ESTUDIO COMPARATIVO DE METODOLOGÍAS DE ASEGURAMIENTO PARA UN SERVIDOR LOCAL Y UN SERVICIO EN LA NUBE.

NORBERTO CÁRDENAS LUNA
1.124.853.746

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN MIGUEL AGREDA DE MOCOA
2021

ESTUDIO COMPARATIVO DE METODOLOGÍAS DE ASEGURAMIENTO ENTRE UN SERVIDOR LOCAL Y UN SERVIDOR EN LA NUBE.

NORBERTO CÁRDENAS LUNA
1.124.853.746

MONOGRAFÍA PARA OPTAR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR

Ing. JOEL CARROLL VARGAS M.Sc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN MIGUEL AGREDA DE MOCOA
2021

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

San Miguel Agreda de Mocoa, 27 de julio 2021

DEDICATORIA

Todos los esfuerzos que me llevaron a conseguir este título, se lo debo exclusivamente a mis padres, quienes día a día se han sacrificado para que pueda salir adelante con mis proyectos, además, de brindar ese apoyo incondicional en todo momento, sin importar las circunstancias ni el momento, a ellos les dedico este triunfo.

AGRADECIMIENTOS

Agradecer a mis padres por demostrar en cada momento su apoyo incondicional en todo el proceso formativo en el cual siempre me acompañaron sin importar los sacrificios que les tocaba hacer.

A mi novia, Rocío por demostrar su cariño y apoyo incondicional que siempre a estado presente en los momentos difíciles.

CONTENIDO

pág.

RESUMEN 11

INTRODUCCIÓN 12

1 PLANTEAMIENTO DEL PROBLEMA 13

2 FORMULACIÓN DEL PROBLEMA 14

3 JUSTIFICACIÓN 15

4 OBJETIVOS 16

4.1 OBJETIVO GENERAL 16

4.2 OBJETIVO ESPECIFICO 16

5 MARCO REFERENCIAL 17

5.1 MARCO TEÓRICO 17

5.1. Computación en la nube (*Cloud Computing*) 17

5.1.2 Software como servicio. 18

5.1.3 Plataforma como servicio. 18

5.1.4 Infraestructura como servicio. 19

5.1.5 Infraestructura local (*On-Premise*). 19

5.1.6 Sistema de gestión de la seguridad de la información – SGSI. 20

5.1.7 ISO/IEC 27005:2008.....21

5.1.8 Magerit.....23

5.1.8.1 Comparativa ISO/IEC 27001 – MAGERIT... **¡Error! Marcador no definido.**

5.1.9 Gestión de información en un servidor en la nube. 25

5.1.10 Aspectos de seguridad. 26

5.1.11 Seguridad de los datos. 26

5.1.12 Gestión Información en un servidor local.....27

5.1.13 Comparativa servidor local y servidor en la nube 27

5.1.14 Problemas de servidor local y un servidor en la nube 30

5.1.15 Servidor en la nube.....30

5.1.16 Servidor local. 32

5.2 MARCO CONCEPTUAL 32

5.3 ANTECEDENTES 33

5.3.1 Antecedente No 1 33

5.4 MARCO LEGAL 33

5.4.1 Ley 1273. 33

5.4.2 Ley 1343. 34

5.4.3 ley 527 de 1999. 34

6 METODOLOGÍA DE DESARROLLO DEL PROYECTO.....35

7 IDENTIFICACIÓN DE LAS PROBLEMÁTICAS DE LAS METODOLOGÍAS DE ASEGURAMIENTO PARA LA SEGURIDAD INFORMÁTICA.....36

8 COMPARATIVA DE LAS METODOLOGÍAS DE ASEGURAMIENTO DE LA INFORMACIÓN. 38

8.1 RED LOCAL.....38

8.1.1 Costos 39

8.1.2 Desventajas.....40

8.2 RED EN LA NUBE 41

8.2.1 Costos 42

8.2.2 Ventajas.....43

9 EVALUACIÓN DE LA METODOLOGÍA.....44

CONCLUSIONES. 47

RECOMENDACIONES. 48

BIBLIOGRAFÍA.....49

LISTA DE TABLAS

pág.

Tabla 1 Características computación en la nube 17
Tabla 2 Desventajas Cloud Computing.....18
Tabla 3 Características infraestructura local.....20
Tabla 4 Modelo PHVA aplicado a los procesos de SGSI.....22
Tabla 5 Ventajas y desventajas ISO/IEC 27005:2008 23
Tabla 6 Ventajas y desventajas de MAGERIT.....24
Tabla 8 Comparativa servidor local y servidor en la nube 28
Tabla 9 Problemas de servidor local y un servidor en la nube.....30
Tabla 9 Comparativa ISO/IEC 27005 y MAGERIT.....36
Tabla 10 Valor de una Firewall FortiGate 400E Series.....40
Tabla 11 CAPEX y OPEX 40
Tabla 13 Comparativo de características CLOUD y ON-PREMISE.....44

LISTA DE FIGURAS

pág.

Figura 1 Capas IT y Capas Cloud.....19

Figura 2 Topología red local 39

Figura 3 Topología red en la nube.....41

RESUMEN

Cada vez que una empresa empieza a crecer y sus procesos de negocio también, se ven obligadas a buscar la mejor solución para que sus sistemas de información operen de la mejor manera. Para muchas se vuelve en una tarea complicada, porque es una dedición que puede marcar el rumbo de su negocio. Hay muchas preguntas que se pueden plantear, pero la mas importar es la elección de un sistema o servicio basado en la nube o servicio local.

Si bien, actualmente los servicios en la nube se han vuelto tan populares y en algunas ocasiones resulta imposible negarse a la adquisición de estos servicios por las grandes ventajas que puede llegar a presentar en un futuro; sin embargo, es muy común ver como personas lideres de TI (Tecnologías de la información) aún debaten entre estas dos opciones, donde se preguntan cual puede operar mejor en temas de accesibilidad, seguridad, escalabilidad, disponibilidad, entre otras.

Por lo anterior, en el presente trabajo se presenta un comparativo de un servidor en la nube y local, donde se detalla las distintas características, ventajas, desventajas y costos que se presentan por la elección de alguno de estos servicios.

INTRODUCCIÓN

En la actualidad, las grandes empresas y algunas medianas compañías están obligadas a administrar el crecimiento exponencial de sus datos generados. Todo esto conlleva al aumento de sus procesos críticos, que por ningún motivo pueden presentar interrupciones. Este escenario plantea una serie de problemas para las organizaciones, entre los que se destacan la capacidad y seguridad para salvaguardar la información de sus procesos, por lo tanto, cada vez se convierte en una actividad difícil de gestionar desde un entorno de infraestructura local. Es aquí donde se preguntan: ¿La información de la empresa están a salvo ante algún desastre natural, malware u otro tipo de amenaza? ¿Se posee la infraestructura adecuada para manejar los datos sin sufrir contratiempos? Si las organizaciones no se sienten en las mejores condiciones para responder las preguntas anteriores, es inevitable pensar en la perdida de la información y que esto puede ocasionar un gran impacto negativo, lo que se debe evitar a toda costa. Además, se debe tener una gran cantidad de recursos económicos para los gastos inicial de la infraestructura tecnológica requerida inicialmente.

Las plataformas en la nube o *CLOUD* nacieron principalmente para enfrentar el escenario mencionado anteriormente, aunque no solo estos. Amazon Web Services, Microsoft Azure y Google Cloud Platform son proveedores de tecnologías en la nube que los profesionales de TI las utilizan para crear, implementar y administrar los servicios a través de internet.

Este tipo de tecnología aportan una gran robustez a los sistemas de las empresas, porque se caracterizan por ofrecer una solución a los escenarios antes descritos. Esta clase de servicios no requieren realizar un mantenimiento del hardware, la inversión en infraestructura es casi nula, aporta gran seguridad de los datos. La poca inversión será reflejada en las terminales y una buena conexión a internet. Actualmente las empresas están migrando sus servicios a la nube, como son los servicios web, email, archivos, etc.

En el presente trabajo tiene como objetivo describir dos metodologías de aseguramiento, donde se realizará una comparativa de las ventajas, desventajas, costos y riesgos que pueden presentar en una infraestructura en la nube y local.

1 PLANTEAMIENTO DEL PROBLEMA

Un sistema de gestión de la seguridad de la información, en las empresas es el que permite establecer las políticas, procedimientos y controles, con la finalidad de que siempre se pueda controlar los posibles riesgos. Sin embargo, en las organizaciones, por lo general en las *pymes*, desde la alta dirección toman la seguridad de la información como gastos y solo implementan algunos controles físicos de la seguridad, lo que resulta una falta sensación de protección, dejando a un lado el cumplimiento de alguna de las metodologías de aseguramiento y al personal de la empresa, sabiendo que estos dos componentes son los que más importancia tienen al momento de proteger la información.

El mayor riesgo de sufrir ciberataques o ciberespionaje son las *pymes,* principalmente por la falta de los recursos y, además, por la poca importancia en este aspecto. Aunque las empresas pequeñas sean atacas no significa que no poseen información importante y confidencial que proteger, sino que, sin darse cuenta pueden ser la puerta trasera de una gran empresa para los atacantes.

La mayoría de los ataques, errores y fallos de la seguridad pueden evitarse con la implementación de un sistema de gestión de seguridad de la información, cumpliendo los diferentes aspectos que se establecen en cada metodología de aseguramiento como son la ISO 27001-2013, COBIT, ITIL, entre otros.

2 FORMULACIÓN DEL PROBLEMA

¿Un estudio comparativo de metodologías de aseguramiento entre un servidor local y un servicio en la nube, permitirá determinar cuál es la técnica más conveniente en el aseguramiento de la información en las empresas dependiendo su aplicabilidad?

3 JUSTIFICACIÓN

Los delitos informáticos cada día son mayores y van creciendo una cantidad considerable de programas malignos en todo el mundo. Esto ha obligado a que profesionales del sector de TI empiecen a especializar sus conocimientos entorno a la seguridad de la información. Lo cual pretende estar al día con las temáticas de cómo operan los ciberdelincuentes y que tipos de metodologías o técnicas utilizan. Esto ha llevado a que las grandes organizaciones sean conscientes del riesgo que están expuestos día a día e inviertan un poco más de recursos para tratar de prevenir posibles ataques cibernéticos.

En Colombia como en muchos países latinoamericanos son víctimas de constantes ataques de seguridad informática, a través de diferentes técnicas delictivas como son los virus, accesos no autorizados a los sistemas de información de sus empresas, entre otros, los cuales intentan sabotear y dañar información importante en las empresas lo que ocasiona pérdidas financieras que pueden llegar a ser invaluables.[1]

Los servicios en la nube en la actualidad cuentan con las grandes certificaciones de seguridad y privacidad existentes. Como es el caso de Microsoft Azure[2] que cumplen un amplio abanico de normas internacionales y especificas dependiendo del sector donde se encuentre su centro de datos como el Reglamento General de Protección de Datos (RGPD), ISO 27001, HIPAA, FedRAMP, SOC 1 y SOC 2, así como normas específicas de cada país, entre las que se incluyen: IRAP en Australia, G-Cloud en el Reino Unido y MTCS en Singapur. Auditorías de terceros rigurosas, como las del Instituto Británico de Normalización.

En este punto es importante reconocer que las empresas con infraestructura *On-Premise*, están expuestas a muchas amenazas informáticas. Para que una PYME pueda acceder a un tipo de certificación, la entidad está en la obligación de hacer una inversión considerable de recursos económicos para poder contemplar todos los parámetros que exigen la normatividad a la cual se pretenda certificar.

Por tal motivo se pretende a través del presente documento dar a conocer y sensibilizar a todas las personas de los beneficios y las metodologías que dispone cada tipo de servicio como lo es basado en la nube o local.

---

[1] SANCHEZ CASTILLO, Zulay Nayiv. Trabajo de grado: Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia [en línea]. repository.unad.edu.co. (2017). [Consultado: 09 de marzo del 2020]. Disponible en internet: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

[2] Microsoft. (s.f.). Microsoft Azure. Recuperado el 08 de octubre de 2018, de https://azure.microsoft.com/es-es/overview/trusted-cloud/

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar un estudio comparativo de las metodologías de aseguramiento entre un servidor local y un servicio en la nube que permita determinar cómo es la seguridad en la gestión de la información

4.2 OBJETIVO ESPECIFICO

- Identificar las posibles problemáticas de las metodologías de aseguramiento para la seguridad informática en gestión de la información de un servidor local y un servicio en la nube
- Comparación de dos metodologías de aseguramiento para la seguridad informática en gestión de la información de un servidor local y un servicio en la nube
- Evaluación de las dos metodologías de aseguramiento para la seguridad informática.

5 MARCO REFERENCIAL

5.1 MARCO TEÓRICO

5.1.1 Computación en la nube (*Cloud Computing*)[3] Es un modelo que permite bajo demanda y por medio de una red de datos a un conjunto de recursos compartidos y configurables (como servidores, redes, almacenamiento de datos, aplicaciones, servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor del servicio. En la siguiente tabla se describen las principales características de la computación en la nube.

Tabla 1 Características computación en la nube

Característica	Descripción
Autoservicio bajo demanda	El usuario adquiere los productos de la computación en la nube a medida que los va requiriendo de forma automática, sin necesidad de la intervención de las personas del proveedor.
Múltiples formas de acceder a la red	Los recursos que provee son de fácil acceso por medio de la red y por diferentes dispositivos de usuario, desde celulares hasta computadores personales.
Recursos compartidos	Todos los recursos (memoria, almacenamiento, acho de banda, máquinas virtuales, etc.) que se proveen en la nube, son compartidos a diferentes usuarios, a quienes se asignan recursos de forma dinámica dependiendo de las peticiones de los usuarios.
Elasticidad	Los recursos son liberados de forma automática y rápidamente.
Servicio medido	Tanto el usuario como el proveedor del servicio tienen acceso al consumo de recursos real por cada usuario, lo que facilidad para el momento de pagar por lo consumido.

Fuente: CIERCO, David. Cloud Computing: Retos de oportunidades [En línea]. Fundaciones IDEAS. 2011. Disponible en https://books.google.com.co/books?id=_fTJXVjOD90C&printsec=frontcover&hl=es#v=onepage&q&f=false

[3] CIERCO, David. Cloud Computing: Retos de oportunidades [En línea]. Fundaciones IDEAS. 2011. Disponible en https://books.google.com.co/books?id=_fTJXVjOD90C&printsec=frontcover&hl=es#v=onepage&q&f=false

Cuando un sistema de información mediante la plataforma SaaS (Software como un Servicio), tanto el aplicativo como los datos son alojados en las instalaciones del proveedor de servicios, a los cuales se puede acceder a través de una red internet mediante cualquier dispositivos móviles o computadores personales.

Tabla 2 Desventajas Cloud Computing

Desventajas
Dependemos de nuestro proveedor de servicio.
Dependemos directamente de una conexión a internet.
Privacidad de la información, es necesario contratar un proveedor que garantice este ítem.

Fuente: el autor.

5.1.2 Software como servicio[4]. (*Software as a service* - SaaS), es un servicio que provee toda la capacidad de que las aplicaciones que el proveedor le suministra corran en una infraestructura en la nube, las cuales pueden ser accesible a través de un navegador web, por ejemplo, correo electrónico. El usuario desconoce de la infraestructura en la cual opera el servicio.

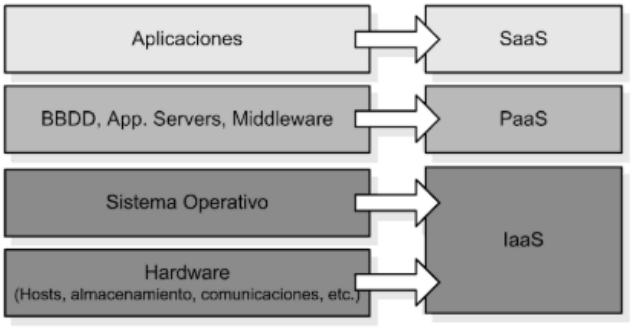
5.1.3 Plataforma como servicio[5]. Conocido como PaaS o *platform as a Service*, este modelo proporciona una capa de aplicación integrada por los principales elementos necesarios para permitir que los desarrolladores puedan desplegar sus aplicaciones. Es un nivel de servicio intermedio. El usuario es el responsable del aprovisionamiento de la plataforma integral, el cual no requiere adquisición o mantenimiento de la infraestructura tanto física como lógica. Un ejemplo es Microsoft Azure.

[4] CIERCO, David. Cloud Computing: Retos de oportunidades [En línea]. Fundaciones IDEAS. 2011. Disponible en https://books.google.com.co/books?id=_fTJXVjOD90C&printsec=frontcover&hl=es#v=onepage&q&f=false

[5] CARPENTIER, Jean-François. La seguridad informática en la PYME: Situación actual y mejores prácticas. [En línea]. Barcelona: Ediciones ENI. 328 p. [Consultado el 28 de noviembre del 2020]. Disponible en: https://books.google.com.co/books/about/La_seguridad_inform%C3%A1tica_en_la_PYME.html?id=LKE5_6gzBmgC&redir_esc=y

5.1.4 Infraestructura como servicio.[6] IaaS, permite a los usuarios acceder a servicios como: el uso de las CPU, capacidad de almacenamiento, máquinas virtuales, sistemas operativos, etc. Todo aquello que está directamente relaciona con la infraestructura IT, el cual es necesario para la construcción de una plataforma tecnológica. Un ejemplo para este modelo, son las máquinas virtuales que ofrecen los proveedores de servicios en la nube, de acuerdo con las necesidades del proyecto, se podrá contratar los recursos adecuados para su implementación.

Figura 1 Capas IT y Capas Cloud



Fuente: MORA PEREZ, José Juan. Capas IT y Capas Cloud. [Imagen]. Capacity Planning IT: Una Aproximación Práctica. Madrid: CreateSpace Independent Publishing Platform. 2012. p. 444. [Consultado: 20 de noviembre del 2018] Disponible en: https://books.google.com.co/books?id=FqU93uMPivMC&printsec

5.1.5 Infraestructura local (*On-Premise*).[7] Cuando se habla de que una infraestructura es *On-Premise*, hace referencia a que se encuentra en las instalaciones de la empresa o cliente. *On-Premise* significa lo mismos que *In-House* o en casa, por ejemplo, una empresa que tenga sus propios centros de datos, sus unidades de almacenamiento, servidores, *switches*, entre otros, este es un caso de una infraestructura *On-Premise*.

[6] MORA PEREZ, José Juan. Capas IT y Capas Cloud. Capacity Planning IT: Una Aproximación Práctica. Madrid: CreateSpace Independent Publishing Platform. 2012. p. 444. [Consultado: 20 de noviembre del 2018] Disponible en: https://books.google.com.co/books?id=FqU93uMPivMC&printsec

[7] PARRA M, Maureen V.; GUILLÉN, Edward P. Servicios de autenticación y autorización orientados a internet de las cosas. En: *Revista Telemática*. La Habana. Universidad Tecnológica de La Habana "José Antonio Echeverría". Mayo – agosto 2018. vol. 17 nro. 2. p. 42 – 51. [Consultado: 30 de noviembre del 2019]. Disponible en http://www.revistatelematica.cujae.edu.cu/index.php/tele/article/view/302/278. ISSN 1729-3804.

Tabla 3 Características infraestructura local

Característica
Todos los componentes mencionados están en las instalaciones de la empresa.
La instalación, mantenimiento y garantía de todos los componentes son responsabilidad de la empresa.
Requiere persona con muchos conocimientos o de terceros.
El personal de TI y mantenimiento pueden tener acceso físico.
La seguridad física y de aplicaciones es responsabilidad de la empresa.
Las certificaciones de los centros de datos, renovaciones, certificaciones de cableados y demás equipamiento que se encuentran dentro del centro de datos son responsabilidad de la empresa dueña del centro de datos.
Las licencias deben ser compradas por la empresa.

Fuente: PARRA M, Maureen V.; GUILLÉN, Edward P. Servicios de autenticación y autorización orientados a internet de las cosas. En: *Revista Telemática*. La Habana. Universidad Tecnológica de La Habana "José Antonio Echeverría". Mayo – agosto 2018. vol. 17 nro. 2. p. 42 – 51. [Consultado: 30 de noviembre del 2019]. Disponible en http://www.revistatelematica.cujae.edu.cu/index.php/tele/article/view/302/278. ISSN 1729-3804.

5.1.6 Sistema de gestión de la seguridad de la información – SGSI.[8] Un SGSI es el concepto central en el cual se constituye la ISO 27001. La gestión de la seguridad debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Para garantizar que la seguridad de la información es gestionada correctamente, inicialmente se debe identificar su ciclo de vida y los aspectos relevantes adoptados para garantizar la confidencialidad, integridad y disponibilidad de la información.

[8] MARTELO, Raúl; MADERA, Jhonny y BETÍN, Andrés. Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). En: *Revista Información Tecnológica*. [En línea]. La Serena – Chile. 2015. vol.26, n.2. p.129-134. [Consultado: 17 de marzo del 2020]. Disponible en <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642015000200015&lng=es&nrm=iso>. ISSN 0718-0764

5.1.7 ISO/IEC 27005:2008. Fue publicada el 4 de junio del 2008. Forma parte de la familia ISO 27000 dedicada a la seguridad de la información. Concuerda con elementos específicos establecidos en la BS 7799-3, además de tomar referencias de estándares reconocidos como "AS/NZS 4360:2004, Risk Management"[9]. Es un complemento de las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005, el cual establece una necesidad de crear un análisis de riesgo, pero no da directrices para su realización[10].

Esta norma es ideal para no tener ninguna duda con los elementos que toda buena metodología de análisis de riesgo debe incluir. Se describe en seis clausulas:

- **Clausula 7 Establecimiento del contexto**: acá se define los objetivos, alcance y la organización para le ejecución de todo el proceso

- **Clausula 8 Valoración del riesgo:** Se obtiene la información necesaria para conocer, valorar y priorizar los riesgos. Esta se divide en:

Identificación del riesgo: Que es lo que provoca las perdidas en la organización.

Análisis del riesgo: utiliza métodos cuantitativos o cualitativos con los que se obtiene información sobre la cuantificación de los riesgos que se identificaron.

Evaluación del riesgo[11]: Se compara los riesgos estimados con los criterios de evaluación y de aceptación de riesgo definidos en el establecimiento del contexto.

- **Clausula 9 Tratamiento del riesgo:** Se define la táctica con la que se va a tratar cada uno de los riesgos valorados.

- **Clausula 10 Aceptación del riesgo:** Se determina que riesgos son aceptados y su justificación.

---

[9] VELASCO CORTES, Ricardo. Gestión del riesgo basado en ISO/IEC 27005:2009 – ISO/IEC 31000:2011 ISO/IEC 28000:2008. [Sitio Web]. Universidad Piloto de Colombia. Bogotá. [Consultado: 18 de diciembre del 2019]. Archivo pdf. Disponible en http://polux.unipiloto.edu.co:8080/00002323.pdf

[10] ROMO DAZA, Karen y ORJUELA RIAÑO, Oscar. Análisis de riesgo y plan de tratamiento de seguridad de la información para una empresa del sector de transporte. [en línea]. Proyecto para optar el título de especialista en seguridad informática. Bogotá D.C. Universidad Piloto de Colombia. Facultad de ingeniería de sistemas. Dirección de Postgrados. 2012. 19 p. [Consultado: 19 de noviembre del 2019]. Disponible en http://polux.unipiloto.edu.co:8080/00000804.pdf

[11] TIPÁN GUAYTA, Kléver. Propuesta de políticas de seguridad de la información para la Corpaire. [en línea]. Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información. Quito. Escuela Politécnica Nacional. Facultada de ingeniería de sistemas. 2012. 28 p. [Consultado: 19 de noviembre del 2019]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf

- **Clausula 11 Comunicación del riesgo:** Se intercambia información sobre los riesgos entre todos los grupos de interés.

- **Clausula 12 Monitorización y revisión del riesgo:** El análisis del riesgo se actualiza con todos los cambios que pudieron afectar la valoración.

La ISO/IEC 27005:2008 sigue el ciclo de Deming, como se describe en la siguiente tabla.

Tabla 4 Modelo PHVA aplicado a los procesos de SGSI

Modelo PHVA	
Planificar (establecer el SGSI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Verificar (hacer seguimiento y revisar el SGSI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C. El instituto. 2006. 8 p.

Tipán Guayta, en su Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información, presenta una tabla donde se describen las Ventajas y desventajas ISO/IEC 27005:2008

Tabla 5 Ventajas y desventajas ISO/IEC 27005:2008

Ventajas	Desventajas
Es un complemento de la ISO 27001 y la ISO 27002.	No es certificable.
Es un estándar internacional lo que permite una mayor adaptación.	No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.
Posee una cláusula completa a la monitorización y revisión de los riesgos.	
Se lo considera en un alcance completo, tanto en análisis como en la gestión de riesgos.	
Posee una fase de adaptación de riesgo, previa su justificación.	
Permite un análisis completo cuantitativo.	

Fuente: TIPÁN GUAYTA, Kléver. Propuesta de políticas de seguridad de la información para la Corpaire. [en línea]. Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información. Quito. Escuela Politécnica Nacional. Facultada de ingeniería de sistemas. 2012. 21 p. [Consultado: 19 de noviembre del 2019]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf

5.1.8 Magerit.[12] Es una metodología de análisis y gestión de riesgos, que fue desarrollada por el consejo superior de administración electrónica de España. MAGERIT ofrece un método para el análisis de riesgos que se pueden presentar en el uso de las tecnologías de información y telecomunicaciones, con el objetivo de tomar los mejores controles que permitan mitigar los riesgos.

MAGERIT, analiza el impacto que puede tener una empresa al momento de que su seguridad informática sea vulnerada, buscando identificar las amenazas que pueden afectar a la empresa y las vulnerabilidades que pueden ser utilizadas por estas amenazas, todo esto permitiendo que se pueda tener un panorama claro sobre las medidas de prevención y corrección. Lo mejor que posee esta metodología es que cuenta con un instructivo o guía el cual se va especificando un paso a paso del análisis de riesgo.

Esta guía se divide en tres partes, que son: Método, donde se hace una descripción de la estructura que debe contar un modelo de gestión del riesgo, se basa en la estructura propuesta por la gestión del riesgo de la ISO. En la segunda parte, es un

[12] CORDERO TORRES, Geovanna. Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgo de la seguridad informática [En línea]. Trabajo de grado previo a la obtención del titulo de ingeniero de sistemas y telemática. Cuenta – Ecuador. Universidad del Azuay. Escuela de ingeniería de sistemas y telemática. 2015. 20 p. [Consultado: 20 de diciembre del 2019]. Disponible en Dspace de la Universidad del Azuay.

catálogo de elementos, se puede decir que es un inventario que pueden utilizar las empresas para enfocar el análisis de riesgo. Y el tercer y último elemento es una guía de técnicas donde se describe técnicas importantes que se implementan en un análisis de riesgo.

Los tres volúmenes son[13]:

- **Volumen 1 – Método:** Es donde se explica en detalle la metodología.

- **Volumen 2 – Catálogo de elementos:** Facilita varios inventarios de utilidad en la aplicación de la metodología, tienen la dimensión y criterio de evaluación, amenazas, tipos de activos, tipos de recursos de información y políticas.

- **Volumen 3 – Guía de técnicas:** Da una introducción a algunas técnicas que se utilizan en la fase de análisis de riesgo, tienen las técnicas específicas para el análisis de riesgo, técnicas generales.

En la siguiente tabla se presenta las principales ventajas y desventajas.

Tabla 6 Ventajas y desventajas de MAGERIT

Ventajas	Desventajas
Se la considera con un alcance completo, tanto de análisis como de la gestión del riesgo. Posee un extenso archivo de inventarios en lo referente a recursos de información, amenazas y tipo de activos. Permite un análisis completo cualitativo y cuantitativo. Dispone de una herramienta de soporte PILAR II Es una metodología líder en España, con buenos referentes de aplicación.	No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. No posee un inventario completo en lo referencia a políticas.

Fuente: TIPÁN GUAYTA, Kléver. Propuesta de políticas de seguridad de la información para la Corpaire. [en línea]. Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información. Quito. Escuela Politécnica Nacional. Facultada de ingeniería de sistemas. 2012. 21 p. [Consultado: 19 de noviembre

[13] TIPÁN GUAYTA, Kléver. Propuesta de políticas de seguridad de la información para la Corpaire. [en línea]. Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información. Quito. Escuela Politécnica Nacional. Facultada de ingeniería de sistemas. 2012. 23 p. [Consultado: 19 de noviembre del 2019]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf

del 2019]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf

5.1.9 Gestión de información en un servidor en la nube.[14] Hace unas dos o tres décadas atrás, las grandes empresas se veían en la necesidad de contar con espacios físicos de gran tamaño para almacenar toda su información. La implementación de esto llevaba a unos costos demasiados altos, una alternativa es la contratación de empresas especializadas a la gestión del archivo, esta fue una opción muy llamativa hasta llegar a posicionarse en el mercado. En la actualidad esta situación ha cambiado gracias a las tecnologías de la información y comunicación (TIC). Una nueva forma de disposición final de la información, la cual funciona con un modelo de almacenamiento en la nube, donde todos los datos están almacenados en un servidor virtual, disponibles desde cualquier sitio.

Por medio de la nube, los datos e información viajan más rápido en ambas direcciones por medio de sistemas de información que son más flexibles a la virtualización de los procesos, esto permite facilidad en la carga y descarga de contenido o la de implementar parches de seguridad a cientos de máquinas[15].

Las compañías que ofrecen los servicios en la nube son: Amazon Web Services, Microsoft Azure, Google Cloud, entre otras, estas son consideradas las opciones más económicas y eficiente para el almacenamiento y procesamiento de datos. El bajo de los costos es una causa para que muchas organizaciones cierren sus centros de datos y pasen a considerar el software y la computación en la nube como un servicio bajo demanda.[16]

Una característica de trabajar en la nube es que todo se simplifica, hay un ahorro tanto de software y mantenimiento de equipos. Todo se encuentra centralizado en internet, los empleados de las empresas acceden a las aplicaciones de estas por medio de una red de internet, sin tener instaladas en sus equipos.

Contar con una buena conexión a internet es muy importante, ya que este es el medio de acceso a las aplicaciones o información. Esto es una buena opción para los empleados porque les permite acceder desde cualquier lugar, incluso desde su casa.

---

[14] HENAO HENAO, Doris Liliana. La nube: gestión de información [En línea]. En: *El Colombiano*. Abril 25 del 2012. [Consultado: 15 de diciembre del 2019]. Disponible en: https://www.elcolombiano.com/historico/especial_tic_la_nube_gestion_de_informacion-JBEC_179275

[15] HARDY, Quentin. How Cloud Computing Is Changing Management. En: *Harvard Business Review*. [En línea]. Universidad de Harvard. 08 de febrero del 2018. [Consultado:16 de diciembre del 2020]. Disponible en: https://hbr.org/2018/02/how-cloud-computing-is-changing-management

[16] Ibid.

5.1.10 Aspectos de seguridad. Las empresas deben tener presente un aspecto muy importante al momento de la implementación de sus servicios en la nube, muchos confunden cloud pública o privado con externo o interno. La implementación en la nube debe evaluar el contexto interno, externo en lo que se refiere a la ubicación de los activos físicos, los recurso y la información. Además de quien hace uso, así como el personal responsable de su gestión, seguridad y cumplimiento de políticas de seguridad.[17]

Lo anterior no quiere decir que, si el activo se encuentra dentro o fuera de las instalaciones de la empresa no afecte a la seguridad y a la exposición del riesgo, al contrario, sí afecta. Pero se entiende que la seguridad también depende de:

- Los tipos de activos, recursos e información que están siendo gestionados
- Quién los gestiona y cómo
- Qué controles se han seleccionado y cómo han sido integrados
- Aspectos relacionados con el cumplimiento legal

5.1.11 Seguridad de los datos. La seguridad en la computación en la nube incluye los controles y la tecnología especifica que permite mitigar o dar cumplimiento a la seguridad de la información. Además de contar con los controles comunes de la seguridad de los datos (control de acceso, cifrado) existen otros dos métodos que ayudan a la gestión de la migración no autorizada de los datos a servicios en la nube como: [18]

- Monitorear los movimientos de grandes volúmenes de datos internos con herramientas especializadas de monitorización de actividad de base de datos (DAM - *Database Activity Monitoring*) y de monitorización de actividad en archivos (FAM - *File Activity Monitoring*).
- Monitorizar la migración de datos a Cloud con filtros URL y herramientas *Data Loss Prevention*.

En la computación en la nube, pública, privada y los diferentes modelos es recomendable proteger los datos en tránsito, esto incluye:

- Los datos moviéndose desde la infraestructura tradicional a los proveedores.

[17] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES. Seguridad en la Nube. Guia Nro 12 Seguridad y privacidad de la información. 2016. [Consultado: 07 de diciembre del 2019]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

[18] Ibid., p. 22

- Cloud, incluyendo público/privado, interior/exterior y otras combinaciones.

- Los datos migrando entre los proveedores de Cloud.

- Los datos moviéndose entre instancias (u otros componentes) en un Cloud determinado.

Existen otras opciones como:

- **Cifrado Cliente/Aplicación:** Los datos son cifrados en un extremo, puede ser en servidor antes de enviar por la red o ya están cifrados y almacenados en un formato adecuado. Incluye cifrado en el cliente local.

- **Cifrado Enlace/Red:** Existen técnicas de cifrado de red estándares como SSL21, VPNs22 y SSH23. Se puede utilizar tanto software como hardware. Es ideal implementar de extremo a extremo, aunque algunas ocasiones no es compatible con todas las arquitecturas.

- **Cifrado basado en proxy:** Esta opción es escogida con más frecuencia para la integración de aplicaciones *legacy*, trata de enviar los datos a un servidor proxy el cual se encarga de encriptar los datos antes de ser enviados por la red.

5.1.12 Gestión Información en un servidor local. Los servidores locales son dispositivos los cuales requieren de un espacio físico, que debe de estar acondicionado para su correcta operación, una configuración y un mantenimiento. La puesta en funcionamiento de este tipo de servidores varía dependiendo de las necesidades de la empresa y las características del servidor, pero por lo general es un proceso que requiere tiempo y un personal experto en el tema.

Cuando una empresa va creciendo, está por lo general va a generar una gran cantidad de información, lo cual requerirá un lugar donde almacenarse de forma segura y un mejor procesamiento de los datos. Los servidores locales cuentan con una capacidad limitada, en sus inicios tendrá que definir muy bien el almacenamiento que necesitará en los próximos años, si no se deberá realizar otra inversión para la adquisición de un nuevo servidor.

5.1.13 Comparativa servidor local y servidor en la nube

Los servidores que se encuentran operando en una empresa requieren varios ítems para que estos pueden operar en condiciones normales y optimas. Si se requiere de alguna certificación en cuanto a infraestructura, seguridad, etc. La entidad será la encargada de realizar el respectivo proceso para poder optar por una de estas

certificaciones, a lo que se requiere de un personal capacitado y de recursos económicos.

Cuando hablamos de un servidor que está alojado en la nube, poseemos unas grandes ventajas, con respecto a lo mencionado anteriormente, es el proveedor del servicio quien se encarga de todo el proceso de certificación y de la implantación de seguridad.

A continuación, se realiza una comparativa de los servidores en la nube y los servidores locales.

Tabla 7 Comparativa servidor local y servidor en la nube

	Servidor local	Servidor en la nube
¿Cómo trabaja?	Trabaja con sistemas que están ubicados en el mismo lugar de la empresa. Los procesos, almacenamiento se realiza internamente, sin la necesidad de una instalación remotas o en la nube	Trabaja con servidores que están en internet o la nube, estos están a cargo de la misma empresa proveedora (*amazon web service, Microsoft*) o de un tercero. Los servidores pueden estar ubicados en cualquier parte del mundo y son utilizados para almacenar información y administrar los datos de una empresa.
Hábitos de uso	En los servidores locales al momento de la implementación se suelen tener gastos de capital para poner en marcha sus actividades, Prefieren tener soluciones confiables por adelantado y saber exactamente cuánto se están gastando	Para sustentar sus actividades en los servidores en la nube, se suele implementar un sistema de pago por consumo, se prefiere una operación económica inicial por sobre la inversión a largo plazo
¿Qué hace cada día?	Las empresas que cuentan con sus servidores locales confían en sus experiencia e innovación para mantener operando estos.	Las empresas que cuentan con sus servidores en la nube confían en sus experiencia e innovación para mantener operando estos.

Tabla 8 (Continuación)

	Servidor local	Servidor en la nube
¿Qué hace cada día?	Entre sus responsabilidades diarias están: Acceder a la información almacenada en los servidores locales. Procesar datos. Verificar el cumplimiento de las políticas de seguridad. Recolectar y revisar la actividad de los usuarios. Diseñar y mantener la infraestructura y el equipamiento de la red local.	Entre sus responsabilidades diarias están: Acceder a la información almacenada en la nube. Procesar datos utilizando aplicaciones implementadas o basadas en la nube. Verificar el cumplimiento de las políticas de seguridad. Establecer permisos para almacenar datos y carpetas en la nube. Implementar rápidamente nuevas aplicaciones, códigos, bases de datos en la nube. Monitorear el ancho de banda de internet.
Ventajas	Control absoluto. Fácil integración con los procesos existentes. Implementación personalizada. Libertad de mantener la privacidad de datos.	Capacidad de escalar. Rapidez y control para implementar actualizaciones. Bajo costos de energía. Simple configuración e implementación.

Fuente: el autor

5.1.14 Problemas de servidor local y un servidor en la nube

En la actualidad disponer de un servidor loca o de un servidor en la nube conlleva a muchas responsabilidades, de las cuales si no se acatan de la mejor manera puede resultar un problema más grande a futuro, a continuación, se presenta unos posibles inconvenientes que pueden resultar para cualquier tipo de tecnología.

Tabla 8 Problemas de servidor local y un servidor en la nube

Servidor local	Servidor en la nube
El costo de mantener todo en funcionamiento.	La posibilidad de que el precio aumente mensualmente.
La posibilidad de que los equipos fallen.	Un soporte costoso sin ayuda personalizada.
Políticas de seguridad débiles o desactualizadas.	Control limitado sobre sus datos. Poco conocimiento sobre como el proveedor aloja sus datos.
El tiempo empleado para la realización de actualización e implementación de software.	Interrupciones por problemas de conexión a internet.
El espacio limitado para un nuevo hardware.	La necesidad de asegurar datos sensibles y bases de datos.

Fuente: el autor

5.1.15 Servidor en la nube. Para los servicios en la nube, dentro de la familia de normas de la ISO está: ISO/IEC 27017 Código de prácticas para los controles de seguridad de la información en base a la norma ISO/IEC 27002 para los servidores en la nube. Esta norma proporciona una serie de controles para los proveedores y clientes de servicios en la nube. A diferencia de otras normas, la ISO/IEC 27017 aclara la responsabilidad y funciones de ambas partes para ayudar que lo servicios en la nube sean lo más seguros como el resto de los datos incluidos en un sistema de gestión de la información.[19]

La norma proporciona un total de 37 controles en la nube, los cuales están basados en la ISO/IEC 27002, además incluye otros 7 nuevos controles *cloud* los cuales son:

[19] BRITISH STANDARDS INSTITUTION. ISO/IEC 27017. Controles de Seguridad para Servicios Cloud. [Sitio web]. [Consultado: 22 de diciembre del 2019]. Disponible en: https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

- Quién es responsable de lo que ocurre entre el proveedor del servicio *cloud* y el cliente *cloud*

- La eliminación/devolución de activos cuando un contrato se resuelve

- Protección y separación del entorno virtual del cliente

- Configuración de una máquina virtual

- Operaciones y procedimientos administrativos relacionados con el entorno *cloud*

- Seguimiento de la actividad de clientes en la nube

- Alineación del entorno de la red virtual y *cloud*

ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI) Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos. Los fundamentos de las mejores prácticas de ITIL proporcionan una base sólida para las organizaciones que tienen sus servidores basados en la nube.

Esencialmente, la nube es otra forma de entregar TI, por lo que muchos de los fundamentos de ITIL y la gestión de servicios de TI no cambian radicalmente. Hay dos cosas en la que ITIl y la nube se enfocan, servicios y procesos. ITIL considera que un servicio es una forma con la que los usuarios ganen valor sin asumir la propiedad, costos por riesgos del servicio. Al usar lo servicios en la nube, las organizaciones no tienen responsabilidad de los riesgos o costos asociados, simplemente están de acuerdo con ciertas funcionalidades y características del servicio y precio que debe pagar.

ITIL proporciona una aplicación fácil, probada, principios, métodos y técnicas que pueden aplicarse a un entorno de la computación en la nube. Ayuda a las organizaciones adaptarse a las soluciones de computación en la nube con un equilibrio adecuado de administración de TI robusta. Además, muchas de las estrategias de ITIL son relevantes para la computación en la nube, con algunos procesos de ITIl que ahora son utilizados de manera más dinámica para adaptarse a la computación en la nube de madera más efectiva.

5.1.16 Servidor local. ITIL proporciona un marco de referencia con las mejores prácticas para la gestión de servicios TI y los procesos conexos, el cual provee un enfoque de alta calidad que permite lograr los más altos estándares de efectividad en la gestión TI. Las empresas que cuentan con sus servidores en un entorno local, independiente de esto, ITIL puede aplicar las buenas prácticas, siempre y cuando el negocio tenga formalizada la gestión TI en una persona o departamento, ya que es imposible aplicar las buenas prácticas en la gestión del servicio si aún no se tiene formalizada la gestión de TI en la empresa. Una de las razones por las cuales es factible la implementación de ITIL es:

- Flexibilidad de ITIL
- Introducir las mejores prácticas en la gestión del servicio aporta una ventaja competitiva.
- Aprovechar el tamaño de las Pymes en la implementación de ITIL

5.2 MARCO CONCEPTUAL

Microsoft Azure: Es una plataforma de la empresa Microsoft, la cual provee diferentes servicios que están basados en la nube, tanto para las aplicaciones hasta servicios para procesar grandes cantidades de datos. También posee infraestructura como lo es el *Cloud Computing.*

Amazon Web Services: Son servicios basados en la nube publica que son ofrecidos por Amazon.com.

Confidencialidad: Desde el punto de vista de un sistema de información, la confidencialidad consiste en la capacidad que puede prestar un sistema para que solo personas o entidades autorizadas tengan acceso a la información.

Disponibilidad: Un sistema de información debe garantizar que en cualquier momento que requiera de el acceso a datos, este debe de responder y no presentar ningún inconveniente de ningún orden.

Integridad: Toda información que se almacene en un sistema de información debe contar con la protección para que esta no sea alterada sin autorización. La violación de la integridad de los datos puede llevarse a cabo a través de una persona, de un dispositivo o desde programa maligno, los cuales pueden modificar, eliminar datos sin previa autorización.

Riesgo: es aquella eventualidad que dificulta el logro de un objetivo. En lo referente a tecnología, el riesgo generalmente se plantea como una amenaza, fijando el nivel de exposición o el valor de perdida.

Magerit: Es una metodología que sirve de guía para ejecutar procesos de análisis de riesgos, además de poseer una lista de lineamientos para la gestión de los riesgos en el campo de la informática y todo lo relacionado alrededor de ellos en las empresas con el objetivo de cumplir con las metas propuestas en cada organización. [20]

5.3 ANTECEDENTES

5.3.1 Antecedente No 1. Análisis comparativo de software para levantar una infraestructura como servicio en cloud computing e implementación de una nube privada.

Autor: Angela María Pérez Castro

El objetivo principal por parte de la autora en el proyecto es la de establecer un método para gestionar fácilmente la infraestructura, la seguridad en le manejo de los datos, económicamente viable y que a futuro puede ser adoptado en la Universidad Técnica del Norte, esto permitirá determinar las dos infraestructuras más utilizadas como servicio y evaluando su instalación, costos y algunas variables métricas.

5.4 MARCO LEGAL

5.4.1 Ley 1273. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones." [21]

---

[20] ORTIZ MANRIQUE, Edwin Omar. Análisis de causas de riesgos en la protección de la información de la empresa soltec-ing y recomendaciones de seguridad [En línea]. Proyecto de grado para optar al título de especialista en seguridad informática. Malaga. Universidad nacional abierta y a distancia. Escuela de ciencias básicas, tecnología e ingenierías. Especialización en seguridad informática. 2018. 21 p. [Consultado: 19 de noviembre del 2019]. Disponible en: Repositorio UNAD. https://repository.unad.edu.co/bitstream/handle/10596/17448/13927687.pdf?sequence=1&isAllowed=y

[21] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 (5 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 47.223 de 5 de enero de 2009. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

5.4.2 Ley 1343. Por medio de la cual se aprueba el “Tratado sobre el Derecho de Marcas” y su “Reglamento”, adoptados el 27 de octubre de 1994. [22]

5.4.3 ley 527 de 1999. “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.” [23]

[22] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1343 (31 de julio de 2009). Por medio de la cual se aprueba el “Tratado sobre el Derecho de Marcas” y su “Reglamento”, adoptados el 27 de octubre de 1994. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 47.887 de 8 de noviembre de 2010. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1343_2009.html

[23] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 (18 de agosto de 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 43.673, de 21 de agosto de 1999. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

6 METODOLOGÍA DE DESARROLLO DEL PROYECTO

Para el desarrollo de la presente monografía se ha propuesta una metodología la cual está basada en 4 etapas las cuales se describen a continuación.

Etapa 1. Estado del arte

En esta etapa se realizará la elaboración de los marcos referenciales, que son los siguientes:

- Marco teórico.
- Marco conceptual.
- Marco legal.

Etapa 2. Identificación de problemáticas de las metodologías de aseguramiento de la información.

Para la identificación de las problemáticas, se realizará en dos metodologías de aseguramiento que son: ISO 27005 y MAGERIT

Etapa 3. Elaboración de la comparativa de las metodologías de aseguramiento de la información.

La comparativa de las dos metodologías de aseguramiento de la información se realizará basándose en diferentes aspectos como ventajas y desventajas.

Etapa 4. Evaluación de la metodología.

Se realizará la evaluación de los dos tipos de infraestructuras, en la nube y local (*On Premise*), donde se detallará en aspectos como, los costos de implementación, seguridad de la infraestructura, escalabilidad entre otros.

7 IDENTIFICACIÓN DE LAS PROBLEMÁTICAS DE LAS METODOLOGÍAS DE ASEGURAMIENTO PARA LA SEGURIDAD INFORMÁTICA.

En este capitulo se llevará una descripción de las metodologías ISO/IEC 27005 y MAGERIT donde se comparará aspectos como sus características, fases que componen cada metodología, ámbitos de aplicación, ventajas y desventaja.

Tabla 9 Comparativa ISO/IEC 27005 y MAGERIT

	ISO 27005	MAGERIT
Características	Está diseñada para ayudar la seguridad de la información apoyada en un enfoque de gestión de riesgos. Directrices para la correcta realización de un análisis de riesgos	No promueve nuevas funciones o mejoras para la implementación de controles de ciberseguridad, sino que recopila de otras normas como son la ISO, CIS, etc. Esta basada en cinco principios que son: Identificación, protección, detección, respuesta y recuperación.
Fases de la metodología.	Alcance. Normativas de referencia. Estructuras. Antecedentes. Visión del progreso de gestión de riesgos de seguridad de la información. Establecimiento del contexto. Tratamiento de riesgo. Aceptación de riesgo. Comunicación del riesgo. Monitorización y revisión del riesgo	Identificar activos, activos relevantes y su interacción y valoración. Determinar las salvaguardas que hay dispuestas y cuan eficaces son frente al riesgo. Estimar el impacto, daño sobre el activo derivado de la materialización de la amenaza. Estimar el riesgo, impacto ponderado con la tasa de ocurrencia de la amenaza

Tabla 9 (continuación)

	ISO 27005	MAGERIT
Ámbito de aplicación	Esta metodología puede ser aplicada a cualquier empresa tanto del sector privado como público, organizaciones no lucrativas, ONGs, o una entidad que gestione un SGSI. Que disponga de la intención de manejar los riesgos que podrían comprender la seguridad de la información en una entidad.	Gobierno, compañías grandes, PYMES, compañías comerciales y no comerciales. La metodología ofrece una aplicación para el análisis y gestión de riesgos de los sistemas de información, denominada PILAR. Esta herramienta es uso gratuito para organizaciones de España y de uso comercial para las organizaciones privada.
Ventajas	Es un complemento de la ISO 27001 y la ISO 27002. Es un estándar internacional lo que permite una mayor adaptación. Posee una cláusula completa a la monitorización y revisión de los riesgos. Se lo considera en un alcance completo, tanto en análisis como en la gestión de riesgos. Posee una fase de adaptación de riesgo, previa su justificación. Permite un análisis completo cuantitativo.	Se la considera con un alcance completo, tanto de análisis como de la gestión del riesgo. Posee un extenso archivo de inventarios en lo referente a recursos de información, amenazas y tipo de activos. Permite un análisis completo cualitativo y cuantitativo. Dispone de una herramienta de soporte PILAR II. Es una metodología líder en España, con buenos referentes de aplicación.
Desventajas	El proceso de certificación es largo, complejo y costoso.	No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir. No posee un inventario completo en lo referencia a políticas.

Fuente: Fuente: RAMÍREZ, Abby. Gestión de riesgos de seguridad de la información introducción al proceso de gestión de riesgos de seguridad de la información metodologías de análisis de riesgos. Barquisimeto: Universidad Centroccidental Lisandro Alvarado. Decanato de ciencias y tecnología. 2015.

8 COMPARATIVA DE LAS METODOLOGÍAS DE ASEGURAMIENTO DE LA INFORMACIÓN.

Para el desarrollo del presente capitulo, se procederá a realizar la comparativa de dos topologías de red: local y en la nube. Donde se analizará las principales características, costos, riesgos y administración que conlleva cada una de estas.

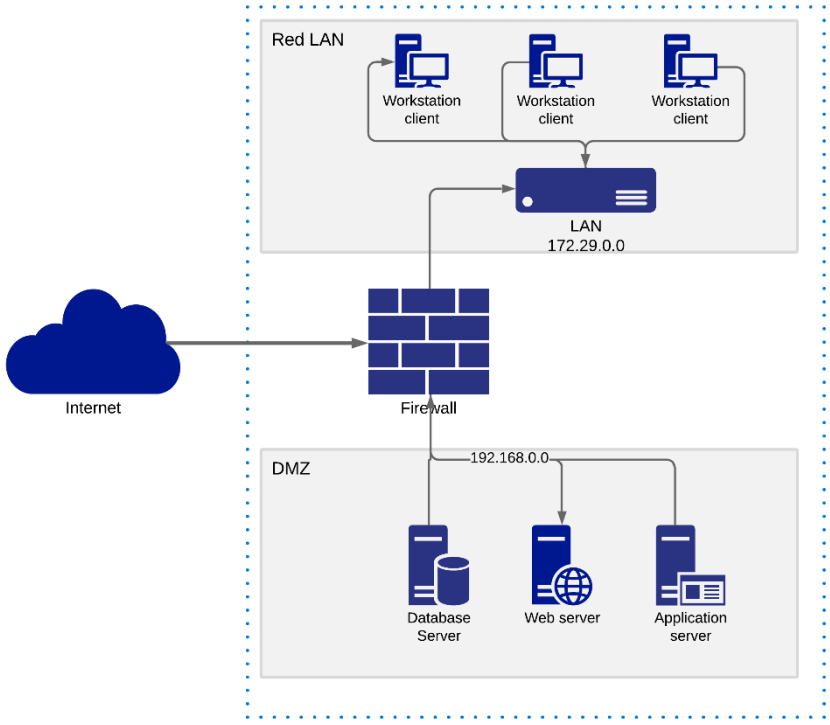
8.1 RED LOCAL

El mundo va cambiando muy rápido y con ello lleva a la aparición de nuevas tecnologías, cada empresa cada día está a una presión para realizar, crecer y poder competir con los demás negocios. Las oficinas de tecnología en las empresas no son diferentes y buscan la forma de ir mejorando sus procesos de la mano de la tecnología para obtener mejores resultados si sacrificar la calidad de su producto.

Con las infraestructuras ON-PREMISE o local, la entidad será la responsable de gestionar todo con respecto a la seguridad de la información y la disponibilidad del servicio. Además, es muy importante que cuente con una dependencia de tecnología, la cual se dedique gran parte a la gestión de la infraestructura, a veces los proveedores ofrecen un soporte post venta, el cual les ayuda a gestionar cualquier inconveniente que se pueda presentar.

En la siguiente figura se observa un diseño sencillo de una topología de red local, en la cual está diseñada bajo una zona desmilitarizada o DMZ, esta es una red local la cual está dentro de red interna y externa (internet) dentro de la empresa.

Figura 2 Topología red local



Fuente: el autor

8.1.1 Costos. Cuando en una empresa opta por la opción de una infraestructura de red *ON-PREMISE* o local, se debe tener presente que, al inicio del proyecto, resulta muy costoso. La entidad deberá asumir todos los costos de los dispositivos físicos necesarios para una operación correcta del servicio de red de datos.

Cabe resaltar, que además de la compra de estos dispositivos debe contar con personal altamente calificado para posteriormente realizar la parte de la instalación, donde se deberá asumir un costo adicional.

Si además de lo anterior, se desea realizar la configuración y puesta en marcha de los equipos, hay otro personal capacitado que requiere para que todo funcione de la mejor manera.

En la entidad que actualmente trabajo, ESE Hospital José María Hernández del municipio de Mocoa – Putumayo, se realizó la cotización de un Firewall marca FortiGate 400E Series, con los siguientes valores:

Tabla 10 Valor de una Firewall FortiGate 400E Series

Descripción	Cantidad	Valor Unitario	Valor Total
FG-400E-BDL Hardware plus 1 Year 24x7 FortiCare and FortiGuard Unified (UTM) Protection	1	**USD 10.000**	**USD 10.000**
		IVA	**USD 1.900**
		Total	**USD 11.900**

Fuente: el autor.

Si de la empresa que desea implementar este tipo de infraestructura, además desea incluir servidores web, de correo electrónico, de domino, etc. Su valor incrementaría en una gran cantidad. El valor de un servidor depende de las características con las que se lo requiera, tanto de memoria, capacidad de almacenamiento, procesador, entre otra.

Cuando se habla de la inversión de bienes de capital se le denomina CAPEX (*CAPITAL EXPENDITURES* o inversiones de bienes de capital), y las de OPEX (*OPERATING EXPENSE* o coste de funcionamiento). En la inversión CAPEX abarca todos los activos que la empresa compra y en OPEX todos los gastos continuos que se requiere para el funcionamiento.

Tabla 11 CAPEX y OPEX

CAPEX	OPEX
Servidores físicos.	Electricidad
Cables, ROUTERS, etc.	Internet
Espacios físicos ocupados.	Mantenimiento preventivo y correctivo
Sistema de seguridad	Personal para monitorización.
Sistema de extinción	
Sistema de refrigeración	
Puesta en marcha	

Fuente: el autor

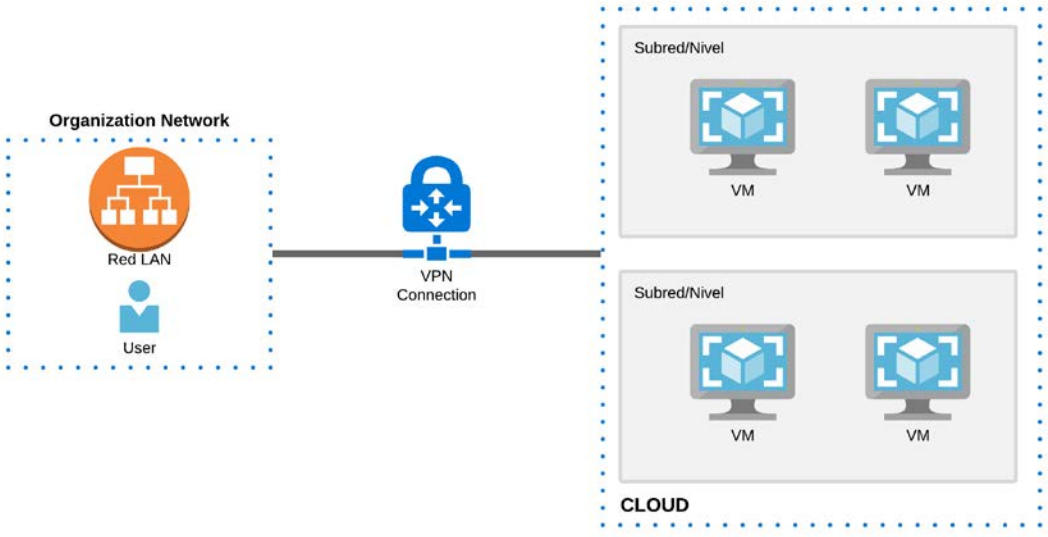
8.1.2 Desventajas. Las principales desventajas que se pueden establecer en la implementación de una infraestructura *ON-PREMISE* o local son las siguientes:

- La inversión económica que se realice al inicio del proyecto puede ser muy elevada. Además, de pagar gastos por la implementación del hardware y software.
- La seguridad y privacidad de la información están a cargo de las empresas, esto puede resultar muy preocupante ya que algunas empresas no están preparadas para implementar todas las políticas o protocolos de seguridad necesarios.
- En los procesos de implementación pueden resultar imprevistos y esto puede tomar mas tiempo de lo planeado.
- Se debe adquirir el hardware adecuado para que el software sea compatible.
- Las infraestructuras ONPREMISE están expuestas a fallas de suministro eléctrico, lo que puede provocar graves fallos en los sistemas de información o hardware.
- Si los servicios en la infraestructura ONPREMISE son accesibles por internet, se puede presentar saturación de la conexión. Ya que las entidades cuentan con una capacidad de conexión limitada.

8.2 RED EN LA NUBE

Todas las empresas hoy en día están expuestas a un cambio tecnológico, sin importar el tipo de infraestructura por la cual hayan optado. Ha resultado una necesidad que las empresas para poder competir en el mercado estén obligadas a realizar una transformación digital, la cual garantice poder competir en el mercado.

Figura 3 Topología red en la nube



Fuente: el autor

La implementación de infraestructura en la nube tiene una serie de beneficios entre los que se destacan los siguientes:

- **Reducción de costos:** Se ve una reducción importante en cuanto a los gastos, ya que el proveedor del servicio en la nube será el encargado de suministrar la infraestructura como parte del paquete de servicio contratado, además, de reducir los costos de mano de obra, compra y actualización de licencias, mantenimiento, alojamiento físico, etc.

- **Optimización del uso de recursos**: Con la implementación de la nube, las empresas únicamente utilizan los recursos de infraestructura necesarios, con esto se reduce el gasto por la inactividad del sistema.

- **Seguridad – Certificaciones**: Los proveedores de servicio en la nube, pueden ofrecer la capacidad de realizar un control a toda actividad realizada en nuestro servicio, con sus sistemas de monitoreo. Además, estos proveedores cuentan con las certificaciones de seguridad más importantes a nivel mundial.

- **Fiabilidad y rendimiento:** La nube se caracteriza por prestar una disponibilidad del 99% del servicio.

- **Recursos:** Los costos que anteriormente se utilizaban para la gestión de la infraestructura ON-PREMISE se puede reasignar a las funciones principales de la empresa.

8.2.1 Costos. Cuando se habla de la nube, pensamos en costos por hardware o software que es lo más lógico para este servicio, pero debemos tener presente que hay otros costos asociados a estos como lo son [24]

- Los costos iniciales: A veces de lo mencionado anteriormente, inicialmente se requiera de inversiones en internet de banda ancha, el cual permitiría conectarse a los servicios en la nube. Nuevos componentes de infraestructura que ayuden a la conexión con los servidores. Tal vez sea necesario de la ayuda de expertos encargados de la transición hacia la nube y además de la parametrización o configuración de los servicios contratados al proveedor *CLOUD*, por último, el personal necesitará capacitación de las nuevas aplicaciones y servicios.
- Los costos recurrentes: La utilización de la nube genera unos costos recurrentes que están asociados con las tarifas de la suscripción, puede ser

[24] INTERNATIONAL DATA CORPORATION (IDC): La migración a la nube: Una decisión cuantitativa. [Sitio web]. Madrid. [Consultado el 19 de abril de 2020]. Disponible en: https://www.ibermatica365.com/wp-content/uploads/2018/05/La-migraci%C3%B3n-a-la-nube-Una-decisi%C3%B3n-cuantitativa-FINAL_318369.pdf

mensual, semestral o anual y demás costos generados por la utilización de los servicios en la nube.

- Los costos de terminación del servicio: Cuando una empresa necesita regresar al modelo de infraestructura local, por diferentes motivos, esto genera unos posibles costos como: extracción de datos de la nube y su respectiva validación, destrucción de la información almacenada en la nube, reconfiguración de la infraestructura para la operación local, multas por terminación de contrato anticipada, personal profesional para la migración.

8.2.2 Ventajas. Los servicios en la nube se caracterizan por proporcionar una gran cantidad de características y opciones para que lo usuarios puedan implementar cualquier tipo de solución en sus plataformas. Esto a permitido que hasta el momento se vuelva una alternativa muy atractiva para las empresas por los grandes beneficios que puede resultar una buena implementación de la nube.

Entre las ventajas más importantes que se puede resaltar son:

- Reducción de costos, la nube le evita a las empresas la adquisición de hardware y el mantenimiento de estos, además de los ahorros en la parte de consumo de energía, soporte, licencias. Por lo tanto, al seleccionar la nube como proveedor de su infraestructura y demás servicios la empresa pasaría a un modelo de costos, únicamente basado en la capacidad requerida para su operación.
- Flexibilidad, cuando la empresa requiera adquirir mayor o menor recursos en sus servidores según sea su necesidad, puede realizarlo muy rápidamente sin la obligación de adquirir activos.
- Soporte, si se requiere adquirir un nuevo servidor o algún tipo de solución, algunos proveedores como el caso de Microsoft Azure, permite la posibilidad de asociarlo en tan solo un par de minutos.
- Disponibilidad, los proveedores de servicios en la nube, se caracterizan por ofrecer una disponibilidad del servicio del 99.9%, cuentan con replica de la información en al menos 3 ubicaciones físicas, lo que permite asegurar una disponibilidad del servicio en todo momento.
- Hibridez,
- Seguridad, Las medidas de seguridad que poseen los proveedores de la nube en sus centros de datos, son las mas sofisticadas y cumplen con los más altos estándares de seguridad, además, de poseer una gran cantidad de certificaciones internacionales con respecto a la seguridad de sus centros de datos.

9 EVALUACIÓN DE LA METODOLOGÍA.

En la actualidad la computación en la nube a crecido tanto en la popularidad ya que su principal atractivo y promesa es la de ahorrar tiempo y costos hasta la de mejorar la agilidad y escalabilidad de las infraestructuras *On-Premise*. Por otro lado, durante mucho tiempo la única oferta para las organizaciones fue la de tener sus servidores en sus lugares de trabajo, que por mucho tiempo también satisficieron las necesidades de las empresas.

Tabla 12 Comparativo de características *CLOUD* y *ON-PREMISE*

CARACTERÍSTICA	CLOUD	ON-PREMISE
Costo	Las empresas que optan por la computación en la nube simplemente deben pagar los servicios que se utilizan, sin ningún cargo adicional por mantenimiento ni licenciamiento.	Para las empresas que apenas inician, deben asumir un costo demasiado alto en la adquisición de todos los equipos necesarios para operar, además, de ser responsables de los costos continuos de los hardware de los servidores como también el consumo de energía y el lugar de alojamiento
Seguridad	Los grandes proveedores mundiales de servicios en la nube día a día implementan controles de seguridad, caracterizándose por cumplir con los más altos estándares, y además de cumplir con las políticas que se establecen en algunos países donde están operando. La seguridad de los recursos en la nube sigue siendo	Cuando una empresa posee su infraestructura *onpremise*, deberá realizar la gestión para optar por alguna certificación, el cual debe cumplir con cada requerimiento que está establecido en la norma, todo esto implica una inversión mayor

	responsabilidad de la empresa que contrata el servicio, y aunque los proveedores prestan servicios de seguridad de acuerdo con lo requerido por el cliente, estos valores son adicionales a la infraestructura base que se aloje en ella	

Fuente: el autor

Tabla 13 (Continuación)

CARACTERÍSTICA	CLOUD	ON-PREMISE
Escalabilidad	Cuando una empresa va creciendo exponencialmente o en momentos de grandes demandas en sus servicios, la nube tiene la facilidad de aumentar sus recursos para operar de forma optima	Cuando las empresas van creciendo las infraestructuras tecnológicas implementadas en sus inicios, muchas veces quedan cortas, no es tan fácil como en la nube, acá implica un costo adicional para los componentes nuevos, además de licenciamiento, mano de obra, etc.
Implementación	Los proveedores mantienen los sistemas en sus servidores, facilitando a las empresas la accesibilidad en cualquier momento.	Las empresas son responsables de realizar las implementaciones de las soluciones con la infraestructura que poseen.
Control	A pesar de que los datos y las claves de cifrado se comparten con el proveedor, la mayoría de estos en la actualidad están ofreciendo un control y privacidad completo con la información de sus clientes, como lo establece Microsoft Azure	En un entorno local, las empresas poseen el control completo de sus sistemas de información y de los datos almacenados, donde se mantiene un 100% la privacidad

Fuente: el autor

CONCLUSIONES.

Se identificaron los problemas en las metodologías de aseguramiento y se concluye que los servicios en la nube son muy útiles y eficientes. Igualmente se identificó la desventaja que este servicio impide que los usuarios puedan tener acceso físico a los servidores donde se almacena sus datos, toda esta responsabilidad del almacenamiento y control recae sobre el proveedor del servicio el cual muchas veces tarda en dar solución.

Se comparó las dos metodologías y se concluye que a pesar de estas desventajas mencionadas en el numeral 8.1.2 del presente documento, los servicios en la nube siguen siendo muy importantes en diferentes empresas, donde las ventajas tienen un mayor peso y por esto es viable correr el riesgo de las desventajas anteriormente mencionadas. Ventajas como: la de no requerir un espacio físico para los servidores, oficinas, licencias de software, actualizaciones, personal especializado para operar y configurar, entre otras.

Con la evaluación de las metodologías se concluye que los servicios en la nube ofrecen una característica significativa como el escalado automático, lo que permite a las aplicaciones de los clientes a operar en condiciones optimas en los momentos de mayor demanda, lo que con las tecnologías *On-Premise* se requerirá adquirir nuevo hardware para operar en mejores condiciones o muchas veces terminará quedándose pequeña u obsoleta.

RECOMENDACIONES.

Si se desea migrar de un tipo de tecnología local (*On-Premise*) a un proveedor de servicios en la nube, primero realizar una evaluación de los costos y riesgos que pueden llevar a cabo esta actividad, por ejemplo, determinar si todo esto proceso resulta critico o es muy viable la transición tanto de sus sistemas de información como los datos, además, de preparar su empresa como el caso de la red de internet, ya que esta juega un papel muy importante.

Seleccionar el mejor proveedor de servicios en la nube, actualmente hay muchas empresas que ofrecen este tipo de servicios, pero si vamos a trabajar con nuestra información, la mejor opción que podemos tener es seleccionando un buen proveedor que nos de un gran respaldo y el cual nos asegure contar con el personal idóneo para la gestión de los servicios.

BIBLIOGRAFÍA

SANCHEZ CASTILLO, Zulay Nayiv. Trabajo de grado: Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia [en línea]. repository.unad.edu.co. (2017). [Consultado: 09 de marzo del 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

Microsoft. (s.f.). Microsoft Azure. Recuperado el 08 de octubre de 2018, de https://azure.microsoft.com/es-es/overview/trusted-cloud/

CIERCO, David. Cloud Computing: Retos de oportunidades [En línea]. Fundaciones IDEAS. 2011. Disponible en https://books.google.com.co/books?id=_fTJXVjOD90C&printsec=frontcover&hl=es#v=onepage&q&f=false

CARPENTIER, Jean-François. La seguridad informática en la PYME: Situación actual y mejores prácticas. [En línea]. Barcelona: Ediciones ENI. 328 p. [Consultado el 28 de noviembre del 2020]. Disponible en: https://books.google.com.co/books/about/La_seguridad_inform%C3%A1tica_en_la_PYME.html?id=LKE5_6gzBmgC&redir_esc=y

MORA PEREZ, José Juan. Capas IT y Capas Cloud. Capacity Planning IT: Una Aproximación Práctica. Madrid: CreateSpace Independent Publishing Platform. 2012. p. 444. [Consultado: 20 de noviembre del 2018] Disponible en: https://books.google.com.co/books?id=FqU93uMPivMC&printsec

PARRA M, Maureen V.; GUILLÉN, Edward P. Servicios de autenticación y autorización orientados a internet de las cosas. En: *Revista Telemática*. La Habana. Universidad Tecnológica de La Habana "José Antonio Echeverría". Mayo – agosto 2018. vol. 17 nro. 2. p. 42 – 51. [Consultado: 30 de noviembre del 2019]. Disponible en http://www.revistatelematica.cujae.edu.cu/index.php/tele/article/view/302/278. ISSN 1729-3804.

MARTELO, Raúl; MADERA, Jhonny y BETÍN, Andrés. Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). En: *Revista Información Tecnológica*. [En línea]. La Serena – Chile. 2015. vol.26, n.2. p.129-134. [Consultado: 17 de marzo del 2020]. Disponible en <https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642015000200015&lng=es&nrm=iso>. ISSN 0718-0764

VELASCO CORTES, Ricardo. Gestión del riesgo basado en ISO/IEC 27005:2009 – ISO/IEC 31000:2011 ISO/IEC 28000:2008. [Sitio Web]. Universidad Piloto de Colombia. Bogotá. [Consultado: 18 de diciembre del 2019]. Archivo pdf. Disponible en http://polux.unipiloto.edu.co:8080/00002323.pdf

ROMO DAZA, Karen y ORJUELA RIAÑO, Oscar. Análisis de riesgo y plan de tratamiento de seguridad de la información para una empresa del sector de transporte. [en línea]. Proyecto para optar el título de especialista en seguridad informática. Bogotá D.C. Universidad Piloto de Colombia. Facultad de ingeniería de sistemas. Dirección de Postgrados. 2012. 19 p. [Consultado: 19 de noviembre del 2019]. Disponible en http://polux.unipiloto.edu.co:8080/00000804.pdf

TIPÁN GUAYTA, Kléver. Propuesta de políticas de seguridad de la información para la Corpaire. [en línea]. Tesis previa a la obtención del grado de Magister (MSc.) en gestión de las comunicaciones y tecnologías de la información. Quito. Escuela Politécnica Nacional. Facultada de ingeniería de sistemas. 2012. 28 p. [Consultado: 19 de noviembre del 2019]. Disponible en https://bibdigital.epn.edu.ec/bitstream/15000/7790/1/CD-4072.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la información técnicas de seguridad. Sistemas de gestión de la seguridad de la información (sgsi). Requisitos. NTC-ISO/IEC 27001. Bogotá D.C. El instituto. 2006. 8 p.

CORDERO TORRES, Geovanna. Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgo de la seguridad informática [En línea]. Trabajo de grado previo a la obtención del título de ingeniero de sistemas y telemática. Cuenta – Ecuador. Universidad del Azuay. Escuela de ingeniería de sistemas y telemática. 2015. 20 p. [Consultado: 20 de diciembre del 2019]. Disponible en Dspace de la Universidad del Azuay.

HENAO HENAO, Doris Liliana. La nube: gestión de información [En línea]. En: *El Colombiano*. Abril 25 del 2012. [Consultado: 15 de diciembre del 2019]. Disponible en: https://www.elcolombiano.com/historico/especial_tic_la_nube_gestion_de_informacion-JBEC_179275

HARDY, Quentin. How Cloud Computing Is Changing Management. En: *Harvard Business Review*. [En línea]. Universidad de Harvard. 08 de febrero del 2018. [Consultado:16 de diciembre del 2020]. Disponible en: https://hbr.org/2018/02/how-cloud-computing-is-changing-management

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES. Seguridad en la Nube. Guia Nro 12 Seguridad y privacidad de la información. 2016. [Consultado: 07 de diciembre del 2019].

Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

BRITISH STANDARDS INSTITUTION. ISO/IEC 27017. Controles de Seguridad para Servicios Cloud. [Sitio web]. [Consultado: 22 de diciembre del 2019]. Disponible en: https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

ORTIZ MANRIQUE, Edwin Omar. Análisis de causas de riesgos en la protección de la información de la empresa soltec-ing y recomendaciones de seguridad [En línea]. Proyecto de grado para optar al título de especialista en seguridad informática. Malaga. Universidad nacional abierta y a distancia. Escuela de ciencias básicas, tecnología e ingenierías. Especialización en seguridad informática. 2018. 21 p. [Consultado: 19 de noviembre del 2019]. Disponible en: Repositorio UNAD. https://repository.unad.edu.co/bitstream/handle/10596/17448/13927687.pdf?sequence=1&isAllowed=y

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 (5 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 47.223 de 5 de enero de 2009. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1343 (31 de julio de 2009). Por medio de la cual se aprueba el “Tratado sobre el Derecho de Marcas” y su “Reglamento”, adoptados el 27 de octubre de 1994. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 47.887 de 8 de noviembre de 2010. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1343_2009.html

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527 (18 de agosto de 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. [En línea]. Santa Fe de Bogotá D.C.: Diario Oficial No. 43.673, de 21 de agosto de 1999. [Consultado: 1 de diciembre del 2019]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

INTERNATIONAL DATA CORPORATION (IDC): La migración a la nube: Una decisión cuantitativa. [Sitio web]. Madrid. [Consultado el 19 de abril de 2020]. Disponible en: https://www.ibermatica365.com/wp-content/uploads/2018/05/La-migraci%C3%B3n-a-la-nube-Una-decisi%C3%B3n-cuantitativa-FINAL_318369.pdf

RAMÍREZ, Abby. Gestión de riesgos de seguridad de la información introducción al proceso de gestión de riesgos de seguridad de la información metodologías de análisis de riesgos. Barquisimeto: Universidad Centroccidental Lisandro Alvarado. Decanato de ciencias y tecnología. 2015