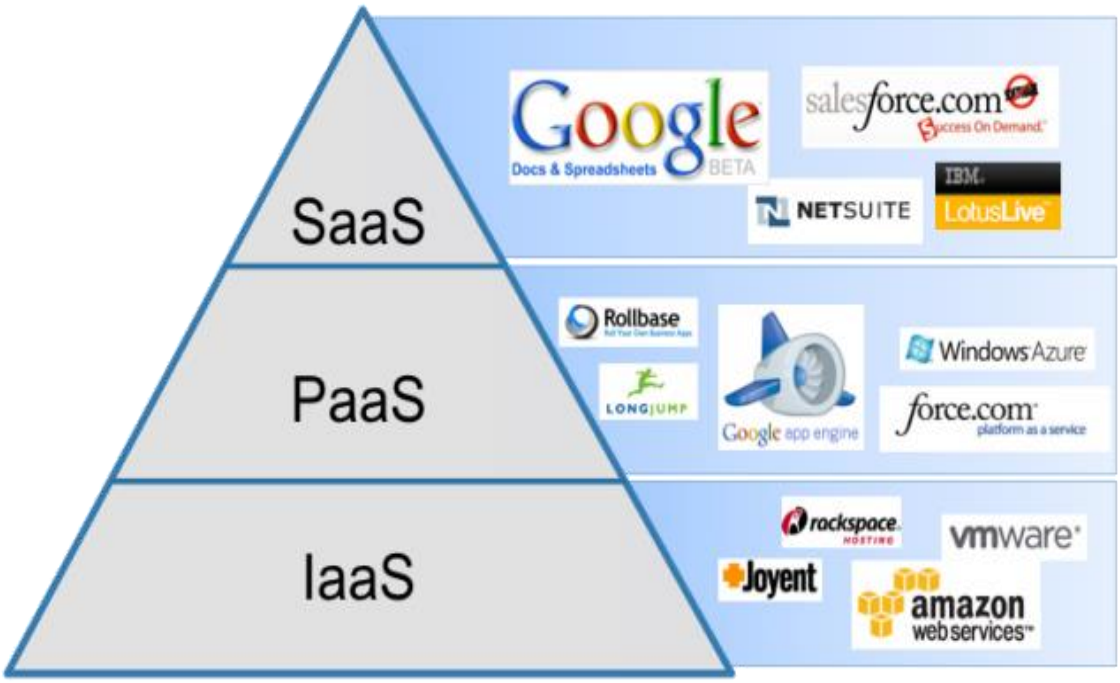

Gráfico 3. Esquema de servicios de Cloud Computing– Autor: Uladech

Ventajas Técnicas

Las ventajas técnicas que ofrece Cloud Computing, son las siguientes:

- Trabaja con tecnología virtual (virtualización)
- Emplea los principios de seguridad informática: disponibilidad, integridad y confiabilidad. Por medio del proveedor al cliente.
- Brinda soporte en todo momento, para cualquier tipo de problema.
- Posee instrumentos y gente capacitada que se encarga de manejar la seguridad de la información y datos del cliente.
- El cliente cuenta con el respaldo de sus datos, ya que el proveedor realiza backup o respaldos de la misma.

Desventajas Técnicas

El Cloud Computing tiene desventajas y no hay que tomárselas a la ligera:

- Bandwidth (ancho de banda), si bien es cierto el internet es la base de la computación en la nube, también exigen que el cliente implemente algunas normas en este servicio para evitar problemas.
- Desconfianza: esto se debe a que los usuarios no aceptan en su totalidad la idea de que su información personal esté en manos de otros.
- Posibles errores en los equipos donde se almacena la información. No es cien por ciento confiable.
- Falta de control de parte de los usuarios hacia los servidores. Esto puede producir problemas en el tiempo de respuesta.
- Migrar datos: esto puede ser crítico al momento de cambiar de proveedor.
- Invasión de privacidad por parte de terceros.

Seguridad Informática en la Nube

La nube es una herramienta tecnológica novedosa para los cibernautas, esto se debe a la gran capacidad que tiene de almacenamiento, aunque la vulnerabilidad de su seguridad es algo que aún no se puede controlar en su totalidad.

Una de las principales vulnerabilidades más críticas es el poco control que poseen en su infraestructura, ya que el usuario le brinda un cierto porcentaje de control al proveedor del servicio de la nube, de esta manera lo expone a posibles vulnerabilidades y el proveedor del servicio no garantiza compromiso de lo que pueda suceder con la información. En la actualidad esta tecnología está siendo objeto directo para los ataques cibernéticos, ya que está

teniendo bastante acogida por los cibernautas, lo cual hace que tenga mayor rentabilidad y la hace atractiva ante estos ataques maliciosos. (Mackay, Baker, & Yasiri, 2017)

Empezando por uno de los factores más relevantes, los cuales son los datos y la seguridad. Las empresas que se encargan de guardar la información de los cibernautas, buscan la manera de que sea de la manera más segura que les sea posible, para esto los proveedores garantizan realizar supervisiones y controles independientes para proteger la información. (Mackay, Baker, & Yasiri, 2017)

No obstante, no es posible decir que alguna medida de seguridad será cien por ciento segura, mejor sería decir que la dirección profesional en la gestión de servicios en la nube, ofrece una considerable seguridad.

Sin embargo, no todo termina ahí, el problema de la seguridad, sigue, va más allá de eso, pues los ataques cibernéticos varían, por lo que la seguridad de la nube es más que solo asegurar la protección de los datos. Además, la información no es tan privada como uno cree, ya que uno mismo sin darse cuenta la expone en internet, por ejemplo, publicando datos personales en las redes sociales. (Mackay, Baker, & Yasiri, 2017)

Para lograr alcanzar algo verdaderamente efectivo, se requiere de varios factores, en los cuales se destacan los actos de los cibernautas, ya que, si los cibernautas no hacen uso apropiado de las medidas de seguridad, no existe la garantía de que no sean objetivos de futuros ataques informáticos.

Los principios en seguridad de Computación en la nube abarcan los siguientes puntos:

- Seguridad física y lógica.
- Implicaciones técnicas.

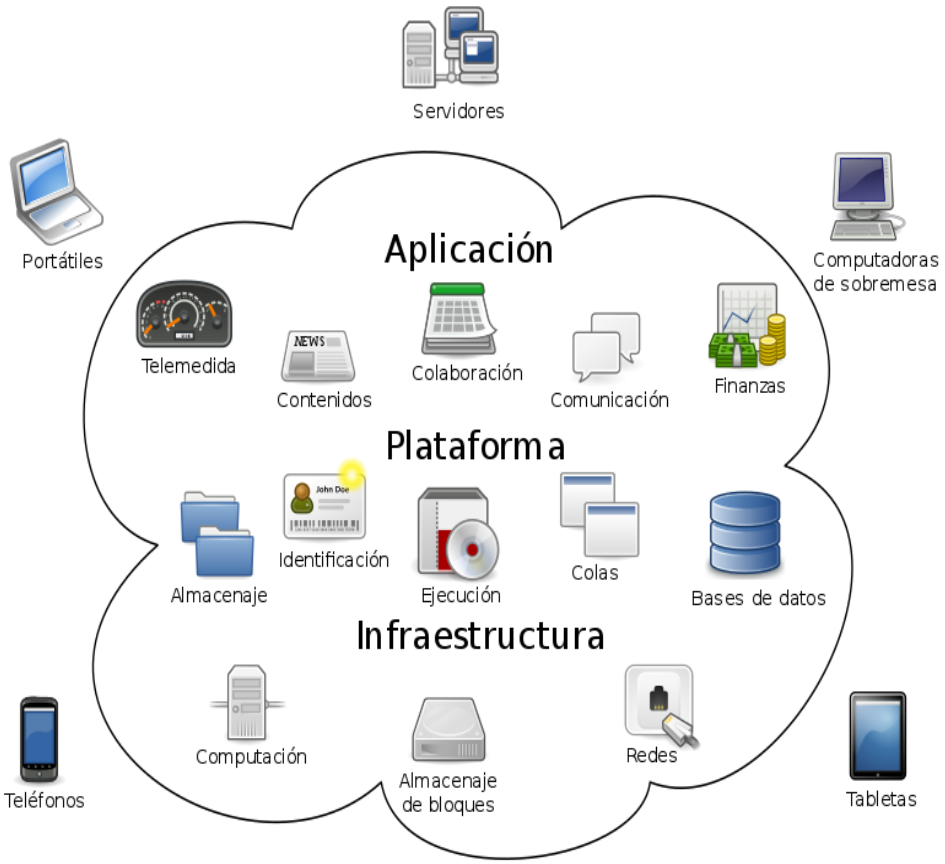

Gráfico 3. Diagrama que muestra esquemáticamente la computación en la nube, con típicos ejemplos de aplicaciones compatibles con ese modelo informático – Autor: Sam Johnston

Aspectos Técnicos de Seguridad

El uso de la computación en la nube conlleva un grupo de grandes riesgos, por lo tanto, la organización especializada en Ciberseguridad Cloud Security Alliance (CSA) determinó las amenazas más potentes en el entorno de Cloud Computing (Computación en la nube): (CSA, 2022)

- Vulneración de la privacidad: sucede cuando la información secreta ha sido robada o copiada por personas no autorizadas.
- Pérdida de información: sucede cuando existen fallas en el sistema de almacenamiento o al momento de transmitir la información.
- Secuestro/intervención de cuentas o servicios: proceso en el que un correo electrónico es robado por personas malintencionadas, con fines maliciosos.

  Interfaz de programación de Aplicaciones insegura: existe la posibilidad de que exploten información o servicios sin ser autorizados, debido a las interfaces débiles.
- Denegación de servicios: invadir una red con fines maliciosos.
- Insider: personas con permiso de acceder a la red o información confidencial del cliente y que hacen usos de la misma para afectar sus principios de seguridad: integridad, confidencialidad, disponibilidad.
- Abusar de los servicios: usar de manera incorrecta los recursos disponibles.
- Diligencia dual insuficiente: usar los servicios de la nube sin tener en cuenta los peligros de la seguridad o sin realizar una comprobación de los controles de privacidad sin autorización y conocimiento del usuario.
- Hipervisores: inseguridades, debilidades y vulnerabilidades dentro de la tecnología que autorizan la validez y uso de la nube. (CSA, 2022)

El Cloud Computing (Computación en la nube) es una tecnología con varias opciones útiles y favorables que benefician a los usuarios, pero que también posee varios problemas seguridad, como se lo ha venido mencionando en el desarrollo de la investigación; y que puede causar grandes problemas, ya que es un objetivo atractivo para los atacantes informáticos, por tener una gran cantidad de información privada.

CONCLUSIONES

- En la plataforma de la nube no cuenta con un resguardo completamente confiable por lo que puede provocar la perdida de información los errores pueden ser del usuario o el sistema.
- Con las medidas de seguridad habladas en el proyecto se puede mejorar la gestión, traspaso y manejo de nuestra información.
- Debemos tener muy en cuenta la seguridad informática ya que es el proceso que nos detecta y previene las falencias de que esta puede tener.
- EL cloud computing es una plataforma muy usada por las personas ya que resguardan la información y que es la más codiciada por los que buscan privar su información.

ANEXO

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE SISTEMAS

Babahoyo, 10 de agosto del 2022

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de: el Sr. **CONTRERAS JIMENEZ DENNY MIGUEL** cuyo tema es: **DIFICULTADES TÉCNICAS DE SEGURIDAD DE LOS SERVICIOS EN LA NUBE** certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio, obteniendo como porcentaje de similitud de [1%]. resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la Institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.

Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

ING. LEÓN ACURIO JOFFRE VICENTE.
DOCENTE DE LA FAFI.

Referencias

Calle Arévalo, M. V. (2016). *Entorno legal sobre seguridad informática del sector financiero cooperativo ecuatoriano (Bachelor's thesis, Universidad del Azuay).*

CASTRO, M. I. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades. 3Ciencias*.

Cierco, D. (2019). *Cloud Computing: Retos y Oportunidades. Obtenido de https://books.google.es/books?hl=es&lr=&id=_fTJXVjOD90C&oi=fnd&pg=PA5&dq=cloud+computing&ots=6ILOOpG7fN&sig=egv6NQz5YrcgBphbyx2Upu9pPkg#v=onepage&q&f=false*.

CSA. (2022). *Emerging Cloud Technologies. Obtenido de https://cloudsecurityalliance.org/*.

GUAIGUA BUCHELI, C. J. (2021). *Algoritmos de seguridad para mitigar riesgos de datos en la nube: un mapeo sistemático.*

LÓPEZ MARTÍNEZ, A., & GADEA RAGA, A. (2016). *Datos personales y Cloud Computing.*

LÓPEZ, P. A. (2010). *Seguridad informática Editex.*

Mackay, B. &. (2017). *Security-oriented cloud computing platform for critical infrastructures. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0267364912001434*.

Mell, P. &. (2017). *The NIST definition of cloud computing. Obtenido de https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/referencespapers.aspx?referenceid=1788248*.

Miranda Cairo, M. V. (2016). *Metodología para la implementación de la gestión automatizada de controles de seguridad informática. 10(2), 14-26.* Revista Cubana de Ciencias Informáticas.

Miranda Cairo, M. V. (2017). *Sistemas de gestión de la seguridad informática.*

MOCHA-GUACHO, G., LÓPEZ, J. E., & PACHECO, J. C. (2018). *Gestión de eventos académicos universitarios: un servicio alojado en la nube.En Conference Proceedings UTMACH.*

Navas Navarro, S. (2015). *Computación en la nube: Big Data y protección de datos personales (Cloud Computing: Big Data and Personal Data Protection). InDret, 4.*

OMAZA SALDAÑA, K. J. (2020). *Arquitectura de Seguridad en la Nube: Revisión de la Implementación en AWS.*

Ramírez, X. G. (2019). *Seguridad en la nube,evolución indispensable en el siglo XXI. Revista vínculos, 16(1), 110-127.*

Voutssas, M. (2010). *Preservación documental digital y seguridad informática. Investigación bibliotecológica, 24(50), 127-155.*